جامعة الجيلالي اليابس-سيدي بلعباس-
كلية الحقوق والعلوم السياسية
قسم الحقوق

الحمـاية الجزائيـة للتعامـلات الإلكترونيـة

أطروحة مقدمة لنيل شهادة دكتوراه علوم تخصص قانون جزائي

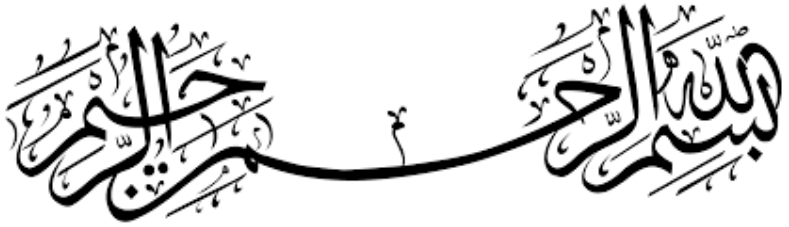
إعداد الطـالبة

بوكـر رشـيدة

أمام اللجنة المؤلـفة من:

أ.دقاسم العيد عبد القادر	أستاذ التعليم العالي-جامعة سيدي بلعباس-	رئيسا
أ.د مكلكل بوزيان	أستاذ التعليم العالي–جامعة سيدي بلعباس-	مشرفا ومقررا
أ.د باسم شهـاب	أستاذ التعليم العالي-جامعة مستغانم-	عضوا
د.عبد اللاوي جواد	أستاذ محاضر أ -جامعة مستغانم-	عضوا

2017



" قَالُواْ سُبْحَانَكَ لاَ عِلْمَ لَنَا إِلاَّ مَا عَلَّمْتَنَا إِنَّكَ أَنتَ الْعَلِيمُ الْحَكِيمُ"

البقرة: 32

صدق الله العظيم

إهـــــــــداء

إلى الشجرتين الباسقتين بظلالهما علينا...

وأفتخر إذ أنني ثمرة من ثمارهما...

والدي الكريمين اطال الله في عمرهما ومتّعهما بالصحة والعافية

إلى قـــــرة عيني إبني♦ ♦ ♦ "محمد ريان"

إلى من وقفو بجانبي في كل الصعاب ♦ ♦ ♦أخـــي و أخـــــواتي

إلى كل من كان له أدنى فضـــل في إعانتي على إخراج هذا المجهـــود

إلى كل طالب للعلم والمعرفة

إليهم جميعا أهذي ثمرة هذا العمل

شكـــر وتقـــدير

أتوجه بالحمد و الشكر لله تعالى الذي ألهمني و أعانني على إتمام بحثي هذا والذي آمل أن أكون قد حققت الغاية المرجوة منه

كما أخص بالشكر والتقدير والامتنان:

الأستاذ الدكتور مكلكل بوزيان الذي تفضل وأشرف على هذه الرسالة، فأعطاني من وقته الثمين وجهده الكبير، ولم يبخل بالإطلاع على تفاصيل الرسالة، وتوجيهها في الطريق القانوني السليم، فكان لي معلما ومشرفا، فله مني وافر الشكر والتقدير واسمى آيات المودة والاحترام.

و إلى كل من أعانني ولو بالكلمة الطيبة

المقدمة

المـــقدمـــة

1-موضوع البحث

لقد كان الإنسان على مرة العصور في حاجة إلى التواصل بينه وبين من يحيط به من أفراد وجماعات، وكان سعيه على تأمين هذا التواصل سببا في العديد من إختراعاته وإبتكاراته، فإشارات موريس وأجهزة الهاتف، والراديو، والتلفاز، لم تكن إلا وسائل لزيادة تفاعل وتواصل الإنسان مع الأوساط المحيطة به أو البعيدة عنه، وحين أتت ثورة الإتصال الخامسة والتي شهدت إبتكارات فاقت كل الإبتكارات السابقة، وذلك بموجب الإندماج التاريخي بين ظاهرتي تفجير المعلومات والمعرفة وثورة الإتصال[1]، كان عالم الإتصالات تجسيدا لحاجة الإنسان إلى التواصل مع أقرانه من بني البشر.

ولا شك أن نظم وطرق الإتصال بين الأفراد قد مرت بتطورات متتابعة، متلاحقة ومتعاقبة على مر العصور، فمن إستخدام الحمام الزاجل[2] إلى ظهور البريد وإستخدام موجات الراديو والهاتف والتلفاز والصحف والمجلات والكتب. وقد أخذت كل وسيلة من هذه الوسائل جزءا من عمر الزمن إلى أن تلتها الوسيلة الأخرى كنتيجة طبيعية لدوران عجلة التقدم، حتى أتت ثورة تكنولوجيا الإتصالات والتي لم تتوقف عند حد معين، وكان من أعظم نتائجها ظهور شبكة الانترنت العملاقة، تلك الشبكة التي بدأت مسيرة العمل كوسيلة إتصال وتبادل للمعلومات ثم أضحت بوابة المعرفة وفضاء إتصالي مفتوح على مصراعيه يزيل الحدود الجغرافية ويجعل من العالم أشبه بقرية إلكترونية صغيرة.

ولايخفى على أحد الدور الذي بدأت تلعبه الأنترنت في تغيير الكثير من نمط المجالات الحياتية العملية من النمط المادي إلى اللامادي، أي ذلك الحيز الإفتراضي (نظام التخزين-نظام التراسل) الذي يعتمد على رقمنة المعلومات وفقا لطريقة ثنائية تعتمد على رقمي صفر وواحد، وذلك نظرا للتيسيرات الهائلة التي قدمتها بما توفره من تفاعل لحظي وتقريب المسافات وإختزال للزمن وإمكانية التعامل عن بعد دون ضرورة التنقل والتخاطب المباشر وحتى التعرف على الطرف المقابل، هذا التغيير الذي أعاد هيكلة التعاملات القانونية خصوصا لتتبنى أشكالا وطرائق جديدة تنسجم مع العصر الجديد، ليتوج بظهور ما يسمى **بالتعاملات الإلكترونية**" التي أصبحت مطلبا هاما سواء للحكومات أو المنظمات العامة أو التجارية وكذلك الأفراد، وذلك نظرا لما يوفره هذا النوع من التعاملات لأطرافها العديد من الخصائص المرتكزة بشكل أساسي على الطبيعة التقنية للوسط الذي تجري فـــيه.

---

[1]- **محمد لعقاب**، مجتمع الإعلام والمعلومات، دار هومة للنشر والتوزيع،الجزائر، 2003، ص ص66-67.

[2]- **حشمت محمدعلى قاسم**، تقنيات الإتصالات وتدفق المعلومات,إدارة الثقافة والنشر بجامعة الإمام محمد بن سعود الإسلامية، المملكة العربية السعودية، 1993، ص10.

والتعاملات الإلكترونية في مفهومها العام تشمل كل تعامل يتم إبرامه أو تنفيذه أو إنهاؤه بوسيلة الكترونية أيا كانت أطرافه، فقد يكون هذا التعامل بين أفراد أو بين جهات حكومية أو غير حكومية، أو بين دول أو مؤسسات دولية، أو بين هذه الجهات المذكورة وبعض آخر، كتعامل الفرد مع الشركات التجارية، أو التعامل مع المصارف سواء فيما بينها أو مع عملائها[1].

وإن كان يحكم على الوسيلة أنها إلكترونية إذا كانت تتخذ تقنية الإلكترون أداة للقيام بدورها، سواء كانت ذات قدرات كهربائية مثل الأجهزة التي تعمل بالقوى الكهربائية كآلات التصوير الفوتوغرافي والورقي، وقد تكون ذات قدرات رقمية مثل الحاسب الآلي الشخصي، أو الحاسب المحمول، وقد يكون الشيء ذا قدرات مغناطيسية أو لا سلكية مثل الهاتف العادي أو الفاكس أو الهاتف المحمول، أو قدرات بصرية كالكاميرات الرقمية، وكذلك الأجهزة والأدوات ذات القدرات الكهرومغناطيسية أو الضوئية أو المؤتمتة[2] . فإن التعاملات الإلكترونية كمصطلح عالمي أبان عن نفسه مع **ظهور الأنترنت**، لأنها أمكن فيها الجمع بين حاستي الإستماع والإبصار بشكل آني فأصبح التواصل فوريا مما ولد التفاعل بين الأشخاص الذين إستغلوا ذلك فإزداد نمو المراسلات والمحادثات والرغبات والطلبات وظهرت العديد من التطبيقات التي تخدم هذه الرغبات: كالبريد الإلكتروني ونقل الملفات، والمحادثة وغيرها من تطبيقات الأنترنت[3]. ومع ظهورها برز إلى الوجود تنوع في المتعاملين الإلكترونيين مثل الوسيط الفني والوسيط النظامي.

وإن كانت التعاملات الإلكترونية تعتمد على إستخدام الوسائل الإلكترونية في **معالجة المعطيات وتبادلها**[4] ، فإنها لا تقتصر على **التعاملات التجارية**[5] فقط كما كان يوحي بذلك المصطلح المتداول من قبل وهو مصطلح التجارة الإلكترونية، وإن كانت تبوأت الصدارة وإستقطبت جل الإهتمام كونها من أكثر المجالات إستفادة من التقنيات الجديدة، ذلك أن التعاملات الإلكترونية لها دلالة أوسع تمتد لتشمل سائر الأنشطة الإدارية والإنتاجية والمالية والخدماتية، فالتعامل الإلكتروني لا ينصرف فقط إلى التعامل في السلعة والبضائع المادية، وإنما

---

[1]–د. **إبراهيم أبو الليل الدوسقي**، توثيق التعاملات الإلكترونية ومسؤولية جهة التوثيق إتجاه الغير المتضرر، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، الجزء الخامس، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ماي، 2003، ص1847.

[2]– **د.عبد الفتاح بيومي حجازي**، التجارة عبر الأنترنت، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2008، ص108.

[3]– **د. خالد ممدوح إبراهيم**، إبرام العقد الإلكتروني، دار الفكر الجامعي،الإسكندرية، 2008، ص29.

[4]– يقصد بالمعالجة الآليّة للمعطيات وفق ما هو متعارف عليها في المجال التقني :مجموعة من العمليات المترابطة والمتسلسلة بدءا من جمع المعطيات وإدخالها إلى نظام المعالجة الآلية ومعالجتها وفقا للبرامج التي تعمل به نظم المعالجة الآلية وصولا إلى تحليلها وإخراجها بصورة معلومات.

[5]–لا تختلف التجارة الإلكترونية كثيرا عن التجارة بصفة عامة من حيث مضمونا ومحترفيها، أما وجه الخصوصية فيها فيتمثل في الحقيقة في وسائل مباشرتها، وبصفة خاصة الطريقة التي تنعقد بها العقود وطريقة تنفيدها، أنظر:

Isabelle poitier, le commerce electronique sur internet, gazette du palais, 4 avril 1996, p4.

وقد عرفها المشرع الفرنسي بموجب المادة 14 من قانون الثقة في الإقتصاد الرقمي بأنها النشاط الإقتصادي الذي بمقتضاه يعرض شخص أو ينجز عن بعد و بالطريق الإلكتروني التزويد بسلع أو خدمات. يدخل أيضا في نطاق التجارة الإلكترونية تلك الخدمات التي تتمثل في تقديم معلومات عبر الخط، و الإتصالات التجارية ووسائل البحث، والدخول إلى المعطيات وإسترجاعها، والدخول إلى شبكة إتصالات أو تسكين معلومات، كل ذلك ولو لم تكن هذه الخدمات تؤدي بمقابل ممن يتلقاها".

Article 14 du **Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique;** J.O n° 143 du 22 juin 2004 .

يحويه كذلك الخدمات غير المادية، ولعل من أهم مجالات التعاملات الإلكترونية حاليا **الحكومة الإلكترونية**[1]، **الإدارة الإلكترونية**[2]، **الأعمال المصرفية والدفع المالي الإلكتروني**[3]، **التصرفات المدنية الأخرى** سواء بإبرامها أو إنهائها عبر الوسائل الإلكترونية كعقود البيع والإيجار بين أشخاص عاديين، والإقرار أو الوقف أو الوصية.

وهذه التعاملات تتفق فيما بينها في كونها تقوم على حاسوب وشبكة وموقع ومعلومات وأطراف، وتعد الشبكة من أهم عناصر التعامل الإلكتروني كونها تضفي على التعامل الطابع الإلكتروني، فتتيح عملية الربط والانتقال وتحقيق عمليات الدخول وضمان تبادل المعلومات، ولتحقيق هذا الإتصال يتدخل أشخاص كثيرون في آلية عمل الشبكة ويسهمون في إتمام ذلك التعامل بأدوار مختلفة تختلف ضيقا وإتساعا وأهمية حسب موقع كل منهـــم.

وفي خضم هذا الواقع التقني الذي تتم فيه التعاملات الإلكترونية عن بعد في صورة معطيات معالجة آليا تنتقل من نظام لآخر عبر شبكة الأنترنت دون دعامات ورقية ملموسة، أو توثيقها ضمن أقراص مغناطيسية أو أقراص مكتنزة (cdrom) ، فإن المستند الإلكتروني سيصبح غالبا هو السند القانوني المعتمد بين أطراف التعامل الإلكتروني، سواء عند إتمام التعاملات في شكل عقود إلكترونية، أو عند تنفيذها عن طريق البطاقات الإلكترونية كبطاقات الإئتمان.

ورغم أن التوقيع بمفهومه التقليدي يعتبر السبيل الرئيسي لإسباغ الحجية على المستند، بإعتباره شرطا جوهريا لصحة المستند العرفي وإسباغ حجيته في الإثبات[4]، إلا أنه ومع ظهور المستند الإلكتروني ظهر التوقيع الإلكتروني من خلال التعاملات الإلكترونية كوسيلة إلكترونية لها أشكال مختلفة.

وهكذا حررت التقنيات المتاحة المعلومات من أسر الورق، وجعلتها تتداول في صورة غير مادية، تحت الشكل الغامض إلى حد ما الذي إتفق على تسميته بالإلكتروني.

---

[1]- الحكومة الإلكترونية هي البوابة الرئيسة للتعاملات الإلكترونية، وقد تعددت التعريفات التي قيلت بشأنها نظرا للأبعاد التقنية والإدارية والتجارية والإجتماعية التي تؤثر عليها، ويمكن تعريفها على أنها نسخة إفتراضية عن الحكومة الحقيقة أي التقليدية مع الفارق أن الأولى تعيش في الشبكات الإلكترونية والأنظمة المعلوماتية، في حين تحاكي الوظائف الثانية التي تتواجد بشكل مادي في أجهزة الدولة، ويمكن تقسيم عمليات الحكومة الإلكترونية إلى أربعة أقسام رئيسية بحيث تصب معظم أعمال تلك الحكومة في أحد تلك الأقسام: **الخدمات الإلكترونية**مثل إصدار شهادات الميلاد ، تجديد رخصة القيادة، **الديمقراطية الإلكترونية** بإستطلاع الشعب إلكترونيا حول قضايا خلافية تهمهم، **التجارة الإلكترونية** مثل بيع الأثاث المستعمل الحكومي في المزاد الإلكتروني، **الإدارة الإلكترونية: غزال عادل**، الحكومة الإلكترونية في الجزائر والنفاذعلى مجتمع المعلومات، الملتقى الوطني الثامن جول مستقبل ثقافة المعلومات والإتصال لدى الشباب في الجزائر بين صناعة المجتمع الجماهيري ومجتمع المعرفة والمعلومات، جامعة باتنة، 9-8 نوفمبر 2014، ص5.

[2]-تعد الإدارة الإلكترونية العمود الفقري للحكومة الإلكترونية، وتعني في أبسط معانيها تحويل كافة الأعمال والخدمات الإدارية التقليدية إلى أعمال و خدمات إلكترونية تنفذ بسرعة عالية ودقة متناهية، أو أنها الإدارة المسؤولة عن تقديم المعلومات والخدمات الإلكترونية بطريقة رقمية للموظفين ومنشآت الأعمال القادرة على الإتصال إلكترونيا عن بعد". **عبد الله بن سليمان**، الأثر الإقتصادي لتطبيق الأعمال الحكومية الإلكترونية، منتدى الأعمال الحكومية الثالث، السعودية، 18-20 سبتمبر 2006، ص2.

[3]-وهو تقديم الخدمات المصرفية أو البنكية بطريقة إلكترونية، كالإستعلام عن الحساب ومتابعة أسعار البورصات وإجراء الحوالات والمقاصة وغيرها من الخدمات المصرفية والبنكية.فضلا عن تمكين الأشخاص من دفع المستحقات المالية كقيمة الغرامات أو الخدمات وتسديد الرسوم بواسطة الوسائل الإلكترونية. **د. رضوان رأفت** ، عالم التجارة الإلكترونية، مركز البحوث والدراسات بالمنظمة العربية للتنمية الإدارية، 1999، ص35.

[4]- **د. ثروت عبد الحميد**، التوقيع الإلكتروني، ماهيته ، مخاطره وكيفية مواجهته ومدى حجيته في الإثبات، دار النيل للطباعة والنشر، القاهرة، 2001، ص43.

إلا أن الإنتقال من مرحلة التعامل الورقي إلى التعامل الإلكتروني أو الرقمنة، فتح باب الجدل على مصرعيه حول صحة هذه التعاملات الإلكترونية ومدى حجيتها في الإثبات، ومستوى أمنها في ضوء الممارسات الغير المشروعة التي يمكن أن تتعرض لها المعلومات المتداولة في بيئتها، ذلك أن الإعتداءات في هذا الميدان كثيرة وذات طابع حديث ومتطور حيث أخذت تستهدف مواقع هذه التعاملات الإلكترونية وما تحويه من المعلومات ذات القيمة التي قد تفوق قيمة الأموال، والأخطر منه هو تغيير الحقيقة في المعلومات المبرمجة التي لها قيمة في الإثبات خاصة إذا كانت تخص إدارة عامة أو مستندات موثقة les actes notarés .

كما أن تزايد أعداد المتدخلين في خدمات الأنترنت دون وجود ضابط يحكم تصرفاتهم أدى إلى صعوبة حصر المسؤولية الناتجة عن تداول المعلومة الواقعة تحت طائلة القانون، مما يثير مخاوف أطراف التعامل الإلكتروني حول أمن هذا التعامل ناهيك عما يتعلق بمعطياتهم الشخصية التي يتم تداولها عبرها، أو حركة معاملاتهم المالية والمشاكل المتعلق بها خاصة مسألة حماية سرية معلوماتهم الرقمية الخاصة ببطاقات الدفع وهوياتهم الرقمية وإستخدامها، فضلا عن مسألة الجهالة بالطرف الآخر كون أغلب العناصر الشخصية التي تتعامل في نطاق التعاملات الإلكترونية قد يتعدى أثرها إقليم الدولة الواحدة، قد يكون مجهول الهوية أحيانا بالنسبة للطرف الآخر.

وهو ما يهدد الثقة والأمان التي يجب أن تكون عليه التعاملات الإلكترونية، فإذا إنهارا كان مؤشرا نحو إنهيار التعامل الإلكتروني، وهذا الأمر يعكس بالضرورة مدى أهمية إرساء وسائل نظامية قانونية لحماية التعامل الإلكتروني من الضرر.

هذا الواقع فرض حتمية التشريع في هذا المجال سواء على المستوى الدولي وكذلك الوطني بمنح الحجية للتعامل الإلكتروني وترتيب مسؤولية التعويض فيه.

فقد اتجهت لجنة الأمم المتحدة لقانون التجارة الدولية إلى إعداد مجموعة من المباديء القانونية التي تحكم التعامل الإلكتروني لتستخدمها الدول نموذجا في تعديل قوانينها الداخلية بغية إزالة العقبات التي تحول دون الإستفادة من التطور الحادث في مجال المعالجة الآلية للمعطيات من إستخدام الوسائل الإلكترونية في التعامل وتخزين المعلومات، وتبقى أهم هذه القواعد القانون النموذجي للتجارة الإلكترونية لعام 1996[1] الذي وإن إهتم بنوع واحد من مجالات التعامل الإلكتروني وهو التجارة الإلكترونية إلا أنه لم ينف إمكانية تطبيق أحكامه

[1]-يهدف القانون النموذجي بشأن التجارة الإلكترونية (القانون النموذجي) إلى التمكين من مزاولة التجارة بإستخدام وسائل إلكترونية وتيسير تلك الأنشطة التجارية من خلال تزويد المشرعين الوطنيين بمجموعة قواعد مقبولة دوليا ترمي إلى تذليل العقبات القانونية وتعزيز القدرة على التنبّؤ بالتطورات القانونية في مجال التجارة الإلكترونية. والغرض من قانون التجارة تحديدا هو التغلّب على العقبات الناجمة عن الأحكام القانونية التي قد لا تكون متنوّعة تعاقديا عن طريق معاملة المعلومات الورقية والإلكترونية معاملة متساوية. وهذه المساواة في المعاملة مقوّم أساسي للتمكّن من استخدام الخطابات اللاورقية، مما يعزّز من الكفاءة في التجارة الدولية.

Loi type de la **Commission des Nations Unies pour le droit commercial international** sur le commerce électronique (1996)

على أي نوع من المعلومات والتي تكون في شكل مستند إلكتروني ، فضلا عن القانون النموذجي للتوقيعات الإلكترونية رقم 56-80 لعام 2001[1].

كما أصدر المشرع الأروبي هو بدوره جملة من التوجيهات، كالتوجيه الصادر في 8 يونيو 2000 بشأن التجارة الإلكترونية[2]، التوجيه رقم 93 / 1999 الخاص بالتوقيعات الإلكترونية[3]، التوجيه رقم 910-2014 المتعلق بتحديد الهوية الإلكترونية وبث الثقة في التعاملات الإلكترونية في السوق الداخلية[4].

وقد شكلت القواعد النموذجية والتوجيهات السابقة مصدر أساسي لمختلف التشريعات لتحديث المنظومة التشريعية الوطنية على نحو يستوعب إستخدام الوسائل الإلكترونية في إثبات التعاملات الإلكترونية، فقد قام المشرع الفرنسي بإدخال تعديلات على مواد القانون المدني الخاصة بالإثبات، وقد كان ذلك بموجب القانون رقم 2000-230 الصادر في 13 مارس 2000 المتعلق بتطويع قانون الإثبات لتكنولوجيا المعلومات والتوقيع الإلكتروني[5]، فأدرج المواد من 1316 إلى 1316-4 في القانون المدني مكرسا بذلك القوة الثبوتية للكتابة والتوقيع الإلكتروني، كما كرس حفظ المستندات الرسمية على دعامة إلكترونية. ليكمل بذلك قانون الثقة في الإقتصاد الرقمي رقم 2004-575 هذه الأحكام فيما يخص الشكلية والذي إعتبر التشريع الرئيسي لقانون الأنترنت في فرنسا.

ولم تكن الدول العربية بمعزل عن الإستفادة من فوائد التعاملات الإلكترونية الإقتصادية والتي أقلها الحد من النفقات لاسيما الورق الذي تستخدمه الدوائر المالية والإدارية[6]، فضلا عن القناعة بضرورة الإستفادة منها في المجالات المتنوعة، حيث عدل المشرع الجزائري القانون المدني بموجب القانون رقم 10-05[7] فإعتبر الإثبات بالشكل الإلكتروني كالإثبات بالكتابة بتوافر شروط معينة، كما أضاف وبموجب القانون 05-02[8] الباب الرابع إلى الكتاب الرابع من القانون التجاري والمعنون في بعض وسائل وطرق الدفع ، ليضمن في

---

[1]-يهدف القانون النموذجي بشأن التوقيعات الإلكترونية (قانون التوقيعات) إلى التمكّن من استخدام التوقيعات الإلكترونية وتيسير استخدامها عن طريق وضع معايير بشأن الموثوقية التقنية اللازمة لتحقيق التكافؤ بين التوقيعات الإلكترونية والخطية. وهكذا، فقد يساعد قانون التوقيعات الدول على وضع إطار تشريعي حديث ومنسّق وعادل يعالج موضوع المعاملة القانونية للتوقيعات الإلكترونية معالجة فعّالة ويضفي اليقين على وضعيتها القانونية.
Loi type de la Commission des Nations Unies pour le droit commercial international sur les signatures électroniques (2001)

[2]-Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique»)*Journal officiel n° L 178 du 17/07/2000 p. 0001 - 0016*

[3]- Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques, j.o n° l013 du 19-01-2000.

[4]-RÈGLEMENT (UE) N° 910/2014 DU PARLEMENT EUROPÉEN ET DU CONSEILK .du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE

[5]-Loi n° 2000-230 du 13 mars 2000, portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, J.O.R.F numéro 62, 14 mars 2000.

[6]-حيث تتكفل الخزينة العمومية الكثير من الأعباء المالية لتزويد مختلف الإدارات والمؤسسات بالأوراق والأدوات المكتبية، حيث تكشف الإحصائيات في الجزائر بأن ما تصرفه بلدية من البلديات الوطنية على اللوازم المكتبية من أقلام وأوراق وكرطوش وغيرها يقدّر بحوالي 300 مليون سنتيم، فـــي الوقت الذي لا تقدّم فيه هذه النفقات الإضافية شيئا للاقتصاد الوطني، عدا أنها تقدّم خدمة للمواطن:
http://www.babalweb.net/ar

[7]-قانون رقم 05-10 المؤرخ في 20 يونيو 2005، جريدة رسمية ، عدد 44، .صادرة في 26 يونيو 2005.

[8]-قانون رقم 05-02 المؤرخ في 6 فيفري 2005، جريدة رسمية، عدد 11، صادرة في 9 فيفري 2005.

الفصل الثالث منه بطاقات السحب والدفع، لكن تبقى أبرز **طفرة تشريعية** عرفها التشريع الجزائري تلك التي عرفتها نصوص القانون رقم 04-15 المؤرخ في 1 فيفري 2015 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين[1] الذي أحدث جو من الثقة لتعميم التعاملات الإلكترونية عن طريق منح الحجية للتوقيع الإلكتروني وترسيخ المباديء العامة المتعلقة بنشاط التصديق الإلكتروني في الفرعين **الإقتصادي والحكومي**، وكذلك ترتيب مسؤولية التعويض عن الضرر فيه.

وإلى جانب المشرع الفرنسي والجزائري، نجد المشرع المصري قد أصدر القانون رقم 15 لسنة 2004 في شأن تنظيم التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات[2]، كما أصدرت تونس القانون رقم 83 لسنة 2000 في شأن المبادلات والتجارة الإلكترونية[3]، وكذلك هو الأمر بالنسبة لسلطنة عمان[4]، والأردن[5] والإمارات[6] وغيرها.

وفي الحقيقة وإن كانت هذه النظم تعنى بتنظيم التعاملات الإلكترونية، إلا أنها لا تخاطب أي تواصل أو تعامل، ففضلا عن إشتراط كون الوسيلة تتخذ تقنية الإلكترون أداة للقيام بالدور في الإبرام أو التنفيذ سواء كليا أو جزئيا، فإنه يشترط في التعامل أن يكون بين شخصين أو أكثر، وهو أمر يقصي المستخدم الوحيد للوسائل الإلكترونية -كشبكة الأنترنت-، فالمستخدم في هذه الحالة يسبح في فضاء الأنترنت ويطفو من وقت لآخر على الويب دون أن يتجاوز ذلك إجراء تراسل أو تبادل أو تعاقد، فهو في هذا الحيز لا يشمله نظام التعاملات الإلكترونية، وإن كان يمكن أن يسأل مسؤولية جزائية طبقا للقواعد المقررة لذلك في قانون جرائم تقنية المعلومات، كما يمكنه باعتباره مستخدم الأنترنت الإستفادة من العمل الذهني المعروض على الشبكة في نطاق الإستعمال الشخصي البحث، ولكنه لا يستطيع أن يستغل هذا العمل تجاريا أو يستعمله بصورة جماعية أو بأي صورة تشكل تعديا على حق المؤلف دون إذن صاحبه[7].

فضلا عن ذلك، فإن قوانين التعاملات الإلكترونية تخاطب الأشخاص الذين يتعاملون مع المعلومة النظامية، والمستند المعلوماتي القانوني، وليس من يتعامل في معلومة غير قانونية كتبادل الصور التي تظهر الأطفال في أوضاع منافية للأداب، وتواجه البعض من التشريعات تلك التعاملات التي تضر بحقوق الأطفال، حيث تعاقب على حيازة تلك الصور مثل القانون الفرنسي بموجب المادة 227-23 عقوبات ويمكن أن يسري

---

[1]- قانون رقم 15-04 المؤرخ في 1 فبراير 2015، المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين، جريدة رسمية، عدد 06، صادرة في 10 فبراير 2015.

[2]-قانون رقم 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات المصري، جريدة رسمية، عدد 17، صادرة في 22 أبريل لسنة 2004.

[3]-قانون رقم 83 لسنة 2000، مؤرخ في 9 أوت 2000، المتعلق بالمبادلات والتجارة الإلكترونية، الجريدة الرسمية ، عدد 64، صادرة في 11 أوت 2000.

[4]-مرسوم سلطاني رقم 2008-69 ، مؤرخ في 17 ماي 2008، المتعلق بإصدار قانون المعاملات الإلكترونية،جريدة رسمية، رقم 864.

[5]- قانون المعاملات الإلكترونية الأردني رقم 85 ، الصادر بتاريخ 11ديسمبر2001، متاح على الموقع الإلكتروني التالي:

http://www.wipo.int/wipolex/ar/details.jsp?id=14964

[6]- القانون الإتحادي رقم 1 لسنة 2006، بشأن المعاملات والتجارة الإلكترونية، جريدة رسمية رقم 442، يناير 2006.

[7]- **د. محمد حسين منصور**، المسؤولية الإلكترونية، دار الجامعة الجديدة، الأزاريطة، 2007، ص198.

التجريم الوارد في المادة 333 مكرر عقوبات جزائري والمادة 178 مكرر ثانيا عقوبات مصري في هذه الحالة.

غير أن الإعتراف بالتعامل الإلكتروني ومنحه الحجية وترتيب مسؤولية التعويض عنه وإن كان يساهم في دعم التعامل الإلكتروني ويضفي الشرعية عليه، فإن الطريق الجزائي يبقى أكثر فاعلية بما يملكه من سلطة الإكراه على تنفيذ القاعدة المنصوص عليها، كما أنه أقل شكلية وأكثر سرعة من الطريق المدني.

وهو ما تنبه له المجتمع الدولي من ضرورة مواجهة جرائم تقنية المعلومات بإعتبارها أفعالا ضارة بالمجتمع بصفة عامة والتي تعد وثيقة الصلة بحركة التعاملات الإلكترونية، حيث أن 95 % من جرائم تقنية المعلومات التي تحدث على الأنترنت هي في الأصل تتعلق بالتعاملات الإلكترونية، ومن هنا تأتي أهمية هذه المواجهة، فكانت الإتفاقية الأروبية لمكافحة الإجرام التقني لعام 2001 ما إصطلح على تسميتها باتفاقية بودابست من أول الإتفاقيات الدولية التي دقت ناقوس الخطر منبهة ومنذرة من خطورة جرائم تقنية المعلومات بصفة عامة مؤكدة على حتمية أن يولي المشرعون الوطنيون جهدهم لتجريم الإنحراف في عالم تقنية المعلومات[1]، أما على المستوى العربي فقد تم ميلاد الإتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر سنة 2010 والتي ألزمت الدول الأطراف بموجب المادة الخامسة منها بأن تجرم مجموعة من الأفعال المبينة في الفصل الثاني منها[2]، إختلطت فيها الجرائم التقليدية بجرائم تقنية المعلومات الحديثة.

---

[1]– شهدت ميلادها العاصمة المجرية بودابست في 23–11–2001، ورغم أن هذه المعاهدة أوروبية المنشأ إلا أنها **ذات نزعة دولية** وذلك لأنها مفتوحة لإنضمام الدول الأخرى حتى يمكن أن تساهم في ضبط وتنظيم مجتمع المعلومات والاتصالات بشكل أفضل تعم فائدته على الجميع. دخلت هذه الاتفاقية حيز النفاذ في الأول من يناير 2007 وذلك بعد المصادقة عليها من قبل (30) دولة بما في ذلك الدول الأربعة من غير الأعضاء في المجلس الأروبي وهي كندا واليابان وجنوب إفريقيا والولايات المتحدة الأمريكية.

وعلى العموم فإن هذه الاتفاقية قد فتحت باب التوقيع والتصديق والقبول والإقرار و الانضمام أمام جميع الدول وهذا عملا بالفقرة (2) من المادة(36) من الاتفاقية بعنوان التوقيع التصديق القبول الإقرار و الإنظمامالواردة ضمن نفس الفصل وكذا عملا بالفقرة (2) من المادة (37) من الاتفاقية بعنوان الانضمام "*adhesion*", وعملا بنفس الفقرة فإن صكوك الانضمام تودع لدى الأمين العام لمجلس أروبا *secretaire generale du conseil de l'europe*.

وهي تعد أول معاهدة دولية لمكافحة الجريمة التقنية تعكس الجهد الواسع والمميز للإتحاد الأوربي ولجان الخبراء فيهما المنصبة على مسائل جرائم تقنية المعلومات وأغراضها منذ أكثر من عشرة أعوام .

وتتكون هذه الاتفاقية من ثمانية وأربعين مادة، موزعة على أربعة أبواب، يعالج الباب الأول منها استخدام المصطلحات، ويتناول الباب الثاني الإجراءات الواجب إتخاذها على المستوى القومي، ويضم هذا الباب ثلاثة أقسام: أولها القانون العقابي المادي أو الموضوعي بشأن الجرائم ضد الخصوصية وسلامة وتواجد معلومات النظام ويمل وصفا لأنواع متعددة من الجرائم، الجرائم المتصلة بالنظام وشاملة إستخدام النظام في التزوير وفي الأفعال الإحتيالية، الجرائم المتعلقة بالمحتوى والمضمون، الجرائم المتصلة بالتعدي على حقوق المؤلف والحقوق المجاورة.

وثانيها للقانون الإجرائي: فيما يتصل بالإجراءات الجزائية شاملة الحفاظ على المعلومات المخزنة والأوامر الخاصة بتسليم الأدلة، ثم يتضمن تفتيش و ضبط معطيات النظام المخزنة وجمع المعطيات في الوقت الفعلي، واعتراض المعلومات.

للإطلاع على النص الكامل لاتفاقية بودابست، يرجى مراجعة الموقع الخاص بالمجلس الأوروبي:
http;//convention .coe.int/treaty/en/treaties/html/185.htm

[2] - حيث نصت المادة 5 منها على ضرورة أن تلتزم كل دولة طرف بتجريم الأفعال المبينة في الفصل الثاني منها وهي: جريمة الدخول غير المشروع، الإعتراض غير المشروع، الإعتداء على سلامة المعلومات، إساءة إستخدام وسائل تقنية المعلومات التزوير، الإحتيال، جريمة الإباحية، الإعتداء على

وهو ما كرسته الإتجاهات التشريعية المقارنة على أرض الواقع، آخذة حظها من ذلك إزاء ترقية العدوان على التعاملات الإلكترونية إلى مستوى الجرائم سواء تم ذلك من قبل أطراف التعامل الإلكتروني أو من الغير ولكن على نهج متباين، ومهما تكن من صياغات وأساليب فالمتفق عليه أن أحكام هذه الجرائم في التشريعات المختلفة جاءت لتحمي **أهم المصالح** في نطاق التعاملات الإلكترونية، من ثقة وأمان وسلامة وسرية، وكل ما يتعلق بهذه التعاملات.

وقد كان أبرز هذه التشريعات التشريع الفرنسي، وقد كان ذلك بموجب منظومة تشريعية متميزة في مجال مكافحة جرائم تقنية المعلومات بصفة عامة، حيث مد الحماية الجزائية المقررة في قانون العقوبات إلى التعاملات الإلكترونية، كما أدخل المشرع الجزائري في قانون التوقيع الإلكتروني نصوصا عقابية هدفها مواجهة الأنماط المتعددة من السلوكات التي يرى أنها تمثل إعتداء على التعامل الإلكتروني، وعلى نفس الخطى كان قد جرم ما سماه "المساس بأنظمة المعالجة الآلية للمعطيات" حماية لها من كافة أشكال الإعتداءات التي تقع على مكوناتها غير المادية، وقد كان ذلك بتعديل قانون العقوبات بموجب القانون رقم 04-15[1]، وقد عزز هذه الحماية بموجب قانون مستقل وهو القانون رقم 09-04[2]المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

أما المشرع المصري وإن نظم قواعد جزائية تستهدف حماية التعاملات الإلكترونية في القانون رقم 15 لسنة 2004 في بعض جوانبها، إلا أنه لم يصدر قانونا لمكافحة جرائم تقنية المعلومات بصفة عامة سواء من الناحية الموضوعية أو من الناحية الإجرائية، وإن كان يسعى لتحقيق ذلك نتيجة مصادقته على الإتفاقية العربية لمكافحة جرائم تقنية المعلومات[3] في الوقت الذي بدأت تعرض على القضاء المصري العديد من القضايا المتعلقة بهذا الموضوع.

الحياة الخاصة، الجرائم المتعلقة بالإرهاب ، بالجرائم المنظمة ، المتعلقة بإنتهاك حق المؤلف والحقوق المجاورة، الإستخدام غير المشروع لأدوات الدفع الإلكترونية.

[1]- قانون رقم 04-15 مؤرخ في 10 نوفمبر 2004، جريدة رسمية ، عدد 71، صادرة بتاريخ 10 نوفمبر 2004.

[2]-قانون رقم 09-04 المؤرخ في 14 شعبان 1430 الموافق لـــ 5 أوت 2009 ، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، جريدة رسمية، عدد 47، الصادرة في 16 أوت 2009.

[3]– قراررئيس جمهورية مصررقم 276 لسنة 2014،بشأن إنضماممصر إلى الإتفاقية العربية لمكافحة جرائم تقنية المعلومات. وقد إنتهت المصادقة على الإتفاقية بقرار رئيس الجمهورية بمشروع قانون لسنة 2016 في شان مكافحة الجريمة الإلكترونية، حيث قدم اللواء تامر الشهاوي عضو مجلس النواب المصري والذي يختص بمكافحة الجرائم الإلكترونية مقترح قانون مكافحة جرائم تقنية المعلومات سنة 2016 ، ويتألف المقترح من 30 مادة، ويستند إلى قانون الاتصالات رقم 10 لسنة 2003، وقانون التوقيع الإلكتروني رقم 15 لسنة 2004، وقرار رئيس الجمهورية رقم 276 لسنة 2014 بشأن انضمام مصر إلى الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، إضافة إلى الدستور وقانون العقوبات المصري ، وقد تضمن تجريم الممارسات الإلكترونية المجرمة، والتي لا يوجد ما يجرمها في القانون المصري، ومنها التزوير الإلكتروني وإنشاء مواقع للتشجيع على الإرهاب أو نقل المعلومات، وتتراوح العقوبات من السجن شهرا حتى الإعدام، في حالة الجرائم الإلكترونية التي يترتب عليها وفاة شخص أو أشخاص أو تهديد الأمن القومي والسلم الاجتماعي، إضافة إلى عقوبات الاختراق الإلكتروني والتزوير وغيرها من الجرائم، كما ينص القانون على عقوبات بحجب مواقع أو إلغاء تراخيصها بأحكام قضائية.

ولم تكن تلك هي المحاولة الأولى من نوعها، بل جاءت محاولة أخرى من مجلس الوزراء في فيفري 2015عندما طالب بتشكيل لجنة لإعداد مشروع قانون بشأن مكافحة جرائم تقنية المعلومات برئاسة السيد وزير العدل السابق وعضوية الجهات الأمنية ولم يصدر قانون بشأنه حتـــى الآن.

للإطلاع على المشروعين أنظـــر:

https://fr.scribd.com/document -

2-إشكالية البحـــث

إن ظهور التعاملات الإلكترونية طرح على مستوى الواقع العملي مجموعة من التساؤلات القانونية المتعلقة بمختلف فروع القانون، ولكن إذا إقتصرنا على الجانب الجزائي نلاحظ أن هناك العديد من التساؤلات المتعلقة بحماية نظام مواقع التعاملات الإلكترونية، وكذا حماية معطيات المتعامل الإلكتروني الشخصية من مخاطر المعالجة الآلية، وتثار كذلك مسألة تقرير مسؤولية الوسيط الفني عن المعلومات الواردة في المحتوى إذا تضمنت الإساءة للمتعاملين في مواقع التعاملات الإلكترونية، أو نشر وقائع تشكل جريمة، وهناك مسألة حماية مضامين التعاملات الإلكترونية التي إرتبطت بشكل عام بالتحول من المستندات التقليدية العادية إلى الدعامات المعلوماتية التي تحتوي على تلك المعلومات التي كانت متواجدة بالمستندات التقليدية، ومثل هذا الأمر يفرض لأسباب تتعلق بإمكانية المساس بسريتها أو بحجيتها، بخاصة إذا كان مجال الحفظ أو التبادل هو العالم الإفتراضي ذاته، وكذلك وسط تكهنات معاصرة بميكنة الإدارة والإنطلاق في فكرة التشغيل الآلي للحكومة الإلكترونية. فضلا عن حماية التوقيع الإلكتروني كأساس يضمن موثوقية التعاملات الإلكترونية في مرحلة إبرامها، وبعدها بإستخدام بطاقات الدفع الإلكترونية خاصة بطاقات الإئتمان.

غير أن الأمر لا يتوقف عند هذا الحد، فالإعتداءات التي تطال التعاملات الإلكترونية نوع من الجرائم الذي يتحدد نطاقه الموضوعي ببيئة لا علاقة لها بالأوراق أو المستندات بل بنبضات إلكترونية، وهو ما خلق مشاكل عديدة حول تتبع الدعوى الجزائية في هذه الجرائم، وصولا لإنزال العقاب على الجاني، وما يستتبعه ذلك من ضرورة المحافظة على الدليل الجنائي من جهة، والحرص على توافر مشروعيته من جهة أخرى.

ويرجع السبب في ذلك إلى أن القواعد الإجرائية قد وضعت لتطبق وفقا لمعايير مادية معينة، ولم تكن مخصصة لهده الظواهر الإجرامية المستحدثة، التي تقع في بيئة إلكترونية يصعب الحصول معها على أثر مادي للجريمة، فضلا عن إمتداد أركانها إلى أكثر من نطاق إختصاص في البلد الواحد بل وإلى أكثر من دولـــة.

وهو ما يطرح على القوانين الإجرائية مشاكل عديدة، تتطلب حلولا قانونية وعملية قد تكون في منتهى الصعوبة، خاصة فيما يتعلق بالكشف عن هذه الجرائم وإثباتها.

وعلى ضوء ما سبق، يتحدد التساؤل الرئيسي لهذا البحث والـــذي تتمحور بشأنه باقي الإشكاليات كالتالي:

إن كانت التشريعات المختلفة قد إنتظمت قواعد جزائية تستهدف حماية التعاملات الإلكترونية، فما مدى نجاعتها في التوصل إلى إرساء نظام حماية جزائي متكامل خاص بهذه التعاملات ذات الطبيعة الإلكترونية خاصة مع تطور إستخدام الوسائل الإلكترونية؟

3-أهداف البحث

ترمي الدراسة إلى تحقيـــق الأهداف التالية:

1- تحديد جوانب القوة في معالجة التشريعات لأوجه الاعتداءات التي تنال من التعاملات الإلكترونية وجوانب الضعف التي تعاني منها لمواجهة هذا النوع من الإجرام وما يستتبع ذلك من ضرورة سد الثغرات التي من الممكن أن يفلت منها الجاني.
2- تحديد الوسائل التي عن طريقها يتحقق التناغم بين التوأمين التشريع الجزائي الموضوعي والتشريع الإجرائي وذلك فيما يتعلق بالإثبات بالأدلة المتحصلة من الوسائل الإلكترونية، والبحث بذلك قد يميط اللثام عن بعض الصعوبات التي تكتنف موضوع إثبات الجرائم التي أوجدتها ثورة الاتصالات عن بعد، والتي مازالت في جانبها الإجرائي تحتاج إلى المزيد من التحليل والتأصيل.
3- إزالة التردد والخوف الذي يعتري المتعاملين الإلكترونيين في الدول النامية من التعامل بالوسائل الإلكترونية، عن طريق تبيان التقنيات التي تسمح باجراء تعاملات الكترونية آمنة باستخدام الوسائل الإلكترونية، ويمكن أن تكون مؤمنة أكثر من الوسائل التقليدية.
4- الرغبة في تقديم بحث يضيف للمكتبة العربية دراسة متعلقة بإحدى الجوانب القانونية للتعاملات الإلكترونية، هذه الأخيرة التي لقيت إهتماما أكبر من طرف الباحثين والأكاديميين في الدول الغربية.

4-أهمية البحث ودوافعه

إن موضوع الحماية الجزائية للتعاملات الإلكترونية موضوع هام يفرضه الواقع ويفرضه المستقبل وله أهمية بالغة من الناحية النظرية والعملية على حـــد سواء:

فمن **الناحية النظرية** نجد أن القانون هو إنعكاس لتطور المجتمع في حقبة زمنية معينة في كافة النواحي، ولا يستطيع مجتمع أن يبلغ مداه من التطور والتقدم دون أن تكون لديه قواعد قانونية تحدد ضوابط ذلك التقدم والرقي بما يخدم مصلحة المجتمع. وهنا تبدو أهمية الموضوع وما يثيره من تساؤلات عن مدى كفاية النصوص الجزائية القائمة سواء المتضمنة في قانون العقوبات أو القوانين الأخرى لمواجهة كافة الصور الواجب تناولها بالتجريم من عدمـــه.

أما من **الناحية العملية** فالموضوع يحتل أهمية متزايدة، خاصة مع الحركة التطورية التي تشهدها التعاملات في الدول الأروبية والتي دفعت المشرع الأروبي إلى إصدار النظام رقم 910-2014 المتعلق بتحديد الهوية الإلكترونية وبث الثقة في التعاملات الإلكترونية في السوق الداخلية من جهة، وبدأ التجارب الأولى لبعض الدول العربية للدخول في هذه الحركة التطورية كما هو حال الجزائر من جهة أخرى، حيث تبنت هذه الأخيرة مشروع الجزائر الإلكترونية 2013 الذي يرمي إلى إحلال نظام إلكتروني متطور شامل وترقيته في قطاع الإتصالات والبنوك والإدارة العمومية وقطاعات التربية والتعليم، ما يجعلها تقدم خدماتها بشكل أفضل وأبسط للمواطين من خلال إتاحة خدماتها على شبكة الأنترنت، ومن أجل تنفيذ هذا المشروع الذي أصبح حل لا مفر منه لترشيد النفقات العمومية بعد إنهيار أسعار البترول، ينبغي توفير بيئـــة آمنة لدعم التعامل بالمستندات الموقعة إلكترونيا على المستوى التقنـــي والقانـــوني.

5-منهـــج البحث

نظرا لخصوصية الموضوع وأهميته في الوقت الحاضر، وتشعب القضايا التي يتطرق لها، فقد إعتمدنا على عدة مناهج علمية تتكامل فيما بينها بهدف إغناء الموضوع ومحاولة الإلمام بكل جوانبه وآخر تطوراته، ومن أجل ذلك فقد إتبعنا منهجا ذا ثلاث أبـــعاد:

منهج تأصيلي يرد النقاط التفصيلية إلى أصولها النظرية، فعندما نعالج جريمة من جرائم التعاملات الإلكترونية نردها إلى الأركان العامة في التجريم، وعندما نعالج الشهادة في مجال الجرائم الواقعة على التعاملات الإلكترونية نردها إلى النظرية العامة في الشهادة.

منهج تحليلي من خلال قيامنا بتحليل النصوص القانونية بالإستعانة بآراء الفقه وأحكام القضاء، والوقوف على ماهو صحيح يفي تطبيقه الحالي إلى الوصول لأفضل الحلول القانونية، وما قد يحتاج إلى تعديل في الفترة القادمة.

منهج مقارن من خلال مقارنة التجارب التشريعية الوطنية التي هدفت لمواجهة هذا النوع من الإجرام في ظل الجهود الدولية والإقليمية، وبما أن العديد من التشريعات المقارنة العربية والأجنبية قد تناولت بالتأثيم الجرائم التي تطال التعاملات الإلكترونية، فقد إرتأينا أن **نركز** في الدراسة على نموذج من التشريعات الأجنبية التي نظمت التعاملات الإلكترونية، وضبطت الإطار العام لزجر جرائم تقنية المعلومات والتي ممكن أن تقع البعض منها في نطاق التعاملات الإلكترونية، وصادقت على إتفاقية بودابست لجرائم تقنية المعلومات وأدخلت العديد من الإرشادات والتوجيهات الصادرة عن المنظمات الدولية المتعلقة بتنظيم التعاملات الإلكترونية في نظامها القانوني وهو **التشريع الفرنسي الذي يبقى دائما مرجعا لواضعي القوانين في بلادنا**[1]، ونموذجا آخر من الدول العربية التي لم تصادق بعد على هذه الإتفاقية ولم تصدر قانون خاص لمكافحة هذا النوع من الإجرام المستحدث الذي يفتقد في كثير من الحالات إلى العنصر المادي الذي يقتضيه القانون الجزائي عادة لقيام الجريمة، والتي يدخل ضمنها العديد من صور الإعتداء على التعاملات الإلكترونية، وهو **التشريع المصري**-وإن كان يسعى لتحقيق ذلك- ما عدا قانون التوقيع الإلكتروني رقم 15 لسنة 2004، وبالطبع لم نقف عند حد المقارنة بل كان **القانون الجزائري** هو نموذجا للتشريعات التي صادقت على الإتفاقية العربية لتقنية المعلومات[2]، ومن أوائل التشريعات العربية الذين آمنوا بضرورة تطوير المنظومة

---

[1]- حيث وقعت عليها في 23-11-2001 وصادقت عليها في 10-1-2006 أنظر:
http://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=YyLDV0Np

[2]- مرسوم رئاسي رقم14-252 مؤرخ في 13 ديالقعدة عام 1435 الموافق ل 8 سبتمبر 2014، متضمن التصديق على الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، جريدة رسمية، عدد57، لسنة2014 .

وقد جاء في ديباجة الإتفاقية العربية بيانا لمخاطر إنتشار تقنية المعلومات كما يلي "...إن الدول العربية الموقعة **رغبة** منها في تعزيز التعاون فيما بينها لمكافحة جرائم تقنية المعلومات التي تهدد أمنها ومصالحها وسلامة مجتمعاتها، **وإقتناعا** منها بضرورة الحاجة إلى تبني سياسة جنائية مشتركة تهدف إلى حماية المجتمع العربي ضد جرائم تقنية المعلومات، وأخذا بالمباديء الدينية والأخلاقية السامية ولاسميا أحكام الشريعة الإسلامية وكذلك بالتراث الإنساني للأمة العربية التي تنبذ كل أشكـــال الجرائم، ومع مراعاة النظام العام لكل دولة...".

القانونية وملائمة الأحكام الجزائية مع ما أفرزته الثورة الرقمية والإتصالية من سلوكات غير مشروعة، بداية من تعديل قانون العقوبات نهاية بقانون التوقيع والتصديق الإلكترونيين.

6-خطة الـــــبحث

إذا كانت الحماية الجزائية للتعاملات الإلكترونية تتطلب مبدئيا من الناحية الموضوعية حماية آلية قيام التعاملات الإلكترونية، وحماية مضمون التعاملات الإلكترونية ذاتها، فإنها لا تكفي لتحقيق حماية شاملة وكاملة لها، دون تكملتها من الناحية الإجرائية.

وبناء على ماسبق سوف نعالج موضوع الرسالة من خلال بابين، نتناول في **الباب الأول** الجوانب الموضوعية للحماية الجزائية للتعاملات الإلكترونية، وقسمنا هذا الباب إلى فصلين، نتناول في الفصل الأول الحماية الجزائية لآلية قيام-أداء- التعاملات الإلكترونية من خلال حماية مواقعها في المبحث الأول، وتقرير المسؤولية الجزائية للوسيط الفني في التعاملات الإلكترونية في مبحث ثاني، وحماية المعطيات الشخصية في مبحث ثالث.

بينما نتطرق في الفصل الثاني للحماية الجزائية لمضمون هذه التعاملات، من خلال حماية المستند الإلكتروني في المبحث الأول، وحماية التوقيع الإلكتروني في المبحث الثاني، وحماية بطاقات الإئتمان في المبحث الثالث.

أما **الباب الثاني** فنتناول فيه الجوانب الإجرائية للحماية الجزائية للتعاملات الإلكترونية، وقسمنا هذا الباب إلى فصلين، إذ ندرس في الفصل الأول قواعد التحقيق في الجرائم الواقعة على التعاملات الإلكترونية من خلال دراسة الاختصاصات المعتادة لضباط الشرطة القضائية في مكافحة الجرائم الواقعة على التعاملات الإلكترونية في مبحث أول، والإختصاصات المتميزة لضباط الشرطة القضائية في مكافحة الجرائم الواقعة على التعاملات الإلكترونية في مبحث ثاني، ومدى تعاون مقدمي الخدمات مع رجال الضبط القضائي في مبحث ثالث.

أماالفصل الثاني فنتطرق فيه لقواعد الإثبات الجزائي والإختصاص القضائي في جرائم التعاملات الإلكترونية من خلال دراسة وسائل الإثبات في جرائم الإعتداء على التعاملات الإلكترونية في مبحث أول، ودراسة الدليل الإلكتروني في مبحث ثاني، ودراسة الإختصاص القضائي بنظر جرائم الإعتداء على التعاملات الإلكترونية في مبحث ثالث.

وفي آخر الدراسة توصلنا لعدد من النتائج والتوصيات يمكن إقتراحها في هذا الموضوع تم إدراجها في خاتمـــة هذا الـــبحث.

البـــاب الأول

الجوانب الموضوعية للحماية الجزائية للتعاملات الإلكترونية

إن التطورالهائل الذي حصل بعد الربط بين وسائل الحوسبة والاتصال، لينقل الحوسبة من النظم المغلقة إلى المفتوحة، أدى إلى إستحداث صور إجرامية لم تكن معلومة من قبل، ومن تلك الصور المستحدثة جرائم الإعتداء على التعاملات الإلكترونية.

ولما أثبت الواقع العملي أن إتبـــاع الأسلوب الوقائي لا يؤدي بمفرده إلى المنع المطلق لهذه الجرائم، فكان لا بد من جزاء جزائي مناسب يواجه هذه الإعتداءات، يتمثل في العقوبات التي تصدرها المحاكم على المعتدين. بما تتميز به من قوة تأثيرها في نفس المعتدي أكثر من الجزاء المدني.

لذا فقد حرص مشرعوا الدول المختلفة على وضع النصوص الجزائية الكفيلة بحماية التعاملات الإلكترونية من نواح عدة. وعن طريق هذه القواعد الجزائية تم تقرير الحماية لآلية أداء التعاملات الإلكترونية فضلا عن مضمونها.

ولذا سوف نقسم الدراسة في هذا الباب إلى الفصـــلين التالـــيين:

الفصل الأول: الحماية الجزائية لآلية أداء التعاملات الإلكترونية

الفصل الثاني: الحماية الجزائية لمضمون التعاملات الإلكترونية

الفصل الأول

الحماية الجزائية لآلية قيام-أداء- التعاملات الإلكترونية

مما لا شك فيه أن آلية قيام–اداء عمل_التعاملات الالكترونية بمختلف أنواعها سواء كانت حكومية أو تجارية أو غيرها قائم على حاسوب وشبكة وموقع ومحتوى، حاسوب يسمح بمعالجة المعطيات، وموقع على الشبكة لعرض المنتجات أو الخدمات، وشبكات إلكترونية تتيح عملية الربط والانتقال وتحقيق عمليات الدخول وضمان تبادل المعلومات خاصة شبكة الانترنت. ولتحقيق الإتصال هذا يتدخل أشخاص كثيرون في آلية عمل الشبكة ويسهمون في إتمام ذلك التعامل بأدوار مختلفة تختلف ضيقا وإتساعا وأهمية حسب موقع كل منهم، وهؤلاء قد تحتويهم عدة دول متفرقة بحيث قد يتواجدون في دول مختلفة، كما تتعدد المؤسسات والشركات الدولية والوطنية التي تقدم الخدمات في شأن الأنترنت.

وفي كثير من التعاملات الإلكترونية تطلب الجهة التي يتعامل معها الشخص أن يقدم معطياته الشخصية لها، سواء أكانت هذه الجهة جهة عامة خاضعة لإدارة الدولة أم كانت جهة خاصة. وذلك لحصوله على الخدمة. دون إدراك منه لمصير هذه المعطيات.

وإذا كانت البيئة الأساسية للتعاملات الإلكترونية على النحو السابق هي شبكة الأنترنت، فإن طبيعة هذه البيئة التي تدور في فلكها هذه التعاملات جعلتها تتميز عن غيرها من وسائط تكنولوجيا المعلومات الأخرى بالسرعة وخفظ التكاليف، إلا أن التعامل بها خلق مشاكل قانونية متعلقة بحماية هذا الموقع. ذلك أن الإعتداءات في هذا الميدان كثيرة وذات طابع حديث ومتطور حيث أخذت تستهدف هذا الموقع وما يحويه من معلومات ذات القيمة الإقتصادية التي قد تفوق قيمة الأموال، كما أن تزايد أعداد المتدخلين في خدمات الأنترنت دون وجود ضابط يحكم تصرفاتهم أدى إلى صعوبة حصر المسؤولية الجزائية الناتجة عن تداول المعلومة[1]، مما يثير مخاوف أطراف التعامل الإلكتروني حول أمن هذا التعامل الإلكتروني خاصة فيما يتعلق بمعطياتهم الشخصية التي يتم تداولها عبرها.

إذا فالحماية الجزائية للآلية قيام التعاملات الإلكترونية تقوم على ثلاث مقومات أساسية، نعرضها بالتحليل من خلال ثلاث مباحث كمايلي:

المبحث الأول: الحماية الجزائية لموقع التعاملات الإلكترونية

المبحث الثاني:تقريرالمسؤولية الجزائية للوسيط الفني في التعاملات الإلكترونية

المبحث الثالث: الحماية الجزائية لمعطيات المتعامل الشخصية

[1]– **د. حسين محمد عبد الظاهر**، المسؤولية القانونية في مجال شبكات الأنترنت، دار النهضة العربية ، القاهرة، 2003، ص18.

المبحث الأول

الحمـــاية الجزائية لموقع التعاملات الإلكترونية

تعتبر التعاملات الإلكترونية أحد المظاهر الرئيسية لعصر تكنولوجيا المعلومات وما يصاحبها من تغيير في أنماط السلوك الإقتصادي والإداري والإجتماعي، فقد أخذت العديد من الحكومات والمنظمات والجامعات وغيرها مواقع الكترونية على شبكة الأنترنت للتواصل مع المتعاملين معها عبر مختلف أنحاء العالم، وذلك نظرا لما يوفره هذا النوع من المعاملات لأطرافها العديد من الخصائص المرتكزة بشكل أساسي على طبيعة الوسط الذي تجري فيه.

ولتوفير البيئة المناسبة لنشأة التعاملات الإلكترونية على إختلاف أنواعها، إتجهت التشريعات سواء الدولية منها والوطنية إلى تقرير الحماية اللازمة للمواقع الإلكترونية وما تحتويه من معلومات مبرمجة آليا، عن طريق تجريم الإعتداءات التي تطال نظم المعالجة الآلية بصفة عامة، وذلك إيمانا منها بعجز النظم القانونية القائمة التي تتناول الجرائم التقليدية عن حماية هذه النظم ومعلوماتها.

ويتخذ الإعتداء على نظام المعالجة الآلية أكثر من شكل، فقد يكون ذلك بالدخول أو البقاء غير المصرح به، أو بالإعتداء على سلامته، وقد يكون في صورة التعدي على المعلومات التي يحتويها.

وعليه فإن تسلسل الأفكار على هذا النحو يقتضي منا تقسيم هذا المبحث إلى المطالب الثلاثة التالية:

المطلب الأول:ماهية الموقع الإلكتروني

المطلب الثاني:الحماية الجزائية لنظام مواقع التعاملات الإلكترونية

المطلب الثالث: الحماية الجزائية لمعلومات نظام مواقع التعاملات الإلكترونية

المطلب الأول

ماهية الموقـــع الإلكتروني

الموقع الإلكتروني هو مكان إتاحة المعلومات على شبكة الانترنت من خلال عنوان محدد، يطلق عليه إسم النطاق أو إسم الحقل أو عنوان الموقع "الدومين"، وهو ضروري حيث يبين موقع الانترنت لمن يسعى للوصول إليه[1]. ومواقع الأنترنت ماهي إلا **نظام معلومـــاتي** نشط يعمل على الانترنت له طابع إتصال عالمي متفاعل ومتنام يخترق الحدود بأسلوب الربط التصويري. ويرتكز عمل مواقع الإنترنت على بروتوكولHTTP الذي يسمح بربط المواقع الموصولة بشبكة الإنترنت فيما بينها.[2]

لقد أضافت نظم المعالجة الآلية الكثير من الجوانب الإيجابية إلى حياتنا، إلا أنها في المقابل جلبت معها جرائم متميزة من حيث المصالح التي مستها، طبيعتها، وسلوكياتها ومحلها ومشكلاتها وفي الغالب في طبائع وسمات مرتكبيها أطلق على تسميتها بـــ "جرائم تقنية المعلومات"، ونظرا لنمو وتزايد التعاملات الإلكترونية عبر شبكة الأنترنت، فإن جرائم تقنية المعلومات وثيقة الصلة بحركة هذه التعاملات إذ تشكل مدخلا سهلا لإرتكاب تلك الجرائم.

إن الطبيعة الخاصة لتلك الجرائم خلقت أزمة القانون الجزائي، حيث تضخم الفارق بين ما ينتج من تقنيات وبين ما يرتكب بصددها من جرائم وبين ما يرصد لها من نصوص تشريعية لمواجهة هذه الظاهرة, خاصة حينما إمتد الاعتداء إلى الأنساق المعلوماتية المختلفة ذات الكيفية المعنوية المتميزة بالضخامة والتنوع.
وفي سبيل ذلك، عمدت بعض الدول إلى تعديل قوانينها الداخلية من أجل توفير الحماية الجزائية لنظم المعالجة الآلية. في حين قامت دول أخرى إلى سن تشريعات خاصة بها، في مقابل ذلك لم تحسم بعض الدول موقفها بعد في التصدي لهذا النوع من الإجرام.ولم يقتصر الأمرعلى المشرع الوطني فحسب، فالخصائص التي تتميز بها هذه الجرائم خاصة أنها خطيرة وعابرة للحدود_ جعلت مختلف الدول توحد صفها في مواجهتها وذلك بابرام عدة إتفاقيات تهدف إلى توحيد التشريعات في هذا المجـــال.
وعلـــى ذلك فإن الوقوف على أبعاد هذه الظاهرة بشكل كامل، يتطلب منا تحديد مفهوم نظام المعالجة الآلية(الفرع الأول)،وتلازم ظهور جرائم تقنية المعلومات بظهوره(الفرع الثاني)، ثم دراسة تطور حمايته الجزائية(الفرع الثالث).

---

[1]- د. **حسين بن سعيد بن سيف الغافري**، الجرائم الواقعة على التجارة الإلكترونية، مقال متاح على الموقع الإلكتروني التالي:
http://www.mohamoon.com/montada/Default.aspx?Action=Display&ID=106198&Type=3

[2]- وهو لا يعمل إلا بواسطة برامج تصفح خاصة Browsers تسمح بالاتصال بالملقمات وبالمواقع المختلفة الموصولة بالشبكة وذلك بالاعتماد على تقنية الهيبرميديا ، وهذه الأخيرة تعد أداة مثالية للتجول في الإنترنت بفضل تقنيات الربط الفائق بين النصوص والصفحات والعناصر داخل الموقع ذاته ، وحتى بين الموقع والمقلمات المختلفة الموصولة بالشبكة وذلك في إطار أو تصور يشبه بالشجرة يسميHypertext أو Hyper ling
نفس المرجع، ص7. أنظر أيضا: القرصنة الإلكترونية , مقال منشور على الموقع الإلكتروني التالي:
http://www.nabdh-alm3ani.net/nabdhat/t33913

الفــرع الأول

مفهوم الموقع الإلكتروني

لما كانت مواقع التعاملات الإلكترونية نظاما معلوماتيا يتضمن العديد من المعلومات المرتبطة بمجالات مختلفة، كان لزاما علينا التطرق لتعريفه، وتبيان عناصره.

أولا- تعريفـــــه

يعتبر نظام المعالجة الآلية للمعطيات الوسيلة الأساسية للقيام بالتعاملات الإلكترونية المختلفة، فلكي يتم التأكد من وجود إعتداء على قواعد معطيات التعاملات الإلكترونية، لا بد أن تكون هناك قاعدة معالجة آلية للمعطيات المتعلقة بهذه التعاملات[1].

وقد ظهر هذا المصطلح منذ السبعينات من القرن الماضي، وما تطلبه التطور التقني من ضرورة القيام بمهام توفير وجمع ومعالجة و**تبادل** المعلومات في نفس الوقت باعتباره الواسطة التي أفرزتها عمليات الدمج بين كل من وسائل الحوسبة والاتصال والوسائط المتعدّدة بما قدمته من قدرة على رقمنة الصوت[2] والصورة وتحويلهما إلى مادة تفاعل بين المستخدم وبين المحتوى.[3]

فمصطلح نظام المعالجة الآليّة هو مصطلح نشأ بهدف وصف الحالة التي نشأت باندماج تقنيات عملاقة هي تقنية نظم المعلومات، وتقنية الاتصالات عن بعد وهندسة التحكم، وقد أدى هذا التزاوج إلى إختراع تقنيات باهرة ساعدت بشكل كبير على تطوير أنظمة معالجة المعلومات بمختلف أشكالها وأنواعها، وأصبحت بالفعل عاملا حاسما في تحديد مصير عالمنا بدوله وأفراده، وأثرت ولازالت تؤثر في شتى مناحي الحياة.[4]

وقد عرفته الاتّفاقية الدّولية لإجرام تقنية المعلومات بموجب الفقرة أ من المادة الأولى 1 من الفصل الأول بعنوان المصطلحات *terminologie*على أنّه***كل آلة بمفردها أو مع غيرها من الآلات المتصلة أو المرتبطة, والتي يمكن أن تقوم سواء بمفردها أو مع مجموعة عناصر أخرى, تنفيذا لبرنامج معين, بأداء معالجة آلية للمعطيات.***

---

[1]-**د. عبد الفتاح بيومي حجازي**، الحماية الجنائية لنظام التجارة الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2001، ص21.

[2]-إن عملية رقمنة الصوت هي عملية بسيطة، وهي في الواقع مجرد تحويل إشارات كهربائية إلى ملفات بيانات حاسوبية، ويقوم الميكروفون في هذه الحالة بتحويل موجات صوت الشخص إلى إشارة كهربائية تعرف بالإشارة الصوتية النظيرية، يتم بعد ذلك تسيير الإشارة الصوتية إلى منافذ داخل الصوت في بطاقة الصوت الرقمي، ويمكن الحصول على الصوت من أية وسيلة تستطيع إخراج إشارة صوتية نظيرية مثل مسجل أشرطة الفيديو : **يونس عرب**، قانون الكمبيوتر،موسوعة القانون وتقنية المعلومات، الطبعة الأولى، منشورات إتحاد المصارف العربية، 2001، هامش رقم 46، ص69.

[3]- أنظر في هذا المعنى: **يونس عرب**، المرجع نفسه، ص 69.

[4]-**علي فاروق علي الحفناوي**، موسوعة قانون الكمبيوتر ونظم المعلومات، قانون البرمجيات_دراسة متعمقة في الأحكام القانونية برمجيات الكمبيوتر، الكتاب الأول، دار الكتاب الحديث ، القاهرة، 2003، ص24.

وكما هو ملاحظ أنّ هذه المادة لم تحدد العناصر التي يتكون منها نظام المعالجة الآلية، بل ركزت على عنصر عملية **المعالجةالآليّة** في التعريف باعتبارها تنطوي على مراحل سابقة ولاحقة، وهو ما يسمح بإعتبار عناصر التبادل المتعلقة بالجوانب الاتصالية بالمعلومات ضمن مفهوم المعالجة. وفي ذات المعنى عرفه المشرع الجزائري بموجب الفقرة ب من المادّة 2 من القانون رقم 09 -04 لسنة 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها حيث على أنّه "*أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة يقوم واحد منها أو أكثر* ***بمعالجة آلية للمعطيات*** *تنفيذا لبرنامج معين*".

أما الوضع في فرنسا فإن مجلس الشيوخ الفرنسي كان قد إقترح تعريفًا لنظام المعالجة الآليّة بمناسبة تعديل قانون العقوبات على أنّه "***كل مركب يتكون من وحدة أو مجموعة وحدات معالجة والتي تتكون كل منها من الذاكرة و البرامج و المعطيات و أجهزة الإدخال و الإخراج و أجهزة الربط والتي تربط بينها مجموعة من العلاقات التي عن طريقها يتم تحقيق نتيجة معينة و هي معالجة المعطيات على أن يكون هذا المركب خاضعا للحماية الفنية***".[1]

والملاحظ أن هذا التعريف قد ركز على وظيفة النظام كونه يقوم بالمعالجة الآلية للمعطيات، كما قد أشار للعناصر المادية والمعنوية التي يتكون منها هذا المركب، واردا إياها على سبيل المثال لا الحصر، وهو مسلك محمود من جانبه ذلك أن العناصر التي يتكون منها نظام المعالجة الآلية هي في تطور مستمر وهو ما يتطلب عدم تقييد التعريف بالعناصر الواردة فيه[2].

لقد أصبح نظام المعالجة الآية مطلب أساسي ولا غنى عنه في التعاملات الإلكترونية، وذلك لعدة أسباب منها السرعة في إنجاز المعاملات، الدقة في الأداء، توفير الجهود، وسهولة إسترجاع المعلومات المخزنة[3].

---

[1]–Le Sénat désirait définir un STAD comme « **tout ensemble composé d'une ou plusieurs unités de traitement automatisées, de mémoires, de logiciels, de données, d'organes d'entrées-sorties et de liaison qui concourent à un résultat déterminé, cet ensemble étant protégé par des dispositifs de sécurité** » Rapp. J. Thyraud Doc. Sénat 1987-88 n°3,p52.

[2]– قد أخذ القضاء الفرنسي بالمفهومالموسع للنظام.حيث قضى في بعض أحكامه باعتبار شبكة الاتصال من النظام، الراديو تليفون من النظام، وقد قضى بنفس الشيء بخصوص قرص *ثابت*، حاسوبمحمول وأيضا هاتف محمول، *شبكـــــــة:*

MAITRE ANTHONY BEM, L'INTRUSION ET LES ATTEINTES AUX SYSTEMES INFORMATIQUES SANCTIONNEES PAR LE DROIT PENAL, , disponible en lingne á l'adresse suivante: http://www.legavox.fr/blog/maitre-anthony-bem/intrusion-atteintes-systemes-informatiques-sanctionnees-3158.pdf
Trib. cor. Paris, 25 fev 2000, disponible en lingne á l'adresse suivante: http://www.murielle-cahen.com/p_references.asp

C.A de Paris, 18 nov. 1992 disponible en lingne á l'adresse .suivante:. http://www.legipme.com/actualite/droit-ntic/intrusion-dans-systeme-traitement-automatique-donnees-stad-reponses-droit.html) C.A de Douai, 7 oct 1992, disponible en lingne á l'adresse.suivante: http://www.legipme.com/actualite/droit-ntic/intrusion-dans-systeme-traitement-automatique-donnees-stad-reponses-droit.html

Haja Rakotozafy, Nguyen Trinh Thiet, les atteintes aux systèmes informatisés de données,realise le 1 mars, 2005, disponible en lingne á l'adresse suivante:. http:\Documents and Settings\user\Desktop\Les atteintes aux systèmes informatisés de données e-juristes org.mht.

[3]-د. **خالد ممدوح إبراهيم**، التقاضي الإلكتروني–الدعوى الإلكترونية وإجراءاتها أمام المحاكم، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2008, ص304.

ثانيا- عناصـــره

سبق وأن رأينا أن نظام المعالجة الآلية هو ذلك النظام الإلكتروني للتعامل مع المعلومات إدخالا ومعالجة وإسترجاعا ونقلا وتبادلا وتفاعلا، ويشمل وسائل الحوسبة والإتصال. وهو بهذا المفهوم يشمل العناصر المادية لوسائل الحوسبة والإتصال من وحدات إدخال معالجة تخزين وإخراج[1]، كما يشمل عناصر غير مادية تتمثل في المعلومات تربط بينها تجهيزات ربط على رأسها شبكة الانترنت. ويمكن أن يخضع للحماية الفنية.

أ- المعلومـــــات

تعد المعلومات المحور الذي تدور حوله تقنية المعلومات، وهي ما سيكون محلا لجرائم تقنية المعلومات، هذه الأخيرة التي لها صلة وثيقة بحركة التعاملات الإلكترونية، إذ تشكل مدخلا سهلا لإرتكاب تلك الجرائم.

تعتبر المعلومات بالنسبة للأجهزة التقنية القلب للإنسان، مما حدى بالبعض[2] إلى إعتبارها بمثابة السلطة الرابعة داخل الدولة، وقد تعددت التعريفات التي رصدت لها سواء على المستوى الفقهي أو التشريعي، إلا أنها تدور حول مفهوم واحد وهي أن المعلومات تشمل: ***نصوص أو صور أو أصوات أو رموز أو برامج التي تمت معالجتها, ومهما كانت الحالة التي تكون عليها سواء كانت معلومات مدخلة (معطيات[3]) معلومات معالجة, مخزنة أو في طور النقل والتبادل ضمن وسائل الاتصال المندمجة مع نظام الحوسبة .***

---

[1]-أنظر كـــل من : **د. صفوت النحاس**، مراجعة د. عبد المنعم يوسف بلال، الحاسبات الشخصية وفيروسات الكمبيوتر، دار النشر هاتيه،دون تاريخ, ص12. **محمود الزهر ومحمد عثمان**، مقدمة الحاسب الآلي، معهد الإدارة العامة، السعودية،دون تاريخ, ص ص10-12. **د. عبد الله بن عبد العزيز موسى**، مقدمة في الحاسب والانترنت، الطبعة الثالثة، دون دار النشر، الرياض، 2005، ص ص7-8.

د. أحمد محمود سعد، نحو إرساء نظام قانوني لعقد المشورة المعلوماتية_المعالجة الآليّة للبيانات بواسطة الحاسب الآلي-، الطبعة الأولى، دار النهضة العربية، القاهرة، 1995، ص50_51.

عـــــلي إبراهيم, ذاكرة الحاسوب *Ram & Rom*, سوريا, مقال منشور على الموقع التالي:

http://www.kutub.info/library/book/5064

مقدمة عن الحاسبات، مقال منشور على الموقع الإلكتروني التالـــــــــــي:

www.mohealth.gov.eg/Sec/Heducation/CompSince1.doc

مكونات الحاسب الآلي, مقال منشور على الموقع التالي:

http://www.kutub.info/library/book/3628.

[2] **-Géraldine DANJAUME, La responsabilité du fait de l'information,Revues** La Semaine Juridique - Edition Générale 3 Janvier 1996 - n° 1,3895.

[3]-عرف المشرع الجزائري المعطيات بموجب الفقرة ج من المادة 2 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال و مكافحتها على أنها" أي عملية عرض للوقائع أو المعلومات أو المفاهيم فيشكل جاهز للمعالجة داخل منظومة معلوماتية بمافي ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها".

والمعلومات وفق التحديد السابق لها أشكال مختلفة في العالم الرقمي، ولكنها لا بد وأن تكون على **هيئة إلكترونية**[21]، ومثل هذا الأمر يقود إلى تقرير نطاق الحماية الجزائية للمعلومات داخل بيئتها الإلكترونية فحسب، ليخرج من نطاقها مادون ذلك من المعطيات التي لم تعالج بعد ولم تدخل إلى نظم معالجة المعلومات. وكذلك المعلومات المعالجة التي إنفصلت وسجلت على شيء مادي لأنّها أصبحت خارج النظام[3].

إن الشكل الإلكتروني التي تتخذه المعلومات مجردة من وسيطها المادي، خلق فضاء للتضارب والتباين في المواقف الفقهية حول **طبيعتها القانونية**[4]، فالإتجاه القديم ربط وصف المال بعنصرين: عنصر المادية في المال والثاني عنصرالقيمة، فإن تخلف أحدهما ينتفي في الشيء وصف المال، أما الإتجاه الحديث فيذهب إلى الأخذ بالمفهوم الموسع للمال ليشمل إلى جانب الأشياء المادية تلك الأشياء غير المادية معتبرا بذلك بقيمتها الاقتصادية ليواكب تلك القيم التي أفرزتها الثورة المعلوماتية.

وإن كنا نؤيد ما ذهب إليه الاتجاه الحديث، إلا اننا نرى أن المال المعلوماتي على عمومه يمكن أن يشكل قيمة اقتصادية هنا، وهذا يؤدي إلى القول بأن النظرة إلى القيمة الإقتصادية ليست نهاية المسار، ذلك أن المال المعلوماتي يمكن أن يأخذ بعدا جديدا بعيدا عن تحديده بالقيمة الإقتصادية، وإنما النظر إليه على أنه يشكل قيمة معلوماتية تبادلية هنا، ففي مقابل شراء أشياء معينة عبر الأنترنت فإن الفرد يحوز أرقام يمكن لمصرف حول العالم قبولها والعمل على تحويلها لصالحه كمبالغ يحتفظ بها له في الوقت الذي يمنحه نفس المصرف صيغة رقمية جديدة عبارة عن أرقام مختلفة يمكنه التعامل بها عبر الأنترنت[5].

---

[1]– ونقصد بذلك أن يكون كل ما يستحدث أو يسجل أو ينقل أو يرسل أو يخزن بصيغة رقمية أو بأية صيغة غير ملموسة تكون قادرة على القيام بالعمليات السابق ذكرها أو نحوها، فكل ذلك ينطبق عليه وصف "**إلكتروني**"، ويمكن فهم مصطلح إلكتروني أكثر من خلال تدخل الآلة في إجراء **المعالجة الآلية على المعلومات بواسطة برنامج معلوماتي**.

[2]– وهو ما أشارت إليه المذكرة التفسيرية لاتفاقية بودابست، حيث ذهبت إلى أن التعريف الوارد ضمن الفقرة ب من المادة الأولى من هذه الاتفاقية يتضمن من ضمن ما يتضمنه عبارة "التي تكون مهيأة للمعالجة *qui se prête a un traitement*,وهذا يعني أن المعلومات لابد أن توضع في شكل يسمح بمعالجتها مباشرة، وفي إطار توضيح المذكرة أكثر لمعنى المعلومات نجدها تشير إلى أنه يجب فهمها على أنها معلومات تأخذ شكلا إلكترونيا، أو أي شكل آخر يسمح بمعالجتها مباشرة، أنظر : **د. هلالي عبد الله أحمد**،الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء إتفاقية بودابست الموقعة في 23 نوفمبر 2001، دار النهضة العربية، القاهرة، 2003، ص47.

[3]– **د. عبد الفتاح بيومي حجازي**، التزوير في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، الإسكندرية، 2008 ، ص 64.

[4]– انظر في هذا المعنى: **محمد خليفة**، الحماية الجنائية لمعطيات الحاسب الآلي–دراسة مقارنة_دار الجامعة الجديدة، الإسكندرية، 2007، ص97, **د. نائلة عادل محمد فريد قورة**، جرائم الحاسب الآلي الاقتصادية–دراسة نظرية وتطبيقية– الطبعة الأولى، رسالة دكتوراه، منشورات الحلبي الحقوقية، بيروت، 2005، ص116، **د. محمد سامي الشوا**، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، 1994، ص179. **د. محمود عبد الله حسين علي**،سرقة المعلومات المخزنة في الحاسب الآلي، الطبعة الثانية، رسالة دكتوراه، دار النهضة العربية، القاهرة، 2002، ص161. **د. عفيفي كمال عفيفي, فتوح الشاذلي**، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون–دراسة مقارنة–، منشورات الحلبي الحقوقية، بيروت، 2003، ص112. **د.السيد عتيق**، جرائم الانترنت، دار النهضة العربية، القاهرة، 2000، ص91، د.**أيمن عبد الله فكري**،جرائم نظم المعلومات–دراسة مقارنة–دار الجامعة الجديدة للنشر، الإسكندرية، 2007، ص 496.

[5]- د. **عمر محمد أبو بكر بن يونس**، الجرائم الناشئة عن إستخدام الأنترنت، رسالة دكتوراه،كلية الحقوق، جامعة عين شمس، 2004، ص405.

ب- الحمـــاية الفنيـــة

يقول البعض[1] أن سرية التعاملات تظهر في منظومة الأمان التي تحيط بالمعلومة ونظامها، وبالتالي فإن المعلومة غير المحمية لا يمكن إعتبارها معلومة سرية.

لم يكن أمن وسلامة نظم التعاملات الإلكترونية في بدء ظهورها على درجة كبيرة من الأهمية، بعكس ماهي عليه الآن، إذ كلما إرتفعت قيمة المعلومات المخزنة في النظام، تنام الفضول لدى البعض للوصول إليها، وهو ما يظهر جليا في إطار المنافسة الحادة في التعاملات الإلكترونية التجارية. وعلى الرغم من توافر أدوات ناجعة في تحقيق الأمان، إلا أنه تنامت في الوقت نفسه أنشطة الإختراقات والتطفل على النظام بهدف الوصول للمعلومات.

رغم إستبعاد التشريعات صراحة شرط الوسائل التقنية لإقرار المسؤولية الجزائية، كما هو محدد في المادة 323-1 عقوبات فرنسي، والمادة 394 مكرر عقوبات جزائري، إلا أن هذه المسالة كانت محل إختلاف فقهي كبير بين مؤيد[2] ومعارض[3]، إلا أنه وأمام وضوح النص يظهر دور القاضي جليا ودور الفقه أيضا، حيث يلتزم بإحترام الإرادة الظاهرة للمشرع، فيما يخص الأنظمة المغلقة التي تظهر طبيعتها الخاصة في عدم إمكانية الوصول المعترف بها للجمهور، إلا في حالة الخطأ، وشرط نظم الأمن لا يعد شرطا مبدئيا

---

[1]-**Croze**: L`apport du droit pénal à la théorie générale du droit de l`informatique (à propos de la loi No 88 - 19 du 5 Janvier 1988 relative à la fraude informatique), J.C.P. 1988, p 13.

مشار اليه لدى : **نادية محمد معوض**، أثرالمعلوماتية على الحق في سرية الأعمال، مجلة كلية الحقوق،الجزء 1، بنها، مصر، ص95.

[2]–par ex:-

Lucas de leyssac, commentation de la loi du janvier , rev droit informatique et des télécoms, 1988, p21, Alterman et blach, la fraude informatique, G.p 1988. 2, doct.530

مشار إليهما لدى :د. **أيمن عبد الله فكري**، المرجع السابق، ص231. وأنظر تأييد هذا الرأي في الفقه العربي: **د. حسام طه تمام**،الجرائم الناشئة عن إستخدام الحاسب الآلي، دراسة مقارنة، رسالة دكتوراه، دار النهضة العربية، القاهرة، 2000، ص267, **د. أيمن عبد الله فكري**، المرجع السابق، ص234. **بلال أمين زين الدين**، جرائم نظم المعالجة الآلية للبيانات في التشريع المقارن والشريعة الإسلامية، دار الفكر الجامعي، الإسكندرية، 2008 , ص267.

[3]–voir:-

Frédéric duflot, les infection informatiques bénéfiques chroniques d'un anathema,(DESS), paris,2003-2004, p28

Xavier LEMARTELEUR, Le scan de ports : une intrusion dans un STAD ?, p3, disponible en ligne a l'adresse suivante:
http://www.juriscom.net/documents/priv20080613.pdf.,

Murielle Cahen, intrusion dans un systeme informatique, disponible en lingne á l'adresse suivante: http://www.murielle-cahen.com/p_references.asp, voir aussi; du même auteur " Actualités Intrusion dans un système de traitement automatique de données (STAD) : Les réponses du droit", disponible en ligne a l'adresse suivante:
http://www.legipme.com/actualite/droit-ntic/intrusion-dans-systeme-traitement-automatique-donnees-stad-reponses-droit.html

من أنصار هذا الرأي في الفقه العربي: **د. نائلة عادل محمد فريد قورة**، المرجع السابق، ص357، **نهلا عبد القادر المومني**، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2008، ص160، د. **علي عبد القادر القهوجي**، المرجع السابق،ص123، **د. عبد الفتاح بيومي حجازي**، جرائم الكمبيوتر والانترنت في القانون العربي النموذجي_دراسة متعمقة في القانون المعلوماتي_الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2006، ص351، **د. محمود عبد الله حسين علي**، المرجع السابق، ص303، **محمد خليفة**، المرجع السابق، ص138،**آمال قارة**، الحماية الجزائية للمعلوماتية في التشريع الجزائري، الطبعة الأولى، دار هومه للطباعة والنشر والتوزيع ، الجزائر، 2006، ص106.

للحماية الجزائية بالنسبة للأنظمة المفتوحة على الجمهور. وهوالرأي الذي استقرّ عليه القضاء الفرنسي وأكّده في عدة أحكام له[1].

ومع ذلك، فإن الحماية الجزائية أيا كانت قيمتها الرادعة لا يمكن أن تحل محل الجهود الواجب بذلها من قبل الملاك والمستغلين لكي يؤمنوا لأنفسهم حماية لأنظمتهم، ولايجب أن يعتمد هؤلاء على الحماية الجزائية وتحميل الدولة المهمة الكاملة لحماية النظام الإجتماعي في هذا المجال، فإن تم ذلك يمكن حينئذ النظر إليها باعتبارها **ظرفاً مشدداً**، أو على الأقل لإثبات الركن المعنوي.

ت- شبكـــــات الــربط

تمثل الاتصالات الجناح الثاني للتقنية العالية، وهي في وجودها أقدم من الحوسبة، يمتد خط نمائها من التلغراف فالهاتف فالتلكس الفاكس...وإن كانت هذه الأجهزة التقنية تستخدم للتواصل تتميز بسرعة الاتصال وفوريته وهي تستخدم عادة في التعاملات، إلا أن **مصطلح التعاملات الإلكترونية** لم يظهر إلا مؤخرا خاصة بعد الربط الذي حصل بين وسائل الحوسبة والاتصال لينقل الحوسبة من النظم المغلقة إلى المفتوحة. مرت هده الوسائل ضمن مسيرة تطور هائلة انتقلت فيها من الاعتماد على الربط السلكي على الربط اللاسلكي، وتطورت إلى إعتماد تقنيات الإئتمار عن بعد وإستغلال الأقمار الصناعية. وفي حقل التقارب مع الحوسبة كان أهم فتح في حقل الاتصالات الانتقال إلى النقل الرقمي للمعلومات بتحويل النصوص والصور التناظرية إلى وحدات رقمية محمولة عبر وسائل الاتصال. وفي هذا الحقل تحققت فتوحات متتالية فكانت ولادة الفاكسملي ومن ثم الربط بين الحواسيب وبناء شبكات المعلومات[2].

يتصور الكثيرون أن شبكات المعلومات تقف عند الأنترنت، لكن هذا يتنافى مع الواقع فثمة شبكات خاصة(انترانت) لمؤسسات الأعمال تربط قطاعاتها وفروعها معا، وثمة شبكات متطورة تربط قطاعات

---

[1]–من ذلك حكم محكمة استئناف باريس في 5 أبريل لعام 1994 حيث جاء في حيثياته أنه"من غير الضروري لقيام جريمة الدخول غير المصرح به أن يكون فعل الدخول قد تم بمخالفة للتدابير الأمنية وأنه يكفي أن يكون هذا الدخول قد تم ضد إرادة المسؤول عن النظام".

" Dans une décision du 5 avril 1994, la Cour d'appel de Paris a précisé que « pour être punissable, cet accès ou ce maintien doit être fait sans droit et en pleine connaissance de cause, étant précisé à cet égard **qu'il n'est pas nécessaire pour que l'infraction existe que l'accès soit limité par un dispositif de protection...«.** La Cour a encore précisé qu'il suffit, pour que l'accès ou le maintien soit «punissable« **que «le maître du système(**(au sens de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel signée à Strasbourg le 28 janvier 1981...) **ait manifesté l'intention d'en restreindre l'accès aux seules personnes autorisées** ,C.A de paris, 5 avril 1994, disponible en lingne á l'adresse suivante:http:\Documents and Settings\user\Desktop\Les atteintes aux systèmes informatisés de données e-juristes_org.mht.

كذلك حكم محكمة إستئناف تولوس في 21 جانفي1999 الذي جاء فيه أنالدخول إلى نظام المعالجة الآلية يندرج تحت القانون الجزائي عندما يكون القيام به من قبل شخص ليس له الحق في الوصول إليه، على أن جهاز السلامة ليس ضروري ، فجاء نصـــه كمـــا يلـــــــي:

"l'accès à un système informatisé de données tombe sous le coup de la loi pénale dès lors qu'il est le fait d'une personne qui n'a pas le droit d'y accéder ; ***la présence d'un dispositif de sécurité n'est pas nécessaire" ;*** C.A de Toulouse, 21 janvier 1999, disponible en lingne á l'adresse suivante: http://www.alain-bensoussan.com/pages/2903

[2]- **يونس عرب**، قانون الكمبيوتر، المرجع السابق، ص30.

ببعضها حول العالم وتوفر خطوط متسعة لتبادل المعطيات من خلال إستخدام شبكات الأنترانت الخاصة بها عبر الشبكة العالمية وحولها (الإكسترانت).

لم تولد شبكة الأنترنت التي نعرفها اليوم عملاقة مرة واحدة كما نراها اليوم، وإنما تدرجت في النمو والتطور فبدت صغيرة ومحدودة في بداية الستينات على شكل "اربانت" لتصبح اليوم شبكة الأنترنت. وقد إرتبط بنماءها وجود التعاملات الإلكترونية. فهي تعتبر أهم وسيلة للتعامل الإلكتروني الحديث على الإطلاق، برز مع ظهورها تنوع للأطراف التعاملات الإلكترونية خاصة الوسيط الفني والوسيط النظامي. بل أن **التشريعات المنظمة للتعاملات الإلكترونية لم تصدر إلا بعد ظهور الأنترنت.**

والانترنت[1] **لغة**[2]: كلمة ذات شقين الأول inter ومشتقة من مصطلح interconnectionويعني الاتصال أو الدخول أو الربط، والثاني net ومشتقة من مصطلح net workوتعني الشبكة، وبذلك فالانترنت هي: الشبكة البينية أو الدخول إلى شبكة الاتصال البينية.

أما إصطلاحا فلقد تعددت التعريفات التي سيقت لبيان مدلولها، وإختلفت بإختلاف زاوية النظر في وضع كل تعريف، فيعرفها البعض على أساس أنها نتاج التطور التكنولوجي الذي قام به علماء التكنولوجيا في هذا المجال، حيث يعد مصطلح حديث الظهور تماما ويرجع الفضل في ظهوره إلى العالمين bob khan و vint serf وهما عالمان أمريكيان إبتكرا القاعدة المعيارية المحددة للإتصال عبر الأنترنت tcp / ipأي بروتوكول الأنترنت الذي يتم الإتصال بشبكة الأنترنت بسهولة ويسر من خلاله, كما يضمن التحكم في الإرسال عبر الأنترنت فيحدد السرعة الملائمة لإرسال المعلومات إلى المتلقي، وكذا ضمان وصول المعلومات إلى متلقيها بصورة سليمة وصحيحة[3].

في حين عرفها البعض على أنها[4]"عبارة عن آلية إتصال مكونة من مفاتيح وأسلاك وأماكن تخزين للمعطيات ودواعم توصيل وروابط اتصال، تعمل في بوتقة واحدة بفضل بروتوكول الانترنت TCP/IP"وفي تعريف آخر بأنها[5] "شبكة معلومات تتكون من عدة شبكات للمعلومات، إذ يتم توصيل إثنين أو أكثر من الحواسيب مع بعضها البعض لتصبح في صورة شبكة للمعلومات التي تتضمنها هذه الحاسبات" أو أنها[6] " شبكة الشبكات، حيث تتكون من عدد كبير من شبكات الحاسوب المترابطة والمتناثرة في أنحاء العالم، ويحكم ترابط تلك الأجهزة وتحادثها بروتوكول موحد يسمى بروتوكول تراسل الانترنت".

---

[1] – الطريق السريع الرقمي، شبكة المعلومات الرقمية، طريق البيانات السريع، طريق المعلومات السريع أو فائق السرعة كلها مصطلحات إستخدمت للدلالة على الأنترنت.

[2] – **بطرس أنطوان**، حضارة الحاسوب والأنترنت، مجلة العربي، الكويت، 2000، ص147.

[3]– une breve histoire de l'internet , article disopnible : http://www.boite-aux-curiosites.com/une-breve-histoire-de-linternet/

[4]-د. **ايهاب السنباطي**، موسوعة الإطار القانوني للتجارة الإلكترونية، دار النهضة العربية، القاهرة، 2007، ص 78.

[5]– **د.محمد السيد عرفة**، التجارة الدولية الإلكترونية عبر الأنترنت، مفهومها والقواعد القانونية التي تحكمها ومدى حجية المخرجات في الإثبات، بحث مقدم إلى مؤتمر القانون و الكمبيوتر والأنترنت، الطبعة الثالثة، المجلد الأول، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة, 1-3 مايو 2000، ص289.

[6]–**د. عمر محمد أبو بكر بن يونس**، المرجع السابق، ص38.

والحقيقة أن جميع هذه التعاريف تعبر عن حقيقة الانترنت، التي يمكن تعريفها ببساطة بأنها **شبكة عالمية تربط عدد كبير من الأجهزة المتناثرة عبر العالم،عبر خطوط وتقنيات الاتصال عن بعد**[1]**، والتي تستخدم في تواصلها بروتوكول تراسل الانترنت**".

ولتحقيق الإتصال بشبكة الأنترنت وإستخدام كافة الخدمات التي توفرها، لا بد من توافر وسائل متعددة تختلف فيما بينها من حيث نطاق إمتدادها والحيز الجغرافي المسموح به لتلك الوسيلة، فهناك ما تستخدم في مدى جغرافي محدود كما يحدث في الربط بين الحواسيب في الشبكات الداخلية أو المحلية، وهناك ما تعمل في نطاق جغرافي أكبر إتساعا مثلما يحدث في ربط النظام الحاسوبي لدولة بأكملها بشبكة الأنترنت عن طريق الربط مع دولة اخرى.

فعن الإتصال الدولي بشبكة الأنترنت، فيتم عن طريق الألياف الضوئية أو عن طريق الأقمار الصناعية, **أما** إتصال الأفراد داخل الدولة الواحدة بشبكة الأنترنت فيتم عبر خطوط الهاتف الثابث[2]، أو بإستخدام خطوط ISDN, أو بإستخدام خطوط T1,T3 ذات السرعة العالية، أوبالإتصال اللاسلكي WI-FI.

قد يعتقد البعض أن شبكة الأنترنت تملكها دولة أو منظمة دولية تقوم بإدارتها، ولكن الواقع أن شبكة الأنترنت لا يملكها أحد، ومن حيث المبدأ لا توجد هيئة رسمية وحيدة حكومية أو غير حكومية للإشراف على الأنترنت، ذلك لأن البنية الأساسية تدار باشراف جهات غير حكومية، أخذت على عاتقها جعل الأنترنت مساحة حرة متاحة للجميع. وتتصدر هذه الهيئات جمعية الأنترنت ISOC (INTERNET SOCIETY)[3] , أما الجهات التي تقوم بإدارة البنية الأساسية للأنترنت فهي: الإتحاد الدولي للإتصالات ITUالذي يشرف على منظومات الإتصالات العالمية، ومنظمة الآيكان ICANN، وهي تشرف على أسماء المواقع وعناوينها(أسماء النطاقات)[4].

لقد غيرت الإنترنت وجه عالم التجارة والأعمال، وقد ساهمت شبكات الإنترنت(والإنترانت والإكسترانت) في تحقيق **الوجود الفعلي** للتعاملات الإلكترونية، ووفقا للدراسات الإحصائية والتقارير الرسمية وتقارير الجهات الخاصة، فان نموا كبيرا ومطردا قد تحقق في سوق خدمات الإنترنت والاتجاه

---

[1]– عرفت الفقرة و من المادة 2 من القانون الجزائري رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ومكافحتها الإتصالات الإلكترونية على أنها: أي تراسل أو إرسال أو إستقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة الكترونية".

[2]– يتم الربط بشبكة الأنترنت من خلال خطوط الهاتف من خلال توفر جزئين: المعدات الصلبة: وتتمثل في جهاز الحاسوب مزود بكارت فاكس (المودم) وخط هاتفي مستقل، وقد ظل الاتصال بشبكة الانترنت في وقت ليس بالبعيد محصورا بجهاز الكمبيوتر، إلا أن التقدم العلمي والتكنولوجي قد أظهر إلى الوجود أجهزة أخرى قادرة على الإيصال بشبكة الانترنت ويمكن عن طريقها إجراء التعاملات الإلكترونية عبر الانترنت، مثال الأدوات الذكية, والتلفون الفضائي وغيرها.**د. محمد أمين الرومي**، التعاقد الإلكتروني عبر الأنترنت، الطبعة الأولى، دار المطبوعات الجامعية، الإسكندرية،2004، ص45.

[3]– وهي مؤسسة أمريكية أنشأت سنة 1991، تهدف إلى تنسيق عمليات الإتصال والإرتباط فيما بين الشبكات. أنظر: **عبد الحسن الحسيني**،القاموس الموسوعي في المعلومات والإتصالات والمعلوماتية القانونية، الطبعة الأولى، مكتبة صادر، بيروت، 2004, ص454.

[4]– نفس المرجع، ص ص456-414.

نحو التعاملات الإلكترونية ، ففي الفترة من 98 وحتى 99 إزداد مستخدموا الشبكة العالمية بنسبة 55% ، وازدادت مواقع الخدمة بنسبة 128 % وازدادت نسبة عناوين المواقع المسجلة بنسبة 137 %[1].

الفرع الثـــاني

تلازم ظهور جرائم تقنية المعلومات بظهور نظام المعالجة الآلية

لقد تلازم ظهور نظام المعالجة الآلية بظهور جرائم تقنية المعلومات خاصة بعد إنتشار الانترنت، لذا أصبحت الحاجة ملحة لوجود تشريع يحمي هذه القاعدة البيانية الضخمة من الاعتداءات خاصة بعد عجز النصوص التقليدية عن توفير الحماية لـــها، وهو ما ستم ملاحظته بإيجاز شديد من خلال النقاط المتقدمة من هذا الفرع.

أولا– مفهوم جرائم تقنية المعلومات

لقد أضافت نظم المعالجة الآلية الكثير من الجوانب الإيجابية إلى حياتنا إلا أنها في المقابل جلبت معها طائفة جديدة من الجرائم أطلق عليها جرائم تقنية المعلومات، جعلتها تتميز بطابع خاص يميزها عن غيرها من الجرائم.

أ– تعريفـــــها

تعد تقنية المعلومات والمعبر عنها في الوقت الحاضر "**بنظم المعالجة الآلية**" المعبر الحقيقي عن مضمون هذه الجريمة والسلوك الذي ظهرت على إثره، وسبق أن رأينا أن نظم المعالجة الآلية مصطلح ظهر نتاج الدمج بين وسائل الحوسبة ووسائل الاتصال.

بناء على ما سبق قد يتبادر إلى الذهن للوهلة الأولى أن مسالة تعريفها متفق عليه من طرف من تناولها، لكن في الحقيقة فإن مسالة تحديد مفهومها من أكثر المشاكل التي ترتبط بهذه الظاهرة، والسبب في ذلك يعود إلى حداثة هذه الجرائم وجانبها التقني الذي لا يعلمه الكثير ممن تناولوها بالدراسة، كما أن قصور بعض التشريعات في تناولها لهذه الجريمة أدى إلى عدم وضع تعريف شافي ينهي الاختلافات بين الفقهاء[2].

---

[1] تقرير:

The industry standardApril 26, 1999 – http://www.thestandard.com

مشار اليه لدى: **يونس عرب**، التجارة الإلكترونية، مقال متاح على الموقع الإلكتروني التالـــــــــــي:

http://www.arablaw.org/Download/E-commerce_General.doc

[2] - أنظر في تعريف جرائم تقنية المعلومات لدى كل من : الفقيه الألماني تيدمان*tiedman*: د.**محمد علي العريان**، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر،الإسكندرية، 2004، ص44. الفقيه (*Richard totty*) و(*anothony hardcastle*): **د. محمد سامي الشوا**، المرجع السابق،ص6.**د. سامي علي حامد عياد**، الجريمة المعلوماتية وإجرام الانترنت، دار الفكر الجامعي، الإسكندرية،2007، ص40. **د. أيمن عبد الله فكري**،المرجع السابق،

ذلك هو الوضع في الكثير من الدول، أما في الجزائر فقد تبنى المشرع الجزائري تعريفا لجرائم تقنية المعلومات وذلك بموجب المادة 2 من الفصل الأول من القانون رقم 09-04الصادر بتاريخ 5 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها تحت عنوان "**مصطلحات**" بأنّها: "*جرائم المساس بأنظمة المعالجة الآليّة للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية*".

ونحن نتفق بدورنا مع هذا التعريف، كونه شمل الاعتداءات الواقعة على النظام بما تنصرف دلالته بالاستناد إلى المادة 2-ب من القانون رقم 09-04 إلى المعلومات والنّظام الذي يحتوي عليها بما في ذلك شبكة المعلومات. فضلا عن الجرائم التي من الممكن أن ترتكب أو يسهل إرتكابها بواسطة نظم الحوسبة مثل الكمبيوتر أو نظم الإتصالات الإلكترونية، والإتصال بالشبكات قد يتم عن طريق الكمبيوتر أو عن طريق أجهزة المحمول النقالة أو أي جهاز يتيح الإتصال.

وأهمية هذا التعريف تبرز **من ناحيتين:** الأولـــى أن وضع معنى محدد لمصطلح يترتب على إستخدامه آثار قانونية ترتبط بمعاملات وحقوق الأفراد، وثانيا أن هذا التعريف يزيل اللبس الذي قد يحدث لدى القارىء للنصوص في فروع قانونية مستحدثة ليس لها مصادر أخرى يمكن الرجوع إليها طلبا للتفسير.

وهذا مسلك جيد لدى المشرع في قوانين المعلوماتية خاصة ما تعلق باستعمال وإساءة استعمال تقنية المعلومات.

وتجدر الإشارة، إلى أن جرائم تقنية المعلومات على النحو السابق بيانه، تقع أثناء عملية المعالجة الآلية للمعطيات وذلك في أي مرحلة من المراحل الأساسية لتشغيل نظام المعالجة الآلية سواء عند مرحلة إدخال المعطيات، أو أثناء مرحلة المعالجة، أو أثناء مرحلة إخراج المعلومات[1].

ص87. د. **شمس الدين إبراهيم أحمد**، وسائل مواجهة الاعتداءات على الحياة الشخصية في مجال تقنية المعلومات في القانون السوداني والمصري_دراسة مقارنة_ الطبعة الأولى، دار النهضة العربية، القاهرة، 2005، ص102.

*david Thomson*في مؤلفـــــه:

david Thompson,current trends in cimputer crime, computer control quarterly, vol. 9,nº 1,1991,p2.

لدى:**منير محمد الجنبيهي**, **ممدوح محمد الجنبيهي**، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2004، ص13.

محمد عبد الله المنشاوي، جرائم الانترنت من منظور شرعي وقانوني، مكة المكرمة ، 1423 هـــ ، بحث منشور على المـــوقع التالـــــي:
http//www.minshawi.com/ginternety.aagstract.htm

[1]- في مرحلة الإدخال حيث تترجم المعلومات إلى لغة مفهومة من قبل الآلة، فيسهل إدخال معلومات غير صحيحة، وفي مرحلة المعالجة الآلية للمعطيات فإنه يمكن إدخال اي تعديلات تحقق الهدف الإجرامي عن طريق التلاعب في البرنامج، أما في مرحلة المخرجات وفيها يتم التلاعب في النتائج التي يخرجها النظام بشأن معطيات غير صحيحة أدخلت فيها معالجة غير صحيحة، **د. نائلة عادل محمد فريد**، المرجع السابق، ص104, **د. خالد ممدوح ابراهيم**، التقاضي الإلكتروني، المرجع السابق، ص 329.

ب- خصائصها

لا شك أن جرائم تقنية المعلومات المرتكبة في العالم الافتراضي لها من الخصائص ما يميزها عن غيرها من الجرائم المرتكبة في العالم المادي الفيزيائي، ولاشك أن هذه الصفات تلحق الجرائم الواقعة على التعاملات الإلكترونية بحكم البيئة التي تتم فيها.

1- جرائم ترتكب عبر تقنية المعلومات أو عليها

إن اتساع حجم تقنية المعلومات وخاصة شبكة الانترنت وسهولة الدخول إليها، والتزايد المستمر في إستخدام هذه التقنية، جعل منها مسرحا لكثير من الأفعال الإجرامية، حيث أصبحت محل العديد من الاعتداءات التي تناولت أنظمتها سواء حوسبة أو إتصال ومعلوماتها، كما أن غالبية الجرائم التقليدية أصبحت ترتكب عبرها.

2- جرائم لا تعرف الحدود الجغرافية

لا تعرف جريمة تقنية المعلومات الحدود الجغرافية، أي أنها من الممكن أن تكون جريمة ذات بعد دولي أو دولية أو داخلية.

جريمة **ذات بعد دولي** إذا اتفق المجتمع الدولي بمقتضى عهد أو مشارطة دولية أيا كانت، على كونها تشكل عدوانا على كل دولة، أو عندما ترتكب الجريمة داخل دولة معينة إلا أنها تمتد خارج إقليم تلك الدولة.

وقد تكون جريمة **دولية** عندما تتعلق بالقانون الدولي، أي عندما يكون أحد أطرافها شخصا دوليا، على نحو ما حدث في التجسس الذي قامت به الولايات المتحدة الأمريكية، عندما إنتهكت أنظمة أعدائها الحاسوبية، وذلك بواسطة أسلحة معلوماتية فتاكة أثناء القصف الجوي للحلف الأطلسي في كوسوفو[1].

ومما يثار في إطار الجريمة الدولية والجريمة ذات البعد الدولي موضوع تدويل ظاهرة الاختراق لكونها جرائم يمكن أن يتأثر بها المجتمع الدولي في عمومه.

وقد تكون جريمة **داخلية** عندما تقع كاملة في نطاق إقليم دولة معينة.

3- صعوبة إكتشاف وإثبات جرائم تقنية المعلومات

وفحوى هده الصعوبة تكمن في أنها جرائم لا تحتاج إلى أي عنف أو سفك الدماء، أو آثار إقتحام، وإنما هي أرقام ومعطيات تتغير أو تمحى تماما من السجلات المخزونة في ذاكرة الحاسبات الآلية[2]، فهي جريمة ترتكب عادة في الخفاء ولا يوجد لها أثر كتابي لما يجري خلال تنفيذها من عمليات حيث يتم نقل المعلومات بالنبضات الإلكترونية[3]وبسبب إمكانية حذف الآثار المعلوماتية المستخدمة في ارتكاب الجريمة خلال ثوان.

---

[1]- **د. عمر محمد أبوبكر بن يونس**، المرجع السابق، ص 195، **د. محمد طارق عبد الرؤوف الخن**،، جريمة الاحتيال عبر الانترنت، منشورات الحلبي الحقوقية،بيروت، 2011، ص 34.

[2]-**عبد العالي برزحو**، مدى امكانية تطبيق القانون الجنائي المغربي على جرائم المعلومات، مجلة الأبحاث والدراسات القانونية، العدد 4، نونبر-دجنبر، 2014، ص58.

[3]-**د. هشام محمد فريد رستم**، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الألات الحديثة، أسيوط، 1994, ص42.

كما أن الجاني من الممكن أن يستخدم إسما مستعارا، أو أن يرتكب جريمته من خلال إحدى مقاهي الانترنت[1].

4- الوسائل المعتمدة على قدرة النظام الحاسوبي هي أداة ارتكاب الجريمة

وفحوى هده الخاصية أن كافة جرائم تقنية المعلومات يكون الحاسوب هو الأداة المستخدمة في إرتكاب السلوك الإجرامي المكون لها. سواء كنا أمام جرائم تقنية بدون إستخدام وسائل الاتصال أو جريمة تقنية باستخدام وسائل الاتصال، وعند الحديث عن الحاسوب لا نقصره على شكله التقليدي فقد يكون ساعة يد أو ضمن الجوال الرقمي أو الحاسوب النقال أو التلفاز الرقمي...

5- مرتكب جرائم تقنية المعلومات ذو معرفة تقنية

حتى يستطيع مجرم تقنية المعلومات من إرتكاب جريمته باستخدام وسائل تقنية المعلومات سواء كانت حوسبة أو إتصال أو ضدهما، فإنه من اللازم أن يكون مرتكبها من ذوي الاختصاص في مجال تقنية المعلومات، أو على الأقل شخص لديه حد أدني من المعرفة والقدرة على إستعمالها والتعامل معها.

ثانيا- دور نظام المعالجة الآلية في جرائم تقنية المعلومات

سبق وأن رأينا أن الجرائم الناشئة في بيئة تقنية المعلومات هي جرائم إرتبطت بجناحي التقنية، والمعنى أنها جرائم تقع أحيانا ضد التقنية ذاتها، وهي تلك الجرائم المستحدثة التي ما بزغت إلا بظهور وسائل الحوسبة والاتصال، وأحيانا أخرى تكون التقنية هي بيئة إتمام وتحقيق الهدف من الجريمة، وهي في أغلبها جرائم تقليدية لا تختلف عن الجرائم التي توالى حدوثها عبر التاريخ، ولكنها اليوم ترتكب في بيئة جديدة بوسائل حديثة.

أ- نظام المعالجة الآلية محل الاعتداء

ويندرج ضمنه الاعتداءات التي لا يمكن تصور حدوثها في العالم المادي الفيزيائي، ولا يجوز أن تتم إلا بوجود نظام المعالجة الآلية باعتباره شرطا في هذه الجرائم فهي جرائم تتم وجودا وعدما عبر النظام.

وقد إتجه المشرع الجزائي إلى حماية النظام كوسيلة فقط لحماية مكوناته غير المادية، ولذلك فإننا نلاحظ أنّ محل الحماية يتحول من شيء لامادي إلى شيء مادي، بمعنى أنّه بدلا من إصباغ الحماية على المكونات غير المادية في حد ذاتها فإننا نتّجه إلى حماية النظام الذي يسمح بمعالجة ونقل المكونات غير المادية.[2]

إن الجرائم التي تقع على المكونات غير المادية لنظام المعالجة الآلية لا تقع تحت حصر كما ونوعا، لأنه كلما زاد الاعتماد على تقنية المعلومات في جميع المجالات ستزداد أنواع الجرائم على النظام.والأمثلة على

[1]-د. **سليمان أحمد فضل**، المواجهة التشريعية والأمنية للجرائم الناشئة عن إستخدام شبكة المعلومات الدولية، دار النهضة العربية، القاهرة، 2013، ص21.

[2]-د. **أحمد حسام طه تمام**،المرجع السابق، ص6.

تلك الجرائم جريمة الدخول غير المصرح به إلى مواقع الشبكات ونظم المعالجة الآلية، وإغراق البريد الإلكتروني[1] بالرسائل غير المرغوبة لتعطيله عن العمل أو زراعة الفايروسات لتدمير المعطيات والملفات المخزنة أو تعديلها، الاستيلاء على المعطيات المخزنة أو المنقولة عبر النظم.

ب- نظام المعالجة الآلية وسيلة الاعتداء

ويندرج ضمنه الجرائم التي سبق النص على تجريمها في قوانين العقوبات وتحديد ماهيتها وأركانها المادية و المعنوية، ولكن الجديد فيها هو وسيلة إرتكابها حيث تعتمد على التقنية الحديثة مما زاد من حدتها و سهل إرتكابها وأظهر عليها تحويرات لتبدو وكأنها جرائم جديدة. فنظام المعالجة الآلية ليس هدف المجرم ولكنه يستخدمه كأداة لتحقيق نتيجته الإجرامية المبتغاة. والاعتداءات السابقة وفقا للتحديد السابق تتجلى بأشكال مختلفة، مثل إستغلال النظام للاستيلاء على الأموال بإجراء تحويلات غير مشروعة أو إستخدام التقنية في عمليات التزييف والتزوير، أو إستخدام التقنية في الاستيلاء على أرقام بطاقات ائتمان واعادة استخدامها والاستيلاء على الاموال بواسطة ذلك أو إتباع الوسائل الالكترونية للتأثير على عمل برمجيات التحكم في الطائرة أو السفينة بشكل يؤدي الى تدميرها وقتل ركابها[2]، أو إستخدام التقنية لارتكاب جريمة غسيل الأموال، الإرهاب الإلكتروني، الترويج والإتجار بالمخدرات عبر الأنترنت ...

بناء على ما سبق، نستنتج أن ثورة الإتصالات قد أفرزت جرائم متميزة من حيث المصالح التي طالتها, مبناها، طبيعتها، وسلوكياتها ومحلها، مما جعل النظم القانونية القائمة التي تتناول الجرائم التقليدية تقف عاجزة عن حماية هذه النظم ومعلوماتها من العديد من الاعتداءات.

ثالثا- الحماية الجزائية لنظام المعالجة الآلية من العمومية إلى الخصوصية

أثارت مسألة مدى إنطباق النصوص الجزائية العامة على الاعتداءات المنصبة على المعلومات المعالجة آليا دون المساس بالوسيط المادي الذي يحملها جدلا واسعا وصل إلى درجة التناقض في المحيط الفقهي، وخلافا واسعا وصل لدرجة التعارض في الوسط القضائي، وإن كان المقام لا يتسع هنا لذكرها،[3] فإننا نكتفي بالقول أن الدراسة التحليلية لمختلف الإتجاهات الفقهية والقضائية أظهرت قصور النصوص التقليدية، وأن محاولة تطويعها لكي تشمل المعلومات لم يسلم بالنقد، ومرد ذلك أن هده النصوص وضعت للتعامل مع سلوك ومحل مادي على خلاف الإعتداءات التي تنصب على المعلومات ذات الطبيعة المعنوية مهما كانت

---

[1]- عرف المشرع الجزائري البريد الإلكتروني بموجب المادة 2 من المرسوم التنفيذي رقم 98-257 الؤرخ في 25 أغشت 1998، المتعلق بضبط شروط وكيفيات إقامة خدمات "انترانت" و إستغلالها على أنه" خدمة تبادل رسائل إلكترونية بين المستعملين.

[2]- **يونس عرب**، جرائم الكمبيوتر والانترنت، المعنى و الخصائص والصور وإستراتجية المواجهة القانونية، بحث منشور على الموقع التالي:
Http://www. Arablaw. org.

[3]- أنظر تفصيلا في ذلك: **بوكر رشيدة**، جرائم الإعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، منشورات الحلبي الحقوقية، بيروت،2011، ص69 ومابعدها.

حالتها، كما أن مبدأ الشرعية بإعتباره حجر الزاوية في أي تشريع عقابي يمنع القاضي من تجريم وقائع أو تطبيق عقوبات لم يرد بها نص تشريعي، فضلا على أن القياس في النصوص الجزائية الموضوعية محظور، وهو الأمر الذي يستدعي إخضاع هذه الجرائم لنص قانوني يجرم التعدي عليها، أو تعديل القائم منها بما يستوعبها.

ونتيجة الوعي التشريعي لإدراك نقاط القصور في النصوص التقليدية التي أصبحت عاجزة عن مد نطاق تجريمها إلى حد شمول هذا النموذج المستحدث، إتجهت بعض الدول إلى تنظيم قانوني خاص بالإعتداء على نظم المعالجة الآلية بما تشمله من معلومات ضمن نطاق جرائم الأموال، كما هو حال المشرع الفرنسي، بإدماجها ضمن الكتاب الثالث الخاص بالجنايات والجنح ضد الأموال، إذ في القسم الثاني من هذا الكتاب _في الاعتداءات الأخرى على الأمواليعالج الباب الأول منه الإخفاء أو الجرائم الأخرى المشابهة أو القريبة منه، وخصص الباب الثاني للإتلاف والتخريب والتعييب, أما الباب الثالث فقد كرسه المشرّع للاعتداءات على أنظمة المعالجة الألية للمعطيات، وعلى نفس النهج سار المشرع الجزائري، ففي القسم السابع مكرر من الفصل الثالث المتعلق بالجنايات والجنح ضد الأموال *crimes et délits contres les biens* اتجه المشرّع الجزائي بالمادة 394 مكرر وما يليها إلى النص على أن تكون نظم المعالجة الآليّة وما تتضمنه من مكونات معنوية محلا للحماية بهذا القانون من صور الاعتداء المختلفة، ومن ثم تكون هذه النصوص الجديدة قد عاملتها معاملة **الأموال** بحمايتها لها على إعتبار أن لها قيمة اقتصادية، وذلك لورود الحماية المقررة لها ضمن الجرائم التي تقع على الأموال.

أما الوضع في بعض الدول العربية، كما هو حال مصر فقد أقر المشرع المصري حماية خاصة لنوع معين من المعلومات ونظم معالجتها، ومن قبيل ذلك ما نصت عليه الفقرة **ه من المادة 23 من قانون التوقيع الإلكتروني**"**توصل باية وسيلة إلى الحصول بغير حق على توقيع او وسيط او محرر الكتروني او إخترق هدا الوسيط او اعترضه او عطله عن اداء وظيفته**"و يترتب على ذلك أنه لا يجوز أن يقاس عليها أي معلومات أخرى تختزنها نظم المعالجة الآلية أيا كان نوعها، ولذلك فهذا النص قاصرا في نطاق الحماية ولا يشمل جميع أنـــواع المعلومات رغم أهمـــيتها.

المطلب الثاني

الحماية الجزائية لنظام مواقع التعاملات الإلكترونية

تعد مواقع التعاملات الإلكترونية كما رأينا أساس تلك التعاملات، فلو أخذنا العقد الإلكتروني[1] كصورة أساسية لهذا النوع من التعاملات[2]، فإن مبدأ السرية هو الذي يحكم عادة العقود العادية كافة كونها تبرم في مجلس واحد، إلا أن ذلك المبدأ يصعب توافره فيما يتعلق بالعقد الإلكتروني كون هذا الأخير يبرم بين طرفين لا يجمعهما مجلس عقد واحد، بل موقع الكتروني أو أكثر من موقع يسمح بالتفاعل، والحوار المفتوح الشامل بين أطراف العقد[3]عبر فضاء مفتوح ومن خلال شبكة دولية متاح للجميع الدخول اليها، مما يثير مخاوف أطراف التعـــامل حول أمـــن هذا التعـــامل.

ولذلك كان من الطبيعي أن يحتاج هذا النظام إلى حماية جزائية في حد ذاته، وهو ما أدركته الكثير من التشريعات المقارنة، فلم يعد في التشريع الجزائري والفرنسي على سبيل المثال محل للجدل حول ما إذا كان الدخول بغش إلى نظام الغير مشكلا جريمة أم لا، ولكن الأمر على خلاف ذلك بالنسبة للتشريعات التي لم تأخذ حظها في تقنين هذا النوع من السلـــوكات.

ويتخذ الاعتداء على نظام مواقع التعاملات الإلكترونية أكثر من شـــكل، ولعـــل أهمها الدخول أو البقاء غير المصرح بهما(الفرع الأول)، والتعدي على سلامة المواقع(الفرع الثاني) .

الفـــرع الأول

تجريم الدخول أو البقاء غير المصرح بهما

في نظم مواقع التعاملات الإلكترونية، يرغب كل متعامل إلكتروني مع النظام في ضمان أمن أن المعلومات المقدمة عبر النظام ليست متاحة إلا لهؤلاء الأفراد المحتاجين إليها، لإتمام الصفقة أو الخدمة أو

---

[1]-**العقد الإلكتروني** عبارة عن إتفاق يتم فيه تلاقي إرادتين أو أكثر عبر شبكة دولية للإتصالات عن بعد تحقق التفاعل الآني بين الموجب والقابل، وذلك بقصد إحداث اثر قانوني يتمثل في إنشاء إلتزام أو نقله أو تعديله أو إنهائه": د. **تامر محمد سليمان الدمياطي**، إثبات التعاقد الإلكتروني عبر الأنترنت، دراسة مقارنة، دار الكتب المصرية، 2009، ص39.

[2]-حسمت بعض التعريفات في شمول تعريف التعاملات الإلكترونية للعقد الإلكتروني كصورة أساسية لها. مثاله مشرع القانون الإتحادي الإماراتي بموجب المادة 1 حينما أشار أن التعاملات الإلكترونية هي"... أي تعامل أو **عقد**..."، كذلك فعل المشرع السعودي حينما نص "... تبادل أو تراسل أو **تعاقد**.." وان كان دلك كذلك، فإن البعض من الفقهذهب أوسع من ذلك حينما إعتبر أن التعامل أو الاتفاق أو العقد ما هو الا تكرار لمضمون العقد كما حدده القانون، لكن لا يشترط أن يكون ذلك العقد مكتوبا، وإنما يكفي أن تكون وسيلته هي المراسلة الإلكترونية أو الإنترنت كوسيلة لهذا التعامل أو التعاقد أو الاتفاق. أنظر: **د. عبد الفتاح بيومي حجازي**، التجارة عبر الأنترنت، المرجع السابق، ص148

بل نجد جانبا من الفقه قصر التعاملات الإلكترونية في صورة العقد الإلكتروني دون الإتفاق أو المعاملة، وعرفه على أنه العقد الذي يتم ابرامه عبرشبكة الأنترنت:**د. محمد حسين منصور**، المرجع السابق، ص 16.

[3]–**صالح المنزلاوي**، القانون الواجب التطبيق على عقود التجارة الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2006، ص39.

لمتابعة القضايا التي قد تنشأ، غير أن المعلومات المقدمة من خلال نظم هذه المواقع عرضة للدخول عليها بشكل غير مصرح به.

تعد جريمة الدخول غير المشروع للمواقع والأنظمة من أكثر الجرائم تأثيرا على السرية، مرتبطة بتكنولوجيا المعلومات في مجال عالم الجريمة، بالرغم من أن هذا النشاط يعد البوابة الرئيسية لارتكاب بقية الجرائم الأخرى الواقعة في فضاء التعامل الإلكتروني، إلا أن فاعله قد يكتفي بمجرد الدخول دون نية إرتكاب جريمة أخرى، وإن كانت الحالة الأخيرة قد أثارت خلافا فقهيا[1] كبيرا بشأن تجريمها. فإننا نرى أهمية وخطورة هذا التجريم، وتنبع أهميتة من كونه يشكل الإطار القانوني الرادع لسلوك يعد أساس بقية جرائم تقنية المعلومات، وهو من قبيل تشديد الحماية للنظام من الجرائم التي قد تقع عليه. أما خطورة هذا التجريم فتكمن في غيابه، حيث أن ترك المعتدين دون عقاب سيؤدي الى التمادي في الإعتداء على النظام حتى ولو كان الهدف من هذا الفعل هو مجرد إثبات الذات والقدرة على إختـــراق الحـــواجز الإلكترونية.

ونظرا لأهمية تجريم الدخول غير المصرح به، فقد أولـــت لها التشريعات إهتماما كبيـــرا على جميع الصعد، فعلى المستوى الدولي والإقليمي نجد إتفاقية بودابست التي نصت عليها في المادة 2[2]، كما نجد الإتفاقية العربية لمكافحة جرائم تقنية المعلومات والتي نصت عليها بدورها في المادة 6.

أما على المستوى الوطني، فقد أولت مختلف التشريعات الأروبية والعربية إهتمامها بمسالة حماية مواقع التعاملات الإلكترونية من الدخول غير المصرح أبرزها المشرع الفرنسي بموجب المادة 323-1 من قانون العقوبات [3]، والجزائري بموجب المادة 394 مكرر من قانون العقوبات.

---

[1]– كان الخـــلاف يدور في اتجـــاهين:

–**الأول رفض الحماية:** حيث يرى هذا الرأي أنه لا توجد ضرورة تستدعي تجريم مجرد الدخول أو البقاء غير المصرح بهما إلى نظام المعالجة الآلية, وخاصة إذا لم يكن لدى الفاعل نية لارتكاب جريمة لاحقة على هذا الدخول او البقاء, ويبرر هذا الاتجاه رأيه أن هذا السلوك لا يخرج عن كونه طريقة لعرض القدرات التقنية والذهنية التي يتمتع بها الشخص الذي قام بهذا الفعل, وهذا الأمر لا يشكل بحد ذاته جريمة تستدعي معاقبة الفاعل, مشار إليه لدى: **نهلا عبد القادر المومني**, المرجع السابق, ص157.

– **الثاني طالب بها:** حيث يذهب هدا الاتجاه إلى ضرورة تجريم الدخول والبقاء غير المصرح بهما إلى نظام المعالجة الآلية حتى لو لم يكن ذلك بقصد ارتكاب جريمة لاحقة فيما بعد, ويعزز هذا الاتجاه رأيه بالإشارة إلى أن هناك خسائر مادية قد تترتب على حالات الدخول غير المصرح به إلى نظام المعالجة الآلية, وقد تكون هذه الخسائر نتيجة مجرد محاولة وقف هذا الدخول, ويمكن الإشارة في هذا الصدد إلى الخسارة التي تحملتها إحدى المعامل الخاصة بتصنيع الأسلحة النووية في كاليفورنيا في الولايات المتحدة الأمريكية التي قدرت بحوالي مائة ألف دولار أمريكي, وهي تكلفة الأبحاث التي أجريت لمحاولة وقف الدخول غير المصرح به الذي قام به أحد الأشخاص إلى نظام المعالجة الآلية الخاص بهذا المعمل, مشار إلى هذه الواقعة لدى: **د. نائلة عادل محمد فريد قورة**، المرجع السابق ، ص ص327– 328.

[2]- Article 2 dispose que "Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pourériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droità tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soitcommise en violation des mesures de sécurité, dans l'intention d'obtenir des donnéesinformatiques ou dans une autre intention délictueuse, ou soit en relation avec un systèmeinformatique connecté à un autre système informatique".

[3]-**Article 323-1du CPf** Modifié par LOI n°2015-912 du 24 juillet 2015 - **relative au renseignement** art. 4 dispose que " Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende. Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 150 000 € d'amende."

وجريمة الدخول غير المشروع كبقية الجرائم يتطلب لقيامها تحقق ركن مادي ويتمثل في فعل الدخول وركن معنوي يتمثل في القصد الجنائي.

أولا- الركـــن المـــادي

تتحقق الجريمة من ركن مادي لا بد من توافره وبدونه لا يتصور قيامها، وبإستقراء النصوص القانونية التي عالجت جريمة الدخول غير المصرح به فان الركن المادي فيها يتكون من سلوك إجرامي يتخذ صورة الدخول، ينصـــب على المعلومـــات ونظـــم معالجتها، كما تعالج التشريعات إلى جانبها فعل البقاء.

أ- الدخول غير المصرح به

مما لا شك فيه أن مجـــرد الدُّخُول إلى نظام المعالجة الآلية لا يشكل فعلاً غير مشروع، وإنمّا يستمدّ هذا الدُّخُول عدم مشروعيّته من كونه **قد تم بغش**، ويكون كذلك في حالة ما إذا كان ضد إرادة المسؤول عن النظام، وبعبارة أخرى **بدون تصريح منه**[1]، ومن تم فإن توافر الرضا ينفى عن السلوك عدم المشروعية.
لم تحدد التشريعات المقارنة المقصود بالدخول غير المصرح به إلى النظام، غير أن الفقه قد تصـــدى لهذه المهمة، ومهما تعددت التعاريف التي قيلت في ذلك إلا انها تدور حول مفهوم واحد هو "**التفاعل الناجح مع النظام**"[2] **ضد ارادة المسؤول عنه, او المسيطر عليه من يملك نتظيمه**".وعناصر التعريف مؤداها مايلـــي:
1- **أي تفاعلات ناجحة مع النظام**, مهما كان حجم هذا التفاعل، ذلك أن التطور المستمر الذي يطرأ على البيئة الرقمية من حيث إمكانية شمولها مظاهر رقمية جديدة يجعل من مسألة تضييق معنى الدخول باعداد نموذج ثابت لشكل التفاعل من أكبر المشاكل التي تعيق حماية النظام من الإختراق، ذلك أن مستخدم النظام يمكن أن يتفاعل معه بطرق لا تعد ولا تحصى. وقد عبرت عنه الإتفاقية العربية بعباره"...**كل اتصال** غير مشروع..." إلى جانب عبارة"...**الدخول**.."، وإذا كانت الشبكات لا تميز بين المشروعية وعدم المشروعية في الدُّخُول إليها فإن القانون يقوم بهذا التمييز فارضا الحماية المشروعة ضد كل محاولة من جانب اللامشروعية، وهو ما كرسه المشرع الجزائري بموجب المادة 394 مكرر من قانون العقوبات التي قررت العقاب على مجرد الدُّخُول إلى نظام المعالجة الآلية.

ووسائل الاتصال بالنظام عديدة، لكن ما يجمعها هو إفتراضها قدرا من المعرفة بتقنية المعلومات. وهو ما تنبهت له التشريعات المقارنة حيث لم تحصر الدخول بوسيلة بعينها بل جاءت شاملة لكل طرق الدخـــول[3].

---

[1] –**Alain-bensoussan**, Fraude informatique, La protéction d'un système informatique par un dispositif de sécurité n'est pas une condition d'application de la loi Godfrain, art. disponible en lingne á l'adresse suivantehttp://www.alain-bensoussan.com/pages/2903/

[2] -**أورين كير ترجمة:** د. عمر بن يونس ، نطاق الجريمة الافتراضية، تفسير الدخول والتصريح به في إطار تشريعات الإساءة إلى الحاسوب، بحث منشور في مجلة القانون، العدد 78، جامعة نيويورك،، نوفمبر 2003، سنة النشر 2004، ص124.

[3]-**Michel Véron**, droit pénal spécial ,6 éme édition, armand colin,paris, 1998, p258.

ويستوي أن يتم الدخول **مباشرة** عن طريق نظام المعالجة الآلية الذي يحتوي على المعلومات والنظام، أو كما سماه البعض الدخول بطريقة إيجابية أو فعالة، وهو ما يستلزم تشغيل النظام إبتداءا للدخول إليه بما يحتوي عليه من معلومات، أو بطريق غير مباشر أو كما سماه البعض[1]**الدُّخُول بطريقة سلبيـــــة** عندما يتم اعتراض عمليات الاتصال من أجل الدخول إلى المعلومات التي يقوم بنقلها وهو ما يعني ضرورة تشغيل النظام بواسطة شخص آخر غير الجاني، بل يقتصر دور هذا الأخير على إعتراضها للوصول إلى المعلومات التي تتضمنها عملية الاتصال. سواء كان ذلك من خلال الدخول إلى شبكة الاتصالات أوالمعلومات أو من خلال **التقاط الإشارات المنبعثة عن النقل الإلكتروني للمعلومات باستخدام وسائل فنية دون الحاجة إلى الدخول مباشرة داخل الشبكة**، ففي هذه الحالة لم يكن هنالك دخول تقني مباشر إلى النظام، وهو ما دفع البعض من الفقه[2] إلى التفرقة بينه وبين الدخول، ومن ثم إستبعاد تجريمه ضمن جريمة الدخول غير المصرح به، إلا أن الرأي الراجح في الفقه اليوم[3] يعتبر أن هناك **دخولا في المعنى القانوني**.

إن الموقف التشريعي لم يكن واحدا في جميع الدول بخصوص تجريم فعل الإعتراض، ففي حين ذهبت بعض التشريعات نحو إفراد نص خاص لتجريم الإعتراض غير المصرح به منفصل عن تجريم الدخول غير المصرح به، كما هو حال المشرع الأردني في المادة 5 من قانون جرائم أنظمة المعلومات[4], والمادة 3 من إتفاقية بودابست والمادة 7 من الاتفاقية العربية. ذهبت بعض التشريعات إلى عدم تخصيص نص قانوني لفعل الإعتراض غير المشروع، إلا أنها في المقابل أعطت مفهوما موسعا للدخول، مما يسمح شموله للإعتراض غير المشروع والإلتقاط غير المشروع للمعلومات أثناء انتقالها باعتبار أنها في النهاية تمثل انتهاكا لإتصال معلوماتي بين النظم المختلفة أثناء عملها، كما هو حال المشرع الفرنسي والذي سار على نهجه المشرع الجزائري.

فبالرجوع للمادة 321–1 عقوبات فرنسي نجدها تجرم فعل الدُّخُول والبقاء بغش داخل نظام المعالجة الآلية بالمفهوم الواسع للكلمة، فهذه المادّة تجرّم الدُّخُول إلى النظام بكامله أو إلى جزء منه كشرط أساسي وجوهري لقيام الجريمة، أي أنّ الجريمة لا تقوم بالدُّخُول إلى أيّ عنصر يحتوي على معلومات متى كان بمعزل عن نظام للمعالجة الآلية للمعلومات، هذا وقد أجمع الفقه الفرنسي من واقع الأعمال التّحضيرية للقانون أنّ نظام المعالجة الآلية في تطبيق المادة 321–1 ينصرف إلى المعلومات والنّظام الذي يحتوي عليها، وكذلك إلى شبكات المعلومات، حيث أحالت المناقشات السّابقة على تبنّي القانون في تعريف نظام المعالجة الآلية للمعلومات إلى التّعريف الوارد لها في القانون الصادر عام 1978، والخاص بالمعلوماتيّة وحماية الحريات، ويشمل تعريف نظام المعالجة الآلية وفق هذا القانون جميع العمليات التي تتمّ آليا، والتي

---

[1] – **Philippe Andrieu**, stad; Accès et maintien frauduleux, disponible en lingne á l'adresse suivante: http://encyclo.erid.net/document.php?id=203 . Frédéric duflot, op. cit, p28.

[2]–**د. شيماء عبد الغني**، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، الإسكندرية،2007، ص104, **فايز محمد راجح غلاب**، الجرائم المعلوماتية فيالقانون الجزائري واليمني، رسالة دكتوراه، كلية الحقوق، جامعة الجزائر 1، 2009، ص195.

[3]–.**Frédéric duflot**, op.cit , p 28.

د. أيمن عبد الله فكري، المرجع السابق، ص 294.

[4]– نصت المادة 5 من قانون جرائم أنظمة المعلومات "كل من قام قصدا بإلتقاط أو بإعتراض أو بالتنصت على ماهو مرسل عن طريق الشبكة المعلوماتية أو اي نظام معلومات يعاقب ...."

تتعلّق بالتّجميع والتّسجيل والإعداد والتّعديل والاسترجاع والاحتفاظ ومحو المعلومات، ومجموعة العمليّات الّتي تتّم آليّا بغرض استغلال المعلومات وخصوصاً عمليّات الرّبط والتّقريب وانتقال المعلومات ودمجها مع بيانات أخرى أو تحليلها للحصول على معلومات ذات دلالة خاصة"[1]ويؤدّي التّوسع في مفهوم نظام المعالجة الآلية وفق القانون الفرنسي إلى نتيجة مؤدّاها أنّ التقاط الإشارات الناجمة عن تبادل المعلومات عبر شبكات المعلومات يعدّ دخولاً لنظام المعالجة الآلية الّذي يحتوي على هذه المعلومات[2].

كذلك الأمر بالنسبة للمشرع الجزائري، فالمتأملّ في الاتجاه التشريعي المعتنق من قبله يلحظ جنوحاً تشريعيًا باتّجاه التّشدد في حماية نظام المعالجة الآلية، لاحَ ذلك في المصطلحات المرنة المعتمدة، ومن مظاهر ذلك التّوسع بالركن المادي للدّخول والبقاء بغش أو غير المصرح به في نظم المعالجة الآلية والّذي يبدو واضحاً من خلال المادة 394 مكرّر من قانون العقوبات الجزائري، حيثُ تُجرّم هذه المادّة فعل الدُّخُول أو البقاء عن طريق الغشّ في كلّ أو جزء من نظام المعالجة الآلية بالمعنى الواسع للكلمة، ويقصد بنظام المعالجة الآلية وفقَ التّعريف الوارد في الفقرة ب من المادّة الثّانية من القانون رقم 09-04 بشأن الوقاية من الجرائم المتّصلة بتكنولوجيات الإعلام والاتّصال ومكافحتها بأنّه:" *أيّ نظام منفصل أو مجموعة من الأنظمة* ***المتّصلة*** *ببعضها البعض أو المرتبطة يقوم واحد منهَا أو أكثر بمعالجة آلية للمعطيات تنفيذاً لبرنامج معين*", وقد سبق وأن رأينا أنه يتكون من مكونات مادية وغير مادية وله القدرة على القيام بوظائف الإدخال والمعالجة والتخزين وإخراج المعلومات، فضلا عن شبكة المعلومات التي تربط نظم المعالجة الآلية ببعض سواء كانت تلك **الاتصالات بطريقة سلكية أو لاسلكية.**

ووفقا لهذا التعريف الموسع فإن المحل الذي ينصب عليه سلوك الجاني في جريمة الدخول أو البقاء غير المشروع يتسع لاستيعاب المعلومات في نظام المعالجة الآلية خلال مرحلة المعالجة والتّخزين والاسترجاع, النظام الذي يتضمنها فضلاً عن الشّبكات ذاتها أو المعلومات المنقولة عبرها، وبالتّالي يشمل تجريم اعتراض عملية نقل المعلومات سواء من خلال الدخول إلى شبكة الاتصالات أو من خلال التقاط الإشارات التي يحدثها جهاز إلكتروني من خلال وسائل التقاط إلكترونية، ويترتب على ذلك أن تصبح هذه الإشارات محلا ينصب عليه سلوك الجاني في جريمة الدخول عن طريق الغش أو غير المصرح به إلى نظم المعالجة الآلية.

---

[1]–وهو ما ذهبت إليه المادة الخامسة من القانون الفرنسي رقم 78-17 في 16 جانفي 1978 المتعلق بالحريات والمعلوماتية المعدل بموجب القانون رقم (2004_801) المؤرخ بتاريخ 6 أوت 2004 كما يلي:

"... Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction...".

[2] –***Rapp. de Jacques thyraud****, j.o.r.f., doc. sénat, 1987-88 1 er section, nº3.,p51.*

وفي نفس الاتجاه أشارت المذكرة التفسيرية لاتفاقية بودابست من أن " ***الاعتراض غير القانوني ربما يكون في بعض البلدان مرتبطا بدقة بجريمة الولوج غير المشروع للنظام المعلوماتي***"[1].

كما عني قانون ولاية Tennessee الأمريكية بتعريف الدخول بدون وجه حق بقوله أنه يعني "كل وسية للإطلاع أو لإعطاء تعليمات أو للإتصال أو لتخزين معطيات أو إستعادة معطيات أو إلتقاط معطيات من نظام كمبيوتر أو شبكة كمبيوتر[2].

بناء على ما سبق، نخلص أن كل من الاعتراض والالتقاط ما هما إلا نموذج من نماذج الدخول بغش، وإن كان ذلك كذلك، فإن فكرة الدخول تختلف عن إستعمال إمكانيات النظام، ومن تم فإن المشرع إذا جرم الدخول فإن ذلك لا يعني أن يقوم الفاعل بإستعمال الجهاز، ومع ذلك فإن كل إستعمال للنظام يشكل بلا ريب دخولا فيه، في حين أن الدخول فيه لا يعني بالضرورة إستعمال النظام[3]، لذلك حرص التشريع الكندي على عقاب كل من يستعمل أو يتسبب في إستعمال نظام الكمبيوتر[4].

2- **ضد إرادة المسؤول عن النظام أو مالكه:** ذلك أن توافر رضا صاحب النظام ينفي عدم المشروعية على الفعل، كأن يكون هناك إتفاق بينهما أو كان الجهازان ينتميان إلى شبكة واحدة وبالتالي فالجهازان يتصلان بالشبكة ذاتها مما يفيد توافر الرضا الضمني بدخول العاملين على الجهاز الخادم للشبكة إلى الأجهزة المنتمية إلى ذات الشبكة[5].كما لا يعد من قبيل الدخول غير المشروع أن يتم ذلك من جهة عاملة لها الحق في مراقبة النظام المتواجد لدى الأفراد مادام أن النظام يسمح لتلك الجهات بممارسة الحق في المراقبة.

ويسمي الفقه الفرنسي هذا الشخص بصاحب السلطة أو السيطرة على النظام، وقد عرفته المادة الثانية 2 من الاتفاقية الخاصة بحماية الأفراد في مواجهة نظم المعالجة الآلية للمعلومات ذات الطابع الشخصي، والتي تبناها المجلس الأوربي في 28 يناير 1989 على أنه"***كل شخص طبيعي أو معنوي, أو كل سلطة عامة أو كل مؤسسة أو جهاز يكون لهم سلطة التصرف في نظام الحاسب الآلي التابع لهم وتقرير مضمونه أو محتواه, وكيفية تنظيمه والهدف منه."***[6]

---

[1]- Dans certains pays, l'interception peut être étroitement liée à l'infraction d'accès nonautorisé à un système informatique.

[2]-texas penal code chapter 33 computer crimes 33,01 definitions:(1) "Access" means to approach, instruct, communicate with, store data in, retrieve or intercept data from, alter data or computer software in, or otherwise make use of any resource of a computer, computer network, computer program, or computer system.
http://www.statutes.legis.state.tx.us/Docs/PE/htm/PE.33.htm

[3]- **د. شيماء عبد الغني**، المرجع السابق، ص106.

[4]- Canadian Criminal Code-Computer Crimes, part ix (offences aginst rights of property)sec.342.1 **Unauthorized use of computer (a)** obtains, directly or indirectly, any **computer service**;
(c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or under section 430 in relation to computer data or a computer system; available at http://laws-lois.justice.gc.ca/eng/acts/C-46/section-342.1.html

[5]- **د. شيماء عبد الغني**، المرجع السابق، ص08.

[6]–Au sens de la législation sur les données personnelles, le « maître du système » est la personne ayant le pouvoir de décider de la mise en oeuvre d'un traitement informatique,
La Convention internationale pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel du 28 janvier 1981 donne la définition suivante du « maître du fichier » : « **la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui est compétent selon la loi nationale, pour décider quelle sera la finalité du fichier automatisé, quelles catégories de données à caractère personnel doivent être enregistrées et quelles opérations leur seront appliquées**. ».

وتكمن أهمية تحديد الشخص المسؤول على النظام في أن تعيينه يسمح بحصر نطاق الأشخاص الذين ينطبق عليهم وصف الدخول غير المصرح، على إعتبار أن المسؤول على النظام هو الذي يملك حق الدخول اليه، أو أن يحصل منه على تصريح بهذا الدخول.

وعادة تتحقق حالات عدم التصريح بالدخول إما بعدم وجود تصريح إطلاقا، كما لو كان الداخل إلى النظام ليس له علاقة به كونه ليس من العاملين لدى الجهة التي يتبعها النظام، وعادة ما يقوم المخترق بإختراق الموقع بالمرور بمرحلتين أساسيتين: **جمع المعلومات** كعنوان الأ بي التابع للسيرفر الذي يضم الموقع المستهدف، وجمع أسماء السكيرابتات المركبة في الموقع ليفحصها إذا كان فيها ثغرات برمجية، وهذه الثغرات تسمح للهاكرز بأن يفعل عدة أشياء ممنوعة[1].

الهجوم وهي مرحلة يتم فيها إستغلال الثغرات، والإستغلال يكون غالبا على شكل روابط، فيقوم الهاكرز بالدخول للوحة تحكم المدير، أو تطبيق أوامر على السيرفر أو رفع ملفات خبيثة كالشل[2].

وإما بتجاوز التصريح بالدخول، وقد عبرت عنها بعض التشريعات صراحة، مثل المشرع الأردني في المادة 3 "...دون تصريح أو بما يخالف أو **يجاوز التصريح**...." وهذا التجاوز يتحقق بأحـــد الأمرين:

- **بتجاوز المجال الذي حدده التصريح:** وتفترض هذه الحالة أن الشخص يملك تصريح بالدخول إلى جزء من النظام فقط، إلا أنه يدخل للجزء الممنوع الدخول اليه. والتجاوز المقصود هنا هو التجاوز في المكان، وقد عبر عنه المشرع الفرنسي في ظل المادة 323-1 عقوبات "...في كل أوجزء..."،وكذلك المشرع الجزائري في المادة 394 مكرر، كذلك هو الأمر بالنسبة للإتفاقية العربية *في* المادة 1/6 "...جزء من تقنية المعلومات.." ، ويفهم من عبارة جزء أن المشرع جرم الدخول الجزئي للنظام بطريق غير مصرح بـــه.
- **بتجاوز الغرض الممنوح من أجله التصريح:** في حين إكتفى المشرع الفرنسي بالتجريم المجرد للدخول عن طريق الغش معتبرا إياه جريمة في حد ذاته، وليس في ما يحصل بعد الدخول فيما إذا كان مصرحا به من التزام بالغرض الذي منح من أجله التصريح أو تجاوزه، وسار على نهجه المشرع الجزائري، فقد عبرت بعض التشريعات عن ذلك صراحة، كما هو حال المشرع الأردني في المادة 3/أ"...أوبما يخالف التصريح...".

وعلى العموم، فإن الدخول غير المصرح به وفق المعنى الذي سبق ذكره يقع من أي شخص وضد أي نظام دون إستثناء، وله طبيعة معنوية، هذه الطبيعة تشبه الدخول في ذاكرة الإنسان، ولتأكيد الاتفاقية العربية لهذه الطبيعة إستخدمت عبارة إتصال إلى جانب الدخول كون هذا الأخير قد يكون له مدلول مادي[3].

---

[1]–**د. سليمان أحمد فضل**، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، القاهرة،2013، ص214.

[2]-http://www.catb.org/esr/faqs/hacker-howto.html

[3]-المدلول المادي للدخول يتمثل في أن الشخص يكون قد حاول الدخول او دخل بالفعل إلى النظام المعلوماتي. **د.عبد الفتاح بيومي حجازي**، جرائم الكومبيوتر والأنترنت في القانون العربي النموذجي،المرجع السابق، ص355.

والأصل أن جريمة الدخول إلى النظام جريمة خطر في غالبية التشريعات المقارنة[1]، مادام أنه لم يلزم لوقوعها تحقق ضرر من نوع معين، فتقع وتكتمل بمجرد إنتهاء السلوك المكون لها وهو الدخول غير المصرح به حتى ولو لم يحصل الفاعل على معلومات، بل حتى لو لم يطلع على أية معلومة، ونستدل على ذلك كون أن التشريعات شددت عقوبة الدخول وضاعفتها إذا ما ترتب عليه ضرر، سواء حدث حذف أو تغيير لمعطيات المنظومة أو تخريب نظام إشتغال المنظومة(الفقرة الثانية والثالثة من المادة 394 مكرر عقوبات جزائري والفقرة الثانية من المادة 323-1 عقوبات فرنسي), أو محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير المعطيات والأنظمة وشبكات الاتصال (الفقرة 2 من المادة 6 من الاتفاقية العربية).

وفي إطار النتائج المترتبة على الدخول غير المصرح به، تثار مسألة هامة ألا وهي إفقاد صاحب الحق السيطرة على النظام الخاص به بسبب قيام المتهم **بتغيير كلمة المرور**، وأمام صعوبة إعتبار هذا النشاط سرقة كون الأمر يتعلق بالإطلاع وليس بالإختلاس من جهة، وإستبعاد إعتبار هذا التغيير تزويرا كون كلمة المرور لا تعتبر محررا[2]، قامت العديد من التشريعات بإدخال نص خاص يحمي كلمة المرور، منها ما تضمنته المادة 18 (I)(b) and (A)(I)(5)(a)1030 § .18U.S.C) من قانون العقوبات الأمريكي الفدرالي التي جرمت تغيير المتهم لكلمة السر الخاصة بنظام الشركة بما يحول دون إستخدام العاملين بالشركة لهذا النظام[3]. كما عاقب المشرع الجزائري بموجب المادة 394 مكرر2 على مجرد حيازة معلومات متحصل عليها من الإعتداء على النظام، والتي يدخل ضمنها كلمة المرور.

ب-البقـــاء غير المصـــرح بـــه

عبر المشرع الفرنسي عن تجريم هذا الفعل صراحة في المادة 323-1 عقوبات "...**أو بقي**...."، كذلك فعل المشرع الجزائري في المادة 394 مكرر عقوبات والمادة 6 من الإتفاقية العربية"...أو البقاء..."

تثور مسالة البقاء غير المصرح به داخل نظام مواقع التعاملات الإلكترونية عندما يتواجد شخص داخل نظام معلومات غير مسموح له بالدخول اليه، وذلك عن طريق الصدفة أو الخطأ كما لوتم حيازة كود العبور نتيجة خطأ في التعامل مع الملفات، فإن هذا الواقع يستبعد الطابع المتعمد الذي يقتضيه القانون[4]، إلا أنه يقرر البقاء داخل النظام وعدم قطع الاتصال به[15]. والبقاء بهذا المعنى لا يختلف عن الدخول غير المصرح به، من

---

[1]– والعلة من وراء تجريم الدخول المجرد غير المشروع هو منع اقتحام النظام الآلي لمعالجة المعلومات بحد ذاته، ذلك أن النظام المعلوماتي يحوي معلومات وبيانات لها قيمة مادية ومعنوية لا تقل عن قيمة الوثائق والأموال والحقوق الآخرى المحمية بموجب التشريعات النافذة، د.**شيماء عبد الغني**, مكافحة جرائم المعلوماتية في المملكة العربية السعودية، مقال متاح على الموقع الإلكتروني التالي:
http://www.shaimaaatalla.com/vb/archive/index.php/t-3955.html

[2]– **د. شيماء عبد الغني**، المرجع السابق، ص116.

[3]- NEVADA CYBERCRIME TASK FORCE NETS HACKER , U.S. Department of Justice, presse release: https://www.justice.gov/archive/criminal/cybercrime/press-releases/2002/sanduskyPlea.htm

[4] –C.A de paris, 4 decembre 1992, disponible en lingne á l'adresse suivantel'http://www.murielle-cahen.com/p_references.asp

[5]- **Frédéric , jérôme pausier et emanual jez**. La criminalité sur l'internet , collection que sais- je ? 1ere édition ,paris p114. Les atteintes aux systèmes de traitement automatisé de données, Art. disponible disponible en lingne á l'adresse suivantehttp://www.celog.fr/silex/tome1/chap_1-1.htm

حيث كون الفعل في ظاهره غير مشروع مما يتعين معه التجريم. وعلى ذلك فإن الرّكن المادي لهذه الجريمة يتمثّل في نشاط إيجابي يتطلّب من الجاني القيام به هو قطع الاتّصال، وإمتناعه عن قطع الاتصال مع النظام يحقق السلوك الإجرامي المتطلّب لقيام الجريمة، ومن ثم فإن هذه الجريمة من جرائم النشاط الإيجابي الذي يتحقّق بالتّرك أو الامتناع[2].

هذا وقد طبّق القضاء الفرنسي نصّ البقاء غير المصرح به في الحكم الشهير لمحكمة إستئناف باريس في 5 أفريل 1994، وجاء في هذا الحكم أنّ القانون يجرّم البقاء غير المصرح به داخل نظام المعالجة الآليّة، سواءً كان الدُّخُول قد تمّ عن طريق الإهمال أو تمّ بطريقة مشروعة إلاّ أنّه إكتسب بعد ذلك صفة اللاّمشروعية كما لو فقد الفاعل حقّه في البقاء...[3].

وعلى العموم فإن البقاء داخل نظام المعالجة الآلية وفق المعنى الذي سبق ذكره، يجعله يتميز بذاتية خاصة مختلفة عن البقاء في البيئة الواقعيّة شأنه في ذلك شأن الدخول، فالدخول إلى العالم الافتراضي له طبيعة معنوية وليست مادية[4]،لكن ما يميزهما أن الدخول جريمة وقتية وهي تعني تخطي الحد سواء كان مجردا أو أدى إلى نتائج معينة، وعليه إذا لم ينص صراحة على البقاء فلا يمكن سحب أحكام جريمة الدخول اليه، في حين أن البقاء جريمة مستمرة، تجرم فعل الإستمرار في النشاط غير المشروع من وقت توافر العلم به والإرادة المتجهة الى تحقيقــه.

وبناء على ذلك، ذهب البعض من الفقه إلى إمكانية الجمع بين الدخول والبقاء، إذ أن جريمة الدخول جريمة وقتية تعقبها جريمة مستمرة هي البقاء، ويرى أصحاب هذا الرّأي أنّه ليس من العدالة أن يتساوى من دخل النظام ثمّ خرج مع من دخله ثمّ بقي فيه، أي بين من إرتكب جريمة واحدة ومن إرتكب جريمتين، وأنّ الأخذ بهذا الرأي يشجّع على العدول عن جريمة البقاء لمن ارتكب جريمة الدُّخُول[5]. ويعترض على ذلك بعضهم –ونؤيده– بالقول أن كل جريمة تقع مستقلة عن الجريمة الأخرى، ويستدل على ذلك بالقول أن المشرّع عندما يستخدم كلمتين أو مصطلحين مختلفين فلابدّ أن يكون لكلّ مصطلح معناه ومدلوله المختلف عن المصطلح الآخر، فمصطلح "**بقاء**" لا يحتوي مصطلح "**دخول**" والعكس كذلك صحيح. فكل فعل من الأفعال نطاقه ومجاله الذي لا يتداخل فيه مع الآخر، وجريمة الدخول وإن كانت جريمة وقتية فإنها ذات آثار

---

[1]-أنظر في تعريف البقاء لدى: **بلال أمين زيد الدين**، المرجع السابق، ص272،**د. أيمن عبد الله فكري**، المرجع السابق، ص238. **د. عمر محمد أبو بكر بن يونس**، المرجع السابق، ص332. **د. محمد حماد مرهج الهيتي**،جرائم الحاسوب ماهيتها, موضوعها, أهم صورها, والصعوبات التي تواجهها–دراسة تحليلية لواقع الاعتداءات التي يتعرض لها الحاسوب وموقف التشريعات الجنائية منها–, الطبعة الأولى، دار المناهج للنشر والتوزيع، عمان، 2006،ص190. **د. علي عبد القادر القهوجي**، المرجع السابق، ص133.

[2]–د. **أيمن عبد الله فكري**، المرجع السابق،ص238, د. **محمد حماد المرهج الهيتي**،المرجع السابق، ص191.

[3]– C.A de paris, 5 avril 1994, **NCP,**104e édition **,** D, paris, 2009, p916.

[4]- أنظر: **أورين كير**، المرجع السابق، ص67.

[5]-Raymons gassin. Fraude informatique, dalloz, 1995, p117.

مشار إليه لدى: **محمد خليفة**، المرجع السابق، ص158.

ممتدة مستمرة في الزمان، وعليه فإذا تحققت جريمة الدخول فلا تقع جريمة البقاء لأنها في تلك الحالة هي أثر من آثار الجريمة وليست فعلا إجراميا مستقلا، وإذا إنتفت جريمة الدخول فإن جريمة البقاء لا تنتفي.[1]

ويكفي لتحقق جريمة البقاء مجرد البقاء بذات المعاني السابقة لفعل البقاء، ولا يتطلب في نموذجها القانوني حسب نص التجريم تحقق نتيجة مادية معينة لها وجودها المحدد في العالم الخارجي، وهو الوضع في المادة 323–1 الفقرة 1 عقوبات فرنسي والمادة 394 مكرر عقوبات جزائري، ولكن هذا لا يمنع من تصور أن يترتب على إرتكابها حدوث نتيجة معينة منظورا اليها وفق مدلولها المادي، مثل حذف أو تغيير المعلومات التي يحتويها النظام، أو تخريب نظام إشتغال المنظومة، وهو ما دفع المشرع الفرنسي إلى تشديد العقاب بموجب الفقرة 2 من المادة 323–1 عقوبات. وكذلك فعل المشرع الجزائري بموجب الفقرة 3 من المادة 394 مكرر عقوبات.

ثانيا– الركـــن المعنـــوي

جريمة الدخول أو البقاء داخل مواقع التعاملات الإلكترونية جريمة عمدية[2]، يتخذ الركن المعنوي فيها صورة القصد الجرمي بعنصريه العلم والإرادة، وهذا ما نص عليه المشرع الفرنسي صراحة في المادة 323–1 عقوبات كما يلي" ***...عن طريق الغش...***",كما أشار إلى ذلك المشرع الجزائري في المادة 394 مكرر من قانون العقوبات.

وعلم الجاني يجب أن يشمل كافة الوقائع التي يتطلبها القانون لبناء أركان الجريمة وإستكمال عناصرها, فضلا عن التكييف الذي تتصف به بعض هذه الوقائع وتكتسب به أهميتها في نظر القانون[3].

ومن قبيل ذلك علمه بأنه ليس له الحق في الدخول والبقاء إلى النظام، فضلا عن علمه بخطورة فعله على المصلحة التي يحميها القانون. وأن فعله ينصب على نظام للمعالجة الآلية ، فإذا إنتفى العلم بالعناصر السابقة إنتفـــى تبعا لذلك القصد الجرمي. كما ينتفي في حالة ما إذا كان دخوله بطريق الخطأ أو الصدفة، إلا أنه يتحتم عليه الخروج من النظام بمجرد علمه أن دخوله غير مصرح به، فاذا لم يفعل ذلك توافر لديه القصد الجنائي منذ اللحظة التي تحقق فيها العلم. ويكون مرتكبا لجريمة البقاء. والى جانب العلم كعنصر في القصد الجنائي لا بد من توافر الإرادة، إلا أنه ونظرا لكون جريمة الدخول والبقاء من الجرائم الشكلية في

---

[1]– أنظر في الاتفاق حول ذات المضمون:**د. أحمد حسام طه تمام**، المرجع السابق، ص ص301–303. **محمد خليفة**، المرجع السابق، ص 44**د. أيمن عبد الله فكري**، المرجع السابق، ص206.

Voir aussi: **Frédéric duflot**, op, cit, p28.

[2]-تنقسم الجرائم تبعا للركن المعنوي للجريمة *selon l'élément moral de l'infraction* إلى جرائم مقصودة *infractionintentionnelles* و جرائم غير مقصودة *infraction nom intentionnelles* و للتمييز بينهما أنظر:

-**philppe conte**, **Patrick Maistre du Chambon**, droit pénal général, 7 eme édition, Armand Collin, paris,2004,p120

-**Gaston Stefani, georges Levasseur, Bernard bouloc**, droit pénal général, 16 emeédition, dalloz,paris, 1997, p231-232.

[3]– أنظر: **د.محمود نجيب حسني**، النظرية العامة للقصد الجنائي، دراسة تأصيلية مقارنة للركن المعنوي في الجرائم العمدية، دار النهضة العربية، القاهرة، 1988، ص51.

التشريعات الحديثة، فإن الإرادة تقتصر على السلوك الإجرامي فتستغرقه بكل مقوماته ولا تمتد إلى النتيجة. بغض النظر عن الباعث أو الغاية على ارتكاب الجريمة.

وإذا كان القانون يتطلب أن يكون الدخول قد تم بطريقة غير مشروعة، فيذهب البعض[1] هنا إلى أن معيار التمييز هو وجود نظام الحماية الفنية. لكن الاتجاه الغالب اليوم هو عدم إشتراط توفر الحماية الفنية لإثبات الركن المعنوي، وهو ما سار عليه كل من التشريع الجزائري والفرنسي[2].

وإن كان هاذين التشريعين إكتفيا بالقصد العام[3]، ذهبت بعض التشريعات إلى تقييد تجريم الدخول بقيد يتعلق بالركن المعنوي، فيستلزم توافر القصد الخاص لدى المتهم، كنية ارتكاب جريمة أخرى كالسرقة أو النصب إلا أن هذه الجريمة لم تتم، كما هو الوضع في قانون إساءة إستخدام الحاسبات الآلية للمملكة المتحدة لعام1990، أونية الحصول لحساب الفاعل أو لغيره ربح أو فائدة غير مشروعة، كما هو الحال في القانون البرتغالي للجرائم المعلوماتية 1991[4].

ثالثا- العقـــــوبــة

متى توافرت أركان الجريمة على النحو السابق، فإن المشرع الفرنسي يعاقب عليها بالحبس سنتين وبغرامة 60000 يورو، وتكون العقوبة بالحبس 3 سنوات وبغرامة 100000 يورو إذا ترتب علـــى نشاط الجاني حذف أو تعديل المعطيات الموجودة بالنظام الخاص بالتعاملات الإلكترونية، أو تعديل تشغيل النظام. وفي حالة ما إذا إرتكب الأفعال السابقة ضد نظام معالجة آلية للمعلومات دات الطابع الشخصي التي تقوم به الدولة فالعقوبة تصبح 5 سنوات حبس وغرامة 150000 يورو.

أما المشرع الجزائري فعاقب عليها بالحبس من 3 اشهر إلى سنة، وبغرامة من 50000 دج إلى 100000 دج، مع مضاعفة العقوبة في حالة ما إدا ترتب على ذلك حدف أو تغيير المعطيات، أما إدا ترتب على ذلك تخريب إشتغال المنظومة فتكون العقوبة الحبس من 6 أشهر إلى سنتين وبغرامة من 50000 إلى 150000 دج.

---

[1]-**د. أحمد حسام طه تمام**، المرجع السابق، ص292.

[2]–TRG de paris, 31 ch corr. 18 septembre 2008, disponible en lingne á l'adresse suivante:http://www.alain-bensoussan.com/pages/2903/

[3]– كان هنالك خلاف فقهي حول كلمة الغش التي استعملها المشرع الفرنسي فيما إذا كان المشرع قد إكتفى بها للدلالة على القصد العام أم استلزم إلى جانب ذلك توافر القصد الخاص، فذهب البعض الى اشتراط توافر القصد الخاص كون أن المشرع قد إستعمل لفظ غش وهو مصطلح يختلف عن عمد أوإرادي،وهو مفهوم مستعار من الغش في جريمة السرقة،وقد عرّفه الفقهاء كالتـــــّالي:

"Il ya accès ou maintien frauduleux, l'orsque l'agent a su qu'il agissait sans droit, qu'il n'était pas autorise ou encore qu'il agissait contre le gré du maître du système

ويدعمون رأيهم هذا بعبارة "بدون حق ومع معرفة السبب" التي جاءت في قرار محكمة باريس 5 أفريل 1994، وقد رد البعض الآخر–ونؤيده– على أن هذه العبارة تنصرف في مدلولها إلى كون أن الفعل يجب ألا يكون نتيجة خطأ بسيط، وإنما لا بد أن يكون إتيانه على علم بصفته غير المشروعة انظـــــر:

Vivant et autres, informatique et droit pénal, les biens informatiques; objets d'une fraude.Lamy informatique 1991. p1511.n°3443. ***Frédéricduflot**, op. cit,p29.*

[4]-**د. نائلة عادل فريد قورة**، المرجع السابق، ص363.

الفرع الثاني

تجريم التعــدي على سلامة نظام مواقع التعاملات الإلكترونية

يعد التعدي على سلامة نظام مواقع التعاملات الإلكترونية من الجرائم المنتشرة في فضاء شبكة الانترنت، وهو يؤدي إلى إربـــاك أو تباطؤ عمل نظام المعالجة الآلية، ومن ثم ينتج عن ذلك تغيير في حالة عمله[1] مهما كانت الجهة التي يخدمها ذلك النظام. وقد إستقرت غالبية التشريعات المقارنة على تجريم هذا السلوك ،حيث جرم المشرع الفرنسي في نص المادة 323-2 عقوبات:"... *"كل من قام* ***بإعاقة*** *أو* ***إفساد*** *نشاط نظام المعالجة الآلية يعاقب..."*[2]. كما تضمنت إتفاقية بودابست نص مشابها في المادة 5 منها كما يلي"...يجب على كل طرف أن يتبنى...**الإعاقة الخطيرة**,...".[3]، أما المشرع الجزائري فقد إستغنى عن وضع نصّ خاص لها، واكتفى بنتيجة إفساد النظام كظرف مشدّد لجريمة الدُّخُول أو البقاء غير المصرح بهما في الفقرة 3 من المادة 394 مكرر"...وإذا ترتب على الأفعال المذكورة أعلاه **تخريب** نظام إشتغال المنظومة تكون العقوبة..."، وإستبعدها كجريمة قائمة بذاتها، وربما يرجع سبب ذلك إلى التّشابه الكبير بينها وبين جريمة التّلاعب بالمعلومات، مما يحول دون التّمييز بينهما في الكثير من الأحيان، على إعتبار أنّ الأفعال التي تتضمّنها جريمة التلاعب تؤدّي هي الأخرى إلى إعاقة النظام وإفساده.

سنحاول فيما يلي تحليل هذه الجريمة من خلال ركنيها المادي والمعنوي على النحــو التالي:

أولا- الــركن المــادي

يقوم الركن المادي لهذه الجريمة على إعاقة وإفساد وظيفة النظام فيما أعد له، ويدخل في ذلك جميع الوظائف التي يقوم بها.

أ_ الإعــاقة :

---

[1]-**د. أحمد حسام طه تمام**، المرجع السابق، ص 351.

[2] – Article 323-2 du C.P.F dispose que :"Le fait **d'entraver** ou de **fausser** le fonctionnement d'un système de traitement automatisé de donné est puni…"

كما نصت عليها المادة الخامسة من اتفاقية بودابست تحت عنوان "الاعتداء على سلامة النظام" *Atteinte à l'intégrité du système* كما يلي"يجب على كل طرف أن يتبنى الإجراءات التشريعية و أية إجراءات أخرى يرى أنها ضرورية للتجريم, تبعا لقانونه المحلي, الإعاقة الخطيرة, إذا تم ذلك عمدا, ودون حق, لوظيفة نظام الحاسب, عن طريق إدخال, أو نقل, أو إضرار, أو محو, أو تعطيل, أو إتلاف, أو طمس البيانات المعلوماتية".

كما عاقب عليها المشرّع في القانون العربي النموذجيفي الفقرة الأولىمن المادة الثالثةوذلك ضمن جريمة إتلاف المعلومات كما يلي"..كل من أتلف نظام المعالجة الآلية أو جزء منه ..", كما جرمها باعتبارها ظرف مشدد في جريمة الدخول غير المشروع وذلك في المادة الثانية السابق الإشارة إليها شأنه في ذلك شأن المشرّع الجزائري

[3]- Article 5 du CPF dispose que"…, l'entrave grave, intentionnelle …"

ويقصد بالإعاقة منع النظام من العمل في كل أو جزء منه[1]، ويكون ذلك بفعل يتسبب في إرباكه عن أداءه لوظائفه المختلفة. مع إنصراف مدلول النظام إلى مكوناته المادية والمعنـــوية.

وتوضح المذكرة التفسيرية لاتفاقية بودابست من جهتها أن مصطلح الإعاقة يرتبط بالأفعال التي تحمل إعتداء على حسن تشغيل النظام، وهذه الإعاقة يجب أن تكون ناجمة عن الإدخال أو النقل أوالإضرار أوالمحو أو الإتلاف أو طمس المعلومات، وتعتبر الإعاقة جسيمة وفقا للاتفاقية عندما تكون المعلومات المرسلة من الحجم أو التواتر بما يحمل ضررا جسيما لقدرة المالك أو المشغل بالنسبة لاستخدام الجهاز أو الاتصال بالأجهزة الأخرى[2].

وقد تكون الإعاقة دائمة،[3] كما في حالة إدخال فيروس تدميري[4]أو قد تبطئ أو تنقص من قدرة النظام فقط على أداء عمله [5] ، وقد تكون الإعاقة مؤقتة أو متقطعة على فترات منتظمة كما إذا تم إدخال قنبلة معلوماتية زمنية مبرمجة ينجم عنها شل النظام عند البدء في تشغيله مثلا أو عند إستخـــدام أحـــد برامج التطـــبيق[6].

هذا ولم يشترط المشرع الفرنسي وسيلة معينة لحصول الإعاقة، وعليه يمكن أن تكون هذه الوسيلة مادية أو غير مادية، وتكون مادية إذا وقعت على العناصر المادية للنظام مثل كسرها، مع الإشارة إلى أن مسالة تجريم مثل هذا الفعل يعتبر تكميلا للأحكام المنصوص عليها في التشريعات الجزائية والمتعلقة بالتدمير أو التخريب للأموال المادية بإضافة حالة تتعلق بالإضرار الوظيفي لتشغيل الأشياء المادية.

وتكون معنوية إذا وقعت على المعلومات، وهي على درجة من الدقة نظرا للطبيعة الفنية للوسائل المستخدمة في إحداثها، مثل تعديل البرنامج في النظام أو إدخال معلومات جديدة أو محو أو تعديل المعلومات المختزنة، أو إرسال العديد من الرسائل الإلكترونية[7] مما يؤدي إلى شل النظام أو عمل برنامج احتيالي[8].

والإعاقة بهذا المعنى تقترب من جريمة التلاعب بالمعلومات، كون أن النشاط الجرمي في هذه الأخيرة يؤدي هو بدوره إلى إعاقة النظام. غير أنه لا يعد من قبيـــل الإعاقة قيام العاملين بالإضراب عن العمل، الأمر الذي يسبب توقف النظام عن العمل، مع الأخذ بالاعتبار أن التفسير الواسع للنصوص المتعلقة بالإعاقة يقتضي فصل إستعمال حق الإضراب عن الأعمال التي يقوم بها العامل بسوء نية وقصد متعمد والتي ينبغي من وراءها إعاقة العمل بالنظام كتحطيم أو كسر أو تدمير ماديات النظام أو تغيير المعلومات أو محوها أو

---

[1]–.FAUSSER OU ENTRAVER LE FONCTIONNEMENT D'UN STAD, disponible en lingne á l'adresse suivante http://www.weka.fr/administration-locale/base-documentaire/msi-intelligence-economique-wk330/securite-les-aspects-juridiques-sl7241030/fausser-ou-entraver-le-fonctionnement-d-un-stad-sl7269910.html

[2] -Rapport explicatif de la Convention sur la cybercriminalité. Série des traités européens - n° 185; Budapest, 23.XI.2001;. P13 S

[3]–**MAITRE ANTHONY BEM**, L'INTRUSION ET LES ATTEINTES AUX SYSTEMES INFORMATIQUES SANCTIONNEES PAR LE DROIT PENAL,disponible en ligne á l'adresse précédente.

On peut citer par exemple le blocage d'un code d'accès (CA Paris, 5 octobre 1994

[4]-être permanent lorsque le système est infesté d'un virus (CA Paris, 15 mars 1995).

[5]L'entrave peut aussi consister en un simple ralentissement ou en une diminution de la capacité de traitement (CA Paris, 5 avril 1994).

[6]–**د. علي عبد القادر القهوجي**، المرجع السابق، ص140.

[7] - TGI paris, 12 ch, 24 mai 2002, http://www.droit-technologie.org/upload/jurisprudence/doc/327-1.pdf

[8]-**د. محمد أمين الشوابكة** ،جرائم الحاسوب والأنترنت، الطبعة الأولى، دار الثقافة للنشروالتوزيع، عمان، 2004، ص 223.

تعديلها على نحو يؤدي إلى إعاقة النظام، فان أفعاله تندرج تحت وصف التجريم المنصوص عليه في اطار المواد السابقة[1].

ب-الإفســـاد:

وهو كل فعل يؤدي الى جعل النظام غير صالح للإستعمال السليم، وذلك بأن يعطي نتائج غير تلك التي كان من الواجب الحصول عليها[2]. ووسائل الإفساد متعددة منها إستخدام القنبلة المعلوماتية التي يدخل عن طريقها معلومات تتكاثر داخل النظام تجعله غير صالح للاستعمال، أو إستخدام فيروس حصان طراودة.

هذا ويميز الفقه بين مصطلحي الإعاقة والإفساد، ويرى أن لكـــل منهما معنى يكمل الآخر حيث يتناول النص من خلالهما جميع الوسائل المستخدمة للإعتداء على النظام، ففعـــل إعاقة النظام يشمل الأفعال الموجهة الى النظام بشكل مباشر بهدف منعه من أداء وظائفه وبحيث يترتب عليه تعطيل مؤقت عن اداء وظائفه، أما الإفساد فهو يشمل الحالات التي يترتب عليها تعطيل النظام عن أداء وظائفه بحيث يكون غير صالح للإستعمال[3].

والإفساد بهذا المعنى يكاد يقترب من التعييب الذي يعدّ ظرفاً مشددا حسب المادة 323-1 من قانون العقوبات الفرنسي[4]، فالتعييب غير العمدي في هذه الحالة إرتبط العقاب عليه بالدخول أو البقاء غير المصرح بهما.

وحتىّ يتحقّق هذا الظّرف لابد أن تتواجد علاقة سببية بين الدُّخُول أو البقاء وبين النّتيجة المشدّدة الّتي هي ذات الظّرف المشدّد في الجريمة، إلاّ إذا أثبت الجاني إنتفاء تلك العلاقة، كأن يثبت عدم صلاحية النّظام للقيام بوظائفه يرجع إلى القوّة القاهرة أو الحادث المفاجئ فينتفي تبعًا لذلك الظرف المشدد، ويعاقب الجاني بالعقوبة المقررّة له(أي على الدخول أو البقاء المجرد فحسب).

لكن الفارق بينهما يتمثل في إرادة النتيجة في جريمة الإفساد، وعدم إرادتها في جريمة الدخول أو البقاء المشددة. ذلك أن المشرع لم يستعمل كلمة غشّ وهو الأمر الّذي وجد معه البعض من الفقه أنّ تلك الجريمة تقع **بطريق الخطأ** في التشريع الفرنسي ولا يتطلّب المشرّع فيها توافر القصد الجرمي، ومن ثمّ لا يمكن تطبيق الظّرف المشدّد إذاَ قصد الجاني النّتيجة المشدّدة, لأنّ ذلك يقع تحت طائلة المادة 323-2 من قانون العقوبات الفرنسي.

وما قيل بخصوص المشرع الفرنسي عن الظرف المشدد يقال بخصوص المشرع الجزائري، الا أن المشرع الجزائري إستخدم مصطلح التخريب وذلك بموجب الفقرة الثالثة 3 من المادّة 394 مكرر بقولها***"وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة..."***.

---

[1]- أنظر:**بلال امين زين الدين**، المرجع السابق، ص324.**د. شيماء عبد الغني**، المرجع السابق، ص128.

[2]- **د. علي عبد القادر القهوجي**، المرجع السابق، ص141.

[3]- **د. نائلة عادل فريد قورة**، المرجع السابق، ص222.

[4]-Article 323-1 du CPF dispose que …. soit une altération du fonctionnement de ce système, la peine est .....

ويقصد بتخريب النظام في هذا الإطار ممارسة أفعال عليه من شأنها جعله غير قابل للاستخدام أو الاستعمال وتعطيله عن أداء المهمة التي وجد من أجلهـــا[1].

وعليه فإن الإفساد كنتيجة قد يقع في القانون الفرنسي كظرف تشديد غير مقصود(المادة(323 –1) من قانون العقوبات الفرنسي) أو كجريمة خاصّة مقصودة، في حين ان هذه النتيجة لا تقع في القانون الجزائري الا غير مقصودة–أي ظرف مشدد– ولا تقع مقصودة على الإطلاق، وهو الأمر الذي نرى فيه ثغرة تشريعية ينبغي التدخل لسدها بنصوص صريحة.

ذلك أنه وإن كان صحيحا أن السلوكات التي تتضمنها جريمة التلاعب بالمعلومات والتي تناولها المشرع الجزائري بالتجريم في المادة 394 مكرر1 تؤدي هي الأخرى إلى إعاقة النظام وإفساده، إلا أن تجريمها بنص مستقل ضرورة تلحها العلاقة التكاملية فيما بين الجريمتين حتى لا يفلت المجرم من العقاب، فالإعاقة يمكن أن تنطوي على التلاعب بالمعلومات، والتلاعب بالمعلومات يمكن أن ينطوي على إعاقة، ومع ذلك فمن الممكن أن يكون تحقق أحدهما دون الآخر ممكن في الواقع العملي[2].

هذا ويجب أن تكون الإعاقة والإفساد دون حق، وبمفهوم المخالفة فإذا كانت الإعاقة لها مبرر قانوني فلا مجال للمتابعة هنا، ومن قبيل ذلك وفق ما ورد في المذكرة التفسيرية لاتفاقية بودابست الأنشطة الشائعة المتضمنة في تصميم الشبكات، أو الممارسات الخاصة بالتشغيل أو التجارة كل أولئك يكون بحق، إذ أن الأمر يتعلق على وجه الخصوص بأنشطة إختبار أمن نظام الحاسب أو حماية النظام والمصرح بها من المالك أو القائم بتشغيله، أو عند إعادة تنظيم نظام تشغيل الحاسب، والذي يحدث عندما يقتنى مشغل النظام كيانا منطقيا جديدا كما في حالة تشغيل كيانات منطقية للولوج عبر الانترنت مما يثبط البرامج المماثلة التي أدخلت من قبل. كل تلك الأنشطة تعتبر شرعية وبالتـــالي لا يتم العقاب عليها ولو نتج عنها إعاقة جسيمة.[3]

ثانيا– الـــركن المـــعنـــوي

لقيام الجريمة قانونا لا يكفي مجرد توافر الركن المادي، وإنما يجب أن تكون هناك رابطة نفسية بين النشاط الإجرامي ونتائجه وبين الجاني، وهده الرابطة هي التي يعبر عنها بالركن المعنوي[4].

وإن لم يحدد المشرع الفرنسي في نص المادة 323–2 شكل الركن المعنوي، إلا ان طبيعة الجريمة تأبى أن تقع بطريق الخطأ، ومن تم فإن جريمة إعاقة أو إفساد نظام المعالجة الآلية جريمة عمديه يتخذ الركن المعنوي فيها صورة القصد الجنائي بعنصريه العلم والإرادة، فيجب أن يعلم المتهم أنه يقوم بفعل الإفساد أو التعطيل وأن من شأن نشاطه هذا أن يؤدي إلى التأثير على أداء وظيفة النظام، وأن يعلم أن ذلك يتم بدون

---

[1]-**د. أحمد فتحي سرور**، الوسيط في قانون العقوبات، القسم الخاص، دار النهضة العربية، القاهرة، 1979, ص303.

[2]– انظر: **د.نائلة عادل فريدة قورة**، المرجع السابق، ص 210.

[3]–د. **هلالي عبد الله احمد**، المرجع السابق، ص92.

[4]–**د. على عبد القادر القهوجي**،شرح قانون العقوبات، القسم العام، المسؤولية الجزائية والجزاء الجزائي، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2009، ص391.

رضاء صاحب الحق في السيطرة على النظام أو ضد إرادته، وأن تتجه إرادته إلى إرتكاب الفعل وإلى تحقيق النتيجة. وتستخلص محكمة الموضوع توافر القصد الجنائي من ظروف وملابسات القضية.

ثالثا-العقــوبــة

متى توافرت أركان هذه الجريمة على النحو السابق، فإن المشرع الفرنسي يعاقب عليها بالحبس لمدة 5 سنوات وبغرامة 150000 يورو، وفي حالة ما إذا إرتكبت ضد نظام للمعالجة الآلية للمعطيات دات الطابع الشخصي التي تنفدها الدولة فتكون العقوبة الحبس 7 سنوات وغرامة 300000 يورو[1].

المطلب الثالث

الحماية الجزائية لمعلومات نظــام مواقع التعاملات الإلكترونية

بإزدياد أهمية المعلومات المعالجة آليا داخل نظم مواقع التعاملات الإلكترونية -مع التقدم العلمي- وتنوعها وضخامتها، إزدادت معها خطورة الإعتداءات التي تهددها، ولمواجهة ذلك، عمدت التشريعات إلى حماية سلامة وتكامل هذه المعلومات، فجرمت التلاعب غير المشروع فيها(الفرع الأول)، كما عززت هذه الحماية بتجريم التعامل فيها(الفرع الثاني).

الفــرع الأول

تجريم التلاعب غير المشروع بمعلومات نظام مواقع التعاملات الإلكترونية

إن السلامة في مجال أمن التعاملات الإلكترونية تعني الحفاظ على المعلومات من التغيير والتعديل من الأشخاص غير المخول لهم بذلك[2]، وإزاء تعدد الإضرار بالمعلومات التي تحتوي عليها المواقع نتيجة العبث بها، تنبهت التشريعات المقارنة إلى ضرورة مواجهتها بنصوص خاصة كون هذا الإعتداء جديد لم يسبق تجريمه من قبل، حيث جرم المشرع الفرنسي التلاعب غير المصرح به بالمعلومات بموجب المادة 323-3 عقوبات[3]، والمشرع الجزائري بموجب المادة 394 مكرر 1عقوبات، ودعت إلى تجريمه إتفاقية بودابست بموجب المادة 4[1] والإتفاقية العربية بموجب المادة 8 .

---

[1]-Article 323-2 du CPFModifié par LOI n° 2015-912 du 24 juillet 2015 relative au renseignement

[2]-**عطا الله وراد خليل**،آليات أمن المعلومات في ظل الإنفتاح المعلوماتي، مجلة كلية الحقوق، العدد6، جامعة بنها،2011, ص612.

[3]- **Article 323-3 du CPF**Modifié par LOI n°2015-912 du 24 juillet 2015 - art. 4 dispose que: " Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € d'amende. Lorsque cette infraction a été commise à l'encontre d'un système de

وإنطلاقا من مقتضيات النصوص السابقة، سنتطرق إلى هذه الجريمة من خلال ركنيها المادي والمعنوي.

أولا- الركـــن المـــادي

بالرجوع للنصوص القانونية السابقة، يمكن القول أن السلوك الإجرامي في هذه الجريمة يتخد صور متعددة:

أ- الإدخال:

ويقصد به إضافة بيان جديد على النظام، ويستوي في ذلك أن يكون موضع الإضافة كان خاليا من المعلومات قبل تحققها أو كانت هناك معلومات سابقة ثم إضافة البيان الجديد اليها,[2]وذلك بهدف التشويش على صحتها. و تغذيّة النّظام بمعلومات مغلوطة أو زائفة فيه لم تكن موجودة في السّابق، أمر يسهل القيام به في أولى مراحل إعداد النظام، وهي مرحلة ادخال المعطيات لمعالجتها، فهذه الأخيرة تجهّز وتحوّل في هذه المرحلة إلى شكل أو لغة مقروءة من قبل الآلة المستخدمة في المعالجة[3].

وفي الحقيقة فإن الإدخال غير المصرح به للمعلومات لا يترتب عليه في كل الحالات تعديل في ذاكرة النظام، فقد يؤدي أحيانا إلى تعديل للمعلومات ذاتها أو حتى لتدميرها، كما في حالة إدخال البرامج الخبيثة **كالقنابل المنطقية والزمنية**[4]، كما قد يؤدي إلى المراقبة والتحكم في الشبكة أو النظام المستهدف **وهو ما يسمى جريمة المساحة الإفتراضية**[5].

---

traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende."

[1]-Article 4 dispose que" Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit,d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques.

2 Une Partie peut se réserver le droit d'exiger que le comportement décrit au paragraphe 1 entraîne des dommages sérieux."

[2]-**د.على عبد القادر القهوجي**، الحماية الجنائية للبيانات المعالجة الكترونيا، دراسة مقدمة إلى مؤتمر القانون والكمبيوتر والأنترنت،المجلد الثاني، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، 1 مايو 2000, ص559**د. عبد الفتاح بيومي حجازي**، مكافحة جرائم الكمبيوتر والانترنت، المرجع السابق، ص378.

[3]- أنظر في هذا المعـــنى: **د.خالد ممدوح إبراهيم**، التقاضي الإلكتروني-الدعوى الإلكترونية وإجراءاتها أمام المحاكم، المرجع السابق، ص329. و أنظر أيضا: **د. عفيفي كامل عفيفي, فتوح الشاذلي**، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، الطبعة الأولى، منشورات الحلبي الحقوقية، 2003، ، ص211.

[4]-**القنبلة المنطقية:** هي نوع من الفيروسات تنشط بمجرد حدوث واقعة معينة مثلبدأ تشغيل النظام أو عند إنجاز أمر معين في النظام أو عند بدأ تشغيل برنامج معين. أما **القنبلة الزمنية:**فهي فيروس ينشط في تاريخ معين محددبالذات فهو يثير حدثا في لحظة زمنية محددة بالساعة واليوم والسنة والوقت اللازم.أنظر:**أمجد حسان**, الفيروسات تهدد أنظمة المعلومات، مقال مقدم إلى ملتقى "الإرهاب في العصر الرقمي" المنعقد بجامعة الحسن بن طلال- عمان_, منشور على الموقع التـــــالي:

http://www.google.com/search?

[5]- جريمة المساحة الإفتراضية هي احتلالا جزءيا او كليا دون وجه حق لمساحة على القرص الصلب لحاسوب المجني عليه ودون علمه بإدخال ملف مملوك للمخترق بقصد لتوصل إلى تحقيق نتائج غير مشروعة. **د.عمر محمد أبو بكر بن يونس**، المرجع السابق، ص337.

ويتميز هذا الفعل بصفة عامة من كونه يقع في غالب الأحيان بمعرفة المسؤول عن القسم المعلوماتي والّذي يسند إليه وظائف المحاسبة والمعاملات الماليّة، لأنّه يكون في أفضل وضع يؤهّله لارتكاب هذا النّمط من التّلاعب غير المشروع[1].

وقد تعرّض القضاء الفرنسي بدوره لجريمة التلاعب غير المصرح به بالمعلومات –في صورة الإدخال غير المصرح به– في العديد من أحكامه، منها إدانة موظف قام بإدخال معطيات غير دقيقة في النظام المعلوماتي لإدارة الشركة وهو في طور الإعداد مما سبب تأخير تشغيل النظام[2]. كما قضت محكمة النقض الفرنسية أن إدخال فيروس "*Frodo*" إلى نظام المعالجة الآلية هو سلوك معاقب عليه وفق المادة 323–3[3].كما ذهبت محكمة جنح باريس إلى إدانة المتهم بتهمة إدخال برنامج *sniffer*, [4],فرغم كون أن هذا البرنامج ليس ضاراً وكثيرا ما يستخدم لاستكشاف أو إصلاح شبكات الانترانت ومع ذلك قامت المحكمة بناءً على التّفسير الصّارم للقانون الجزائي بتطبيق المادّة 323–3 عليه[5]. كما أيّدت محكمة النقض الفرنسية عام 1994 حكماً بإدانة أحد الأشخاص بتهمة إتلاف المعلومات لقيامه بإدخال معلومات غير صحيحة تتعلّق بالنّسب الخاصّة بضريبة المبيعات في نظام المعالجة الآلية، وذلك في الاستمارات الخاصة بذلك، ثم قام بإدخال بعض هذه المعلومات إلى نظام المعالجة الآلية[6].

أما في الجزائر، فتعد قضية قرصنة البنك الكندي caisse populaire des jardins من طرف (ف.محمد) واحدة من أول وأبرز القضايا التي تم فيها تطبيق النص الخاص بجريمة التلاعب بالمعلومات في صورة الإدخال، وتتلخص وقائع هده القضية في قيام طالب ماستر إعلام آلي (ف.محمد امين) بإرسال برامج فيرورسية ضمن أنظمة الدفع الإلكتروني مهمتها تسجيل المعطيات الرقمية أثناء إستعمال بطاقات الدفع من طرف الزبائن ليتم إستعمالها فيما بعد لتحويل الأموال وإقتناء مشتريات عبر الأنترنت، منشيء بذلك موقع شبيه بالموقع الرسمي للبنك الكندي، ليقوم ببيع الموقع الإلكتروني بعد أن تلقى طلبات كثيرة لبيعه وذلك لنيكولا ديمون وجوليان دوبوا وقريقوري فيين، وقدم للمحاكمة بتهمة تصميم وإدخال عمدا وعن طريق الغش لمعطيات للمعالجة الآلية في منظومة معلوماتية والمتاجرة فيها أدت إلى تعديل معطيات تلك المنظومة وجنحة التقليد والسرقة، وأدانته المحكمة تطبيقا لأحكام المواد 394 مكرر1 و 394 مكرر 2، والمادة 151 و151 و153 من القانون 03–05 المتعلق بحقوق المؤلف و الحقوق المجاورة، مع تبرئة ساحته من جنحة السرقة[7].

---

[1]–**د.عبد الفتاح بيومي حجازي**، مكافحة جرائم الكمبيوتر والانترنت، المرجع السابق، ص378.

[2] - Crim. 5 janv. 1994, JCP E I 359, cité par: **Chilstein David**. Législation sur la cybercriminalité en France. In: Revue internationale de droit comparé. Vol. 62 N°2,2010 p562

[3] -Cass, crim, 12 décembre 1996, bull, crim, n°465. NCP,104e édition , D, paris, 2009, P918.

[4]- TGI Paris, 1° ch. Corr., 16 décembre 1997, Ministère public c/ Golovanisky, cité par M.jougleux philippe, op, cit, p41.

[5]- يفهم من ذلك ان القانون وضع قاعدة تفيد حظر قيام الغير بإتيان إدخال معلومات على اية شاكلة.

[6]. Cass, crim, 5 janvier 1994,JCP. E, 1994, I. 359, NCP,104e édition , D, paris, 2009, p918.

[7]– محكمة عنابة، قسم الجنح،حكم رقم 07357/10 ، بتاريخ 28–06–2010، قضية جنحة تصميم وإدخال عمدا وعن طريق الغش لمعطيات للمعالجة الآلية والمتاجرة فيها أدت إلى تعديل معطيات تلك المنظومة وجنحة التقليد وجنحة السرقة، ضد (ف. محمد)، غير منشورة.

ب-التـــعديل:

ويشير هذا المصطلح إلى قيام الغير ممن لا يملك إحداث تعديل في المعلومات، باحداث تغييرات عليها، وذلك باستخدام وظائف نظام المعالجة الآلية[1].

هذا وقد إستخدمت الإتفاقية العربية مصطلح "**حجب**" المعلومات للتعبير عن التعديل، ذلك أن حجب المعلومات دون محوها لا يمكن أن يشكل إزالة لها، فإخفاء أحد الملفات مثلا لا يترتب عليه محو بل يؤدي فقط إلى تعديل في قائمة الملفات، وبالتالي فإن الحجب لا يعدو أن يكون تعديلا للمعلومة.

هناك من يرى[2] بأن عبارة التعديل تدل تحديدا عن العدوان الفيروسي، إلا أننا نرى أن التعديل وإن كان ينصرف في مدلوله إلى الفيروسات، إلا أنه لا يقتصرعليها فالتعديل يمكن أن يتم عن طريق إمداد البرنامج بمعلومات مغايرة تؤدي الى نتائج مغايرة عن تلك التي صمـــم البرنـــامج لأجلـــها[3].

ت-الإزالـــة:

تشكل إزالة المعلومات واحدة من أكثر صور التعدي على سلامة معلومات التعاملات الإلكترونية شيوعا، وهو ما دفع العديد من التشريعات إلى تجريمها، وإن إختلفت فيما بينها في المصطلحات الدالة على هذا الفعل، فبينما إستخدم بعضها تعبير"الإزالة"، كما هو شأن المشرع الجزائري والفرنسي، إستخدم بعضها مصطلحات عديدة لكن ما يجمعها أنها تحمل معنى الإزالة مثل الإضرار، المحو، الإتلاف، الطمس كما جاء في إتفاقية بودابست، والتدمير أو المحو كما جاء في المادة 8 من الإتفاقية العربية.

ويشير مصطلح الإزالة إلى إقتطاع خصائص مسجّلة على دعامة ممغنطة عن طريق محوها أو عن طريق طمسها-أي ضغط خصائص أخرى فوقها (خصائص جديدة تطمس الخصائص القديمة)، وكذلك عن طريق تحويل ورصّ خصائص مزالة في منطقة محفوظة من الذّاكرة.[4] والإزالة بهذا المعنى تفترض الوجود السابق لعملية الإدخال.

هدا وقد قضى قسم الجنح المختص بمحكمة وهران بوقوع فعل **الإدخال والتعديل والحدف** بطريق الغش معطيات في نظام المعالجة الآلية للمعلومات في حق المتهمة المشرفة على الجهاز رقم 7 التابع لمصلحة التنظيم العام لولاية وهران والتي قامت بالتلاعب بمعطيات خاصة بسيارتين، حيث ثبت ان هادين الأخيرتين موجودتين في بنك المعلومات بجهاز الإعلام الآلي التابع لمصلحة التنظيم العام لولاية وهران ولكن غير

---

[1]-**د. نائلة عادل فريد قورة**، المرجع السابق، ص217.

[2]-**د. عمر محمد ابو بكر بن يونس**، الجرائم الناشئة عن إستخدام الأنترنت، المرجع السابق. ص363.

[3]- في تطبيقات ذلك أنظر: **د. عبد الفتاح بيومي حجازي**، النظام القانوني لحماية التجارة الإلكترونية، الكتاب الثاني، الحماية الجنائية لنظام التجارة الإلكترونية،دار الفكر الجامعي، الإسكندرية،2002، ص51.

[4]-**محمد خليفة**، المرجع السابق، ص184.

موجودتين بمصلحة التعريفات، وان المتهمة هي الوحيدة التي تملك كلمة السر للولوج لجهاز الإعلام الآلي الحامل رقم 7 وهو الوحيد المختص بعملية الحدف[1].

فضلا عن الأفعال السابقة، جرم المشرع الفرنسي فعل حيازة او نقل أو إستخراج أو إعادة إنتاج بغش المعلومات، بموجب التعديل الدي أدخله على قانون العقوبات بالقانون رقم 2014-1353 [2] وهي أفعال كلها تنطوي تحت التلاعب بالمعلومات المعالجة آليا، والملاحظ أن هذه الصياغة التي جاء بها المشرع سدت بفعالية الفراغ الدي كان موجودا بصدد جريمة سرقة المعلومات السرية في نطاق الأعمال، خاصة من خلال عبارة d'extraction frauduleus ,والعقوبة جاءت أكثر صرامة من السرقة العادية[3].

يتضح من العرض السابق لصور التلاعب بالمعلومات، أن موقف التشريعات إتسم بالبساطة إذ لم تتعمق في التفاصيل كأن تحدد الجهة التي يتبع لها النظام، كما أن تلك الصور التي أوردتها يفهم منها أنها واردة على سبيل الحصر، وهو الأمر الذي يضيق نطاق التجريم، فكان الأولى بالمشرع أن يضع معيارا عاما يجرم كل ما من شأنه أن يمس بسلامة وتكامل المعلومات. هذا من جهة.

ومن جهة أخرى، فإن الأفعال السابقة لا يتمّ المعاقبة عليها إلاّ إذا ارتكبت بدون تصريح، ولا يهم في ذلك إذا كان للشخص في البداية تصريح بالدخول أو البقاء أو لا،حيث قضي في فرنسا[4] بأنه لا يشترط في الإزالة أو الإلغاء المعاقب عليه بالمادة 323-3 عقوبات فرنسي أن يرتكب بواسطة شخص ليس له حق الدخول إلى النظام.

أما ما يخص محل هذه الجريمة، فبما أن الأفعال السّابقة تنطوي على التّلاعب في المعلومات التي يحتويهاَ النّظام، فهذا يعني أنّ النّشاط الإجرامي في هذه الجريمة إنّما يرد على محلّ محدّد وهو المعطيات التي تمّت "**معالجتها آليا**"، والتّي يحتويها النظام وتشكل جزءا منه وهو ما يستخلص بوضوح من خلال نصّ المادة 394مكرر1 من قانون العقوبات الجزائري كما يلي"بطريق الغش المعطيات التي **يتضمنها**" وكذلك المادة323-3من قانون العقوبات الفرنسي كما يلي"...المعطيات التي **يتضمنها**" *les données qu'il* ***...contient...***",

وعليه يخرج من نطاق الحماية المعطيات التي لم تعالج، وتلك التي لم تبدأ بعد مراحل معالجتها، وتلك التي عولجت وانفصلت عن النظام.

---

[1]– مجلس قضاء وهران، قسم الجنح، القطب الجزائي المتخصص، قسم الجنح المختص، حكم رقم 12/00016،بتاريخ 25-07-2012 . قضية جنحة المساس بأنظمة المعالجة الآلية للمعطيات، ضد (ب. نجية واخرون)، غير منشور.

[2]Au premier alinéa de l'article 323-3 du code pénal, la première occurrence du mot : « ou » est remplacée par les mots : «, d'extraire, de détenir, de reproduire, de transmettre, ».- **LOI n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme (1)** JORF n°0263 du 14 novembre 2014.

[3]- **Noé MARMONIER**, Le vol de données informatiques article disponible en lingne á l'adresse suivante, http://www.legavox.fr/blog/noe-marmonier/donnees-informatiques-20088.pdf

Didier frochot; vers la notion juridique de vol de donnees; http://www.les-infostrateges.com/actu/14121921/vers-la-notion-juridique-de-vol-de-donnees

Emmanuel Cauvin; Vers une nouvelle Cité électronique;**Books on Demand**; paris.2016 , p181.

[4]- Cass, crime, 8 decembre, 1999-bull, n° 296. , **NCP,**104e édition **,** D, paris, 2009, p918

هذا وتجدر الإشارة إلى أن إستخدام المشرع الجزائري لعبارة "**يتضمنها**" النظام تجعل من المحل الذي ينصب عليه سلوك الجاني في جريمة التلاعب بالمعلومات ليس المعلومات المخزنة أو المعالجة فحسب بل تشمل المعلومات أثناء نقلها وتراسلها، أي إعتـــراض عملية نقل المعلومات وإجراء تعديل أو إضافة لها، ذلك أن النظام وفق مفهومه المحدد بموجب الفقرة ب من المادة 2 من القانون رقم 09-04 ينصرف إلى نظم الحوسبة والاتصال وما نتج عن إندماجهما، وهو ما يجعل من الأفعال التي تستهدف المعلومات المخزنة أو المنقولة من فكرة الاعتداء على النظام.

وما قيل بخصوص المشرّع الجزائري يقال بخصوص المشرّع الفرنسي، فبقراءة المادّة 323-3 من قانون العقوبات، نجدها لم تحدّد حالة المعلومات محلّ التّلاعب، وهو ما يسمح باستيعاب أفعال التلاعب بالمعلومات المنقولة عبر النظم ضمن مظلّة الـــتّجريـــم.[1]

وعلى العموم، فإنجريمة التّلاعب غير المصرح به بالمعلومات من الجرائم الماديّة التي لا يكفي لقيامها العدوان المحتمل أو التّهديد بالخطر في سلامة المعلومات ووفرتها وإنمّا لابدّ من وقوع ضرر فعلي على هذه المعلومات ألا وهو تغيير حالتها من خلال الأفعال المتمثّلة للنشاط الجرمي في هذه الجريمة مهما كان مقدار الضرر. هذا هو الوضع في التشريع الجزائري والفرنسي، أما الاتفاقية العربية فقد ربطت تجريم الإعتداء على المعلومات بوقوع ضرر جسيم، حيث نصت "للطرف أن يستلزم لتجريم...تتسبب **بضرر جسيم** ", وهو ما يضـــيق في نظرنا من نطاق التجريم.

ثانيا- الركـــن المعنـــوي

أوضحت التشريعات التي تناولت تجريم التلاعب بالمعلومات الركن المعنوي لهذه الجريمة بتطلبها أن ترتكب عن طريق "**الغش**" كما فعل المشرع الجزائري والفرنسي، أو"**قصدا و بدون وجه حق**" كما فعلت الاتفاقية العربية، وهو ما يستفاد منه أن هذه الجريمة تقوم بمجرّد توافر القصد العام بعنصريه العلم والإرادة، ويتطلب القصد العام فيها أن يعلم الجاني أنّه يقوم بإحدى الأفعال التي أوردها النص القانوني، أي يعلم أنه يقوم بإدخال أو إزالة أو تعديل غير مصرّح به على معلومات نظام المعالجة الآلية، وأنّ من شأن أفعاله هذه أن تؤدّي إلى نتيجة هي تغيير حالة المعلومات[2]، وأن تتجه إرادته إلى ارتكاب هذا الأفعال وإلى تحقيق هذه النتيجة.

---

[1]- أنظر في الاتفاق حول ذات المضمون:

Vergutch(pascal), la repression des délits informatiques dans une perspective international, these, université de Montellier1, 1996, p224

مشار إليه لدى: **د. نائلة عادل محمد فريد قورة**، المرجع السابق، ص206.

وإن كان المشرع الفرنسي يعاقب على أفعال التّلاعب التي تقع على المعلومات وكذلك **طرق معالجتها أو نقلها** وذلك بموجب المادة (462-4) السّابقة.

[2] **PhilippeAndrieu** , «stad : Altération, modification, suppression... : », in *Encyclopédie juridique des Biens informatiques*, 19 novembre 2004, disponible en lingne á l'adresse précédente.

ويتضح من خلال البناء المعنوي للنصوص السابقة أن التشريعات لم تستخدم عبارات دالة على تطلّب القصد الخاص أو نيّة خاصّة كنية الإضرار أو قصد الإضرار بالغير، وهو الأمر الّذي يستفاد منه أنّ هذه الجريمة تقوم بمجرّد توافر القصد العام. وهو ما استقرّ عليه القضاء في فرنسا وأكده في عدة أحكام له[1].

ثالثا- العقــوبة

متى توافرت أركان هذه الجريمة على النحو السابق، فإن المشرع الفرنسي يعاقب عليها بالحبس لمدة خمس سنوات وبغرامة 150000 يورو، وفي حالة ما إذا ارتكبت هده الجريمة ضد نظام معالجة للمعطيات دات الطابع الشخصي التي تنفذها الدولة، تصبح العقوبة الحبس 7 سنوات وغرامة 300000 يورو.

أما المشرع الجزائري فعاقب عليها بالحبس من 6 أشهر إلى 3 سنوات وغرامة من 500000 دج إلى 2000000 دج.

الفــرع الثانـــي

تجريم التعامل في معلومات غير مشروعــة

أشارت المذكرة التفسيرية لاتفاقية بودابست على أن "جرائم الإعتداء على نظم المعالجة الآلية يتطلب لارتكابها حيازة وسائل الولوج كأدوات القرصنة أو أي أدوات أخرى، وأنّ هناك دافعًا قوياً للحصول على هذه الوسائل لأغراض إجراميّة، ممّا قد يؤدّي إلى خلق نوع من السّوق السّوداء لإنتاج وتوزيع مثل هذه الأدوات"، وتضيف المذكرة التفسيرية "ومن أجل **وقاية أكثر فعالية من هذه المخاطر** فإنه يجب على قانون العقوبات أن يحظر الأفعال الراجحة الخطورة من المنبع قبل إرتكاب الجرائم المشار إليها في المواد (02 إلى 05)[2].وهو المسلك الذي إتبعته العديد من التشريعات، فنجد المشرع الفرنسي قد نص على مجموعة من الأفعال تصبّ كلّها في التّعامل في معلومات صالحة لأن ترتكب بها إحدى الجرائم التي تمسّ سريّة المعلومات أو سلامتها أو إتاحتها ووفرتها، وذلك بموجب المادة 323-3-1 من قانون العقوبات المعدلة بالقانون رقم 2013-1168 كما يلي " كل من يقوم بدون مبرر قانوني خاصة البحث أو للأمن المعلوماتي باستيراد أو حيازة أو توفير أو وضع تحت التصرف تجهيزات, أدوات. برنامج معلوماتي أو كل معطيات مصممة أو معدة لارتكاب واحدة أو أكثر من الجرائم المنصوص عليها في المواد 323-1 إلى 323-3 يعاقب..."[13].

---

[1]Cass. crim., 8 décembre 1999, . Cass, crim., 5 janvier 1994, Cité par **Alain bensoussan**, Fraude informatique, Les atteintes à un système de traitement automatisé de données, disponible en lingne á l'adressesuivante:http://www.alain-bensoussan.com/pages/2903/

[2]-Rapport explicatif de la Convention sur la cybercriminalité,op; cit; p 14

[3]- Art 323-3-1(crée par la LCEN art 46) du C.P.F Modifié par **LOI n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale,**JORF n°0294 du 19 décembre 2013 page 20570

وإلى جانب المشرع الفرنسي نجد المشرع الجزائري الذي نص على نفس المعنى، وذلك بموجب الفقرة الأولى من المادة 394 مكرر2 على أنه "يعاقب بـــ...تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم", كما جاء نفس المضمون في المادة 9 من الاتفاقية العربية.

أكثرمن ذلك، ذهب المشرع الجزائري إلى تخفيف آثار الاعتداءات المحتملة على المعلومات فيما إذا أسفرت على معلومات معينة وذلك بتجريم التعامل فيها سواء بإفشائها أو نشرها أو استعمالها، حيث نص في الفقرة2 من المادة 394 مكرر2 على: "..حيازة أو إفشاء أو نشر أو إستعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم".

إنطلاقا من مقتضيات النصوص السابقة، سنتطــرق إلى هذه الجــريمة من خلال ركنيها المادي والمعنوي كمايلي:

أولا- الركــن المــادي

ونميز هنا بين صورتين، التعامل في معلومات صالحة لإرتكاب جريمة، والتعامل في معلومات متحصلة من جريمة.

أ-التّعامل في معلومات صالحة لارتكاب جريمة

يتحقق التعامل في معلومات صالحة لإرتكاب جريمة وفق النصوص السابقة بسلوكات مختلفة، وهي على قدم المساواة في تحقيق النّشاط الإجرامي المكوّن للركن المادي للجريمة.

1-التصمــيم: ويتمثل في إعداد معلومات صالحة لارتكاب الجريمة، وعادة يقوم به المختصون في هذا المجال كمصممي البرامج، مثاله تصميم برنامج من أجل الوصول إلى نظم المعالجة الآلية أو تصميم برنامج لأهداف تخريبية مثل البرامج الفيروسية، أو إنشاء مواقع لإستعمالها في القرصنة الإلكترونية.

تطبيقا لذلك قضت محكمة عنابة بتوافر الجريمة في حق الشخص الذي قام بتصميم وإنشاء مواقع شبيهة بالمواقع الرسمية لبعض البنوك، وعند محاولة الزبائن إجراء عمليات مصرفية بحساباتهم البنكية وجدوا أنفسهم في المواقع الخاطئة التي أنشانها القراصنة دون علم فيقدمون لهم الأرقام الحسابية التي تستعمل فيما

---

texte n° 1 , dispose que: ''Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition unéquipement, un instrument, un programme informatique ou toute donnée conçus ou spécialementadaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 estpuni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée."

بعد لتحويل الأموال أو للشراء عبر الأنترنت، وقد قام بتحويل ما قيمته 1000000 دولار أمريكي منذ سنة 2005، وقد كان أغلب ضحاياه هم زبائن البنك الكندي caisse populaire des jardins[1].

2-البحـــــث:على خلاف التشريعات السابقة، نص المشرع الجزائري في المادة "394 مكرر 2"**...أو بحث ...في معطيات...يمكن ان ترتكب بها الجرائم...**"

لو تأمّلنا قليلاً في البناء المادي لهذه المادّة لوجدنا أنّها توسّع في نطاق التجريم، حيث أنها لم تقصر كلمة بحث على كيفية تصميم المعلومات وإعدادها لأن ترتكب بها الجرائم السابقة، كما يكشف عليه السيـــــاق اللغوي والمنطقي للمادة بأن جاءت عبارة بحث بعد عبارة التصميم مباشرة، بل تمتد لتشمل البحث عن المعلومات بإعتبارها وسيلة يمكن أن ترتكب بها الجريمة، وإن كان الأصل في ذلك لا يعد جريمة، ومثالها البحث عن كلمة سر النظام أو شيفرة الدخول أو غيرها.

3- **التجمـــــيع:** لا يوجد تعبير موحد بين التشريعات للدلالة على هذا الفعل، ففي حين آثر المشرع الجزائري مصطلح التجميع، إستعملت الاتفاقية العربية مصطلح الحيازة، كما فعل ذلك المشرع الفرنسي متأثرا باتفاقية بودابست، فضلا عن إستخدام هذه الأخيرة إلى جانب مصطلح الحيازة مصطلح الحصول من أجل الاستخدام.

ويقصد بالتجميع في هذا الإطار جمع عدد من المعلومات التي تشكّل خطرًا كبيرًا، حيث من الممكن أن ترتكب بها إحدى جرائم الاعتداء على نظم المعالجة الآلية، من ذلك تجميع برامج تسمح بتجاوز إجراءات الحماية المنطقيّة[2]. والتجميع بهذا المعنى يقتضي بداية حيازة المعلومة، ومن ثم فإن الحيازة تندرج ضمن مصطلح التجميع وإن كان أوسع نطاقا منها. هذا وقد وردت عبارة الحيازة في التشريع الفرنسي كناية عن حيازة البرامج الفيروسية تحديدا[3].

أما عن مصطلح الحصول للاستخدام الذي آثرت إتفاقية بودابست إستخدامه، فيشير إلى نيّة استخدام المعلومات المتحصّل عليها دون اشتراط ضرورة توفّر مجموعة منها، والأخيره هي ما يتطلبها مصطلح التجميع دون ضرورة توافر نيّة لدى الفاعل باستعمالها.

4- التوفيـــــر: يشير مصطلح التوفير أو الوضع تحت التصرف إلى إتـــاحة المعلومات التي تمكن من إرتكاب الجرائم السابقة وجعلها في متناول الغير، بل وتحت تصرفه وحيازته، ومن قبيل ذلك وضع برامج الاختراق أو كلمات السر أو شيفرة الدخول للنظام على الخط، أو تجميع الرّوابط بين الخطوط المتشعّبة من أجل تسهيل الوصول إلى هذه المعلومات، وذلك عن طريق الإحالة لبرنامج يتصل ببرامج مصمّمة على سبيل

---

[1]-محكمة عنابة، قسم الجنح،حكم رقم 07357/10 ، بتاريخ 28-06-2010، قضية جنحة تصميم وإدخال عمدا وعن طريق الغش لمعطيات للمعالجة الآلية والمتاجرة فيها أدت إلى تعديل معطيات تلك المنظومة وجنحة التقليد وجنحة السرقة، ضد (ف. محمد)، غير منشور.

[2] – **Alain-bensoussan**, Fraude informatique-cybercriminalite -disponible en lingne á l'adresse suivante : http://www.alain-bensoussan.com/pages/2644/.

[3] -Rapp. pour avis de **Madame Tabarot**, député, pour la Commission des lois, disponible en ligne á l'adresse suivante: http://www.assemblee-nationale.fr/12/rapports/r0608.asp.

المثال للإتلاف[1]، بل أنّ القضاء الفرنسي قد توسّع في تفسير مدلول التّوفير ليشمل الكشف أو الإفشاء العلني للثغرات الأمنيّة في النظام [2].

5-النشـــــر: نص على هذا الفعل كل من التشريع الجزائري واتفاقية بودابست، في حين لم نجد له ذكرا لا في التشريع الفرنسي ولا في الاتفاقية العربية، ويقصد بالنشر في هذا الإطار إذاعة المعلومات محلّ الجريمة وتمكين الغير من الإطّلاع عليها[3]، هذا وقد أشارت المذكّرة التّفسيرية إلى أنّ مصطلح النّشر ينبغي أن يمتّد ليشمل كل نشاط من شأنه نقل معلومات إلى الآخرين[4].

6-الاتجـــــار: آثر المشرع الجزائري إستخدام مصطلح الاتجار بما يسمح باستيعاب مختلف التعاملات التي يتصوّر وقوعها على المعلومات من بيع واستيراد وشراء وغيره، في حين إستخدم المشرع الفرنسي مصطلح "استيراد", أما إتفاقية بودابست إستخدمت مصطلح البيع والاستيراد، وكذلك فعلت الاتفاقية العربيـــــة.

ويشير مصطلح الاتّجار بالمعلومات إلى تقديمها للغير بمقابل، ولا يهم هذا المقابل إذ يستوي أن يكون نقديًا أو عينيًا أو يقتصر فقط على مجرّد خدمات أو غير ذلك[5].من قبيل ذلك الإتجار في كلمة المرور أو شفرة الدخول أو برنامج مصمم بشكل أساسي لإرتكاب جرائم الاعتداء على النظم.

وتطبيقـــــا لذلك قضي في الجزائر بقيام **جنحة المتاجرة في منظومة معلوماتية** في حق المتهم الذي قام بإنشاء موقع مشابه للموقع الخاص بالبنك الكندي مع علمه بأن الموقع يخص طرف لا علاقة له به، كما أن الأشخاص الذين إتصلو به عجزو على إنشاء الموقع ومع ذلك قام المتهم بالإستجابة لطلبهم بالرغم من عدم معرفته بهم شخصيا، وقام ببيع الموقع بمبلغ 500 إلى 900 دولار كندي للإستعمال للإحتيال على الأشخاص للحصول علي هوياتهم لإستعمالها في أغراض تجارية غير قانونية[6]، كما قام بإنجاز البرامج الإلكترونية سنيفر وباعها عن طريق الأنترنت لعدد من الأشخاص وكسب منها مبالغ مالية.

ب- التّعامل في معلومات متحصّله من جريمة

هذه الصورة من التعامل إنفرد بهـــا المشرع الجزائري، إذ لا نجد لها ذكرا في التشريعات المقارنة, ولعل ذلك ينم عن سياسة المشرع في الحماية، حيث ضيق من نطاق الأشخاص الذين يمكن أن يتعاملوا في المعلومات المتحصلة من جرائم الاعتداء على نظام التعاملات الإلكترونية للحفاظ على ما تبقى من سريتها.

---

[1] -Rapport explicatif de la Convention sur la cybercriminalité,op cit; p14.

[2]-Cass, crim **27 octobre 2009**, disponible en lingne á l'adresse suivante;http://www.globenet.org/IMG/pdf/Cour_de_cassation_FULL_DISCLOSURE_criminelle_Chambre_criminelle_27_octobre_2009_09-82-346_Publie_au_bulletin_SURLIGNE.pdf.

- Cass, crim **22 décembre 2009**, disponible en lingne á l'adresse suivante; http://blog.crimenumerique.fr/tag/atteintes-aux-stad/.

[3]– **محمد خليفة**، المرجع السابق، ص201.

[4]-Rapport explicatif de la Convention sur la cybercriminalité,op; cit ,p14.

[5]-**محمد خليفة**, المرجع السابق, ص204.

[6]- محكمة عنابة، قسم الجنح، حكم رقم 07357/10 ، بتاريخ 28-06-2010، قضية جنحة تصميم وإدخال عمدا وعن طريق الغش لمعطيات للمعالجة الآلية والمتاجرة فيها أدت إلى تعديل معطيات تلك المنظومة وجنحة التقليد وجنحة السرقة، ضد (ف. محمد)، غير منشور.

وتتمثّل هذه الجريمة بأحد الأفعال التي نصت عليها المادة 394 مكرر2 في فقرتها الثانية وهي الحيازة , الإفشاء، النشر والاستعمال، وهي على قدم المساواة في تحقيق النشاط الإجرامي.

1-الحيـــازة: الحيازة سيطرة إرادية لشخص على شيء، وهي ليست حقا بل مركز واقعي، هذا الأخير قد يكون مشروع أو غير مشروع، ففي الحالة الأخيرة يستخلص منه المشرع بعض الآثار، مما يعني أنه يعتد به ويجعل منه نظاما قانونيا يكفل له شروط معينة للحماية[1]. وهو وضع الحيازة في هذه الجريمة، إذ تكون **دائمًا** غير مشروعة ذلك أنّه يشترط أن تكون متحصّله من إحدى جرائم الاعتداء على نظم المعالجة الآلية وفق ما ورد في البند الثاني من المادة 394مكرر2 من قانون العقوبات. والحيازة على النحو السابق بيانه تقوم على عنصرين: مادي ومعنوي[2].

قوام العنصر المادي هو السيطرة على المعلومات، وذلك بالتاثير عليها تأثيرًا يتفاوت حجمه تبعًا لنوع الحيازة، وصور هذا التاثير متنوعة، وأبرزها إفناء هذه المعلومات أو التعــديل منها أو توجيهها في إستعمال معين.

أمـــا قوام الركن المعنوي فهو إرادة السيطرة على المعلومات، فما يأتيه الحائز من أفعال ليس وليد المصادفة، وهي ليست عارضة بل صادرة عن إرادة الاحتفاظ بالمعلومات وإستبقاء السيطرة عليها مدة معينة. وتفترض هذه الإرادة العلم بمضمون المعلومات كونها متحصلة من جريمة، وبدخولها في نطاق السيطرة عليها. وتطبيقا لذلك فإن من يخزن كلمة مرور تحصل عليها من إختراق موقع في نظام يحوزه شخص معين لا يدخله في حيازة حائز هذا النظام اذا كان لا يعلم بوجود هذه المعلومات.

2-الإفشـــاء: يفترض الإفشاء مثله في ذلك مثل فعل النشر إنتقال المعلومات من حيازة الجاني إلى غيره من الأشخاص، حيث أنّه يقوم بتقديم هذه المعلومات غير المشروعة إلى غيره ولا يقصرها على نفسه، وهو ما يفّرق هذين الفعلين عن فعل الحيازة التي ينحصر فيها وجود المعلومات غير المشروعة لدى الحائز دون تقديمها لغيره[3].

ولا ينبغي أن يفهم فعل النشر السابق بيانه أن يكون القائم على إتيانه ملزماً بموجب وظيفة معينة أو عقد أو التزام ما بكتمان هذه المعلومات[4]، وهو ما يستفاد من الصيغة المطلقة التي جاءت عليها الفقرة الثانية من المادة 394 مكرر2، بل هو شخص تحصّل على هذه المعلومات عن طريق إرتكابه لجرائم الاعتداء على النظام وأراد المشرّع أن يمنعه من إفشاءها رغبة منه في تضييق نطاقها.

3-النشـــــر:وهو الفعل الذي يقوم به عادة المخترقون للمواقع الإلكترونية وحصولهم على معلومات سرية أو شيفرة الدخول أو كلمة سر نظام المعلومات، والقيام بنشرها رغبة في إظهار مقدرتهم على تحدي وقهر النظم.

---

[1]- **د. محمود نجيب حسني**, شرح قانون العقوبات القسم الخاص، دار النهضة العربية، القاهرة، 1992،ص834.

[2]- المرجع نفسه, ص835, **د.فتوح عبد الله الشاذلي**، شرح قانون العقوبات القسم الخاص، دار المطبوعات الجامعية، الإسكندرية، 2001، ص452.

[3]- أنظر في هذا المعنى: **محمد خليفة**، المرجع السابق، ص209. وأنظر أيضا: **د. أسامة أحمد المناعسة، جلال محمد الزعبي، صايل فاضل الهواوشة**، جرائم الحاسب الآلي والانترنت، دار وائل للنشر، عمان، د.ت، ص 223.

[4]- **محمد خليفة**, المرجع السابق, ص208.

هذا ولم يحدد نص المادة 394 مكرر2 وسيلة معينة يتم بها النشر، وعلى ذلك يستوي أن يتم النشر بطريقة تقليدية عن طريق الكتابة، أو عن طريق الانترنت يمكن للجميع الوصول إليها باستخدام أبسط برامج التصفح. و يكفي في ذلك أن يتم النشر ولو لمرة واحدة ليجعل الفعل قائما.

4-الاستعمـــــال: ويشير هذا الفعل إلى استعمال المعلومات المتحصل عليها بعد دخول غيــر مشــروع أو غيره، ورغم أن فعل الإستعمال يختلف عن فعل الإفشاء، غير أنه لا يتصور وجود حالات يتم فيها الإستعمال دون إعلام للغير، أي دون إفشاء، وعنصر الإستعمال عنصرا واسعا ومطاطا، فالتجريم يرمي إلـــى معاقبـــة الإستعمال مهما كانت كيفيته أو غرضه.

هذا كان عن صور النشاط الإجرامي في جريمة التعامل في معلومات غير مشروعة، أما عن محل الجريمة، ففي صورتها الأولى وهي جرائم التعامل في معلومات صالحة لارتكاب جريمة, فهو يكمن في المعلومات **المخزنة** أو**المعالجة** أو **المرسلة** حسب المادة 394 مكرر2 من قانون العقوبات الجزائري، أو "**تجهيزات أو أدوات** او"**البرامج والمعطيات حسب المادة** 323-3-1 عقوبات فرنسي، على أن تكون هذه الوسائل مصممة أو معدة **خصيصا** لارتكاب واحدة أو أكثر من جرائم الاعتداء على نظم المعالجة الآلية. وعليه فإن مجال تطبيق التجريم وفق المادة 323-3-1**مزدوج:** فمن جهة فإن الأفعال المعاقب عليها متعلقة باستيراد أو حيازة أو توفير تجهيزات, أدوات... لكن **بشرط** أن يكون إنشاء هذه الأدوات وتعديلها من أجل إرتكاب جريمة من جرائم الاعتداء على نظم المعالجة الآلة[1].ولعل أنه سلك في ذلك مسلك اتفاقية بودابست[2] في المادة 6 منها وبالتالي فإنّ هذا النّص يستبعد عادةً الأجهزة ذات الاستخدام المزدوج[3].

أما بالنسبة للاتفاقية العربية، فما قيل بخصوص المشرع الفرنسي يقال بشأنها، وهو ما يستفاد بوضوح من عبارة "...**مصممة او مكيفة..**"الواردة في المادة 9 من الإتفاقية.

اما عن المحل في الصورة الثانية لهذه الجريمة فهو المعلومات المتحصل عليها من خلال إرتكاب إحدى جرائم الاعتداء على النظم وفقا للشرح الذي تم تناولنـــه في الفقرات السابقة.

وفي الأخير يجدر التنويه، إلى أن هذه الجريمة هي من الجرائم الشكلية أي أنّها تقع وتكتمل بمجرّد وقوع الفعل المكوّن لها دون أن يتطلّب المشرّع في نموذجها القانوني حسب نصوص التّجريم أيّة نتيجة إجراميّة تترتب على الفعل.

ثانيا- الركــن المعنــوي

التعامل في معلومات غير مشروعة جريمة مقصودة، ومنه لمساءلة مرتكبها يجب توافر القصد الجنائي بعنصريه العلم والإرادة، وهو ما يستفاد من عبارة "عمدا" أو "عن طريق الغش" التي وظفها المشرع

---

[1] -**Xavier LEMARTELEUR**, Le scan de ports : une intrusion dans un STAD ?disponible en ligne a l'adresse précédente.

[2] -وبالرجوع إلى المادة السادسة منها نجدها تحدد نطاق هذه الجريمة بالأجهزة التي يمكن القول معها أنها قابلة أو معدة خصيصًا لغرض ارتكاب الجرائم و ذلك بقولها "*أي جهاز, يحتوي على برنامج معلوماتي, مصمم أو موفق* ***بشكل أساسي*** *لغرض ارتكاب إحدى الجرائم المنصوص عليها وفقا...*".

[3] –Rapport explicatif de la Convention sur la cybercriminalité,op; cit , p15.

الجزائري في المادة 394 مكرر2 من قانون العقوبات، وعبارة"..بدون مبرر شرعي الموظفة في المادة 323-3-1 عقوبات فرنسي.

وعلم الجاني يجب أن يحيط بكافة العناصر الداخلة في تشكيل الجريمة، وأن تتجه الإرادة إلى تحقيق أحد المظاهر السلوكية التي نص عليها المشرع.

والقصد العام على النحو السابق بيانه لا يكفي لقيام الجريمة في صورتها الأولى، بل لا بد من توافر القصد الجنائي الخاص في التشريع الجزائري، وهو اتّجاه القصد في التعامل بهذه المعلومات إلى الإعداد والتّمهيد لاستعمالها في ارتكاب جريمة من جرائم الاعتداء على نظام المعالجة الآلية، ذلك أنّ هذه المعلومات غير معدة خصيصا لارتكاب الجريمة كما أشارت إليها المادّة السّابقة، بما يعني أنّها ذات استخدام **مزدوج** فكما يمكن أن تستعمل لأغراض مشروعة كأغراض الحماية مثلا فإنها في المقابل يمكن أن تستعمل في أغراض غير مشروعة.

أما في التشريع الفرنسي، فعبارة "**دون مبرر شرعي**" التي أضافها مجلس الشيوخ[1] والواردة ضمن المادة 323-3-1 من قانون العقوبات تنصرف إلى القصد العام فحسب، ذلك أن هذه الأدوات والبرامج والمعلومات كما أشارت إليها المادة السابقة **معدة أو مصممة خصيصا لارتكاب الجريمة،** فصفتها الثابتة هذه هي التي تجعل من القصد الجرمي العام كافيا لقيامـــها.

هذا كان عن الجريمة في صورتها الأولى، أما الصورة الثانية وهي التعامل في معلومات متحصلة من جريمة، وبالرجوع للمادة 394 مكرر2 عقوبات جزائري نجدها تنص على ما يلي" ...**عمدا وعن طريق الغش...**"كما تنص"...**لأي غرض كان المعطيات...**"

لو تأملنا قليلا في التعبير الذي إستخدمه المشرع لقلنا أن المشرع تطلب القصد الخاص من خلال إستعماله لفظ "**الغش**" إلى جانب "**عمدا**"، لكن إذا ما رجعنا إلى البند الثاني باستخدامه "**لأي غرض كان**" يفهم منه مهما كان قصد الجاني والوقائع التي ينصرف إليها من خلال التعامل في هده المعلومات، ومن ثم فإن عبارة عن طريق الغش لا تتعدى وظيفتها التأكيد على عـــبارة القصد الجنائي العام.

---

[1]- ذلك ان نص المادة 323-3-1 المتبنى في القراءة الأولى من طرف الجمعية الوطنية كالتالي:"كل من يقوم بحيازة أو توفير تجهيزات, أدوات. برنامج معلوماتي أو كل معطيات مصممة أو معدة لارتكاب الجرائم المنصوص عليها في المواد 323-1 إلى 323-3 يعاقب بالعقوبة المقررة للجريمة نفسها أو بعقوبة الجريمة الأشد. نص المادة السابقة الذكر لا يطبق عندما يكون حيازة أو وفرة التجهيزات, الأدوات برنامج معلوماتي أو كل معطيات مبرر باحتياجات البحث العلمي و التقني أو لحماية و أمن شبكات الاتصالات الإلكترونية و الأنظمة المعلوماتية, و عندما تستخدم بواسطة مؤسسةعمومية أو خاصة فيكون ذلك وفق تصريح مسبق لدى الوزير الأول بمقتضى الكيفية المنصوص عليها بواسطة المادة 18 من القانون المتعلق بالثقة بالاقتصاد الرقمي". وقد راى مجلس الشيوخ ان الحل المقترح من طرف الجمعية الوطنية يستطيع أن يحدث صعوبة جدية في التطبيق, فالنص المقترح من طرف الجمعية الوطنية يعرض فعلا مؤسسة تحوز الفيروسات لهدف البحث للملاحقة القضائية إذا أهملت الحصول على التصريحات كلما استعملت الفيروسات لأغراض مشروعة. فاضاف عبارة دون مبرر شرعي.انظر:

Valérie Sédallian, Légiférer sur la sécurité informatique : la quadrature du cercle ?p14, disponible en lingne á l'adresse précédente.

Eric Filiol, Les virus informatiques: théorie, pratique et applications, 2 edition , collection iris, springer, france 2009, p202.

ثالثا- العقـــوبـــــة

متى ما توفرت أركان جريمة التعامل في المعلومات على النحو السابق، فإن المشرع الفرنسي يعاقب عليها بالعقوبة المقررة للجريمة نفسها، وهو مسلك حسن من قبله بسبب أنه ليس من المنطق أن نعاقب على جريمة هي بمثابة **أعمال تحضيرية**[1] لجريمة معينة من عقوبة أشد من عقوبة هذه الأخيرة، وهذا ما جانبه المشرع الجزائري حيث قرر لها عقوبة الحبس من شهرين إلى 3 سنوات وبغرامة من 1000000 دج إلى 5000000 دج.

في الأخير يبقى لنا أن نشير أنه وعلاوة على العقوبات السابق الإشارة إليها، ونظرا لوعي المشرع بخطورة المساس بنظم المعالجة الآلية التي تقوم عليها التعاملات الإلكترونية، وما يترب عن ذلك من تهديد جدي للمصالح المرتبطة بها، أورد المشرع الجزائي في كل من فرنسا والجزائر نظام حماية جزائي يتميز بأنه **واسع من حيث نطـــاق المتابعة وصارم من حيث العقوبـــات.**

حيث استوجب تمديد ميدان المتابعة الجزائية إلى **المرحلة المادية التي تتوسط العزم والبدء في التنفيذ.-اتفاق جنائي**-وحدد عقوبتها بالعقوبة المقررة للجريمة ذاتها المعد لارتكابها والتحضير لها، وذلك وفقاً لما جاء في نص المادة 323-4 عقوبات فرنسي، والمادة 394 مكرّر 5عقوبات جزائري.

كما لم يتوقف نطاق المتابعة عند ردع الفعل التام فقط، بل تعداه إلى المحاولة-الشروع-، وذلك وفقا لما جاء في المادة 394 مكرر7عقوبات جزائري والمادة 323-7 عقوبات فرنسي، ورغم إستحسان هذا التجريم بالنسبة للجنح السابقة بموجب نص، فإن مسألة تطبيق الشروع في بعضها يتنافى والقواعد العامة، وذلك كون أن معظمها تعتبر جرائم شكلية مما لا يتصور فيها الشروع . كما أن نص المادة 394 مكرر 7 بموضعها وعلى خلاف المادة 323-7 عقوبات فرنسي يشمل الشروع في الإتفاق الجنائي، بما يعني تجريم الشروع في الشروع، وهو ما كان محل إنتقاد شديد من الفقـــه[2].

ولم تقتصر رغبة المشرع في ضمان حماية أكثر فاعلية للمساس بمواقع نظم التعاملات الإلكترونية فقط في تمديد المتابعة الجزائية إلى الشروع. بل أن هذه الإرادة تظهر، أيضا وعلى وجه الخصوص،

---

[1]- **محمد خليفة**، المرجع السابق، ص192.

[2]-ذهب جانب من الفقه إلى القول بأنّه لا يوجد شروع في الاتّفاق على سند من القول أنّ الاتفاق حالة نفسيّة تقع عند الجناة في لحظة واحدة ولا تحتمل البدء ولا الانتهاء فهو لا يقع إلاّ كاملاً ولا يتصوّر فيه البدء في التّنفيذ. **د. السعيد مصطفي السعيد**, الأحكام العامة في قانون العقوبات، الطبعة الثانية، مكتبة النهضة المصرية، مصر، 1953، ص350. وعلى نقيض الاتّجاه السّابق ذهب اتّجاهإلى القول بإمكانيّة تصور الشروع في الاتّفاق, محتجًا بأنّه طالما كانت أركان الشّروع متصوّرة, ولم يكن القانون متضمنًا نصًا خاصًا يقضي بعدم العقاب عليه فلا وجه للقول بالرّأي السابق, فليس صحيحًا أنّ الشّروع في الاتفاق غير متصور, إذ الدّعوى إليه أو الحمل عليه بدء في التّنفيذ, فإذا توافر القصد الجرمي و لم يتم لأسباب لا دخل لإرادة الجاني فيها فالعقاب على الشروع متعين إذا كان الاتفاق جناية إذ لا يتطلب العقاب عليها نصًا خاصًا, و إذا كان الاتفاق جنحة فلا بد من وجود هذا النص. **د. محمود نجيب حسني**، شرح قانون العقوبات، القسم العام، النظرية العامة للجريمة والنظرية العامة للعقوبة والتدبير الإحترازي، الطبعة الخامسة، دار النهضة العربية، القاهرة، 1982، هامش رقم 1، ص 490.

ونذهب إلى ما ذهب إليه الاتّجاه الأول من عدم جواز العقاب على الشّروع في الاتّفاق بسبب من أنّ الاتّفاق في حد ذاته مرحلة متقدّمة على إتيان الجرائم المتّفق عليها, وإن كان المشرّع قد جرّم مرحلة سابقة عليها فإنّ تجريمها في هذه المرحلة يعتبر تجريم لإرادات لم تلتق بعد ما يترتّب عليه مساس بالقاعدة العامة في قانون العقوبات التي تقضي بـــ:"***عدم العقاب على النوايا و سرائر النفس***", لأنّه أقرب ما يكون إلى تجريم النّوايا أو تبنيّ فكرة الشّروع في الشّروع إن صح القول وهو ما لم يقل به أحد.

في واقعة توسيع هذه المتابعة إلى الأشخاص الاعتبارية، حيث نصت المادة394 مكرر4 كما يلي "*يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي*".وإلى جانب المشرع الجزائري نجد المشرع الفرنسي يقر بدوره مسؤولية الشخص المعنوي في مجال المعالجة الآلية للمعلومات وذلك بموجب المادة 323-6 كما يلي" يحكم *على الأشخاص المعنوية بالمسؤولية الجزائية وفقاً للشروط المحددة في المادة121-2.."*[1].

أما **صرامتة في الردع** فنلمسها من خلال تشديده العقوبات الأصلية، المتمثلة في الحبس والغرامة الموقعين على الأشخاص الطبيعية وذلك متى كانت المعلومات الّتي تم العدوان عليها تتعلق بالدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، حسب المادة 394 مكرر3 عقوبات جزائري، وذلك نظراً للخطورة البالغة التي تنجم عن الاعتداء عليها، أو كانت الإعتداءات ضد نظام المعالجة الآلية للمعطيات دات الطابع الشخصي التي تنفدها الدولة حسب الفقرة 3 من المادة 323-1 والفقرة 2 من المادة 323-2 والمادة 323-3 عقوبات فرنسي.أو أن الجرائم تم إرتكابها من جماعة منظمة ضد نظام للمعالجة الآلية للمعطيات الشخصية التي تنفدها الدولة حسب المادة 323-4-1 عقوبات.

فضلا عن ذلك، جعل من النتيجة المترتبة ظرفاً مشدّداً للعقوبة في جريمة الدخول أو البقاء غير المصرّح بهما، بموجب المادة 394مكرر وكذلك فعل المشرع الفرنسي في الفقرة الثانية من المادة 323-1عقوبات

كما تظهر جدية وصرامة المشرع كذلك من خلال وضعه عقوبات تكميلية معينة تتمثل **في مصادرة**الأجهزة والبرامج والوسائل المستخدمة، مع إغلاق المواقع والمحل أو مكان الإستغلال، مع الإحتفاظ بحقوق الغير حسن النية، وذلك حسب المادة 394 مكرر 6 عقوبات جزائري. وكذلك فعل المشرع الفرنسي بموجب الفقرة 3 و4 من المادة 323-5 من قانون العقوبات، بل أن هذا الأخير وسعياً منه لتحقيق مبدأ تفريد العقوبة نص على عدة عقوبات تكميلية بموجب المادة نفسها، كالمنع لمدة 5 سنوات أو أكثر من إصدار شيكات، ولا يمنع هذا من إسترداد شيكات السحب الموجودة لدى المسحوب عليه والشيكات المعتمدة.

[1]–Art 323-6 du C.P.F Modifié par **LOI n° 2009-526 du 12 mai 2009 de simplification et de clarification du droit et d'allègement des procédures,**dispose que "Les personnes morales déclarées responsables pénalement, dans les conditions prévues parl'article 121-2,

المبحث الثاني

تقرير المسؤولية الجزائية للوسيط الفني في التعاملات الإلكترونية

يعتبر الوسيط الفني أداة الوصل وقناة الإتصال بين كافة المتعاملين الإلكترونيين على إختلاف أنواعهم ومراكزهم، فهو محرك أساسي ويترتب على عدم تأديتة الواجب المناط به، قطع كافة قنوات الإتصال و آليات المفاوضات والإبرام بين أطراف التـــعامل.

وحيث أن وسطاء الخدمة بأنواعهم المختلفة ذوي علاقة بشكل أو بآخر فيما يتعلق بآلية عمل التعاملات الإلكترونية، لأن كل منهم يؤدي جزءا من نظام "العملية المعلوماتية" التي تتعلق بهذه التعاملات. فهم بالتالي لهم دور إيجابي في حماية النظم التي تتعامل بشبكة الأنترنت من **المحتويات غير المشروعة**[1] مثل **الدعاية العنصرية والخلاعيـــة.**

مع التطوُّر الهائل الذي شهدته تقنية الإنترنت، إتسع الجدل الدائر بين الفقه والقضاء حول مسؤولية مقدمي الخدمات خاصة عن المعلومات الواردة في ذلك المحتوى إذا تضمنت الإساءة للمتعاملين في مواقع التعاملات الإلكترونية، أو نشر وقائع تشكل جريمة، فكيف يتم تأصيل المسؤولية الجزائية عن هذه الجرائم؟ فهل يتم الإرتكاز على المباديء القانونية القائمة، أم لا بد من إرساء نظام عادل للمسؤولية لمكافحة هذه المضامين المضرة، بوضع نظام قانوني خاص بهؤلاء المتدخلين؟

ومما لا شك فيه أن من شأن تحديد المسؤولية الجزائية لمقدمي الخدمات الوسيطة في شبكة الأنترنت يؤدي بالضرورة إلى نوع من الحماية الجزائية للتعاملات الإلكترونية، ويســـاهم في تأمينها، مما يشجع المتعاملين على ٱلإقدام على التعامل بواسطة الأنترنت.

ولذلك فإن الإجابة على السؤال تقتضي منا التعرض أولا لتحديد الوسيط الفني المتدخل في شبكة الأنترنت ومن تم في التعامل الإلكتروني وتحديد دوره، ثم موقف القانون المقارن من المسؤولية الجزائية للمتدخل في التعاملات الإلكترونية، ولذا سنقسم الدراسة في هذا المبحث إلى المطالب التالية:

المطلب الأول: الوسيط الفني كطرف من أطراف التعاملات الإلكترونية

المطلب الثاني: تقرير المسؤولية الجزائية للوسيط الفني وفق النصوص القائمة

المطلب الثاني: تقرير المسؤولية الجزائية للوسيط الفني بموجب نصوص خاصة

---

[1]– إن تعبير "مشروع" تعبير قانوني نجده في العديد من المعاهدات الدولية، ويرتبط بمفاهيم أخرى كالأخلاق والنظام العام والآداب العامة التي تتطور من بلد إلى آخر، عند تحديد مفهومه تؤخذ بعين الإعتبار الأيديولوجيات والسياسات والديانات التي تتغيرفي الزمان ايضا. ويمكن وضع عدة نشاطات تحت عنوان مضامين غير مشروعة منها المزاحمة غير المشروعة، الإستغلال الجنسي للقاصرين عبر الأنترنت ، الصور الفاحشة، المواقع التي تحرض على العنف، الدعايات المبغضة: أنظر: **د. أودين سلوم الحايك**، مسؤولية مزودي خدمات الأنترنت التقنية، المؤسسة الحديثة للكتاب، طرابلس، لبنان،2009 ، ص106 ومايليها.

المطلب الأول

الوسيط الفني كطرف من أطراف التعاملات الإلكترونية

إن إشكالية تحديد المسؤولية الجزائية عن المضامين المضرة، يقتضي منا التمييز بين الوسطاء في خدمة الأنترنت، وتبيان كل دور فيهم، إلا أنه ولما كان الوسيط الفني طرفا من أطراف التعامل الإلكتروني، يتقاسم معه صفته كوسيط، متدخل آخر أدرجت الكثير من الدراسات بحث مسؤوليتة مع الوسيط الفني، ولرفع اللبس بينهما فضلنا أن نقوم بتمييز وتحديد أطراف التعامل الإلكتروني بداية.

الفرع الأول

تصنيف أطراف التعامل الإلكتروني

لقد تعددت التصنيفات التي أوردها الفقه لأطراف التعامل الإلكتروني، فالبعض يصنفهم معتمدا على كيفية مسار المعلومة، والبعض يدخل أي شخص يقوم بالإتصال بالأنترنت، والبعض يصنفهم تصنيف تقني يوضح أقسام التقنيين، في حين يصنفهم البعض الآخر مهملا دور الوسيط بينهما، والبعض يدخل أطرافا ليست من التعامل الإلكتروني كما هو الشأن بالنسبة للشاحن ناقل الأشياء عن طريق الوسائل التقليدية[1].

إن فصل التشابك بين المتدخلين في التعامل الإلكتروني يتم على أساس تقسيمهم إلى أطراف حسب نوعية الأعمال التي يقومون بها.

ومن هنا برز دور قانون الأونسترال النموذجي بشان التجارة الإلكترونية ليصنف أطراف التعامل الإلكتروني إلى فئات هادفا من ذلك تحديد من تسند إليه رسالة المعلومات–**المستند الإلكتروني**[2]–، ومن يتحمل مسؤولية مافيها من معلومات، فقسمهم إلى (منشيء– مرسال إليه– ووسيط)، أما قانون الأونسترال الموذجي بشان التوقيعات الإلكترونية فقد تضمن ثلاث أطراف أيضا وهم (الموقع –مقدم خدمات التصديق– المعتمد)، والسبب وراد تغير أطراف التعامل الإلكتروني بين القانونين هو نظرة كل منهما للجهة التي نظر من خلالها كل منهما إلى المستند، فالأول عالج المستند الإلكتروني من ناحية من يسند إليه، أما الثاني فعالج وضع المستند من ناحية توثيق إرتباطه بمن أرسله، وقد نظرا هاذين القانونين عند التصنيف للعمل الذي يقوم به المتعامل الإلكتروني ودوره فيه، وهو هدف أساسي لكل أنظمة التعاملات الإلكترونية.

---

[1]- أنظر في هذه التقسيمات لدى: **سعيد بن محمد الغافري**، التعويض في التعامل الإلكتروني–دراسة في النظام السعودي مع التأصيل و المقارنة–رسالة دكتوراه فلسفة في العلوم الأمنية ، جامعة نايف العربية للعلوم الأمنية، الرياض، 2012، ص118 وما بعدها.

[2]-المستند الإلكتروني هو" **معلومات لها اهمية أو قيمة قانونية يتم نشاءها أو إرسالها أو إستلامها أو تخزينها أو غير ذلك من العمليات المتصلة بها بطريقة إلكترونية أو بأية وسيلة أخرى مشابهة، مصحوبة بتوقيع الكتروني.**

وعندما إتجهت الدول إلى سن تشريعاتها المتعلقة بالتعاملات الإلكترونية، إعتمدت التصنيف الوارد في قانوني الأونسترال النموذجي بدمجهما ليظهر أطراف التعامل الإلكتروني في 3 فئات رئيسية: المنشئ– المرسل إليه–ووسيط بينهما، وفي النقاط التالية تفصيل لكل من هؤلاء الأطراف.

أولا– المنشيء والمرسل إليه

أ–المنشيء

يشير مصطلح المنشيء إلى الطرف الذي يرسل تعامل الكتروني، وعمليا فإنه في التراسل الإلكتروني هناك من يرسل رسائل الكترونية في فضاء الأنترنت دون تحديد منه لجهة معينة، كما أن هناك من يرسل إلى شخص محدد ولكن ليس بقصد إنشاء تعامل معه. ولذلك فالمنشيء للرسائل الإلكترونية على نوعين: قسم لا علاقة له بنظم وقوانين التعاملات الإلكترونية وقد أسماه البعض[1] بالمنشئ غير التعاملي، والآخر تقصده تلك النظم و يسمى "**المنشيء**".

والمنشيء غير التعاملي هو الشخص الذي ينشر خارج إطار التعاملات الإلكترونية محتويات بوسائل الكترونية. أما المنشئ فقد عرفه قانون الأونسترال النموذجي بشان التجارة الإلكترونية بموجب الفقرة ج من المادة 02 بأنه الشخص الذي يعتبر أن إرسال أو إنشاء رسالة المعلومات قبل تخزينها، إن حدث قد تم على يديه أو نيابة عنه، ولكنه لا يشمل الشخص الذي يتصرف كوسيط فيما يتعلق بهذه الرسالة[2].

والمنشيء كونه يقوم بفعل إجابي فقد تضمن التزاما منه كالتزامه بالشفافية وفقا لمقتضيات حسن النية التي يقتضيها بث الثقة في التعاملات الإلكترونية، وأن يدلي إلى مقدم الخدمة بالمعلومات الصحيحة المتعلقة بهويته[3]. ويترتب بالطبع على عمله مسؤولية جنائية في حالة ما إن نسب إليه عملا يعد جريمة.

ويشير مصطلح "**شخص**" إلى كون أن المنشيء قد يكون شخص طبيعي أو معنوي، كما أن المشرع قد أزال اللبس الذي يمكن أن يقع فيه المرسل اليه حين تلقيه رسالة المعلومات من قبل الوسيط، فالرسالة تعتبر صادرة من المنشيء ولو وصلت له عن طريق الوسيط. ويكون دور هذا الوسيط هو نقل الرسالة وقد يسأل مسؤولية جزائية في حالة إرتكابه فعل يعتبر جريمة، وهذه المساءلة تعد من بين الوسائل القانونية لحماية التعاملات الإلكترونية[4].

---

[1]–**سعيد بن محمد الغافري**، المرجع السابق، ص122.

[2]-Article 2 alinéa C dispose que Le terme “expéditeur” désigne la personne par laquelle, ou au nom de laquelle, le message de données est réputé avoir été envoyé ou créé avant d’avoir été éventuellement conservé, mais non la personne qui agit en tant qu’intermédiaire pour ce message;

[3]–**سليمان عبد الحميد عثمان محمد**، مسؤولية مزود الخدمة المعلوماتية في القانون البحريني، بحث ضمن كتاب: المعاملات الرقمية و قانون الأنترنت، منشورات المنظمة العربية للتنمية الإدارية، القاهرة، مصر، 2006، ص168.

[4]–**د. عبد الفتاح بيومي حجازي**، التجارة عبر الأنترنت، المرجع السابق، ص115.

ب- المرسل اليـــه

عرفه قانون الأونسترال النموذجي بشأن التجارة الإلكترونية بموجب الفقرة د من المادة 02 الشخص الذي قصد المنشيء أن يتسلم رسالة المعلومات، ولكنه لا يشمل الشخص الذي يتصرف كوسيط فيما يتعلق بهذه الرسالة[1].

وعليه فالمرسال إليه هو شخص محدد بعينه قصد المنشيء وصول رسالته اليه، فقد يكون مستهلك أو منتج، وكما سبق تعريف المنشيء فإنه يخرج من عداد المرسل اليه الوسيط، كونه واسطة في انتقال الرسالة وليس مقصودا بمحتواها.

ثانيا- الوسيـــــط

إذا كانت بعض التعاملات العادية تتطلب تدخل وسيط لإتمامها كما هو شأن الوسطاء الماليين أو وسطاء النقل أو السماسرة...، فإن التعامل الإلكتروني في حاجة لوسطاء أكثر من التعامل العادي، كون التعامل يتم عن بعد وعبر وسائل إلكترونية مما يثير مسألة الجهالة بالطرف الآخر، وهو ما يتطلب وسيط يطمئنان إليه.
تنحدر كلمة وسيط 'intermédiaire من أصل لاتيني intermedius ، وهي تعني من يكون الوسط بين حدودين. كما تختص أيضا بمن يكون في موضع وسط بين شيئين، كرابط أو كنظام إنتقالي بحيث يؤمن لهما التواصل[2].

وقدعرفه قانون الأونسترال النموذجي بشأن التجارة الإلكترونية بموجب الفقرة ه من المادة 02على أنه الشخص الذي يقوم نيابة عن شخص آخر بإرسال أو إستلام أو تخزين رسالة المعلومات أو بتقديم خدمات أخرى فيما يتعلق برســـالة المعلومـــات هذه[3].

والوسيط على النحو السابق بيانه على فئتين: **الفئة الأولى** وتشمل الوسطاء النظاميين، **الفئة الثانية: :** تشمل الوسطاء الفنيون [4].

أ- الوسطاء النظـــاميون

هؤلاء هم القسم الثاني من الوسطاء في التعامل الإلكتروني، ويسمى وسيط نظامي أو قانوني لأن له أثرا في المركز القانوني للأطراف، فمعيار التمييز بينه وبين الوسيط الفني هو تخصصه في واسطة تعامل الكتروني قانوني وليس فني، ذلك أن هذا الدور الأخير منوط بالوسيط الفني[1].

---

[1]- Article 2alinéa d dispose que Le terme "destinataire" désigne la personne qui, dans l'intention de l'expéditeur, est censée recevoir le message de données, mais non la personne qui agit en tant qu'intermédiaire pour ce message;:

[2]- http://www.larousse.fr/dictionnaires/francais/interm%C3%A9diaire/43741?q=intermediaire#43662

[3]- Article 2 alinéa é dispose que Le terme "intermédiaire" désigne, dans le cas d'un message de données particulier, la personne qui, au nom d'une autre, envoie, reçoit ou conserve le message ou fournit d'autres services afférents à celui-ci; f) Le terme "système d'information" désigne un système utilisé

[4]-**سعيد بن محمد الغافري**، المرجع السابق ، ص 135، **د. محمد حسين منصور**، المرجع السابق، ص22، **فاروق محمد الأباصيري**، عقد الإشتراك في قواعد المعلومات عبر شبكة الأنترنت ، دراسة تطبيقية لعقود التجارة الإلكترونية الدولية، دار النهضة العربية ، القاهرة، 2003، ص9.

وبالرجوع لقوانين التعاملات الإلكترونية، نجد نوعان من المتدخلين يمكن أن ينطبق عليهما معنى وسيط نظامي أو قانوني وهما: **مقدم خدمة التصديق، الوسيط الإلكتروني.**

1-مقدم خدمة التصديق

تحظى التعاملات الإلكترونية بأهمية قصوى، حيث أن الهاجس الأول والأخير في هذا النوع من التعاملات هو الثقة والأمان، هذان العنصران أهم الضمانات التي يتعين توافرها لإزدهار هذه التعاملات. ولتحديد هوية المتعاملين وكذا حقيقة التعامل ومضمونه، فقد إستلزم ذلك وجود طرف ثالث محايد موثوق به، يقوم بطرقه الخاصة بالتأكد من صحة صدور الإرادة التعاقدية ممن تنسب إليه، والتأكد من جدية هذه الإرادة وبعدها عن الغش والإحتيال، بما يسمح بتوثيق التعامل الإلكتروني وتحديد هوية المتعاملين وتحديد حقيقة التعامل ومضمونه[2].

ويتمثل هذا الطرف المحايد في جهة مختصة-طبيعية أو معنوية-وظيفتها توطيد العلاقات وتوثيقها بين الأشخاص الذين يعتمدون على الوسائط الإلكترونية خاصة شبكة الأنترنت في إبرام تصرفاتهم. تعمل هذه الجهة بترخيص من السلطات المختصة في الدولة وتحت إشرافها، ضمن أحكام تحدد نظامها وماهية الواجبات الملقاة على عاتقها ومدى مسؤوليتها عن الأضرار التي تلحقها بالمتعاقدين أو الغير.

2-الوسيـــط الإلكترونـــي[3]

لقد أدى التطور الهائل في ثورة الإتصالات والمعلومات إلى ظهور الوسيط الإلكتروني في التعاملات الإلكترونية، وأصبح واقعا إمكانية إجراء التعامل فيما بين الإنسان والآلة، أو بين الآلة والآلة، ووفقا لذلك يستطيع جهاز الحاسوب أن يبرم تعامل الكتروني مع إنسان أو مع جهاز حاسوبي آخر، فيصبح بذلك وكيلا إلكترونيا يبرم العقود والتعاملات الإلكترونية. وبناء على ذلك سمي وسيط نظامي، لأنه ينسق بين طرفين تلقائيا دون تدخل من أي إنسان، معتمدا على البرمجة السابقة له[4].

وتجدر الإشارة إلى أن فكرة البرامج القادرة على التصرف ليست فكرة حديثة الظهور، إذ أنها ترجع في ظهورها إلى منتصف الخمسينات من القرن الماضي، حيث تم إبتداع برامج الذكاء الإصطناعي، وهي برامج

---

[1]- **سعيد بن محمد الغافري** ، المرجع السابق، ص145.

[2]- **د. إبراهيم الدوسقي ابو الليل**، الجوانب القانونية للتعاملات الإلكترونية، دراسة للجوانب القانونية للتعامل عبر أجهزة الاتصال الحديثة (التراسل الإلكتروني)، مطبوعات جامعة الكويت، 2003، ص272.

[3] - وسيط مؤتمت، وكيل إلكتروني هي مصطلحات أطلقت على الوسيط الإلكتروني في التعاملات الإلكترونية، وقد ظهر إستخدامه لأول مرة في وثائق لجنة الأمم المتحدة للقانون التجاري الدولي (الأونسترال) الصادرة باللغة العربية ، ثم استخدمته بعد ذلك بعض قوانين الدول العربية المعنية بالتعاملات الإلكترونية ومنها ، القانون الإتحادي رقم 1 لسنة 2006 بشان المعاملات والتجارة الإلكترونية(المادة 1) ، وكذلك القانون الأردني للمعاملات الإلكترونية (المادة 2) . بينما نجد بعض القوانين لم تستخدم هذا المصطلح مثل قانون التوقيع الإلكتروني الجزائري لسنة 2015، وكدا قانون التوقيع الإلكتروني المصري لسنه 2004

[4]-**د. عبد الفتاح بيومي حجازي**، التجارة عبر الأنترنت، المرجع السابق، ص132.

ومن أمثلة ذلك: شراء تذاكر من شركة الطيران عن طريق موقعها على الأنترنت، أن يطلع على مواعيد الرحلات وعلى ثمن التذكرة، ويقوم بحجز مقعد في الطارة ويدفع المقابل المادي بإحدى وسائل الدفع الإلكترونية، ثم يستلم تذكرة السفر ويطبعها لديه في منزله، فتنشا في هذه الحالة علاقة تعاقدية بين الشخص الطبيعي والوسيط الإلكتروني .**د. خالد ممدوح ابراهيم**، إبرام العقد الإلكتروني، مرجع سابق، ص208.

تتسم بخصائص معينة تميزها عن غيرها من البرامج، يمكن أن تعمل دون أن تخضع لسيطرة الإنسان وتدخلـــه المباشـــر[1].

ويتوقع من الأجيال المتطورة للحواسيب والتي من الممكن أن تظهر بفعل التقدم التكنولوجي أن يعمل الوسيط الإلكتروني بشكل مستقل وأن يعدل حسب مقتضى الأحوال من التعليمات التي تمت برمجته بها من قبل الشخص الذي يعمل لحسابه، وبناء عليه أدرجت البعض من التشريعات المنظمة للتعاملات الإلكترونية نصوصا تحدد، خصائصه وحدود تعاملاته ونسبة هذه التعاملات للشخص الطبيعي مبرمج الجهاز[2].

إهتم البعض من الفقه بدراسة هدا الوسيط المؤتمت محاولين وضع تعريف مناسب له يتلائم مع طبيعته، فقد عرفه البعض[3] على أنه برنامج الكتروني معد ليتصرف نيابة عن شخص معين، والبعض[4] الآخر يعرفه بأنه برنامج من برامج الحاسب الآلي يتميز بخصائص أربعة في عمله هي الإستقلالية والقدرة على التعامل مع غيره من البرامج أو الأشخاص والقدرة على رد الفعل والمبـــادرة. وقد تبنى البعض من المشرعين التعريف الثاني للوسيط، وهو حال المشرع الإماراتي في قانون المعاملات والتجارة لسنة 2006 في المادة الأولى منه[5].

يتضح من التعريفات السابقة أنها لم تتفق على مفهوم موحد له، فالبعض بنى التعريف على الخصائص الذاتية للوسيط، والبعض الآخر عرفه من خلال المهمة التي يقوم بها، ولا يكتمل التعريف إلا بالجمع بينهما، وبناء على ذلك يمكن تعريفه على أنه" ***برنامج معين يقوم بعمل نيابة عن الشخص الذي يستخدمه، و يكون له في قيامه بهذا العمل قدر من الإستقلالية والقدرة على التفاعل مع الآخرين ورد الفعل والمبادرة" .***

ومن أمثلة الوسطاء النظاميين الذي يتم إستخدامهم لغرض التفاوض الوكيل Tête-à-Tête المطور من قبل معهد ماساشوستس للتكنولوجيا، والوكيل Kasbah المطور من قبل نفس المعهد والذي يتدخل في إبرام العقد[6].

ب- الوسطاء الفنيـــون

---

[1]- **Emily M.Weitzenboeck**, Electronic Agents and the Formation of Contracts,Available at: http://128.176.101.170/eclip/documentsII/elecagents/contract_formation.pdf

آلاء يعقوب النعيمي، الوكيل الإلكتروني مفهومه وطبيعته القانونية، مجلة جامعة الشارقة للعلوم الشرعية و القانونية، المجلد 7، العدد2، يونيو 2010، ص153.

[2]– **سعيد بن محمد الغافري**، المرجع السابق، ص155، د. **خالد ممدوح إبراهيم**، التعاقد عبر الوكيل الإلكتروني، مقال متاح على الموقع الإلكتروني التالـــــــي:

http://kenanaonline.com/users/basune1/posts/804329.

[3] - Building an agent, A strategy white paper written for IBM, Available at: http://www.devx.com/assets/download/14089.pd

[4]Lenny Foner, Agent and Appropriation, Available at: http://foner.www.media.mit.edu/people/foner/Julia/Julia.html -

[5] – حيث عرفت المادة 1 من القانون الإتحادي الوسيط الإلكتروني المؤتمت على أنه "برنامج أو نظام إلكتروني لوسيلة تقنية المعلومات التي تعمل تلقائيا بشكل مستقل كليا أو جزئيا دون إشراف من أي شخص طبيعي في الوقت الذي يتم فيه العمل أو الإستجابة له.

[6]– حول أنواع الوسيط النظامي انظر: **آلاء يعقوب النعيمي**، المرجع السابق، 162.

إن تشغيل شبكة الأنترنت يتطلب تضافر جهود الوسطاء الفنيون، فمنهم من ينقل الخدمة عن طريق خطوط الإتصال، ومنهم من يمكن المستخدم من الوصول إلى الموقع، ومنهم من يخزن المعلومات أو ينتجها أو يوردها[1]، ولعل أهم هؤلاء الوسطاء الفنيون هم: متعهد الوصول إلى الشبكة، متعهد الإيواء، ناقل المعلومات. وهؤلاء تخصصهم فني وليس قانوني، ونظرا لكون دراستنا في هذا الباب تقتصر على الحماية الجزائية لآلية أداء التعاملات الإلكترونية، فإن تقرير مسؤولية الوسيط النظامي تخرج من إطار هذا الباب ونرجيء الحديث عنها في الباب الثاني عند دراسة مضمون التعاملات الإلكترونية.

الفـــرع الثاني

مهام الوسيط الفني في التعامل الإلكتروني

إن التعامل الإلكتروني يتطلب تشغيل الوسائل الإلكترونية وعلى رأسها شبكة الأنترنت، ولما كانت هذه الأخيرة عبارة عن أنشطة متعددة تشارك كل واحدة منها في عملية تشغيل أجهزة تخزين المعلومات وبثها وعرضها، فإنها تتطلب في المقابل أشخاص قائمين على هذا التشغيل، يطلق عليهم إسم "**الوسطاء في خدمة الأنترنت**"، ويعرفهم جانب من الفقه[2] على أنهم "كل مقدم خدمة الذي يسمح بإتصال الأطراف أو تسهيل المعاملات بينهما، على الأنترنت، كما يسهل إستضافة، إرسال وفهرسة المحتوى والمنتجات والخدمات على هذه الشبكة.

ينحصر دورهم في تمكين المستخدم من الدخول إلى شبكة الأنترنت والتجول فيها والإطلاع على مايريد[3]. وهؤلاء دورهم فني بحث قائم على التعاطي مع الأجهزة والبرامج وتشغيلها، وليس قائما على التوثيق والتصديق، ذلك أن هذا الدور الأخير منوط بالوسطاء النظاميين.

وإن كان لكل وسيط فني وظيفته، إلا أن التـــطور التقني يؤدي أحيانا إلى تشابك الأدوار، فالوسيط التقني يمكنه أن يجمع عدة وظائف، وفيما يأتي سيتم تناول أنواع هؤلاء الوسطاء من خلال النقاط التالية.

أولا–متعهد الوصول إلى الشبكة

[1]– د. **محمد حسين منصور**، المرجع السابق، ص150.

[2]-. **Blandine Poidevin**,La responsabilité des intermédiaires de l'Internet au vu du rapport Lescure, article disponible en lingne á l'adresse suivante http://www.jurisexpert.net/la-responsabilite-des-intermediaires-de-linternet-au-vu-du-rapport-lescure/

[3]-أنظر:**د.عبد الرحمن عبد الله السند**، الأحكام الفقهية للتعاملات الإلكترزنية، الطبعة الثالثة، دار الوراق، الرياض، 2006. ص87. د. **عبد الفتاح بيومي حجازي**، النظام القانوني لحماية التجارة الإلكترونية، الحماية الجنائية لنظام التجارة الإلكترونية، المرجع السابق، ص134. **د. جميل عبد الباقي الصغير**، الأنترنت والقانون الجنائي، الأحكام الموضوعية المتعلقة بالأنترنت، دار الفكر العربي، القاهرة، 2001، ص115.

متعهد الوصول إلى الشبكة هو من مراكز التوزيع التي تتألف منها الأنترنت، وهو موصول بالشبكة بإستمرار، فهو الممر الإلزامي لوصول المستخدم إليها، إعتبره البعض من الفقه نقطة وصول وترحيل إلى الأنترنت[1]. وبصفته متعهدا، يلتزم تقنيا بوصل المستخدمين بالشبكة من خلال أجهزة الكمبيوتر العائدة اليهم بواسطة موديم.

عرفه المشرع الجزائري بموجب الفقرة د من المادة 2 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها على أنه "أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الإتصال بواسطة منظومة معلوماتية و/أو نظام للإتصالات. كما حددته المادة 9 من القانون الفرنسي رقم 2004 -575 المتعلق بالثقة في الإقتصاد الرقمي على أنه الشخص الذي يؤمن نشاطه خدمة التوصيل بشبكة إتصالات الكترونية[2].

مما تقدم نستنتج أن متعهد الوصول يقوم بدور فني بحث في توصيل العميل إلى شبكة الأنترنت، بمقتضى إتفاق بينهما، فهو لا يقدم المعلومة أو محتوى المواقع الإلكترونية بل تقتصر مهمته على إيصال المستخدم إلى الأنترنت عن طريق أجهزته الخاصة[3]. وعمله على النحو السابق بيانه أقرب من عمل الموزع في الصحافة المكتوبة[4].

ثانيا-متعهد خدمة الإيواء

هذا المزود هو من أكثــر المزودين الذين تتجه اليهم الأنظار، لأنه يؤمن مسافة على الشبكة لنشر المضامين التي قد تكون غير مشروعة والمضرة بالغير. وقد حدده المشرع الفرنسي بموجب المادة 6 من القانون رقم 2004-575 على أنه كل شخص طبيعي أو معنوي يقدم -ولو مجانا- خدمات بواسطة وسائل الإتصال عبر الخط: تخزين الرموز والكتابات والصور والأصوات أو الرسائل أيا كانت طبيعتها لفائدة مستعملي هذه الخدمات[5]. يشمل التحديد الأخير جميع الأشخاص الذين يؤمنون التخزين ولو بطريقة ثانوية[6].

---

[1]- Valérie Sédallian Droit de l'Internet: réglementation, responsabilités, contrats, Collection Association des utilisateurs d'Internet, Éd. Net Press, 1997,p123.

[2]- fourniture d'accès à un réseau de communications électroniques, Article L32-3-3 duCode des postes et des communications électroniques, Créé par **Loi n° 2004-575 du 21 juin 2004 – art 9 JORF 22 JUIN 2004 pour la confiance dans l'économie numérique.**

[3]-**د. عبد الفتاح بيومي حجازي**، الجرائم المستحدثة في نطاق تكنولوجيا الإتصالات الحديثة، المركز القومي للإصدارات القانونية، القاهرة، 2011، ص94.

[4]-**اكمل يوسف السعيد يوسف**، المسؤولية الجنائية لمقدمي المواد الإباحية للأطفال عبر الأنترنت، مجلة البحوث القانونية والإقتصادية، كلية الحقوق جامعة المنصورة، 2011، ص 32.

[5]- Art 6-1-2 du **Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.** Modifié par**LOI n° 2016-444 du 13 avril 2016 visant à renforcer la lutte contre le système prostitutionnel et à accompagner les personnes prostituées**

[6]- **د. اودين سلوم الحايك**، المرجع السابق، ص42.

فالإستضافة هي عملية تخزين مستمرة للمعلومات على ملقمات المورد المضيفة تؤدي الى جعل المعلومات جاهزة للإسترجاع وبمتناول الأشخاص الذين يرغبون في الإطلاع عليها[1].

وقد عرفه المشرع الجزائري بموجب الفقرة 2/د من المادة 2 من القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ومكافحتها على أنه أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الإتصال أو لمستعمليها.

وعمل المتعهد على النحو السابق بيانه يتشابه إلى حد كبير بعمل مدير التحرير في الصحف المكتوبة الذي يخصص مساحة إعلانية لإعلانات شركة معينة[2].

مما سبق نخلص إلى أن متعهد الإيواء يعتبر بمنزلة المؤجر لمكان على الشبكة، إذ يعرض صفحات الواب على حاسباته، ويكون للمستأجر حرية نشر ما يشاء أو إنشاء مواقع الكترونية[3]، مع تمكينه من الوصول إليها بواسطة الأنترنت في كل الأوقات عن طريق ما يتم توفيره من وسائل تقنية وإعلامية.

ويذهب البعض إلى إعتبار العقد الرابط بين مزود المأوى والمشترك بمثابة عقد ايجار، حيث يقوم مزود المأوى بكراء بعض الفضاءات على موزعه لكل من يريد خزن المعلومات فيها[4]. والعقد المبرم بينهما يسمى عقد الإيجار المعلوماتي وهو عقد بمقتضاه يضع مقدم الخدمة تحت تصرف المشترك بعض إمكانيات أجهزته أو أدواته المعلوماتية على شبكة الأنترنت"[5].

ثالثا- ناقــل ومورد المعلــومات

إن ناقل المعلومة يتولى مهمة النقل المادي لها بوسائله الفنية، بحيث يقوم بالربط بين الشبكات، تنفيذا لعقد نقل المعلومات بين الحاسبات المرتبطة بمواقع الأنترنت أو بمستخدي الشبكة، وتتولى تلك المهمة عادة شركات الهاتف وشركات الخدمات اللاسلكية[6]، مثل **شركة الإتصالات الجزائرية** التي تقوم بمهمة ناقل المعلومات في الجمهورية الجزائرية. وينحصر دور الناقل في تأمين نقل المعلومة والربط بين الوحدات المختلفة، ولذلك فمن المفترض كقاعدة عامة عدم مراقبته أو علمه بالمعلومات التي تعبر الشبكة بواسطته[7].

---

[1]- TGI Nanterre, 1ère ch. A, 8 décembre 1999, Lynda Lacoste c. Multimania et autres, disponible à l'adresse suivante : http://www.juriscom.net/txt/jurisfr/img/tginanterre19991208.htm.

[2]**- STROWEL (A.) et IDE (N.)** Responsabilité des intermediaries: actualités, législatives ET jurisprudantielles,Droit et Nouvelles Technologie. P. 10. disponible en lingne á l'adresse suivante; http://www.droittechnologie.org 28/12/2010

[3]- **د. عبد الفتاح بيومي حجازي**، الجرائم المستحدثة في نطاق تكنولوجيا الإتصالات الحديثة، المرجع السابق، ص100.

[4] – **د. اللومي عبد الرؤوف**، المسؤولية التقصيرية على شبكة الأنترنات، المجلة القانونية التونسية ، مركز النشرالجامعي، تونس، 2007، ص66.

[5] –**د. خالد ممدوح إبراهيم**، إبرام العقد الإلكتروني، المرجع السابق، ص105. أكثر تفاصيل عن عقد الإيجار المعلوماتي انظر: **عبد المهدي كاظم ناصر، حسين عبيد شعواط**، عقد الإيواء المعلوماتي، مجلة الكوفة للعلوم القانونية والسياسية , العدد 21، جامعة الكوفة، 2014.

[6]– **د. محمد حسين منصور**، المرجع السابق، ص166 ، **د. جميل عبد الباقي الصغير**، الأنترنت والقانون الجنائي،المرجع السابق ، ص159.

[7]-Voir article L34 duCode des postes et des communications électroniques , Modifié par **Loi n° 2005-516 du 20 mai 2005 relative à la régulation des activités postales.**

أما مورد المعلومة فهو شخص طبيعي أو معنوي يتوسط بين مؤلف مضمون الموقع ومستخدم الأنترنت الذي يرغب في الإطلاع على ذلك الموقع، فهو يقوم بتحميل النظام بالمعلومات التي قام بتأليفـــها أو جمعها حول موضوع معين، أي أنه يتولى الإختيار والتجميع والتوريد للمادة المعلوماتية حتى تصل إلى الجمهور عبر الشبكة[1].

رابعا- موردي المحتوى المعلوماتي

هو الذي يغدي الشبكة بالمعلومات، فهو أهـــم أشخاص الأنترنت على الإطلاق سواء أكان هو منتج المعلومة أم مصدرها أم مؤلفها، أم كان مجرد صاحب حق في نشرها وبثها عبر الأنترنت، فقد يكون شخصا عاديا وقد يكون مهنيا، متخصصا في جمع المعلومات وتزويد الشبكات بها ويتحمل عبء إنشاء وجمع المعلومات المتعلقة بموضوع معين. لذلك فهو المسؤول الأول عن تلك المعلومات التي يتم بثها بواسطة الشبكة[2].

والواقع أنه يمكن أن يتولى القيام بوظائف عدة، فبالإضافة إلى وظيفته الأصلية كمنتج للمعلومات ومذيع لها، فهو يمتلك أيضا أجهزة خدمة الوصول، وهو كمحترف إنتاج وبث المعلومات يمكن أن تثور مسؤوليته، بحسب الأحوال عن المعلومات المزيفة والناقصة والمشينة أو الفاضحة التي يعدها وينشرها على موقعه[3].

يتضح لنا مما سبق أن مفهوم الوسيط الفني لا يطلق على مسمى واحد، فلكل متدخل معنى ومفهوم وتعريف مغاير عن الآخر، فضلا عن دور وطبيعة عملهم المختلفة من جهة وتشابكها أحيانا من جهة أخرى، وإن كانت المسؤولية الجزائية في معناها الأعم الأشمل على تعبير عن ثبوت نسبة الوضع الإجرامي للواقعة المادية التي يجرمها القانون إلى الشخص الذي إرتكب الجريمة أو ساهم في إرتكابها[4] ، فهو الأمر الذي يثير إشكالية بيان مدى **مسؤولية كل منهم عن السلسة المعلوماتية المتواصلة عبر الشبكة؟**

المطلب الثاني

تقرير المسؤولية الجزائية للوسيط الفني وفق النصوص القائمة

إن هناك شبه إجماع على أن المسؤولية عن نشر المعلومات غير المشروعة يتحملها الطرف الذي قرر نشر تلك المعلومات على شبكة الأنترنت[5]، لكن هذا الحل الأولى سرعان ما يتلاشى إذا ما علمنا أن تحديد

---

[1]- د. **محمد حسين منصور**، المرجع السابق، ص168.

[2]– **د. عايد رجا الخلايلة**، المسؤولية التقصيرية الإلكترونية،دار الثقافة للنشر والتوزيع، عمان، 2009 ، ص58.

[3]–**د. محمد حسين منصور**، المرجع السابق، ص182. **ماء العينين السعداني**، الإطار القانوني للمصادقة على التعاملات الإلكترونية، مجلة قانون وأعمال، العدد الثاني، دجنبر، 2011 ، ص113.

[4]–**د. أحمد عوض بلال**، الجرائم المادية، المسؤولية الجنائية بدون خطأ، دراسة مقارنة، دار النهضة العربية، القاهرة، 1993، ص45.

[5]- **Pierre. TRUDEL**, La responsabilité sur Internet, texte préparé pour le séminaire *Droit et Toile*, Bamako, organisé par l'UNITAR (Institut des Nations unies pour la formation et la recherche), en association avec OSIRIS (Observatoire sur les Systèmes d'Information, les Réseaux et les Inforoutes au Sénégal) et l'INTIF (Institut francophone des nouvelles

الطرف المتسبب في النشر يعتبر أمرا صعبا في العالم اللامادي، وأمام هذا الوضع لا يبقى إلا قيام المسؤولية ضد الوسطاء الفنيين الذين يمكن تحديدهم بسهولة، رغم أن تدخلهم على الشبكة لم يكن إلا لإيصال المعلومات بشتى أنواعها إلى المستعمل[1].

إن عدم تنظيم المشرع لهذه المسألة قد جعل باب الإجتهاد مفتوحا أمام الفقهاء ليخوض كل منهم في أغوار هذه المسألة، فهناك من دعا إلى إعفائهم من المسؤولية كون أن وظيفتهم تقنية بحتة ولإستحالة مراقبة المعلومات التي يكونون طرفا فيها، وهناك من طالب بإقامة مسؤوليتهم في كل الحالات[2]. وبين هذا وذاك نرى أنه كلما تشددنا في إقامة مسؤولية مزودي ووسطاء الأنترنت زاد حرصهم على فرض الرقابة الذاتية على المعلومات لدرء المسؤولية عنهم، بالمقابل كلما تجاهلنا إقامة مسؤولية هؤلاء المزودين أدى ذلك إلى وجود أكبر للمعلومات غير المشروعة على الشبكة، وإزداد تبعا لذلك تقاعس المزودين عن إستخدام الوسائل اللازمة للحد أو لمنع إنتشار المعلومات[3].

لم يقف القضاء حين عرض هذا النوع من المسائل عليه مكتوف الأيدي تجاه تقرير مسؤولية الوسيط الفني، وكذلك فعل الفقه، وذلك بمحاولة تحديد مسؤوليته وفقا لطبيعة العمل الذي يؤديه، وبصفة خاصة مدى الرقابة التي يمكن أن يقوم بها على المحتويات غير المشروعة التي تتم عبر الخدمة التي يقدمـــها.

لكن السؤال المطروح في هذا الصدد: **هل أن القواعد القانونية الموجودة تكفي لتاطير المسؤولية الجزائية على الشبكة العنكوتية ام انه يجب سن قواعد جديدة؟**

في فرنسا وقبل صدور القانون رقم 2000-719[4] المعدل لأحكام قانون حرية الإتصالات، أثير تســاءل حول إمكانية تطبيق نظام النشر الصحفي والذي يأخذ بنظام **المسؤولية التتابعية**[5] عن الجرائم الصحفية على عمل موردي خدمات الأنترنت؟ وبالنتيجة مامدى جدوى هذا الحل المستقى في هذا الصدد؟

---

technologies de l'information et de la formation) de l'Agence intergouvernementale de la Francophonie Bamako, 27 mai 2002, p17.*disponible en lingne á l'adresse suivante*:
http://pierretrudel.chairelrwilson.ca/cours/drt6929f/Resp.internet-trudel.pdf

[1]- **Olivier cachard** , droit du commerce electronique , RDAI, N 3,2004,P394.

[2]-انظر: **اللومي عبد الرؤوف**، المرجع السابق، ص49.

Pierre. TRUDEL, OP,CIT, P02.

[3]-انظر: **د.عايد رجا الخلايلة**، المرجع السابق، ص22، **محمد عرسان ابو الهيجا، علاء الدين فواز الخصاونة**، المسؤولية التقصيرية لمزوي خدمات الأنترنت عن المحتوى غير المشروع، دراسة في التوجيه الأروبي الخاص بالتجارة الإلكترونية، مجلة الشريعة والقانون، العدد الثاني والأربعون، جامعة الإمارات العربية المتحدة، أبريل 2010، ص22.

[4]**- LOI no 2000-719 du 1er août 2000 modifiant la loi no 86-1067 du 30 septembre 1986 relative à la liberté de communication, JORF n°177 du 2 août 2000.**

[5]-المسؤولية التتابعية تعتبر من بين صور المسؤولية الجنائية المفترضة إلى جانب المسؤولية الجنائية عن فعل الغير، فهي نظام استثنائي من القواعد العامة في المسؤولية الجزائية، لأن المسؤولية فيها مفترضة، ويختلف اساس المسؤولية الجزائية بالتتابع عن اساس المسؤولية الجزائية عن فعل الغير، في أن أساس الأولى أن المساهم في ارتكاب الجريمة لا يعرف على وجه الدقة موقعه من احداث الواقعة الإجرامية: فاعل اصلي ام شريك...،اما بالنسبة لأساس المسؤولية عن فعل الغير انه لم يمكن التوصل إلى مرتكب الواقعة اصلا،ويرى البعض من الفقهاء ان هذا النظام من المسؤولية هو نظام استثنائي يخالف مبدا الشرعية الجزائية فيما هو مقرر بشان مبدا شخصية العقوبة، وفيما يتعلق بالمساهمة الجنائية، لأن القانون يفترض وجود مسؤولية جنائية تمت اقامتها على اساس وهمي مصدره القانون، و من ثم تعد نظاما استثنائيا، وكان يتعين وفقا للعدالة تطبيق القواعد العامة في المسؤولية بشانه، فالقانون في هذا النظام الإستثنائي يفترض وجود من هو مسؤول امامه عما ارتكب من جرائم.انظر: **د. رشدي محمد علي محمد عيد**، الحماية الجنائية الموضوعية للمعلومات عبرشبكة الأنترنت، دار النهضة العربية، القاهرة، 2013، ص370.

أصدر قسم التقارير والدراسات بمجلس الدولة تقريرا في شأن الأنترنت والخطوط الرقمية الذي وافقت عليه الجمعية العمومية للمجلس في 2 جويلية 1998، ومن بين ما تعرضه التقرير المسؤولية القانونية لمقدمي الخدمات الوسيطة بالأنترنت، حيث إستبعد تطبيق المسؤولية التتابعية عليهم كون الأنترنت يتسم بالتعقيد ولا يسمح بتطبيق أحكام هذا النوع من المسؤولية، مع تأكيده على تطبيق الأحكام العامة للقانون الجزائي بشأن الأعمال الوسيطة الخاصة بالأنترنت، مع الأخذ بعين الإعتبار معرفة المضمون غير المشروع وتوافر القصد الجنائي والإجراءات المتخذة لمراقبة النشاط والقدرة على المراقبة[1]. إلا أن هذا الموضوع قد حسم على خلاف ذلك على المستوى القضائي، بحيث قضت محكمة إستئناف باريس بمسؤولية الشخص الذي يقوم بايواء المواد المتعلقة بالأنترنت على أساس أن هذه الخدمة تدخل ضمن الخدمات السمعية البصرية، وأقامت مسؤوليته على أســـاس المسؤولية التتابعية والتي يفترض أنها تتعلق بجرائم الصحافة[2].

أما على المستوى الفقهي، فقد إنقسمت الآراء إلى إتجاهين. إتجاه يرى إعمال قانون الصحافة على البث من هذه الشبكة، حيث أن مزود الخدمة يقوم بالنشر فهو يتماثل مع ما يقوم به مدير التحرير في الصحف من قيامه بدور النشر، ومن تم مساءلة مزود الخدمة باعتباره مديرا للتحرير[3] على أساس **المسؤولية التتابعية**« responsabilité en cascade » التي تضمنها قانون الصحافة لسنة 1881 بمقتضى المادة 42 منه،[4]التي جعلت رئيس التحرير أو الناشر هو المسؤول أولا، فإذا لم يوجد تقع المسؤولية على المؤلف، فإن لم يكن فالطابع، فان لم يكن فالبائع أو الموزع أو ملصق الإعلانات بصفتهم فاعلين اصليين. وإذا كان رئيس التحرير أو الناشر معروفا فإنه يسال جنائيا كفاعل أصلي عن الجريمة، ويسأل المؤلف باعتباره شريكا[5].

1- Conseil detat: INTERNET ET LES RÉSEAUX NUMÉRIQUES, Etude adoptée par l'assemblée générale du Conseil d'État, section du rapport et des études, le 2 juillet 1998. Paris : La Documentation française, 1998. 266 p. ; 24 cm. (Les Études du Conseil d'État). ISBN 2-11-004102-1. ISSN 1152-4561. 95 F. voir le site: **HTTP://BBF.ENSSIB.FR/CONSULTER/BBF-1999-01-0125-009**

د. مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة، 2012، ص125 وما يليها.

[2]- CA paris, 10 février 1999,D.1999,jur.389,note Nathalie mallet –pourjol:disponible en lingne á l'adresse suivantehttp://fr.jurispedia.org/index.php/Responsabilit%C3%A9_des_interm%C3%A9diaires_techniques_de_l'internet_(fr),

[3] –**د. شيماء عبد الغني**، المرجع السابق، ص169.

[4]-Art 42 du **Loi du 29 juillet 1881 sur la liberté de la presse** , dispose que: " Seront passibles, comme auteurs principaux des peines qui constituent la répression des crimes et délits commis par la voie de la presse, dans l'ordre ci-après, savoir :
1° Les directeurs de publications ou éditeurs, quelles que soient leurs professions ou leurs dénominations, et, dans les cas prévus au deuxième alinéa de l'article 6, de les codirecteurs de la publication ;
2° A leur défaut, les auteurs ;
3° A défaut des auteurs, les imprimeurs ;
4° A défaut des imprimeurs, les vendeurs, les distributeurs et afficheurs.

وقد عارض القضاء الفرنسي تطبيق نص المادة 42 من القانون 29 جويلية 1881 على البث الإداعي والتلفزيوني أنظـــــــر:
Cour de cassation, chambre criminelle, 8 octobre 1979, n°77-92.297. Bulletin criminel chambre criminelle n°272 p.735.
وهو مادفع المشرع الفرنسي إلى وظع نظام خاص يتكيف مع الإتصال السمعي البصري، وهو القانون رقم 82–652 المتعلق بالإتصالات السمعية البصرية. وجاءت المادة 93 –3 لتتضم المسؤولية التتابعية.

[5]Art 43 du **Loi du 29 juillet 1881 sur la liberté de la presse** Modifié par Ordonnance du 26 août 1944, art 15 v. init., Modifié par Loi n°52-336 du 25 mars 1952 - art. 5 JORF 26 mars 1952

وقانون الإتصالات السمعية البصرية رقم 82-652 بمقتضى المادة 93-3 منه[1] التي نقلت نظام المسؤولية بالتتابع إلى النطاق السمعي البصري وفقا للترتيب التالي: مدير البرنامج أو مؤلف الرسالة واخيرا المنتج، ونفس الأمر بالنسبة لشبكة الأنترنت باعتبارها نظام سمعي بصري، بشرط أن تكون الرسالة غير المشروعة التي يجري بثها سابقة التخزين أي مسجلة قبل عرضها[2] ذلك انه إذا كانت مذاعة على الهواء فان رئيس التحرير لا يستطيع أن يمارس رقابة على الرسالة، فيسأل تبعا لذلك صاحب الرسالة باعتباره فاعلا اصليا. ولم ترى محكمة النقض الفرنسية في المسؤولية التتابعية ما يخالف مبدأ الأصل في البراءة[3].

أما الإتجاه الثاني، فرفض مساءلة مزود الخدمات على أساس المسؤولية المفترضة لمخالفتها لقرينة البراءة، مادام أنها تقيم قرينة قاطعة على مسؤولية رئيس التحرير وما يليه في سلم التسلسل[4].

واذا ما أردنا ترجيح أحد هذه الإتجاهات، فسوف نجد أنفسنا نوافق الرأي الثاني، إستنادا إلى أصل البراءة الذي يحتم أن تقوم النيابة العامة بإثبـــات الركن المادي والمعنوي في جانب المتهم حتى تقوم مسؤوليته، ولا يكلف المتهم باثبات براءته. فضلا على ذلك لا يصلح تشبيه سلسلة المتدخلين في مجال الأنترنت مع تلك المتوفرة في مجال الصحافة، فالطبيعة الفنية المعقدة لتقديم الخدمات عبر الأنترنت تجعل من تداخل أدوار الوسطاء الفنيين أمـــرا ممكنا، وعلى ذلك لا يمكن فصل الحلول القانونية عن الإعتبارات الفنية.

وإدراكا من المشرع الفرنسي لخصوصية عمل الوسيط الفني، تدخل بموجب القانون رقم 2000-719 المؤرخ في 1 اوت 2000 المعدل للقانون رقم 86-1067 المؤرخ في 30 سبتمبر 1986 المتعلق بحرية الإتصالات، حيث اضاف المادة 43 -8[5] والتي قررت عدم قيام المسؤولية المدنية أو الجزائية للأشخاص المعنوية أو الطبيعية التي تقوم بدون مقابل أو بمقابل بالتخزين المباشر والدائم لتضع تحت تصرف الجمهور إشارات أو كتابة أو صور أو أصوات أو رسائل كيفما كانت طبيعتها عن محتوى هذه الخدمات، إلا في

---

[1]- Art **93-3** du**Loi n° 82-652 du 29 juillet 1982 sur la communication audiovisuelle** dispose que: " Au cas où l'une des infractions prévues par le chapitre IV de la loi du 29 juillet 1881 sur la liberté de la presse est commise par un moyen de communication au public par voie électronique, le directeur de la publication ou, dans le cas prévu au deuxième alinéa de l'article 93-2 de la présente loi, le codirecteur de la publication sera poursuivi comme auteur principal, lorsque le message incriminé a fait l'objet d'une fixation préalable à sa communication au public.
A défaut, l'auteur, et à défaut de l'auteur, le producteur sera poursuivi comme auteur principal.
Lorsque le directeur ou le codirecteur de la publication sera mis en cause, l'auteur sera poursuivi comme complice.
Pourra également être poursuivie comme complice toute personne à laquelle l'article 121-7 du code pénal sera applicable.
Lorsque l'infraction résulte du contenu d'un message adressé par un internaute à un service de communication au public en ligne et mis par ce service à la disposition du public dans un espace de contributions personnelles identifié comme tel, le directeur ou le codirecteur de publication ne peut pas voir sa responsabilité pénale engagée comme auteur principal s'il est établi qu'il n'avait pas effectivement connaissance du message avant sa mise en ligne ou si, dès le moment où il en a eu connaissance, il a agi promptement pour retirer ce message.

[2]-د. **جميل عبد الباقي الصغير**، القانون الجنائي والأنترنت، المرجع السابق، ص129.

[3]-Crim,23 fev,2000,Rev.sec.crim.2000.p642

[4]-**د. شيماء عبد الغني**، المرجع السابق، ص 172.

[5]-« Art. 43-8.du **LOI no 2000-719 du 1er août 2000**–dispose que: Les personnes physiques ou morales qui assurent, à titre gratuit ou onéreux, le stockage direct et permanent pour mise à disposition du public de signaux, d'écrits, d'images, de sons ou de messages de toute nature accessibles par ces services, ne sont pénalement ou civilement responsables du fait du contenu de ces services que :
« - si, ayant été saisies par une autorité judiciaire, elles n'ont pas agi promptement pour empêcher l'accès à ce contenu ;
ayant été saisies par un tiers estimant que le contenu qu'elles hébergent est illicite ou lui cause un préjudice, elles n'ont pas procédé aux diligences appropriées »

حالتين: هما حالة عدم تنفيذ الأمر القضائي الصادر بإلزامه بمنع الوصول إلى هذا المضمون، وحالة ما إذا قدر الغير وجود مضمون غير مشروع أو من شأنه الإضرار بحقوقه، وعدم إتخاد الإجراءات اللازمة لمنع بث هذا المضمون رغم التنبيه عليه بذلك.

والملاحظ على هذا النص، أنه جعل الأصل هو مسؤولية الوسيط الفني، وإستثنى منه الحالتين سالفتي الذكـــر، وهو ما يمكن القول معه أن المشرع تبنى مسؤولية مخففة، كما أن النص جاء عاما فلم يميز بين المسؤولية المدنية والجزائية وهو ما يستشف من عبارة ".... ne sont pénalement ou civilement responsables ..." الواردة في المادة 43-8 ، ولم يبين شروط قيام المسؤولية الجزائية في حالة عدم قيام متعد الإيواء بإزالة المضمون غير المشروع، بناء على إخطار الغير حين يقدر هذا الأخير عدم مشروعية المضمون، فصياغة النص على النحو السابق بيانه خولت الأفراد سلطة تقدير ما يعد مشروعا ومالايعد كذلك، ورتبت المسؤولية الجزائية لمتعهد الإيواء حال إمتناعه عن إزالة المضمون أو منع وصـــول الجمـــهور إليه، رغم إخطار الغير له بذلك، وهو ما يخالف صراحة مبدأ الشرعية، الأمر الذي دعا المجلس الدستوري إلى القضاء بعدم دستورية الحالة الثانية[1].

ليقوم عام 2004 منتهجا في ذلك نهج التوجيه الأروبي رقم 2000-31 [2]، بتبني ضوابط قانونية خاصة ومتوازنة أرسى فيها النظام القانوني لمقدمي خدمات الإنترنت، من حيث تحديد طبيعة عملهم والتزاماتهم، ومسؤولية كل منهم في مواجهة السلسلة المعلوماتية المتواصلة عبر الشبكة.

المطلـــب الثـــالث

تقرير المسؤولية الجزائية للوسيط الفني بنصوص خاصة

لقد بدت الحاجة ماسة لإيجاد تنظيم تشريعي متكامل يُحدد المركز القانوني لمقدمي خدمات الإنترنت أو الوسطاء الفنيين في التعامل الإلكتروني، مبينامسؤولية كل منهم عمّا يُرتكب من أعمال غير مشروعة عبر الأنترنت، الأمر الذي لا يُمكن تكريسه إلا بتضافر جهود التشريعات على مختلف الأصعدة.

هذه الحقيقة كانت نواة عمل البرلمان الأُوروبي الذي تبنَّى بالإجماع في 8 حزيران 2000م التوجيه رقم 2000/31، والمتعلِّق "ببعض الأوجه القانونية لخدمات شبكات المعلومات، وبصفةٍ خاصَّة التجارة الإلكترونية، في السوق الداخلية والذي تمَّ تخصيص القسم الرابع منه لتنظيم المركز القانوني للوسطاء في خدمات الإنترنت، والتي سارت على هديه التشريعات الأروبية ومنها التشريع الفرنسي. فبهدف نقل القواعد الخاصة التي تبنَّاها المشرِّع الأُوروبي لتنظيم مسؤولية مقدمي الخدمات إلى تشريعه الداخلي، تبنَّى المشرِّع

[1]- V. la décision du Conseil constitutionnel n 2000-433 DC en date du 27 juillet 2000 ; JORF n°177 du 2 août 2000.

[2]-Directive 2000/31/CE du Parlement européen et du Conseildu 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur ("directive sur le commerce électronique") *Journal officiel n° L 178 du 17/07/2000 p. 0001 - 0016*

الفرنسي، قانوناً حول "الثقة في الاقتصاد الرقمي" رقم 2004-575 المؤرخ في 21 جوان 2004 والذي أنشأ مسؤولية مستقلة لمزودي خدمات الأنترنت بموجب المادة 5 إلى المادة 9 منه. وإعتبارا من هذا التاريخ أصبح لمقدمـــي خدمات الإنترنت في فرنسا نظامهم القانوني الخاص.

أما على صعيد التشريع الجزائري، فقد جاء قانون التوقيع الإلكتروني خالياً من أيِّ نصٍ يُعالج هذه المسألة. ولربما أنه عند إصدار هذا القانون، أراد مشرعنا التريُّث في تقنين المسألة لحين استقرارالحلول، ووضوح الرؤية، وتبيُّن أبعاد هذا المجال الذي يتسِّم بسرعة التطوُّر وبصعوبة تحديد الأدوار والأنشطة فيه. ومع اتضاح الرؤية، وفي ظل وجود العديد من التشريعات المقارنة التي عالجت هذه المسألة، تدخل المشرع مؤخرا بموجب القانون رقم 16-02 المعدل والمتمم للأمر رقم 66-156 والمتضمن قانون العقوبات[1] ليرسي بذلك بيئة تشريعية خاصة ومتوازنة ايمانا منه لخصوصية تقديم خدمات الوساطة على الإنترنت.

سنتطرق في هذا المطلب إلى موقف التشريع الأروبي والفرنسي(الفرع الأول) ثم التشريع الجزائري والمصري بشان المسؤولية الجزائية للعاملين في مجال الأنترنت(الفرع الثاني).

الفرع الأول

تقرير المسؤولية الجزائية للوسيط الفني في ظل التوجيه الأروبي والقانون الفرنسي

نصَّت المادة 6-1-3 من القانون الفرنسي حول "الثقة في الاقتصاد الرقمي: "أن أفعال مقدمي خدمات الإنترنت الخاطئة لا يُمكن أن تدخُل في نطاق التجريم إلاَّ إذا ثبت علمهم الفعلي بالمضمون الإلكتروني غير المشروع، وعلى الرغم من علمهم هذا لم يتخذوا الإجراءات اللازمة لشطبه، أو على الأقل لمنع وصول الجمهور إليه[2]. وهو بهذا جاء متفقاً بهذا الخصوص مع الاتجاه العام للتوجيه الأُوروبي حول "التجارة الإلكترونية"، حيث وضع التوجيه مبدأ عام هو عدم مسؤولية الوسيط الفني إلا في أحوال معينة، وبشروط خاصة، مع إهتمامهً في تحديد مسؤولية متعهدي الوصول والإيواء دون غيرهم من مقدمي خدمات الإنترنت، ولذلك يوصف نظام المسؤولية الذي تبناه بنظام "**عدم المسؤولية أو المسؤولية المشروطة**"[3].

أشار التوجيه بموجب المادة 43 أن مقدم الخدمة لا يسأل قانونا إذا كان عمله يقتصر على النقل أو التخزين، أي عندما لا يساهم بأية صورة كانت في المعلومات المنقولة وبما يفترض عدم تدخله في تعديلها، أما التدخل الفني الخاص بعملية النقل فلا يثير المسؤولية حيث أنه لا يمثل تدخل في المعلومات والمعطيات

---

[1]-قانون رقم 16-02 مؤرخ في 14 رمضان علم 1437 الموافق لـــ 19 يونيو سنة 2016، يتمم الأمر رقم 66-156 المؤرخ في 18 سفر عام 1386 الموافق لـــ 8 يونيو سنة 1966 و المتضمن قانون العقوبات، جريدة رسمية، عدد 37، مؤرخة في 22 يونيو سنة 2016.

[2]-Article 6-1-3 du LCEN Modifié parLOI n° 2016-444 du 13 avril 2016 visant à renforcer la lutte contre le système prostitutionnel et à accompagner les personnes prostituées. dispose que "Les personnes visées au 2 ne peuvent voir leur responsabilité pénale engagée à raison des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de l'activité ou de l'information illicites ou si, dès le moment où elles en ont eu connaissance, elles ont agi promptement pour retirer ces informations ou en rendre l'accès impossible."

[3]- **أشرف جابر السيد**، مسؤولية مقدمي خدمات الأنترنت عن المضمون الإلكتروني غير المشروع، دراسة خاصة لمســؤولية متعهــدي الإيــواء، دار النهضة العربية، القاهرة، 2010، ص78.

ذاتها[1]، وفيما يتعلق بمن يقوم بخدمة تخزين المعلومات، فإنه ملزم بمقتضى المادة 46 من التوجيه بمجرد العلم بعدم مشروعية المعلومات المخزنة القيام بسحبها أو منع الوصول اليها[2].

والأصل وفقا للمادة 14-1 من هذا التوجيه هو **عدم مسؤولية متعهد الإيواء** عن مضمون المعلومات التي يتم إيواءها بناء على طلب العميل، وذلك ما لم يثبت علمه بالمضمون غير المشروع ، سواء علم فعليا أو من خلال الملابسات والظروف بالنسبة للمضمون الذي يكون غير مشروع بشكل ظاهري أو جلي، كما أن للدول الأعضاء وفقا للفقرة 3 من المادة 14 ان تلزم مقدمي خدمات الأنترنت، سواء عن طريق القضاء أو السلطة التنفيذية بإتخاذ كل ما يلزم لوقف الإعتداء أو تلافي حدوثه.

كما نجد المادة السادسة من القانون الفرنسي المتعلق بالثقة في الإقتصاد الرقمي تنص على عدم مسؤولية متعهد الإيواء المدنية، أو الجزائية عن المضمون الإلكتروني غير المشروع الذي يأويه إذا لم يثبت علمه بعدم مشروعيته[3]. وقد أعفاه –أيضًا– نص هذه المادة من المسؤولية، إذا قام بمجرَّد علمه بأسباب عدم مشروعية هذا المضمون، أو بالوقائع والظروف التي تُضفي عليه صفة عدم المشروعية، باتخاذ ما يلزم من أجل شطبه، أو منع وصول مستخدمي الشبكة إليه.

ولكن، يثور التساؤل حول وسيلة إثبات علم متعهد الإيواء بعدم مشروعية المضمون الإلكتروني الذي يأويه. لقد بيَّن نص المادة السادسة المذكورة أعلاه بأن هذا العلم يثبت بمجرَّد أن يكشف له الشخص المتضرِّر طالب وقف البث عن هويَّته، ويُحدِّد له المضمون المشتكى منه وأسباب عدم مشروعيته، ويُزوِّده بما يُثبت قيامه بإرسال نسخة من طلب وقف المضمون غير المشروع إلى صاحبه أو مُؤلِّفه، ولا بد أن يكون هذا التبليغ مُحدَّد التاريخ[4]. وهكذا، فإنه يلزم لقيام مسؤولية متعهد الإيواء المرور بمرحلتين أساسيتين: بدايةً يجب إثبات علمه بعدم مشروعية المضمون الإلكتروني الذي يأويه، ويتمَّ ذلك عادةً من خلال الإخطار الذي يتم توجيهه إليه، ومن ثُمَّ إعطاؤه فرصةً من أجل وقف البث، وفي حال عدم قيامه بذلك، فإنه يتحمَّل المسؤولية[5].

وينسجم مبدأ عدم المسؤولية الذي جاء في المادة 14-1 من التوجيه مع ما نصت عليه المادة 15-1 التي حظرت على الدول الأعضاء فرض إلتزام عام سواء برقابة المعلومات التي يتم تداولها أو تخزينها، أو البحث عن الوقائع أو الملابسات التي تشير إلى وجود نشاط غير مشروع،وهو ما كرسه المشرع الفرنسي في

---

[1]-Un prestataire de services peut bénéficier de dérogations pour le "simple transport" et pour la forme de stockage dite "caching" lorsqu'il n'est impliqué en aucune manière dans l'information transmise. Cela suppose, entre autres, qu'il ne modifie pas l'information qu'il transmet. Cette exigence ne couvre pas les manipulations à caractère technique qui ont lieu au cours de la transmission, car ces dernières n'altèrent pas l'intégrité de l'information contenue dans la transmission.

[2]- Afin de bénéficier d'une limitation de responsabilité, le prestataire d'un service de la société de l'information consistant dans le stockage d'informations doit, dès qu'il prend effectivement connaissance ou conscience du caractère illicite des activités, agir promptement pour retirer les informations concernées ou rendre l'accès à celles-ci impossible. Il y a lieu de procéder à leur retrait ou de rendre leur accès impossible dans le respect du principe de la liberté d'expression et des procédures établies à cet effet au niveau national. La présente directive n'affecte pas la possibilité qu'ont les États membres de définir des exigences spécifiques auxquelles il doit être satisfait promptement avant de retirer des informations ou d'en rendre l'accès impossible.

[3]-voir : **D. MELISON**, "Responsabilité des hébergeurs: une unité de régime en trompe l'œil", juriscom.net 25 avril 2005, disponible en lingne á l'adresse suivantewww.juriscom.net, p. 3 et s.

[4]- **أحمد قاسم فرح**، النظام القانوني لمقدمي خدمات الأنترنت –دراسة تحليلية مقارنة، –،مجلة المنارة، المجلد 13 ، العدد 09، 2007، ص365.

[5]– **اشرف جابر السيد**، المرجع السابق، ص79، **أحمد قاسم فرح**، المرجع السابق، ص 365.

الفصل 6-1-7 من قانون 21 جوان 2004، ومع هذا أجازت المادة 15-2 من التوجيه الأروبي فرض نوع من الرقابة المحدودة والمؤقتة على هذه المواقع، في بعض الأحوال[1].

ويبدو عدم فرض مثل هذا الإلتزام أمرا منطقيا، إذ يعد الوفاء به في حكم المستحيل على متعهد الإيواء الذي يؤوي على خادمه مئات الآلاف من مواقع الويب، فضلا على أن عملية الإيواء ذاتها تتم عادة الكترونيا وبصفة تلقائية دون اتصال مباشر بين متعهد الإيواء وصاحب الموقع محل الإيواء[2].

وبالمقابل، لم يُحمِّل التوجيه الأوروبي المسؤولية **لمتعهد الوصول** إلا في حال أن رفض التعاون مع السلطة العامة أو القضائية في الدولة التي يُمارس أعماله فيها، فيما تطلبه منه بصورة قانونية[3]. فوفقاً لنص المادة 12 من هذا التوجيه، على متعهد الوصول المبادرة إلى شطب المضمون الإلكتروني غير المشروع الذي يمر من خلاله، أو منع الوصول إليه بمجرَّد علمه، أو إخطاره من قِبل السلطات المختصة، أو من قِبل الشخص المتضرِّر بأسباب عدم المشروعية.

وفيما يتعلَّق **بناقل المعلومات،** والذي يقوم في سبيل تسريع عملية اتصال العملاء بشبكة الإنترنت بتخزين نسخة مؤقتة على أجهزته عن صفحات الويب المطلوبة (caching)، فإن المادة 13 من التوجيه الأوروبي نصت على عدم إمكانية مساءلته إلا إذا ثبت أنه هو مصدر المضمون المعلوماتي غير المشروع، أو أنه قام بالتغيير فيه أثناء عملية نقله أو تخزينه بشكلٍ أضفى عليه صفة عدم المشروعية، أو أنه تقاعس عن وقف بث المضمون المعلوماتي غير المشروع، رغم تحقق علمه بعدم المشروعية[4].

كما نجد المادة التاسعة من القانون الفرنسي 2004-575 قد عالجت الوضع بالنسبة لمتعهد الوصول وناقل المعلومات. وجاءت هذه المادة متفقةً مع أحكام المادتين: 12 و13 من التوجيه الأُوروبي حول "التجارة

---

[1]-Les États membres peuvent instaurer, pour les prestataires de services de la société de l'information, l'obligation d'informer promptement les autorités publiques compétentes d'activités illicites alléguées qu'exerceraient les destinataires de leurs services ou d'informations illicites alléguées que ces derniers fourniraient ou de communiquer aux autorités compétentes, à leur demande, les informations permettant d'identifier les destinataires de leurs services avec lesquels ils ont conclu un accord d'hébergement.

[2]-**اشرف جابر السيد**، المرجع السابق، ص79.

[3]- **Luc GRYNBAUM**, "LCEN. Une immunité relative des prestataires de services Internet", Communication-Commerce électronique, Études, Septembre 2004, nº 28, p37 et S.

[4]-Article 13 dispose que"Les États membre veillent à ce que, en cas de fourniture d'un service de la société de l'information consistant à transmettre, sur un réseau de communication, des informations fournies par un destinataire du service, le prestataire ne soit pas responsable au titre du stockage automatique, intermédiaire et temporaire de cette information fait dans le seul but de rendre plus efficace la transmission ultérieure de l'information à la demande d'autres destinataires du service, à condition que:

a) le prestataire ne modifie pas l'information;

b) le prestataire se conforme aux conditions d'accès à l'information;

c) le prestataire se conforme aux règles concernant la mise à jour de l'information, indiquées d'une manière largement reconnue et utilisées par les entreprises;

d) le prestataire n'entrave pas l'utilisation licite de la technologie, largement reconnue et utilisée par l'industrie, dans le but d'obtenir des données sur l'utilisation de l'informationet

e) le prestataire agisse promptement pour retirer l'information qu'il a stockée ou pour en rendre l'accès impossible dès qu'il a effectivement connaissance du fait que l'information à l'origine de la transmission a été retirée du réseau ou du fait que l'accès à l'information a été rendu impossible, ou du fait qu'un tribunal ou une autorité administrative a ordonné de retirer l'information ou d'en rendre l'accès impossible.

2. Le présent article n'affecte pas la possibilité, pour une juridiction ou une autorité administrative, conformément aux systèmes juridiques des États membres, d'exiger du prestataire qu'il mette fin à une violation ou qu'il prévienne une violation.

الإلكترونية"، فنصت على عدم إمكانية مساءلتهم: مدنياً أو جزائياً إلاَّ إذا ثبت أنهم مصدر هذا المضمون الإلكتروني غير المشروع، أو في حال أن بحثوا عنه، أو غيَّروا في محتوياته، وقاموا بإيصاله إلى مستخدمي الشبكة لجذبهم، لما في ذلك من إخلال بالتزامهم بالحياد التام، وبعدم التدخُّل في المضمون المعلوماتي الذي يمُر من خلالهم[1].

كما نصت المادة 6-1-8 من نفس القانون على أنه للقضاء أن يصدر أمرا على عريضة في مواجهة متعهد الوصول أو الإيواء، بإلزام أي منهما بإتخاد التدابير اللازمة لتفادي الضرر أو وقفه حال حدوثه، وعدم تقيده بهذا الأمر يمكن حينئذ إدانتـــه. ومن بين المسائل التي تساهم في إقرار مسؤولية متعهد الوصول إخلاله بواجب أخلاقي وهو وضع بعض وسائل تصفية المعلومات على ذمة حرفائه[2].

ومما سبق يتضح بأن التوجيه الأروبي بما تضمنه من نصوص وعلى غرار المشرع الفرنسي يلزم مزود الخدمة بإتخاد إجراءات سريعة لإزالة أو تعطيل الوصول إلى المعلومات، وذلك بعد تحقق المعرفة الحقيقية أو الفعلية، ويُؤخذ عليه، في هذا الصدد سكوته، شأنه في ذلك شأن المشرِّع الفرنسي، عن مسألة تنظيم أحكام المسؤولية بالنسبة لباقي مقدمي خدمات الإنترنت، خاصةً **مورِّد المعلومات**.إلا أنهما يبقيان متميزان بالمقارنة مع بعض التشريعات العربية.

الفرع الثاني

تقرير المسؤولية الجزائية للوسيط الفني في التشريع الجزائري والمصري

لم تتعرض بعض التشريعات العربية لموضوع المسؤولية الجزائية للمتدخلين في الأنترنت عن الجرائم التي تمس التعاملات الإلكترونية، كما هو حال المشرع المصري، دلك أنه لم يصدر تشريع جديد ينظم هذا الأمر كما أنه لم يقم بتعديل ماهو قائم من التشريعات الجزائية، وإلى أن يتم هذا التدخل فإننا نتفق مع الجانب الفقهي[3] الذي يرى أن المسؤولية الجزائية للمتدخلين عن الجرائم التي تقع على التعاملات لإلكترونية لا يجب أن تقوم إلا في ضوء القواعد العامة للقانون الجنائي، والمباديء الدستورية الخاصة بمبدأ المسؤولية الشخصية و مبدأ المساواة بين المواطنين أمام القانون.

أما في الجزائر فإن النصوص التي تشير إلى مسؤولية هؤلاء عامة وقليلة جدا، وبطيعة الحال لا يتصور وضع مباديء قانونية مالم تكن هناك إلتزامات واضحة ومحددة تقوم على عاتقهم. والإشكال يتعلق بإمكانية

---

[1]-**Th. VERBIEST et É. WÉRY**, "Le droit de l´internet et de la société d´information", n° 401, p. 219.

مشار إليه لدى: **أحمد فرح**، المرجع السابق، ص365.

[2]-**اللومي عبد الرؤوف**، المرجع السابق، ص55.

حيث فرضت المادة 6 من القانون 2004 على متعد الوصول تبصير عملائه بوسال تتقية التي تسمح بتقييد الوصول إلى بعض الخدمات أو إرشادهم اليها أو إلى أكثرها فعالية لكنها لم تقرر جزاء جزائيا عن الإخلال بهذا الإلتزام ولو بفرض الغرامة.

[3]-**د. مدحت عبد الحليم رمضان**، الحماية الجنائية للتجارة الإلكترونية، المرجع السابق، ص133، **أسامة فرج الله محمود الصباغ**، الحمـــاية الجنائيـــة للمصنفات الإلكترونية ، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 2011، ص178.

إثـــارة مسؤولية الوسيط الفني إستنادا إلى المرسوم التنفيدي رقم 98-257 الذي يضبط شروط وكيفيات إقامة خدمات أنترانت واستغلالها[1]، والقانون رقم 09-04 المتعلق بجرائم تكنولوجيات الإعلام والإتصال ، حيث ينص المرسوم رقم 98-257 في مادته 14 على جملة من الإلتزامات العامة على الوسيط الفني، إلا أنه لم تفرض جزاءا عن الإخلال بهذه الإلتزامات ولو بفرض الغرامة[2].

أما القانون رقم 09-04 فقد أوجبت المادة 12 منه على الوسيط الفني التزامان أساسيان:

الأول: التدخل الفوري لسحب المحتويات التي يتيحون الإطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن. وهو نفس النهج الذي سلكه التوجيه الأروبي والمشرع الفرنسي كما سبق بيانه.

الثاني: وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بوجودها، وهو ماكرسه المشرع الفرنسي في المادة 6 من القانون رقم 2004- 575 [3].وعلى الرغم من أهمية هذا الإلتزام إلا أن هنالك صعوبة تعترضه من الناحية العملية، حيث تتوقف فاعلية الجزاء المترتب على الإخلال به على فرض وجود هذا الجزاء، على وجود حد أدنى من الجودة والكفاءة لبرامج التنقية كمعيار يتقيد به الوسيط الفني، وهو أمر مفتقد لتفاوت الإمكانيات الفنية بين الوسطاء، بما يخل بمبدأ المساواة في التنافس بين هؤلاء، إلا أن هذه الصعوبة سرعان ما تفقد مفعولها إذا ما علمنا أن المشرع لم يرتب على الإخلال بهذا الإلتزام أي جزاء.

ذلك هو الوضع قبل صدور القانون رقم 16-02 المعدل والمتمم للأمر رقم 66-156 والمتضمن قانون العقوبات، ذلك أن هذا القانون أضاف المادة 394 مكرر 8 التي نصت على أنه **دون الإخلال بالعقوبات الإدارية المنصوص عليها في التشريع والتنظيم الساري المفعول، يعاقب بالحبس من سنة إلى 3 سنوات و بغرامة من 2000000 دج إلى 10000000دج او باحدى هاتين العقوبتين فقط، مقدم خدمات الأنترنت بمفهوم المادة 2 من القانون رقم 09-04 الذي لا يقوم رغم اعداره من الهئية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها او صدور امر او حكم قضائي يلزمه بذلك:**

---

[1]-مرسوم تنفيدي رقم 98-257 ، مؤرخ بتاريخ 25غشت 1998، المتضمن شروط وكيفيات إقامة خدمات أنترنات وإستغلالها، جريدة رسمية، عدد 63، صادرة بتاريخ 26 غشت 1998.

[2]-حيث نصت المادة 14 من المرسوم التنفيدي رقم 98-257 على أنه:يلتزم مقدم خدمات أنترنات خلال ممارسة نشاطاته بمايأتي:

-تسهيل النفاذ إلى خدمات أنترنات، حسب الإمكانيات المتوفرة إلى كل الراغبين في ذلك بإستعمال أنجح الوسائل التقنية.

-المحافظة على سرية كل المعلومات المتعلقة بحياة مشتركيه الخاصة وعدم الإدلاء بها إلا في الحالات المنصوص عليها في القانون.

-إعطاء مشتركيه معلومات واضحة ودقيقة حول موضوع النفاذ إلى خدمات أنترنات وصيغة مساعدتهم كلما طلبوا ذلك

-عرض أي مشروع خاص بإستعمال منظومات الترميز على اللجنة

-إحترام قواعد حسن السيرة بالإمتناع خاصة عن إستعمال اية طريقة غير مشروعة سواء تجاه المستعملين أو إتجاه مقدمي خدمات أنترانت الآخرين.

-تحمل مسؤولية محتوى الصفحات وموزعات المعطيات التي يستخرجها ويأويها، طبقا للأحكام التشريعية المعمول بها.

- إتخاذ كل الإجراءات اللازمة لتأمين حراسة دائمة لضمون الموزعات المفتوحة لمشتركيه قصد منع النفاذ إلى الموزعات التي تحتوي معلومات تتعارض مع النظام العام أو الأخلاق.

[3]-حول تدابير التنقية أو المنع، وموقف القضاء الفرنسي منها أنظر: **أشرف جابر السيد**، المرجع السابق ص27.

1-بالتدخل الفوري لسحب او تخزين المحتويات التي يتيح الإطلاع عليها او حعل الدخول اليها غير ممكن عندما تتضمن محتويات تشكل جرائم منصوص عليها قانونا.

2-بوضع ترتيبات تقنية تسمح بسحب او تخزين المحتويات التي تتعلق بالجرائم المنصوص عليها في الفقرة ا او جعل الدخول اليها غير ممكن.

ولعل بهذا النص التشريعي الجزائي لم يقم المشرع مسؤولية مقدم الخدمة إلا اذا لم يحترم الأمر أو الحكم الصادر عن السلطة القضائية أو الإعذار الموجه اليه من الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها والقاضي باتخاد الإجراءات اللازمة لمنع الوصول الى المعلومات المتنازع فيها، وفي صورة عدم احترام مقدم خدمة الأنترنت لهدا تترتب مسؤوليته. وتجدر الإشارة إلى أن المشرع لم يميز بين مقدمي خدمات الأنترنت المشار اليهم في المادة 2، وسبق أن رأينا أن هذه الأخيرة تناولت بالتعريف كل من متعهد الوصول ومتعهد خدمة الإيواء، وهو ما يعني أن النص يشملهما معا.

وهو إتجاه نحو إقصاء الألتزام العام بمراقبة المعلومات المنقولة من طرف متعهد الوصول أو التي يتم ايوائها من طرف متعهد خدمة الإيواء، ما عدا المراقبة المفروضة عليهما في الحالات السابقة، وهو حل تشريعي له ما يبرره في الواقع، إذ أنه من غير الممكن على مقدم الخدمة مهما كانت إمكانيته مراقبة جميع المعلومات على شبكة الأنترنت والتي تقدر بمئات الملايين.

والملاحظ أن المشرع الجزائري على غرار المشرع الفرنسي يعتبر أن محتوى المعلومات يجب أن يكــون غير شرعي **بصفة موضوعية**، كصدور حكم قضائي يقضي بعدم شرعية بعض المعلومات. وعلى خلاف ذلك فإن الأمر يصبح خاضعا لإجتهاد مقدم الخدمة، وهو ماجعل المجلس الدستوري الفرنسي ينادي بعدم إقرار مسؤولية مقدم الخدمة إلا إذا كانت المعلومة المتنازع فيها غير شرعية بصورة واضحة[1].

مما سبق، يتضح إذن أن هناك ميل نحو إقرار عدم مسؤولية مقدم الخدمة، وهو نفس النهج الذي سلكه المشرع [2] ومجلس الدولة في فرنسا[3].

كما فرض القانون 09-04 وفي اطار مساعدة السلطات المكلفة بالتحريات القضائية على الوسيط الفني حفظ المعطيات المتعلقة بحركة السير بسنة واحدة ابتداء من تاريخ التسجيل، وهي المعطيات التي حددتها المادة 11 كتلك التي تسمح بالتعرف على مستعملي الخدمة والمرسل اليه أو المرسل اليهم الإتصال.

---

[1]- Voir:Décision n° 2004-496 DC du 10 juin 2004 du Conseil constitutionnel relative a la Loi pour la confiance dans l'économie numérique; Journal officiel du 22 juin 2004, page 11182, texte n° 3 http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/2004/2004-496-dc/decision-n-2004-496-dc-du-10-juin-2004.901.html

[2]-voir : art 6-1-8 du loi**n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique**

[3]-**Luc GRYNBAUM** Loi « Confiance dans l'économie numérique » : une version définitive proche de la version originale de la Directive « commerce électronique » Communication Commerce électronique - Juin 2004 - n° 6

;p"38,

مشار اليه لدى: **اللومي عبر الرؤوف**، المرجع السابق، ص55.

وفي حالة الإخلال بهذا الإلتزام بما يؤدي إلى عرقلة حسن سير التحريات القضائية، يعاقب الشخص الطبيعي بالحبس من 6 اشهر إلى 5 سنوات وبغرامة من 50000 دج إلى 500000 دج، اما الشخص المعنوي فيعاقب وفق القواعد المقررة في قانون العقوبات.

المبحث الثالـــث

الحمـــاية الجزائيـــة لمعطيات المتعامل الشخصية

من الطبيعي أثنـــاء التعاملات الإلكترونية أن تطلب الجهة التي يتعامل معها الشخص أن يقدم معطياته الشخصية لها، حتى تسمح له بالحصول على خدمة أو سلعة ما، ليجد هذه المعطيات بعد مدة يتم استعمالها من قبل نفس الجهات أو جهات أخرى، فعند معالجة هذه المعطيات الشخصية، فإن هنالك نظاما خفيا في التعامل مع هذه المعطيات الشخصية[1]، يطلق عليه معالجة المعطيات ذات الطابع الشخصي وهو يشكل إعتداء على هذه المعطيات لأنها تعطي صورة واضحة عنه.

كل هذا دفع المشرع في العديد من الدول إلى التدخل لوضع إطار قانوني يحكم هذه المعالجة، بحيث تكون هذه المعالجة ظاهرة ويعلم بها من تخصه هذه المعطيات فضلاً عن حقه في الاعتراض عليها وتعديل معطياته أو إلغائها إذا كانت غير دقيقة أو ناقصة، وإن إختلفت خطتها في ذلك في موضع النص على هذه الحماية، فهناك من إتجهت نحو إصدار أحكام خاصة تعاقب بموجبها على المساس بالمعطيات الشخصية بشكل عام، ومن أمثلة هذه التشريعات التشريع الفرنسي بموجب القانون رقم 78–17 بداية[2]والتشريع التونسي بموجب القانون المتعلق بحماية المعطيات الشخصية لسنة 2004[3].

وهناك من لم تقر أحكاما خاصة للمساس بالمعطيات الشخصية بصفة عامة، غير أنها تتناول حماية الخصوصية المعلوماتية ومايتعلق بها من معلومات يتم تداولها أثناء التعاملات الإلكترونية من خلال قوانين التعاملات والتواقيع الإلكترونية، ومن أمثلة هذه التشريعات التشريع الجزائري والمصري. وهناك من تجمع بين الإتجاهين السابقين، وهو حال التشريع التونسي.

وعلى هدي ما تقدم، سنتناول موضوع الحماية الجزائية للمعطيات الشخصية من خلال المطالب التالية:

المطلب الأول:المعطيات الشخصية في بيئة التعاملات الإلكترونية

المطلب الثاني: الحماية الجزائية للمعطيات الشخصية في التشريع الفرنسي والتونسي

المطلب الثالث: الحماية الجزائية للمعطيات الشخصية في التشريع الجزائري وبعض التشريعات الآخرى

---

[1]– **سامح عبد الواحد التهامي**، ضوابط معالجة البيانات الشخصية –دراسة مقارنة بين القانون الفرنسي والقانون الكويتي، المؤتمر العلميالقانونيالثانيلكليةالقانونالكويتيةالعالمية – 15/16 فبراير 2015، ص1.

[2]-**Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés**;

[3]– قانون عدد 63 لسنة 2004، مؤرخ في27 جويلية 2004 متعلق بحماية المعطيات الشخصية. جريدة رسمية ، صادرة 30 جويلية 2004.

المطلـــب الأول

المعطيـــات الشخصية في بيئة التعاملات الإلكترونية

تحرص المجتمعات خاصة الديمقراطية منها على كفالة الخصوصية، وتعتبره حقا مستقلا قائما بذاته، ولا تكتفي بسن القوانين لحمايته بل تسعي إلى ترسيخه في الأذهان، وذلك بغرس القيم النبيلة التي تلعب دورا كبيرا وفعالا في منع المتطفلين من التدخل في خصوصيات الآخرين وكشف أسرارهم[1].

ونظرا لتضاعف إستخدام تكنولوجيا الإعلام والإتصال التي كان لها الدور الكبير في إقتحام حصون هذا الحق وإختراقه، فقد تضاعف الإهتمام بهدا الحق، مع الإنتقال من حماية الخصوصية إلى الإهتمام أكثر بحماية **المعطيات الإسمية أو الشخصية**، وفي هذا المناخ ظهرت أهمية الجهود الدولية والإقليمية والوطنية في وضع الإطار القانوني لحماية خصوصيات الأفراد من تأثيـــر المعلـــوماتية.

وعلى هدي ما تقدم سنتناول مفهوم المعطيات الشخصية محل الحماية الجزائية(الفرع الأول) وصور تهديد التقنية لها في بيئة التعاملات الإلكترونية(الفرع الثاني)والجهود الدولية والإقليمية لحمايتها(الفرع الثالث)

الفرع الأول

مفهوم المعطيـــات الشخصية في بيئـــة التعاملات الإلكترونية

إن الحق في الخصوصية، و كما يعرف في النظام اللاتيني بالحق في الحياة الخاصة، هو حق إحترام سرية وخصوصية الأشخاص من أي تدخل مادي أو معنوي، وهو حق عميق الجدور من الوجهة التاريخية[2].

ويشير كل من مصطلح **خصوصية المعلومات** أو **حماية المعطيات الشخصية أو الإسمية**، في حق الشخص في أن يتحكم بالمعلومات التي تخصه، وهذا المبدأ مرتبط بتطور تكنولوجيا الإعلام والإتصال، وهده المعلومات يطلق عليها خاصة كونها تتعلق بالشخص داته كإنسان: مثل الإسم والعنوان ورقم الهاتف وحالة الدخل والعرق والعمر والوضع الصحي وغيرها من المعلومات التي تأخذ شكل معطيات وثيقة الإرتباط بكل شخص طبيعي معرف أو غير معرف[3].

لقد أثير موضوع الخصوصية المعلوماتية سنة قبل مؤتمر الأمم المتحدة الأول لحقوق الإنسان، طرحه alain westin وa.miller، أعطى الكاتبان للخصوصية المعلوماتية تعريفا، إذ إعتبرها WESTINأنها"

---

[1]– **د.حسين بن سعيد الغافري**، الحماية القانونية للخصوصية المعلوماتية في ظل مشروع قانون المعاملات الإلكترونية العماني، ورقة مقدمة لمؤتمر أمن المعلومات والخصوصية في ظل قانون الإنترنت القاهرة 2–4 يونيو 2008م، متاح على الموقع التالي:
http://www.startimes.com/?t=18471627

[2]-أنظر في ذلك تفصيلا لدى: د. **محمد عبد المحسن المقاطع**، حماية الحياة الخاصة للأفراد وضماناتها في مواجهة الحاسب الآلي،مطبوعات جامعة الكويت، 1992، ص13 ومابعدها.

[3]–**يونس عرب**، دور حماية الخصوصية في تشجيع الاندماج بالمجتمع الرقمي– ورقة عمل مقدمة الى :– ندوة أخلاق المعلومات – نادي المعلومات العربي – 16–17 اكتوبر 2002 –،عمان ، الاردن، ص7.

حق الأفراد في تحديد متى وكيف وإلى أي مدى تصل المعلومات عنهم للأخرين"، أما a.miller فاعتبرها القدرة على التحكم بدورة المعلومات التي تتعلق بهم.

وكان الغرض من خلال هذه الدراسات الأكاديمية هو منع إساءة إستخدام الحكومة للمعطيات التي يصار لمعالجتها آليا أو إلكترونيا أو تقيد إستخدامها وفق القانون فقط، دون حماية الأفراد من مخاطر التقنية التي تتهدد حياتهـــم الخاصـــة بصفـــة عامة.

وقد كان للتطورات التقنية وتحديدا إنشاء بنوك المعلومات وتزايد إستخدام الكمبيوترات الكبيرة فائقة السرعة التي يمكنها حفظ كميات هائلة من المعطيات وتداولها بسرعة ليست فقط ضمن إطار دولة واحدة و إنما على مستوى دول العالم قاطبة بما في ذلك المعطيات الخاصة بالأفراد مثل الإسم واللقب والعنوان والرقم الهاتفي ورقم البطاقة البنكية والضمان الإجتماعي، تاريخ الولادة...، في ترسيخ مفهوم خصوصية المعلومات بالمحتوى المشـــار إليـــه، إضافة إلى ذلك ومع تعاظم حجم التعاملات الإلكترونية خاصة التجارية منها و إتساعها، إتضحت أيضا القيمة التجارية للمعطيات ذات الطابع الشخصي.

وعلى النطاق التشريعي، أحاط التوجيه الأروبي رقم 95/46/ ce حول حماية الأفراد فيما يخص معالجة المعطيات وحرية حركتها بمسألة وضع تعريف للمعلومات الشخصية التعريفية أو الإسمية، وذلك بموجب الفقرة أ من المادة 2 منه كون أنها تعني ***كل المعلومات المتعلقة بشخص طبيعي معرف أو قابل للتعريف، يعد قابل للتعرف عليه (الشخص المعني)الشخص الدي يمكن معرفته بصفة مباشرة أو غير مباشرة لاسيما بالرجوع إلى رقم تعريف أو إلى عنصر أو عدة عناصر خاصة مميزة لهويته الطبيعية، الفيزيولوجية النفسية الإقتصادية الثقافية الإجتماعية***"[1]. وفي نفس المعنى كانت قد عرفت إتفاقية حماية الأفراد المتعلقة بالمعالجة الآلية للمعطيات الشخصية رقم 108 [2] المعطيات الشخصية بموجب المادة 2-أ على أنها ***كل المعلومات المتعلقة بشخص طبيعي معرف أو قابل للتعرف عليه".***

من خلال ما سبق، يمكن القول أن الخصوصية كمفهوم على إطلاقه أصبح يدمج في رحمه العديد من المفاهيم: **خصوصية المعلومات** المتصل بفهوم **حماية المعطيات الإسمية** والمتعلق بمواجهة الإعتداءات على المعطيات الشخصية وتنظيم الحق في هذه المعطيات وسيطرة صاحبها عليها، الخصوصية الجسدية أو المادية، خصوصية الإتصالات العادية والإلكترونية وغير ذلك من من أوجه الحماية ذات الطبيعة أو المحتوى المادي أو المعنوي.

والمعطيات الشخصية على النحو السابق بيانه لا يتغير مفهومها في مجال التعاملات الإلكترونية، إذ تعني تلك المعطيات المتعلقة بأطراف التعامل الإلكتروني، فنجد الكثير من هيئات الحكومة والقطاع الخاص تجمع معطيات مفصلة عن المتعاملين معها، تتعلق بالوضع المادي أو الصحي أو التعليمي او العائلي أو العادات الإجتماعية أو العمل، وتستخدم الحاسبات وشبكات الإتصال في تخزينها ومعالجتها وتحليلها والربط بينها

[1]-**Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données**

[2]-Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Série des traités européens - n° 108, Strasbourg, 28.I.1981.

وإسترجاعها ومقارنتها ونقلها، وهو ما يجعل فرص الإطلاع عليها على نحو غير مأدون به أو بطريق التحايل أكثر من دي قبل ويفتح مجالا أوسع معها لإساءة الإستخدام، او توجيهها توجيها منحرفا أو خاطئا، أو مراقبة الأفراد وتعرية خصوصياتهم أو الحكم عليهم حكما خفيا من واقع سجلات المعطيات الشخصية المخزنة إلكترونيا[1].

الفــرع الثاني

صور تهديد المعطيات الشخصية في بيئة التعاملات الإلكترونية

إن معظم معاملاتنا صارت تتم بشكل إلكتروني، فبطاقات الهوية هي معطيات رقمية مسجلة لدى المؤسسات الحكومية يتم من خلالها الإستدلال على هوياتنا الشخصية، الترتيب للسفر عن طريق الأنترنت حجز تذاكــر الطيران، دفع الفواتير وغيرها فكلها تتم عن طريق كتابة معطيات شخصية على صفحات أو تطبيقات تلك المواقع بطريقة تمكنها من الإستدلال علينا لتقديم الخدمة المطلوبة كالإسم ورقم الهاتف وعنوان البريد الإلكتروني والسن والجنس وغيرها، وهذا خلف آثارا إيجابية عريضة لا يستطيع أحد إنكارها، إلا أنه قد صاحب هذا الشعور بمخاطر تقنية المعلومات على المعطيات الشخصية سواء من الأفراد أو من السلطة بإمكانية جمعها وتخزينها والإتصال بها وجعلها متاحة على الخط، أكثر من ذلك، فإن كل إتصال بالأنترنت يمكن أن يترك أثرا ما دون أن يدرك مستخدم الشبكة ذلك على شكل سجلات رقمية حول الموقع الذي زاره والوقت الدي قضاه على الشبكة والأمور التي بحث عنها والوسائل التي أرسلها والخدمات والبضائع التي قام بطلبها في سجلات تتضمن تفاصيل دقيقة عنه، وهو ما يثير مخاطر إساءة إستخدام هذه المعطيات خاصة في الدول التي لا تتوفر فيها مستويات الحماية القانونية لهذه المعطيات، وتتزايد المخاطر يوما بعد يوم وتظهر في مصادر رئيسية وهي قواعد معطيات الحاسب التي يسهل التلاعب بالمعلومات الرقمية وتحليلها وتركيبها وارسالها وتخزينها ومن السهل استخدامها واحداث اساءة بها بغرض ما او بدون غرض، فضلا عن تكنولوجيا جمع المعلومات وما تمثله من مخاطر حقيقة على خصوصية المعلومات، وهو ما سوف نلاحظه في النقاط المتقدمة من هذا الفرع.

أولا– قواعد معطيات الحاسب[2]

تقوم قواعد معطيات الحاسب بتخزين المعلومات ومعالجتها بطريقة تجعلها تتجاوز حدود الزمان والمكان، فما أن يتم تخزين المعلومات الشخصية القيمة في الوقت الحاضر في قاعدة المعطيات حتى تصبح قابلة لأن يتم تجميعها لإعادة تكوين الماضي، وإستخدام قواعد المعطيات في الأنترنت سهلت القدرة على الوصول إلى المعلومات والحصول عليها، والكثير من الوكالات الحكومية والشركات الخاصة قامت بتحويل

[1]- **وليد السيد سلوم**، ضمانات الخصوصية في الأنترنت،دار الجامعة الجديدة،الإسكندرية ،2012، ص 653.

[2]-المرجع نفسه، ص216.

قواعد معطياتها الورقية على قواعد معطيات آلية، والتي تم ربطها حديثا بالأنترنت وببعضها البعض، وأصبح من خلال الأنترنت الحصول على معطيات إسمية للشخص في أقل من ثانية، مثل الإسم ورقم التلفون عنوان الإقامة تاريخ الميلاد رقم الضمان الإجتماعي وغيرها. والتطور السريع للتقنيات التي تستخدمها الحكومات والشركات أصبح يهدد المعطيات الإسمية من مخاطر المعالجة الآلية.

ثانيا-جمـــع المعلومـــــات

بالرغم من أن جمع المعلومات لا يشكل تهديدا مباشرا لخصوصية المعلومات حيث إذا لم يحدث إنكشاف للمعلومات فلن يكون هناك تهديد، ولكن من جهة أخرى إذا تم جمع المعلومات بطريقة خفية وواسعة الإنتشار كلما زاد خطر تهديد المعطيات الخاصة، والمعلومات التي يتم جمعها عبر الأنترنت يمكن تقسيمها إلى فئتين: الأولى تلك المعلومات التي يتم الكشف عنها إراديا وذلك للإشتراك بخدمات المواقع على الشبكة أو للتسوق عبر الأنترنت أو تسجيل معلومات لصالح شركات التأمين، والثانية تلك التي لا يتم الكشف عنها إراديا الدي يلزمه نوعا من التتبع خلسة، وكلا النوعين يهدد خصوصية المعلومات.

ومن الطرق التي يمكن من خلالها جمع المعلومات عن الفرد والتعـــرف علـــيه:

أ- إستعمال ملفات تعريف الارتباط**cookies**" التي تمكن من الوصول إلى المعطيات الخاصة بالمتعامل الإلكتروني، وهي تقنيات تستخدمها الشركات التجارية والإعلانية بشكل أساسي لتساعدها في تذكر الصفحات المفضلة لدى المستخدمين وإرسال البريد الدعائي لهم وتجمع معلومات تعريفية مثل الإسم والعنوان ورقم التلفون والبريد الإلكتروني وأرقام الحسابات أو المعلومات الأخرى المماثلة[1]. والتقنية الأكثر خطر وهي برمجيات **التتبع والإلتقاط**، وهي وسيلة تتبع لجمع أكبر قدر من المعلومات السرية والخاصة عن طريق أنظمة جمع المعلومات[2].

ب-**المتاجر الإلكترونية** وغيرها من منصات الويب، التي تقوم بتحميل بيانات عملائها بعد موافقتهم لأغراض دعائية.وهنا يوصي الخبراء بضرورة إلقاء نظرة على المعطيات والتأكد من إزالة علامة إختيار الموافقة على نشر المعلومات الشخصية عند التسجيل.

ت-**استعمال بروتوكولات الإتصال عبر الأنترنت** بين أجهزة الحاسب الآلي، فعن طريق تتبع عنوان البروتوكول يتم الوصول إلى المعطيات الشخصية للمستخدمين والتعرف أيضاً على موقع الجهاز الذي يقوم بعملية التصفح على الإنترنت.

ث-**الويب باجز" 2(Web Bugs)** [3]، وهي عناصر غيرمرئية تتضمنها صفحات البريد الإلكتروني والمواقع الإلكترونية. وتعمل على إرسال المعلومات الخاصة بحركة المستخدم على الموقع الإلكتروني كَنَسخ أو تحميل الصفحات، كما تُمكن من التعرف على توقيت إطّلاع المستخدم على بريده الإلكتروني، وما إذا

---

[1]- المرجع نفسه، ص182.

[2]-**د. أيمن عبد الله فكري**، المرجع السابق، ص659.

[3]-**سارة الشريف**، خصوصية البيانات الرقمية، سلسلة أوراق الحق في المعرفة، مركزدعم لتقنية المعلومات، القاهرة، ص3.

كان قد قام بإرسال البريد لآخرين. أيضاً يتم استخدام تلك العناصر في تحليل صفحات الإنترنت، وقد تتواجد في ملفات الصور وتحمل أسماء متعددة تختلف طبقاً لمكان وجودها، وهي عادةً عناصر غير ضارة ولا تعد من الفيروسات؛ إلا أن خطورتها تكمن في نوع المعلومات التي تقوم بجمعها، ويمكن توفير بعض الحماية للمعطيات الشخصية من تطفل عناصر Web Bugsعن طريق إغلاق ملفات الكوكيز من متصفح الإنترنت.

مما سبق يتبين لنا أن هناك تحديات جديدة أوجدتها تقنية المعلومات خاصة الأنترنت في مواجهة حماية المعطيات الشخصية، فهي زادت من كم المعطيات المجمعة و أتاحت عولمة المعلومات والإتصالات، وبالتالي فقدان المركزية وآليات السيطرة والتحكم، وإن كان هدا التهديد أصبح أمرا مسلما به، حيث إستطاع التغلب على عوائق المسافة والموانع المادية وتجاوز عقبة الزمن، فمثل هذا الأمر إستدعي في منطق البناء الواحد للشخصية الإنسانية إعتراف القانون ببناء الشخصية الإنسانية التي ترتبط بها مجموع المعطيات الشخصية، خاصة مع الإنطلاق في تطبيق فكرة الإدارة الإلكترونية بحيث يكون هناك تفاعل تام بين التشريع من جهة والعمل الإداري من جهة أخرى. ولقد كان مثل هذا الأمر محل إهتمام دولـــي وإقليمـــي ووطنـــي.

الفرع الثالث

الجهود الدولية والوطنية لحماية المعطيات الشخصية

نظرا لمخاطر المعالجة الآلية للمعطيات الشخصية وإزدياد أنشطة جمع وتخزين ونقل وتبادل هذه المعطيات عن طريق التقنيات الحديثة من قبل الدولة أو القطاع الخاص، ظهرت عدة قوانين وطنية ودولية كرد فعل لذلك، كان الهدف الأول منها هو تشجيع التعاملات الإلكترونية، بمعنى خلق بيئة آمنة تسمح بتطورها كون هذا يعد شرطا أساسيا لتطور هذا النوع من التعامـــلات.

أولا- الجهود الدولية لحماية المعطيات الشخصية

أ- منظمة التعاون ٱلإقتصادي والتنمية OCDE[1]

تضم هذه المنظمة في عضويتها 29 دولة حتى أواخر 2000 وغرضها الرئيسي تحقيق أعلى مستويات النمو الإقتصادي لأعضائها. وضعت هذه المنظمة سنة 1978 قواعد إرشادية من أجل حماية الخصوصية ونقل المعطيات وأوصت الأعضاء بالإلتزام بها، تغطي الأشخاص الطبيعيين فقط وتطبق على القطاعين العام والخاص، وتتعلق بالمعطيات المتعلقة بالمعالجة الآلية أو غير الآلية، وتتضمن التوجيهات المباديء الثمانية الرئيسية للحق في حماية المعطيات الخاصة، وهذه المبادي هي تحديد حصر عمليات جمع المعطيات،

[1]-**علي كريمي**، تأثير التطور التكنولوجي على حقوق الإنسان الحياة الخصوصية وحماية البيانات الشخصية نموذجا، مجلة أبحاث، الفعل الإحتجاجي بالمغرب، مقاربة الإنسان والسلوكات والقيم، العدد 61،62 ، 2015، ص86. **د.أيمن عبد الله فكري**، المرجع السابق، ص673.

الإقتصار على طبيعة المعطيات الشخصية وتحديدها وتحديد الغرض وحصر الإستخدام بالغرض المحدد و توفير وسائل حماية وأمن المعلومات والعلانية والحق في المشاركة.

وقد لعب دليل OCDE دورا رئيسيا وكان له تأثير في دفع الدول المختلفة إلى إصدار تشريعات وطنية تغطي هذا المجال، ويطلق على هذه التشريعات في الدول الناطقة بالفرنسية إسم **قوانين المعطيات** أو قوانين حماية المعطيات lois sur la protection des données أما في الدول الناطقة باللغة الإنجليزية فيطلق عليها قوانين حماية الخصوصية privacy protection laws[1].

ب-مجلس أروبـــا[2]

لعب هذا المجلس دورا كبيرا في إخراج ووضع إتفاقية عالمية بشأن حماية الخصوصية، ففي عام 1981 تبنت لجنة من وزراء مجلس أروبا إتفاقية حماية الأفراد في نطاق المعالجة الآلية للمعطيات الشخصية وأصبحت نافذة 1985، وإهتمت بتطوير ما جاءت به توصيات OCDE الغير ملزمة، وصارت هذه الإتفاقية ملزمة للأعضاء المتعاقدين، وإنحصر نطاقها في الأشخاص الطبيعيين وبالملفات المؤتمتة ومن تم قررت 10 مباديء تمثل الحد الأدنى لمعايير حماية الخصوصية المتعين على الدول الأعضاء تبنيها في التدابير التشريعية، وهي متقاربة مع مباديء منظمة التعاون الإقتصادي والتنمية.

وتغطي قواعد الإتفاقية مسائل نقل وتبادل المعطيات بين الدول المتعاقدة، كما تمنع نقل المعطيات إلى خارج الحدود، إلا إلى الدولة التي توفر لها حماية موازية، مع إستثناءات من هذه القاعدة، ثم أن مجلس أروبا من خلال لجنة الخبراء العاملة في حقل حماية المعطيات، قد أصدر سلسلة من الدلائل التوجيهية المعتمدة على الإتفاقية وتتعلق بمايلـــي:

حماية المعلومات الطبية المؤتمة، والإحصاءات، وقاعدة المعلومات الخاصة لأغراض التسويق، وقاعدة المعلومات الخاصة لأغراض الضمان الإجتماعي أو لأغراض البوليس والمعطيات الجنائية وقواعد المعلومات الخاصة بأغراض التوظيف وكذلك خدمات الإتصال.

ج- الإتحاد الأروبـــي

بدأ إهتمامه بموضوع حماية المعطيات الشخصية في نفس اللحظة التي طرحت فيها مسالة الإهتمام بحقوق الإنسان على المستوى العالمي مند منتصف سبعينيات القرن المنصرم، وهكذا فإن هذه الهيئة أولت جهودا بشأن توحيد القواعد المقررة في قوانين حماية الخصوصية، فمند عام 1976 صدرت عنه تعليمات عديـــدة:

- تعليمات 8-4-1976: تتعلق بحماية الأفراد من أنشطة التقييم الألي للمعطيات.

[1]-Thus, it is common practice in continental Europe to talk about "data laws" or "data protection laws" (lois sur la protection des données), whereas in English speaking countries they are usually known as "privacy protection laws", https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[2]- **علي كريمي**، المرجع السابق، ص86.

– تعليمات 8–5–1979: المتعلقة بحماية الأفراد في مواجهة التطور التقني لمعالجة المعطيات وتعليمات بنفس الموضوع في 9–3–1989.

–كما قدم الإتحاد حزمة أدلة توجيهية متكاملة حول حماية المعطيات كان من حصيلتها دليل 1995 بشأن حماية الأفراد فيما يتصل بمعالجة المعطيات الشخصية وحرية نقلها، وهو الدليل المقرر من قبل البرلمان الأروبي ومجلس أروبا إضافة إلى دليل 1997 المتعلق بحماية معطيات الإتصالات.

وإلى جانب هذه الجهود ذات الطابع الدولي والإقليمي هناك كذلك جهود مجموعة الثمانية الكبار وجهود منظمة التجارة العالمية، وهي على التماس مع تطور حقوق الإنسان وتكنولوجيا المعلومات وتأثيرها عليها بالخصوص.

ثانيا– الجهــود الوطنيـــة

لقد كان لإستخدام **الحواسيب** بكثرة في تخزين المعلومات الخاصة بالمواطنين في مختلف الدول، وإنتشار **الأنترنت** كدعامة لتيسير إنتقال هذه المعطيات عبرها عاملا أساسيا لتدخلها لحماية هذه المعطيات من مخاطر المعالجة الآلية، وقد تزعمت السويد مجموع الدول التي وضعت تشريعا لحماية المعطيات الشخصية عند إصدارها لأول قانون بهذا الشأن سنة 1973 وهو القانون رقم 289 الصادر بتاريخ 11 نوفمبر 1973 وقد تعرض هذا القانون لتعديلات عدة مرات تبعا لتطور تقنية المعلومات لتضع قانونا جديدا حول المعلومات الشخصية سنة 1998، ولكي تعطي بعد أقوى لمسالة حماية معلومات الشخصية فإنها قد أدمجتها في الدستور السويدي لسنة 1988 بعد تعديله.

وإلى جانب السويد، نجد دولا أخرى غربية إهتمت بالمعالجة الآلية للمعطيات الشخصية ولعل أهمها فرنسا، حيث إلتزم المشرع الفرنسي فيها بمستوى من الحماية التشريعية الشاملة التي جاء النص عليها في الإتفاقية الأروبية المتعلقة بحماية الأفراد بالنظر إلى المعالجة الآلية للمعطيات الشخصية لسنة 1981 وما تم إقراره من قواعد وفقا لما يقضي به التوجيه الأروبي رقم 46/95/ ec كما يلتزم بالقواعد المقررة في التوجيه الأروبي رقم EC/66/97 بشان معالجة المعطيات الشخصية وحماية الخصوصية في قطاع الإتصالات[1]، فضلا عن التوجيه الأروبي رقم 58/2002/ EC[2] بشان معالجة المعطيات الشخصية والحياة الخاصة في إطار الأنترنت، وكذلك التوجيه الأروبي رقم 2009 /136/ EC [3] بشأن حماية حقوق الأفراد مستخدمي شبكات الإتصالات الإلكترونية والخدمـــات.

[1]-Directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications ***Journal officiel n° L 024 du 30/01/1998 p. 0001 - 0008***

[2]-DIRECTIVE 2002/58/CE DU PARLEMENT EUROPÉEN ET DU CONSEIL du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques),

[3]-DIRECTIVE 2009/136/CE DU PARLEMENT EUROPÉEN ET DU CONSEIL du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) n° 2006/2004 relatif à

وتطبيقا لذلك أصدر بتاريخ 6-1-1978 قانون المعلوماتية والحريات الذي تم تعديله عدة مرات مند ذلك التاريخ وتتميمه بعدة مراسيم، والتي أصبحت نصوصه فيما يتعلق بالمعطيات الشخصية جزءا من الحماية التي يفرضها قانون العقوبات بشأن حماية الخصوصية.

وقد أنشأ هذا القانون سلطة إدارية مستقلة هي اللجنة الوطنية للمعلوماتية والحريات التي من مهامها المراقبة والإشراف على جمع ومعالجة وإستغلال المعلومات الشخصية، وتمكين الأفراد من نيل حقوقهم الإلكترونية المشروعة في مواجهة تطور الأنترنت ونظم المعالجة الحديثة للمعطيات الشخصية مثل حق الإستعلام والحق في الإطلاع والوصول والتصحيح والإعتراض والأمن والسريـــة المعلوماتية.

وينطبق هذا القانون وفقا للمادة الثانية فقرة 1 منها على المعالجة الآلية للمعطيات الشخصية، فضلا عن المعالجة الغير آلية للمعطيات الشخصية أو التي يراد تخزينها في ملفات، بإستثناء المعالجات المستخدمة في أنشطة شخصية بحثة عندما يفي بشروط تلك المعالجة"[1].

والنمـــاذج المشار إليها تهم الدول الغربية بمافيها تلك التي كانت مصدر صناعة تكنولوجيات الإعلام الحديثة، أما الدول العربية فلم تكن هي الأخرى بمنأى عن تمكين ترسانتها القانونية من وسائل ناجعة للحماية من مخاطر المعالجة الآلية للمعلومات الشخصية، وتاتي على رأسها تونس، فدعما لترسانة القوانين السالبة للحرية، والهادفة إلى إضفاء صبغة شرعية لتعسف السلطة وتجريد المواطن من حقوقه الأساسية، أصدرالمشرع التونسي القانون الأساسي عدد 63 لسنة 2004 المؤرخ في 27 جويلية 2004 المتعلق بحماية المعطيات الشخصية ناسجا إياه وفق التوصية الأروبية رقم CE/95/46، حيث نص في الفصل الأول منه على "**لكل شخص الحق في حماية المعطيات الشخصية المتعلقة بحياته الخاصة بإعتبارها من الحقوق الرئيسية المضمونة بالدستور...**". وقد سعى المشرع بمقتضى هدا القانون إلى وضع آليات الحماية وإقرار إجراءات مشددة تهدف جميعها إلى تحقيق التوازن المنشود بين ضروريات المعالجة وواجب الحماية،وقد أنشـــأ سلطـــة إداريـــة مستقلة وهي الهيئة الوطنية لحماية المعطيات الشخصية" من مهامها تحديد الضمانات الضرورية والتدابير الملائمة لحماية المعطيات الشخصية.، كما صدر الأمر عدد 3003 لسنة 2007 المؤرخ في 27 نوفمبر 2007 ليضبط طرق سيرها، والأمر عدد 3004 لسنة 2007 المؤرخ في 27 نوفمبر 2007 المتعلق بضبط شروط وإجراءات التصريح والترخيص لمعالجة المعطيات الشخصية، والأمر عدد 1753 لسنة 2008 المؤرخ في 5 ماي 2008 المتعلق بتعيين رئيس وأعضاء الهيئة .

فضلا عن ذلك، قام المشرع التونسي بحماية المعطيات الشخصية من خلال القانون عدد 83 لسنة 2000 المتعلق بالمبادلات والتجارة الإلكترونية وذلك في الباب السادس منه.

---

la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs

[1]-Article 2 alinéa 1 dispose que" La présente loi s'applique aux traitements automatisés de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers, à l'exception des traitements mis en oeuvre pour l'exercice d'activités exclusivement personnelles, lorsque leur responsable remplit les conditions prévues à l'article 5.

ولإعطاء حماية للمعطيات الشخصية قيمة قانونية حقوقية أكثر أهمية وأكثر حجية، نص المشرع في الفصل 24 من الدستور الصادر بتاريخ 26 جانفي 2014 "تحمي الدولة الحقوق الخاصة، وحرمة المساكن، وسرية المراسلات والإتصالات والمعطيات الشخصية".

أما الوضع في بعض التشريعات كما هو حال المشرع الجزائري –وعلى غرار المشرع المصري–، فنجده لم يتخذ نصا إطاريا رغم توضيح المدير العام لمجتمع المعلومات والوسائل التقنية بوزارة البريد وتكنولوجيات الإعلام والإتصال في نوفمبر 2014 على هامش إفتتاح صالون تكنولوجيات الإعلام والإتصال في خدمة أمن المواطن أن هناك مشروع قانون يتعلق بحماية المعطيات الشخصية على الأنترنت، إلا أنه لحد الساعة لم يرى النور. إلا أنه في المقابل قد أقر حماية للمعطيات الشخصية في نصوص متفرقة من قانون التوقيع والتصديق الإلكترونيين.

المطلـــب الثـــاني

الحماية الجزائية للمعطيات الشخصية في التشريع الفرنسي والتونسي

تناولت بعض التشريعات المنهج الخاص بوضع نصوص عامة يتم من خلالها إقرار حماية جزائية للمعطيات الشخصية، فالمشرع الفرنسي وبموجب القانون رقم 78–17 المؤرخ في 6 يناير 1978 والخاص بالمعالجة الإلكترونية للمعلومات الاسمية الذي اشتهر باسم قانون المعلوماتية والملفات والحريات، ونظرا لخطورة ما يترتب على معالجة المعلومات الاسمية من تهديد لخصوصيات الأفراد، فقد أحالت المواد من41–44 والمادة 46 من القانون رقم 17لسنة 1978 المعدلة بالقانون رقم 1336 –1992 المؤرخ في 16 ديسمبر 1992 من قانون العقوبات الفرنسي الجديد إلى المواد من 226–16 إلى 226–24 من ذلك القانون الأخير في شان الجرائم التي تقع بالمخالفة لأحكام القانون الأول مع إجراء تعديلات في بعض هذه الجرائم, هذا وقد ألحق المشرّع الفرنسي تعديلا آخر على هذه الجرائم وذلك بموجب القانون رقم 2004_801 المؤرخ في 6 اوت 2004[1] المعدل لقانون العقوبات وكذا القانون رقم 78–17وذلك بما يتماشى والتوجيه الأوربي رقم 1995 و2002. حيث اضاف مواد جديدة إلى قانون العقوبات وهي المواد 226–16–1–أ, 226–16–1, 226–18–1, 226–19–1و226–22–1, 226–22–2 , كما أضاف بعدها المادة 226–17–1 بموجب المادة 39 من الأمر رقم 2011–1012 المتعلق بالاتصالات الإلكترونية[2]. كما قام بتعديل آخر للمادة 226–19 بموجب القانون رقم 2012-954 المؤرخ في 6 أغسطس 2012 بشأن التحرش الجنسي، كما أضاف بموجب

[1]-laLoi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi 78-17 du 6 janvier 1978 relative À l'informatique, aux fichiers et aux libertés.

[2]-**Ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques** , JORF n°0197 du 26 août 2011.

القانون رقم267-2011[1] المادة 226-4-1، كما أدخل البعض من التعديلات بموجب القانون رقم 2016-41[2] المتعلق بتحديث النظام الصحي، والقانون رقم 2017-86 المتعلق بالمساواة في المواطنة[3].

وبالرغم من تنظيم النصوص السابقة لجملة من الإعتداءات التي تنال المعطيات الشخصية، إلا أننا يمكن أن نجمعها في ثلاث طوائف: الأولى : الجرائم المتعلقة بالمعالجة الآلية للمعطيات الشخصية، والثانية الجرائم المتعلقة باستخدام المعطيات الشخصية المعالجة آليا، وأخيرا جريمة انتحال أو سرقة الهوية الرقمية. هدا ما سنتناوله بالتحليل من خلال الفروع المتقدمة من هذا المطلب وذلك مع عمل مقارنة مع القانون التونسي نظرا لتنظيم هذا الأخير لهدا النوع من المعطياتبموجب القانون عدد 63 لسنة2004 المؤرخ في 27 جويلية 2004 المتعلق بحماية المعطيات الشخصية.

الفــرع الأول

الجرائم المتعلقة بالمعالجة الآلية للمعطيات الشخصية

جرم المشرع الفرنسي العديد من السلوكات المتعلقة بالمعالجة الآلية للمعطيات الإسمية أو الشخصية، وكذلك فعل المشرع التونسي في القانون المتعلق بحماية المعطيات الشخصية، سنتناولها بالتفصيل كمايلي:

أولا-المعالجة الآلية للمعطيات الشخصية دون مراعاة الشكليات القانونية المطلوبة

ينص المشرع عادة على ضرورة إعمال المعالجة الآلية للمعطيات الشخصية لإحترام اجراءات وشكليات معينة، كما ينبغي على الشخص الذي يجري هذه المعالجة أن يفي بصفة لاحقة بالشروط التي يمكن أن تعرض عليه من جانب الجهة المختصة عند أداء هذه الشكليات، فقد كانت المادة 14 وما يليها من قانون 1978 الفرنسي تنص على ضرورة إعمال المعالجة الآلية للمعطيات الشخصية لإحترام إجراء التصريح السابق تحت رقابة اللجنة القومية للمعلوماتية والحريات، وعندما يؤول وضع البطاقة المعلوماتية لشخص معنوي عام فإن هذه البطاقة لا يمكن إنشاءها إلا بمقتضى مرسوم بعد رأي اللجنة، أما حاليا فالقانون 2004-801 نظم هذه المسالة حسب طبيعة المعطيات المعالجة ومدى خطورتها، كما تطلب المشرع التونسي شكليات معينة في عملية المعالجة نضمتها كل من المادة 7 والمادة 15 من القانون عدد 63 لسنة 2004.

أ-الركــن المــادي

يتحقق الركن المادي لهذه الجريمة بسلوك يرتكبه الجاني وهو فعل المعالجة الإلكترونية للمعطيات الشخصية أو الإسمية بدون مراعات الشكليات التي ينص عليها القانون، وقد يتخذ صورة عدم إعلام اللجنة

[1]-LOI n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure
[2]-**LOI n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé;** JORF n°0022 du 27 janvier 2016
[3]- **LOI n° 2017-86 du 27 janvier 2017 relative à l'égalité et à la citoyenneté , jORF n°0024 du 28 janvier 2017**

المختصة أو بدون تصريح منها أو طلب منها، أو إستخدام رقم التسجيل الخاص بالمعطيات الشخصية دون ترخيص، أو إجراء المعالجة بدون إحترام القواعد التبسيطية أو قواعد الإعفاء. ينصب هذا السلوك على محل معين وهو المعطيات الشخصية.

1-محـــل النشـــاط الإجرامـــي

إن النشاط الإجرامي في هذه الجريمة إنما يرد على محل محدد وهو المعطيات الشخصية، وقد عرفها المشرع الفرنسي بموجب المادة 2 من قانون 6 جانفي 1978 المعدل بالقانون 2004-801 على أنها المعلومات المتعلقة بالشخص الطبيعي والتي تسمح بتحديده، سواء بشكل مباشر أو بشكل غير مباشر بالرجوع إلى رقم تعريف أو إلى عنصر أو إلى عدة عناصر مميزة له لتحديد ما إذا كان الشخص قابلا للتعرف عليه، يلزم الأخذ بالإعتبار مجموع الوسائل التي من شانها التمكين من تعريفه"[1].

وبعبارة قريبة من ذلك إعتبرت المادة 1/2 من التوجيه الأروبي رقم 46/95 أن المعطيات ذات الطابع الشخصي هي كل معلومة متعلقة بشخص طبيعي معرف أو قابل للتعرف عليه بصفة مباشرة أو غير مباشرة لا سيما الرجوع إلى رقم تعريف أو إلى عنصر أو عدة عناصر خاصة مميزة لهويته الطبيعية الفزيولوجية النفسية الإقتصادية أو الإجتماعية.

كما عرفها المشرع التونسي في المادة 4 و5 من قانون حماية المعطيات الشخصية على أنها كل المعطيات مهما كان مصدرها او شكلها والتي تجعل شخصا طبيعيا معرفا أو قابلا للتعريف بطريقة مباشرة او غير مباشرة من خلال مجموعة من المعطيات أو الرموز المتعلقة خاصة بهويته او بخصائصه الجسمية او الفيزيولوجية او الجينية او النفسية او الإجتماعية او الإقتصادية او الثقافية.

ويلاحظ على هذه التعاريف أنها تتطلب أن تتعلق المعطيات بالأشخاص الطبيعية، وهو ما يعني إقصاء الأشخاص المعنوية من نطاق هذه الحماية، ولعل السبب في قصر نطاقها على الأشخاص الطبيعية وحدها كون أن حماية هذا النوع من المعلومات هو حماية للحق في الحياة الخاصة الذي يعد من الحقوق المتعلقة بالشخصية الإنسانية، فإتصال هذا الحق بالإنسان أحد المظاهر المميزة للشخصية الإنسانية[2] . ومع ذلك وفي بعض الحالات وجد أن القانون يطبق على الممثلين القاونيين للأشخاص المعنوية عندما يتم ذكرها بالإسم في ملف[3].

---

[1] **Article 2 /2 dispose que** -Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.

[2] -**د.نعيم مغبغب**، مخاطر المعلوماتية والأنترنت، المخاطر على الحياة الخاصة وحمايتها، دراسة في القانون المقارن، منشورات الحلبي الحقوقية، بيروت، 1998، ص133.

[3] -Sur les conditions d'applicabilité de la loi aux personnes morales. Voir notamment, CNIL, Délibération n° 84- 28 du 3 juillet 1984. J. Frayssinet, A propos du droit d'accès des personnes morales, D. 21 mai 1992, n° 80, p. 253
Voir aussi: **Ibrahim Coulibaly**, La protection des donn´ees `a caract`ere personnel dans le domaine de la recherche scientifique, THÈSE Pour obtenir le grade de DOCTEUR DE L'UNIVERSITÉ DE GRENOBLE, Universit´e de Grenoble, 2011.p15.

وحتى تكتسب المعطيات الطابع الشخصي يجب أن تسمح بتحديده، ويكون التحديد **بشكل مباشر** حينما تتعلق هذه المعلومات بإسم ولقب الشخص مثلا وصورته أو فيديو خاص به او بيانات بيومترية تسمح بتحديده مباشرة، أما التحديد بشكل غير مباشر فيكون حينما يتعلق الأمر مثلا برقم الضمان الإجتماعي أو رقم الزبون أو رقم العامل[1].

ويعتد القضاء الفرنسي بحق العامل في الحياة الخاصة عند استخدامه لأدوات العمل، فلا يجوز لرب العمل فتح الملفات التي تم تحديدها من قبل العامل على انها ذات محتوى شخصي في القرص الصلب للكمبيوتر[2].

وقد أثار عنوان بروتوكول الأنترنت IP[3]الكثير من النقاش حول إعتباره من المعلومات التي تسمح بتحديد هوية الشخص بشكل غير مباشر، أي اعتبارها من قبيل المعطيات الإسمية؟

إعتبرت اللجنة الوطنية للمعلوماتية والحريات في بيان لها أن عنوان بروتوكول الأنترنت مثل رقم الهاتف يدخل ضمن مفهوم المعطيات الشخصية المحددة في المادة 2 من القانون 6 جانفي 1978لأنه يتيح التعرف بشكل مباشر أو غير مباشر على الشخص[4].

أما القضاء الفرنسي فقد إختلفت أحكامه حول هذه المسالة، حيث قضت محكمة إستئناف باريس في 15 ماي 2007[5] أن هذه السلسلة من الأرقام –عنوان بروتوكول الأنترنت– لا تشكل في الواقع معطيات شخصية، كونها لا تسمح بتحديد هوية المستخدم الذي يستخدم الحاسب الآلي على وجه التحديد، وفي قرار آخر لها في 27 أفريل 2007[6] في قضية مشابهة قضت بأن عنوان بروتوكول الأنترنت لا يمكن أن يكتسي الطابع الشخصي لأنه يحدد جهاز الكمبيوتر وليس مستخدمه، وهذا الأخير يمكن تحديده فقط في إطار إتخاد بعض الإجراءات القضائية حينما يتم إستخدام الجهاز لأغراض غير مشروعة. كما نقضت محكمة النقض الفرنسية حكم محكمة إستناف رين rennes القاضي بإخلاء سبيل المتهم cyrille الذي إستخدم برنامج

---

[1]-**Thiébaut Devergranne,** Donnees personnelles, articledisponible en ligne a l'adresse suivante:
: https://www.donneespersonnelles.fr/donnees-personnelles,**ANTHONY BEM, La** protection des données à caractère personnel par les droits français et européen, articledisponible en ligne a l'adresse suivante:

: http://www.legavox.fr/blog/maitre-anthony-bem/protection-donnees-caractere-personnel-droits-16105.htm#.VvfUjNKLQSk

[2]-Cass Crim 17 mai 2005,chamber sociale, nº de pourvoi:03-40017

[3]-وهو برتوكول يتكون من عدد 32 بت في شكل رقمي، يأخذ شكل التنقيط العشري Dotted Decimal Form مثل رقم 62.127.30.236، حيث يشير الجزء الأول من اليسار إلى المنطقة الجغرافية، والجزء الثاني لمزود الخدمة، والثالث لمجموعة الحاسبات الآلية المرتبطة، والرابع يحدد جهاز الحاسبات الإلكترونية الذي تم الإتصال منه.

[4]- Article du 2 août 2007 disponible en ligne a l'adresse suivante:
: http://www.cnil.fr/linstitution/actualite/article/article/ladresse-ip-est-une-donnee-a-caractere-personnel-pour-lensemble-des-cnil-europeennes.
Délibération de la CNIL n° 2006-294, 21 décembre 2006

[5]-CA paris 15 mai 2007,cité par: **Murielle cahen**, L'ADRESSE IP EST ELLE UNE DONNEE PERSONELLE, article disponible en lingne á l'adresse suivante:
http://www.murielle cahen.com/publications/p_donnees3.asp?

6- Cour d'appel de Paris, 13ème chambre, section B Arrêt du 27 avril 2007, Anthony G. / SCPP, accessible sur legalis.net

pair à pairمما سمح له بتحميل إحدى المقطوعات الموسيقية الخاصة بالمجني عليه وتم التعرف عليه من خلال عنوان بروتوكول الأنترنت الخاص به، كون محضر جمع الإستدلالات باطل لعدم الحصول على إذن من اللجنة الوطنية للمعلوماتية والحريات، ونقضت محكمة النقض حكم محكمة الإستئناف، وقضت ان ذلك لا يمثل معالجة للمعطيات الإسمية المتعلقة بالجرائم المنصوص عليها في المواد 25،9،2 من القانون رقم 17-1978.[1]

وفي حكم آخر تم إعتبار أن عنوان بروتوكول الأنترنت هو بيان ذا طابع شخصي يسمح بالتعرف على الشخص من خلال تحديد كمبيوتر معين[2] .

من خلال ما سبق يتضح أن أحكام القضاء تتضارب حول اعتبار عنوان بروتوكول الأنترنت من المعطيات الشخصية، ومن جهتنا نرى أن عنوان بروتوكول الأنترنت وإن كان يسمح بالتّعرف على هوية الحاسوب المرتبط بالانترنت ومن تم الوصول إلى هوية الشخص، إلا أن مصداقيّة الهويّة عبر الانترنت (*IP*) تتقلّص كثيراً إذا علمنا أنّ هذا الأخير يمكن أن يكون ساكنا أو ديناميكي، وهذا يعني أن الشخص إذا قام بالإتصال بالأنترنت يتم تعيين عنوان بروتوكول جديد، وهنا يمكن القول أن مجرّد وجود شخص في الجزائر فإنه يملك فورًا هوية رقمية محددة حقا حال وجوده على الانترنت, إلاّ أنّه إذا حدث وانقطع الإرسال فإن الشخص إذا عاد من جديد إلى الانترنت فإن الهويّة السّابقة لن تكون له وإنّما لغيره، فضلا عن ذلك فإن الإتصال بالأنترنت حينما يكون مرتبط بأكثر من جهاز كما هو الحال في مقاهي الأنترنت يدل في هذه الحالة على هوية أكثر من مستخدم، وهو ما يتنافى ومدلول المعطيات الشخصية المقصود في القانون رقم 17-78 في كونها معطيات تدل على شخصية صاحبها **بشكل دائم** وليس مؤقت، محدد وحصري. أكثر من ذلك، هنالك برامج عديدة على شبكة الأنترنت تعطي ميزة التصفح دون كشف الهوية مثل super free pmptp vpn accounts.

وبالرغم من ذلك لا بد من بسط الحماية على هذا العنصر في حالات معينة، ويكون ذلك بإعتماد نص قانوني واضح ودقيق حول مفهوم المعطيات الشخصية.

2- النشـــاط الإجرامـــي

يتمثل في فعل المعالجة الإلكترونية للمعطيات، سواء كان في شكل جمع وتسجيل وتنظيم وتخزين تعديل إسترجاع أو إستخدام، نقل، نشر أو توفير أو محاذاة، محو أو تدمير المعطيات الشخصية[3]، وكذلك جميع العمليات المتعلقة باستغلال قواعد المعطيات أو الفهارس أو السجلات أو البطاقات أو بالربط البيني[4]،

---

[1]-Cass, Crim 13 janvier 2009, N° de pourvoi: 08-84088

[2]- TGI Paris, 5 mars 2009,cité par: Roland Magdane c,http://www.legavox.fr/blog/maitre-anthony-bem/valeur-juridique-ordinateur-comme-element-12271.htm#.Vviiq9KLQSk

[3]-Art 2/3 du loi 78-17 ,Modifié par Loi n°2004-801 du 6 août 2004 - art. 1 JORF 7 août 2004 . Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

[4]-الفقرة 1 من المادة 6 من القانون عدد 63 لسنة 2004 التونسي المتعلق بحماية المعطيات الشخصية.

دون مراعاة الشروط القانونية المطلوبة، كتلك الواردة في القانون الفرنسي رقم 17- 1978 المعدل أو الواردة في القانون التونسي الخاص بحماية المعطيات الشخصية.

وعليه توجد شكليات سابقة للمعالجة الإلكترونية، كما ينبغي على الشخص الذي يجري هذه المعالجة أن يفي بصفة لاحقة بالشروط التي يمكن أن تعرض عليه من جانب السلطة الإدارية عند أداء هذه الشكليات، وسابقا كانت الشكليات في فرنسا تختلف وفق لطبيعة الشخص المسؤول عن المعالجة، أما بعد التعديل بالقانون رقم 108-2004 أصبحت المعالجة تختلف وفقا لطبيعة المعطيات المعالجة ومدى خطورتها.

2-1 عدم إعلام اللجنة المختصة أو بدون تصريح منها أو طلب رايها

ورد النص على هذه الجريمة في المادة226-16[1] من قانون العقوبات الفرنسي، ويتحقق النشاط المادي لهذه الجريمة بأي معالجة إلكترونية للمعطيات الشخصية دون إتخاذ الشكليات اللازم إستفاءها مسبقا ولو بإهمال منه. وقد نظم المشرع هذه الشكليات في القسم الرابع من القانون 17-78[2].في السابق كانت المعالجة التي تتم لصالح القطاع العام من ذلك بنوك المعلومات التابعة للسلطة التنفيدية وأجهزتها من خلال مواقع الأنترنت تخضع بشكل منتظم إلى رأي مسبق d'un avis préalable للجنة الوطنية للمعلوماتية والحريات ، بينما المعالجات التي تتم للقطاع الخاص كبنوك المعلومات التي تنشئها شركات التأمين والبنوك كانت تتطلب اجراء اعلان déclaration أمام اللجنة الوطنية للمعلوماتية والحريات، أما الآن فالمبدأ هو ضرورة إجراء **إعلان** مسبق déclaration préalable للمعالجة أمام اللجنة سواء تعلق الأمر بالقطاع العام أو الخاص[3].

وبشكل إستثنائي نص القانون على حالات تكون فيها المعالجة محل إعلان **مبسط**[4] كتحديد الغرض من المعالجة وتحديد مدة حفظ المعطيات الشخصية. فضلا عما سبق هناك بعض المعالجات يجب ان تكون محل **تصريح** من اللجنة بسبب حساسية المعطيات محل المعالجة مثل المعطيات دات الطابع السياسي او الفلسفي او الديني او متعلقة بالجرائم والعقوبات او تدابير الأمن...[5]، وهناك البعض من المعالجات الخاصة بالقطاع العام لا يمكن ان تحصل على تصريح إلا بعد أن تقدم للجنة أمرا مكتوبا ومسببا، وتختلف الجهات التي تعطي

---

[1]-Article 226-16du CPF dispose que: " Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en oeuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

Est puni des mêmes peines le fait, y compris par négligence, de procéder ou de faire procéder à un traitement qui a fait l'objet de l'une des mesures prévues au 2° du I de l'article 45 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

[2]-déclaration auprès de la CNIL, autorisation préalable à la CNIL déclaration simplifiée, voir chapitre iv , loi 78-17 , voi aussi Centre national de la recherche scientifique:http://www.cil.cnrs.fr/CIL/spip.php?article1427

[3]- **Nicolas Courtheoux** ,Les sanctions pénales dans la loi 78-17 relative à l'informatique, aux fichiers et aux libertés, article disponible en lingne á l'adresse suivante :

http://www.e-juristes.org/les-sanctions-penales-dans-la-loi/

[4]-Voir art 24 loi n° 78-17 Modifié par Loi n°2004-801 du 6 août 2004 - art. 4 JORF 7 août 2004

[5]-Voir art 25 loi n° 78-17 Modifié par Loi n°2004-801 du 6 août 2004 - art. 4 JORF 7 août 2004

التصريح لمثل هذه المعالجات، ويتضمن طلب الرأي بعض المعلومات المحددة مثل الغرض من المعالجة، مدة حفظ المعطيات...[1].

وإلى جانب المشرع الفرنسي، نجد المشرع التونسي ينص بدوره بموجب المادة 7 من القانون 2004 على ضرورة اخضاع كل عملية معالجة معطيات شخصية **لتصريح** مسبق يودع بمقر الهيئة الوطنية لحماية المعطيات الشخصية، وكما هو الشان في التشريع الفرنسي، أخضع المشرع التونسي معالجة المعطيات الحساسة المتعلقة بصفة مباشرة أو غير مباشرة بالأصول العرقية او الجينية او بالمعتقدات الدينية او بالأفكار السياسية او الفلسفية او النقابية إلىضرورة الحصول على **ترخيص** من الهيئة الوطنية لحماية المعطيات الشخصية.

ويعتبر هذا النوع من السلوكات من جرائم الخطر، أي ان المشرع يستشعر خطورة الجاني من السلوك المجرد الذي يقوم به ولا يرتب على حصوله أثر مادي ضار حتى يتم عقابه.

2-2 استخدام رقم التسجيل الخاص بالمعطيات الشخصية بدون ترخيص

ورد النص على هذه الجريمة في المادة 226-16-1[2] من قانون العقوبات الفرنسي، ويتحقق النشاط المادي لهذه الجريمة باي معالجة إلكترونية للمعطيات الشخصية والمدرجة *ضمن المعطيات التي تحمل رقم تسجيل لأشخاص في السجل القومي، للتحقق من الشخص الطبيعي خارج نطاق الترخيص, وبدون مراعاة الشروط الواردة في القانون رقم 17 لسنة 1978."*

3-2 عدم احترام القواعد التبسيطية أو قواعد الإعفاء

ورد النص على هذه الجريمة في المادة 226-16-1 -أ[3] من قانون العقوبات الفرنسي، و يتحقق النشاط المادي لهذه الجريمة بمعالجة إلكترونية للمعطيات الشخصية *وفقا للشروط الواردة في المادة 24 من القانون رقم 17-78 بدون احترام القواعد التبسيطية او قواعد الإعفاء التي وضعتها اللجنة الوطنية للمعلوماتية و الحريات.*

ب- الركــن المعــنوي

[1]-Voir art 27 loi n° 78-17 Modifié parLOI n°2016-41 du 26 janvier 2016 - art. 193

[2]-Art 226-16-1 du CPF dispose que :" Le fait, hors les cas où le traitement a été autorisé dans les conditions prévues par la loi n° 78-17 du 6 janvier 1978 précitée, de procéder ou faire procéder à un traitement de données à caractère personnel incluant parmi les données sur lesquelles il porte le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

[3]-**Article 226-16-1-A** du CPF. Créé par Loi n°2004-801 du 6 août 2004 - art. 14 JORF 7 août 2004 dispose que " Lorsqu'il a été procédé ou fait procéder à un traitement de données à caractère personnel dans les conditions prévues par le I ou le II de l'article 24 de la loi n° 78-17 du 6 janvier 1978 précitée, le fait de ne pas respecter, y compris par négligence, les normes simplifiées ou d'exonération établies à cet effet par la Commission nationale de l'informatique et des libertés est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende

بالنسبة لجريمة معالجة المعطيات الشخصية دون إعلان اللجنة المختصة أو تصريح منها أو طلب رأيها, إعتبرتها محكمة النقض الفرنسية من الجرائم المادية التي يفترض توافرالقصد الجنائي فيها بمجرد إرتكاب الفعل[1]، وذلك خلافا لقضاء الموضوع الذي تطلب توافر القصد الجنائي في الفعل.

ونرى من جهتنا أن استخدام المشرع لعبارة إهمال y compris par négligence الواردة في نص المادة 226-16 يدل على أن هذه الجنحة تقع عن طريق العمد أو عن طريق الخطا غير العمدي أي الخطأ.

أما في التشريع التونسي فلا تقع هذه الجريمة إلا مقصودة، ونستدل على ذلك بعبارة " **كل من يتعمد**" الواردة في نص الفصل 90 من القانون 2004.

وعن جريمة إستخدام رقم التسجيل بدون ترخيص تعد من الجرائم العمدية ويرجع ذلك لطبيعة الأفعال المكونة لها، يتطلب لقيامها القصد الجنائي بعنصريه العلم والإرادة، فالجاني يجب أن يعلم بالطابع الشخصي للمعطيات، وأن المعالجة تتم الكترونية دون مراعاة الشروط القانونية، وأن تتجه إرادته إلى القيام بهذه المعالجة.

أما الجريمة المتعلقة بعدم إحترام القواعد التبسيطية وقواعد الإعفاء فيتخذ الركن المعنوي فيها صورة القصد الجنائي بعنصريه العلم والإرادة. وهو ما يستفاد صراحة من عبارة procédé ou fait procéder بما يفيد القيام بالفعل عن عمد و إرادة، فضلا عن ذلك تميز نص المادة 226-16-1-أ من قانون العقوبات من ناحية البناء المعنوي بأن المشرع استخدم فيه عبارة إهمال"y compris par negligence وهو الأمر الذي يستفاد منه أن هذه الجريمة تقوم حتى وإن تم ارتكابها عن طريق الخطأ غير العمدي.

ت- العقــوبــة

يعاقب المشرع الفرنسي على هذه الجريمة بعقوبة الحبس خمس سنوات وغرامة 300000 يورو، هذا بالإضافة إلى العقوبات الإضافية المنصوص عليها في المادة 226-31 من قانون العقوبات، وإمكان معاقبة الشخص المعنوي- فضلا عن عقوبة الغرامة- بالعقوبات المنصوص عليها في المادة 131-39، وذلك طبقا للمادة 226-30 عقوبات، كما يحكم بمسح أو حذف كل أو بعض المعطيات التي كانت محلا للجريمة، و يكون ذلك في حضور الأفراد ووكلاء عن اللجنة الوطنية للمعلوماتية والحريات[2].

أما المشرع التونسي فيعاقب على تلك الجريمة بموجب الفصل 90 من قانون 2004 بالسجن مدة عام و بخطية قدرها خمسة الاف دينار.

---

[1]-Cass crim 3Decembre 1987,Bull,Crim n 381.

مشار اليه لدى:**د. مدحت رمضان عبد الحليم**، الحماية الجنائية للتجارة الإلكترونية، المرجع السابق، ص94.

[2]-Voir Article 226-22-2 du CPF Créé par Loi n°2004-801 du 6 août 2004 - art. 14 JORF 7 août 2004

ماشاء الله عثمان محمد الزوي، الحماية الجنائية لحرمة الحياة الخاصة في التشريع الليبي بالمقارنة مع التشريعين الفرنسي والمصري، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 2012، ص227.

ثانيا- المعالجة الآلية للمعطيات الشخصية دون إحترام الالتزامات الأمنية

للحفاظ على أمن المعطيات الشخصية، جرم المشرع الفرنسي عدم أخد الإحتياطات المعقولة حسب الأصول العلمية لحماية هذه المعطيات بموجب المادة 226-17[1] من قانون العقوبات، وهو نفس النهج الذي اتبعه المشرع التونسي حيث الزم بموجب المادة 18 كل شخص بأن يتخد الإحتياطات اللازمة للمحافظة على أمن المعطيات، وبناء عليه عاقب المشرع بموجب الفصل 94 كل من يخالف ذلك.

وتقوم هذه الجريمة على ركنيين، مادي ومعنوي وهو ما سيتم تفصيله فيمايلـــي:

أ-الركـــن المـــادي

ويتحقق النشاط المادي لهذه الجريمة بالمعالجة الإلكترونية للمعطيات الشخصية دون تطبيق التدابيرالمنصوص عليها في المادة 34 من القانون رقم 78-17 في 6 يناير 1978 .

وتنص المادة 34 على ضرورة أخد الإحتياطات اللازمة نظرا لطبيعة المعطيات والمخاطر الناجمة عن المعالجة للحفاظ على أمن المعطيات خاصة منع تشويهها أو إتلافها أو وصول شخص غير مرخص له بذلك إليها.

والملاحظ أن المشرع الفرنسي إستخدم مصطلحات واسعة الدلالة، تغطي كل الإحتياطات اللازمة للحفاظ على أمن المعطيات دون حصرها في إحتياط معين، وذلك ضد أي فعل من شانه تشويه أو إتلاف هذه المعطيات أو الوصول إلى هذه المعطيات دون ترخيص. وقد سبق بيان الأفعال التي تأخد هذه الصور من التعدي على معطيات النظام، فنحيل إليها.

هذا وقد وسع المشرع التونسي دائرة التجريم إلى كل إضرار بالمعطيات، وهو ما يستفاد بوضوح من عبارة"..من تعديلها او **الإضرار** بها أو الإطلاع عليها..." الواردة في الفصل 18 من قانون 2004. إلا انه في المقابل حصر هذه الإحتياطات في الفصل 19 من نفس القانون فيمايلي:

- عدم وضع المعدات والتجهيزات المستعملة في معالجة المعطياتالشخصية في ظروف أو أماكن تمكن من الوصول إليها من قبل أشخاص غير مأذون لهم بذلك.
- عدم إمكانية قراءة السندات أو نسخها أو تعديلها أو نقلها من قبل شخص غير مأذون له بذلك.
- -عدم إمكانية إقحام أي معطيات في نظام المعلومات دون إذن في ذلك وعدم إمكانية الإطلاع على المعطيات المسجلة أو محوها أو التشطيب عليها.
- عدم إمكانية استعمال نظام معالجة المعلومات من قبل أشخاص غير مأذون لهم بذلك.

[1]Article 226-17 du CPF Modifié par Loi n°2004-801 du 6 août 2004 - art. 14 JORF 7 août 2004 dispose que:" Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en oeuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

- إمكانية التثبت اللاحق من هوية الأشخاص الذي نفذوا إلى نظام المعلومات والمعطيات التي تم إقحامها وزمن ذلك والشخص الذي تولى ذلك.
- -عدم إمكانية قراءة المعطيات أو نسخها أو تعديلها أو محوها أو التشطيب عليها أثناء إحالتها أو نقل سندها.
- -الحفاظ على المعطيات عبر إحداث نسخ منها احتياطية وآمنة.

أما عن المحل الذي ينصب عليه النشاط فيتمثل في المعطيات الشخصية، ونحيل في ذلك إلى ما سبق تفصيله في هذا الشأن.

ب-الركـــن المعنـــوي

تعتبر هذه الجريمة من الجرائم غير العمدية، يتحقق الركن المعنوي فيها عن طريق الإهمال، على الرغم من أن المادة 226-17 من قانون العقوبات الفرنسي، والفصل 94 من القانون التونسي الذي أحال للفصل 18 و19 لم يتحدث عنه بشكل صريح، وذلك لأن غياب الإحتياطات تستند إلى الإهمال.

ت-العقـــوبـــة

يعاقب المشرع الفرنسي على هذه الجريمة بالحبس خمس سنوات وغرامة ثلاثمائة الف يورو، إلى جانب العقوبات التكميلية المنصوص عليها في المادة 226-31 عقوبات، كما يمكن معاقبة الشخص المعنوي بالعقوبات المنصوص عليها في المادة 131-39 طبقا للمادة 226-30 عقوبات فضلا عن الغرامة.

أما المشرع التونسي فيعاقب عليها بموجب الفصل 94 بالسجن مدة ثلاثة اشهر وبخطية قدرها ألف دينار.

ثالثا-المعالجة الآلية للمعطيات الشخصية مع إعتراض صاحبها

تنص الفقرة 2 من المادة 6 من القانون رقم 801 لسنة 2004 على أنه لا يمكن أن ترد المعالجة الآلية إلا على المعطيات الشخصية التي تجمع وتعامل بصورة مشروعة وصحيحة، كما أعطت المادة 38[1] من القانون 17-78 الحق للشخص الطبيعي الإعتراض على معالجة معطياته لأسباب مشروعة، كما جرم المشرع المعالجة الإلكترونية للمعطيات الشخصية في حالة إعتراض الشخص المعني على تلك المعالجة وذلك بموجب المادة ***226-18-1***[2] من قانون العقوبات المضافة بموجب القانون 2004-801.

[1]Article 38 du CPF modifiee par loi 2004-801dispose que: Toute personne physique a le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement.

[2] -Article 226-18 du CPF Modifié par Loi n°2004-801 du 6 août 2004 - art. 14 JORF 7 août 2004 dispose que "Le fait de procéder à un traitement de données à caractère personnel concernant une personne physique malgré l'opposition de cette personne, lorsque ce traitement répond à des fins de prospection, notamment commerciale, ou lorsque cette opposition est fondée sur des motifs légitimes, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

وإلى جانب المشرع الفرنسي، نجد المشرع التونسي الذي عاقب على هذا الفعل بموجب الفصل 91 من قانون 2004 كمايلي"يعاقب...الذي يواصل معالجة المعطيات الشخصية رغم إعتراض المعنـــي بالأمر.."

أ-الركن المـــادي

يتحقق الركن المادي لهذه الجريمة عن طريق نشاط يرتكبه الجاني يتمثل في الإستمرار في معالجة معطيات شخصية تخص شخصا طبيعيا على الرغم من إعتراض هذا الشخص، وهو يشكل نوعا من ممارسة الحق في **النسيان على شبكة الأنترنت**[1]، والملاحظ ان المادة 226-18-1 عقوبات فرنسي تتطلب أن يمارس هذا الإعتراض في حالتين محددتين: الحالة الأولى أن يكون هذا الإعتراض قائما على **أسباب مشروعة**، بما يدل وجود حق القيام بتجميع معطيات إسمية بغرض معالجتها معلوماتيا، مع ضرورة التناسب بين المعلومات والهدف من تسجيلها، فمثلا في حال تسجيل معطيات عن المرضى العقليين لا محل لوضع بيان عن الطلاق او عن الديانة لعدم وجود ضرورة حيوية تبرر ذلك[2].

وأن الأشخاص المعنية لا يمكن أن تعترض على ذلك إلا إذا كان لديها أسباب مشروعة تبرر هذا الإعتراض، وهو نفس الشرط الذي تضمنه المشرع التونسي في الفصل 42، حينما نص"...و **لأسباب وجيهة ومشروعة وجدية** ..."

ولم يحدد المشرع ولا القضاء المقصود بالأسباب المشروعة، مايعني أن إرادة المشرع إتجهت بوضوح حول حماية مصلحة الشخص الذي تتم المعالجة لصالحه.

والحالة الثانية هي حينما **تستخدم معطياته الخاصة به لأغراض بحثية خاصة التجارية منها**. وطبقا للفقرة الأخيرة من المادة 38 من القانون 17-78 المعدلة، فإن حق الإعتراض لا يطبق في الأحوال التي تتم فيها المعالجة بنص قانوني لتعلق المعالجة في هذه الحالات بالمصلحة العـــامة.

وما تجدر الإشارة إليه أن القانون لم يحدد شكلا معين لهذا الإعتراض، فهذا الحق يمارس مباشرة من قبل الشخص المعني بالمعطيات المعالجة، وقضت محكمة النقض أن حق الإعتراض يقدم للجنة الوطنية للمعلوماتية والحريـــات[3].

وفي الأخير يجدر التنويه إلى أن هنالك نظام خاص بممارسة الإعتراض على المعالجة الآلية في مجال الصحة، حيث يؤخذ في الإعتبار حق الإعتراض بمافي ذلك الأشخاص المتوفين.[4]

---

[1]-**Thiébaut Devergranne**, Le droit d'opposition institué par la loi informatique et libertés, article disponible en lingne á l'adresse suivante:https://www.donneespersonnelles.fr/droit-opposition

[2]-**د. عبد الفتاح بيومي حجازي**، النظام القانوني لحماية التجارة الإلكترونية، المرجع السابق، ص76.

[3]-Cass. crim., 28 sept. 2004, **Thiébaut Devergranne**, Le droit d'opposition institué par la loi informatique et libertés, disponible en ligne a l'adresse précédente.

[4]- ففي حالة ما إذا تطلب البحث جمع وتحديد العينات البيولوجية، يجب أخذ الموافقة الصريحة من الأشخاص المعنيين قبل تنفيذ المعالجة، فيما يخص المعلومات الخاصة بالأشخاص المتوفين بمافي ذلك الواردة في الشهادات التي تظهر سبب الوفاة يمكن أن تكون محل معالجة إلا إذا أعرب الشخص في حياته عن رفضه كتابيا. أنظر المادة 56 من القانون 17-78. والمادة 226-19-1 من قانون العقوبات الفرنسي.

ب-الركــن المعــنوي

تعد هذه الجريمة من الجرائم العمدية، يأخذ فيها الركن المعنوي القصد الجنائي العام بعنصريه العلم والإرادة، إذ يجب ان يعلم الجاني بأنه يقوم بمعالجة الكترونية، وهده المعالجة تنصب على معطيات شخصية تتعلق بشخص، وأن هذا الشخص سبق واعترض على هذه المعالجة، وان تتجه إرادته إلى الفعل وإلـــــى النتيجة.

ت-العقوبــة

يعاقب المشرع على هذه الجريمة بالحبس خمس سنوات وغرامة ثلاثمائة الف يورو، بالإضافة إلى العقوبات التكميلية التي تطبق على الأفراد، وقد يحكم القاضي بمسح جميع او بعض المعطيات الإسمية التي كانت محلا للجريمة.

أما المشرع التونسي فيعاقب عليها بموجب الفصل 91 بالسجن مدة عام وخطية قدرها خمسة الاف دينار .

"رابعا- المعالجة الآلية للمعطيات الشخصية بدون تبصير ذوي الشأن في مجال البحث الطبي

أجريت دراسة عام 2003 على استخدام الإدارة الطبية السجلات الإلكترونية لحفظ المعطيات الخاصة بالمرضى، وتبين ان المرضى عموما لا يمانعون في حفظ معطياتهم الشخصية في سجلات الكترونية، ومع ذلك كان لديهم تخوف وقلق من أن معطياتهم قد تكون عرضة لخطر القرصنة وإنتهاك أمن المعلومات[1]. وعلى هذا الأساس إهتم المشرع الفرنسي بحماية المعطيات الإسمية في مجال البحث الطبي بمقتضى المادة **226-19-1** "[2]من قانون العقوبات الفرنسي، أما المشرع التونسي وإن نظم في الفصل 62 معالجة المعطيات الشخصية المتعلقة بالصحة، إلا أنه لم يكفل حماية مباشرة في حال الإخلال بمقتضيات هذا الفصل، بل جرم جوانب أخرى مثل تلك المتعلقة بالشخص القائم عن المعالجة بأن يكون من قبل الأطباء أو الأشخاص الخاضعين بحكم مهامهم إلى واجب الحفاظ على السر المهني بمقتضى الفصل 63 الذي أحال إليه الفصل 87.

أ-الــركــن المــادي

---

[1]- **Post note ,** Data protection and medical research,January 2005 , n 235, p3

[2]-Article 226-19-1 du CPFCréé par loi 2004-801 dispose que: En cas de traitement de données à caractère personnel ayant pour fin la recherche dans le domaine de la santé, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende le fait de procéder à un traitement :

1° Sans avoir préalablement informé individuellement les personnes sur le compte desquelles des données à caractère personnel sont recueillies ou transmises de leur droit d'accès, de rectification et d'opposition, de la nature des données transmises et des destinataires de celles-ci ;

2° Malgré l'opposition de la personne concernée ou, lorsqu'il est prévu par la loi, en l'absence du consentement éclairé et exprès de la personne, ou s'il s'agit d'une personne décédée, malgré le refus exprimé par celle-ci de son vivant.

يتحقق الركن المادي لهذه الجريمة عن طريق نشاط يرتكبه الجاني يتمثل في المعالجة الآلية للمعطيات الشخصية التي تستهدف البحث في مجال الصحة دون إعلام الشخص المعني بها مسبقا بما يجمع عنه من معلومات إسمية، وحقه في التعديل والاعتراض عليها، فضلا عن عدم الحصول على معلومات عن الجهة المرسل إليها هذه المعلومات.

كما يتحقق الركن المادي أيضا بقيام الجاني بإجراء المعالجة على الرغم من إعتراض صاحب الشخص المعني، أو كان الحضر بمقتضى القانون، أو عنـــدما يتعلق بشخص متوفى على الرغم من رفضه خلال حياته أو رفض أهلـــه ذلك.

أما إذا عدنا للقانون التونسي، فنجده يجرم بصفة عامة كل نشر للمعطيات الشخصية الواقع معالجتها في إطار البحث العلمي في حالة عدم موافقة المعني بالأمر أو ورثته أو وليه على ذلك صراحة وذلك بموجب الفصل 87 من قانون 2004.

ب-الـــركن المـــعنـــوي

تعد هذه الجريمة من الجرائم العمدية، يأخذ فيها الركن المعنوي القصد الجنائي العام بعنصريه العلم والإرادة، إذ يجب أن يعلم الجاني بكافة العناصر الداخلة في تشكيل الجريمة، ومن قبيل ذلك علمه بأن فعله ينصب على معطيات ذات طابع شخصي، أو أن يعلم بإعتراض صاحب الشان في ذلك، أو أن القانون يحضر عليه مثل هذه المعالجات، فضلا عن علمه بخطورة الفعل على المصلحة التي يحميها القانون. فإذا إنتفى العلم بأحد العناصر السابقة إنتفى تبعا له القصد الجنائي.

إضافة إلى ضرورة توافر العلم، لابد من توافر الإرادة، والإرادة في القصد الجنائي لا بد أن تتجه إلى إرتكاب الفعل وإلى تحقيق النتيجة.

ت-العـــقوبـــة

يعاقب المشرع على هذه الجريمة بعقوبة الحبس خمس سنوات وغرامة ثلاثمئة ألف يورو، بالإضافة إلى العقوبات المنصوص عليها في المادة 226-31 عقوبات، مع إمكانية معاقبة الأشخاص المعنوية طبقا للمادة 226-30 عقوبات.

خامسا-المعالجة غير المشروعة للمعطيات الشخصية

تناول المشرع الفرنسي بالتجريم بموجب المادة 226-18 ،226-20 ،226-19مجموعة من الأفعال إستشعر بخطورتها على المعطيات الشخصية، وتشمل هذه الأفعال العمليات التي ترد على هذه المعطيات من جمعها وتخزينها بشكل غير مشروع. وهو ما سنحاول بيانه من خلال التعرض لأركان الجريمة وعقوبتها كمايلي:

أ-الركـــن المـــادي

1-الجمع غير المشروع للمعطيات الشخصية

من المباديء الأساسية التي إعتمدها القانون 17-78 في الفقرة الثانية من المادة 6 وهو مبدأ المشروعية، بأن تتم عملية جمع المعطيات بطريقة مشروعة وقانونية[1]، وبناء عليه جرم بموجب المادة 226-18 "[2] من قانون العقوبات عملية جمع المعطيات الشخصية بطريق الغش أو بطريقة غير قانونية.

ويقابل هذا النص الفصل 88 من القانون التونسي رقم 2004 الذي جرم كل من يحمل شخصا على إعطاء موافقته على معالجة المعطيات الشخصية بإستعمال الحيلة أو العنف او التـــهديد.

ويتحقق الركن المادي في نشاط يرتكبه الجاني يتمثل في جمع المعطيات بطريقة لا تخلو من الإحتيال و الغش.

والملاحظ أن المشرع الفرنسي قد إستخدم عبارات عامة تسمح بأن تنطبق على الكثير من الحالات، مثاله عملية جمع عناوين البريد الإلكتروني دون علم الجهات المعنية[3]، جمع المعطيات دون موافقة اللجنة الوطنية للمعلوماتية والحريات[4] .

وإذا كان المشرع الفرنسي يجرم صورة واحدة من صور المعالجة ألا وهو فعل "**الجمع**"، فان المشرع التونسي كان اوسع حينما نص في الفصل 88" على "..**معالجة المعطيات الشخصية...**"، على ان يكون ذلك باستعمال **الحيلة أو العنف أو التهديد.**

2-التخزين والمعالجة غير المشروعة للمعطيات الشخصية الحساسة

ينص المشرع الفرنسي في الفقرة 1 من المادة 8 المعدلة من القانون 17-78 على حضر تجميع أو معالجة المعطيات الحساسة كتلك المتعلقة بالآراء السياسية أو الفلسفية أو الدينية أو غيرها، وعلى هذا الأساس فقد جرم بموجب المادة 226-19[5] فعل تخزين أو حفظ المعطيات الحساسة. وكذلك فعل المشرع التونسي بموجب فصل 87 الذي احال للفصل 13 و14 من قانون 2004.

---

[1]Article 6 alinéa 2 du loi 17-78 dispose que " Les données sont collectées et traitées de manière loyale et licite"

[2]- article 226-18 du CPF Modifié par Loi n°2004-801 du 6 août 2004 - art. 14 JORF 7 août 2004 dispose que " Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

[3]- Cass, Crim,du 14 mars 2006 (n°05-83-423) cité par,**Thiébaut Devergranne**, Le principe de loyauté et de licéité de la collecte des données. Articledisponible en ligne á l'adresse suivante: https://www.donneespersonnelles.fr/le-principe-de-loyaute-et-de-liceite-de-la-collecte-des-donnees

[4]-Cass Crim 13 janvier 2009, n de pourvoi:08-84088.

[5]-Article 226-19du *CPF*Modifié par LOI n°2017-86 du 27 janvier 2017 - art. 171 dispose que : Le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée, sans le consentement exprès de l'intéressé, des données à caractère personnel qui, directement ou indirectement, font apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales des personnes, ou qui sont relatives à la santé ou à l'orientation sexuelle ou à l'identité de genre de celles-ci, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

Est puni des mêmes peines le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée des données à caractère personnel concernant des infractions, des condamnations ou des mesures de sûreté.

ويقوم الركن المادي لهذه الجريمة بقيام الجاني بتخزين طائفة من المعطيات الشخصية في ذاكرة معلوماتية على أن تكشف هذه المعطيات بشكل مباشرأوغير مباشرعن أصول عرقية أوإثنية أو آراء سياسية، فلسفيةأودينية، أوالانتماء النقابي للأفراد،أوالتي تتعلق بالصحة أوالميول الجنسية.

والسبب في تجريم مثل هذه الأفعال إستبعاد أي تمييز يقوم على الأصل العرقي أو الديني أو السياسي الأمر الذي يخل بمبدأ المساواة، وذلك من أجل حماية الفكر والرأي والتعبير والعقيدة، فضلا على أن هذه المسائل تدخل في نطاق الحياة الخاصة بمعناها الواســع[1].

وقد إشترط المشرع لقيام هذه الجريمة عدم موافقة الشخص المعني بها، والرضا حسب المادة 226-19 يجب أن يكون صريحا، أو في غير الأحوال التي يجيزها القانون، وهو ما أشارت إليه الفقرة الأخيرة من المادة 8 من القانون رقم 17-78 على أن هذا الحظر لا يخص المعالجة المبررة للمنفعة العامة. وقد إشترط المشرع التونسي بموجب الفقرة 2 من الفصل 14 أن يكون الرضا بأي وسيلة تترك أثرا كتابيا، على أن هذا الحظر لا يخص المعطيات التي أصبحت تكتسي صبغة عامة بشكل بين، أو إذا كانت معالجتها ضرورية لخدمة الأغراض التاريخية أو العلمية أو إذا كانت ضرورية لحماية المصالح الحيوية للمعني بالأمر.

كما يتحقق الركن المادي بقيام كل من يخزن أو يحفظ في ذاكرة معلوماتية المعطيات الشخصية المتعلقة بالجرائم أو الإدانات أو تدابير الأمن في غير الأحوال التي ينص عليها القانون، وذات الفعل جرمه المشرع التونسي بموجب الفصل 13 من قانون 2004 كما يلي "تحجر المعطيات الشخصية المتعلقة بالجرائم او بمعاينتها او بالتتبعات الجزائية او بالعقوبات او بالتدابير الإحترازية او بالسوابق العدلية".

وفي ذلك أجازت المادة 9 من القانون 17- 78 معالجة هذه النوعية من المعطيات للمحاكم والسلطات العامة والأشخاص المعنوية التي تدير مؤسسات عامة التي تتصرف في حدود صلاحيتها العامة. فتدخل صحيفة السوابق الجنائية الوطنية في نطاق الإستثناء، صحيفة الحالة الجنائية الوطنية لمرتكبي الجرائم الجنسية[2].

وتجدر الإشارة إلى أن المشرع الفرنسي فضلا عن تجريم تخزين المعطيات في ذاكرة معلوماتية، جرم المعالجة الإلكترونية للمعطيات الشخصية التي لا تقتصر على ممارسة الأنشطة الشخصية البحثية، وهوما نصت عليه المادة 226-23 عقوبات[3].

3- الحفظ غير المشروع للمعطيات الشخصية

نص المشرع الفرنسي في الفقرة 5 من المادة 6[4] من قانون 17-78 على مبدأ مهم، وهو مبدأ التوقيت والمعروف أكثر تحت إسم "**حق النسيان**"[1]، هذا المبدأ ينص على ضرورة أن يتم حفظ المعطيات لمدة محددة،

---

[1]-**د. عبد الفتاح بيومي حجازي**، النظام القانوني لحماية التجارة الإلكترونية ، المرجع السابق، ص79.

[2]-**ما شاء الله عثمان محمد الزوي**، المرجع السابق، ص238

[3]Article 226-23 du CPfModifié parLoi n°2004-801 du 6 août 2004 - art. 14 JORF 7 août 2004, dispose que : Les dispositions de l'article 226-19 sont applicables aux traitements non automatisés de données à caractère personnel dont la mise en oeuvre ne se limite pas à l'exercice d'activités exclusivement personnelles.

[4]-Article 6 alinéa5 DU LOI 17-78 modif 5° Elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées.

وعمليا هذه المدة يتم تحديدها من قبل المسؤول عن المعالجة الذي يقدر ذلك بناء على غرض المعالجة[2]. وتطبيقا لذلك جرم المشرع الفرنسي حفظ المعطيات الإسمية خارج الوقت المصرح به وفقا للطلب أو الإعلان السابق بموجب المـــادة 226-20 عقوبات [3] .

ويتحقق الركن المادي في هذه الجريمة بقيام الجاني بحفظ المعطيات الشخصية لمدة اطول من المدة المسموح بها قانونا، بناء على الترخيص أو الراي أو الإعلان المسبق، مالم يتم هذا الحفظ لأغراض تاريخية أو إحصائية أو علمية، أو بمعالجة تلك المعطيات لأغراض أخرى غير تلك المقصودة لما بعد المدة المسموح بها قانونا حسب المادة 226-20 عقبات فرنسي، اما في التشريع التونسي فيتحقق عن طريق عدم مسح المعطيات.

وفي نفس السياق، جرم المشرع التونسي بموجب الفصل 94 الذي أحال للفصل 45 و64 من قانون 2004. عدم إعدام المعطيات بمجرد انتهاء الأجل المحدد لحفظها بالتصريح او بالترخيص، كما جرم كل من يجري معالجة لمدة تتجاوز المدة الضرورية لتحقيق الغرض الذي أجريت من اجله.

ب-الـــركن المعنـــوي

يقوم الركن المعنوي لهذه الجريمة على القصد الجنائي العام بعنصريه العلم والإرادة، وهو ما دلت عليه طبيعة الأفعال، ويتحقق ذلك بعلم الجاني بكافة العناصر الداخلة في تشكيل الجريمة كعلمه بأنه يعالج معلومات شخصية حساسة، أن هذا السلوك يحمل تهديدا للمصلحة المحمية، ولا يكفي العلم بل يجب ان تكون ارادته متجهة إلى تحقيق أحد المظاهر السلوكية التي نص عليها المشرع في المادة *226-18 ،226-20 ،226-19 عقوبات فرنسي. و الفصل 94 ,87،من القانون التونسي المتعلق بحماية المعطيات الشخصية.*

ت-العقـــوبـــة

ومتى قامت الجريمة بركنيها المادي والمعنوي ، يعاقب الجاني بالحبس 5 سنوات وغرامة 300000 يورو ،بالإضافة إلى العقوبات التكميلة المنصوص عليها في المادة 226-31 عقوبات، وإمكان معاقبة الأشخاص

---

[1]**-sur ce point voir : Thiébaut Devergranne** Le droit à l'oubli sur Internet : petit guide juridique pour faire valoir ses droits, article disonible:https://www.donneespersonnelles.fr/droit-a-l-oubli

[2] **-Thiébaut Devergranne,** Le principe de temporalité, disponible en ligne á l'adresse suivante*:* https://www.donneespersonnelles.fr/le-principe-de-temporalite

[3]-Article 226-20du CPF dispose que: "Le fait de conserver des données à caractère personnel au-delà de la durée prévue par la loi ou le règlement, par la demande d'autorisation ou d'avis, ou par la déclaration préalable adressée à la Commission nationale de l'informatique et des libertés, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende, sauf si cette conservation est effectuée à des fins historiques, statistiques ou scientifiques dans les conditions prévues par la loi.
Est puni des mêmes peines le fait, hors les cas prévus par la loi, de traiter à des fins autres qu'historiques, statistiques ou scientifiques des données à caractère personnel conservées au-delà de la durée mentionnée au premier alinéa."

المعنوية، زيادة عن عقوبة الغرامة بالعقوبات المنصوص عليها في المادة 131 –39 طبقا للمادة 226–30 عقوبات.

كما يمكن الحكم بمسح أو حذف كل أو بعض المعطيات المعالجة التي كانت محلا للجريمة بحضور المعني بالمعطيات ووكلاء من اللجنة الوطنية للمعلوماتية والحريات، طبقا للمادة 226–22–2 عقوبات، ويلاحظ أن فعل جمع المعطيات الشخصية بشكل غير مشروع يشكل جريمة مستمرة لا يحسب التقادم فيها إلا من تاريخ وقوعها[1].

أما المشرع التونسي فعاقب على جريمة المعالجة باستعمال الحيلة أو التهديد أو العنف بموجب الفصل 88 بالسجن مدة عام وبخطية قدرها خمسة آلاف دينار، أما جريمة معالجة المعطيات الحساسة فعاقب عليها الفصل 87 بالسجن مدة عامين وبخطية قدرها عشرة آلاف دينار.

سادسا– الانحـــراف عن الغـــاية من المعـــالجة

نص المشرع الفرنسي في الفقرة 2 من المادة 6[2] من قانون 17–78 على مبدأ اساسي وهو مبدأ الغرض من المعالجةLe principe de finalité ، وهو أن يتم تجميع المعطيات لأغراض محددة واضحة ومشروعة وأن لا تتم المعالجة بطريقة تتعارض مع هذه الأغراض. وبناء عليه قام بتجريم فعل الإنحراف عن الغرض المحدد للمعالجة بموجب المادة ***226– 21***[3]عقوبات، وقد عرف مرتكب هذه الجريمة بنصه في المادة : من حاز بيانات شخصية *بمناسبة قيامه بتسجيلها, تصنيفها,نقلها أو أي شكل من أشكال المعالجة, وحول من غايتها التي وضعت لأجلها.*

وإلى جانب المشرع الفرنسي نجد المشرع التونسي يعاقب في الفصل 94 كل من يخالف أحكام الفصل 12، وتنص هذه الأخيرة على عدم جواز معالجة المعطيات الشخصية في غير الأغراض التي جمعت.

وتقوم هذه الجريمة على ركن مادي قوامه نشاط الجاني المتمثل في فعل إساءة إستغلال المعطيات، ينصب هذا السلوك على محل محدد وهو المعطيات الشخصية، وركن معنوي يتمثل في القصد الجنائي.

أ–الركـــن المـــادي

---

[1]-Cass, Crim 4 mars 1997, Bull, Crim, n 83.

مشار اليه لدى: **ماشاء الله عثمان محمد الزوي**، المرجع السابق, ص240.

[2]Article 6-2 du loi 17-78 Modifié par LOI n°2016-41 du 26 janvier 2016 - art. 193 dispose que : Elles sont collectées pour des finalités déterminées, explicites et légitimes…."

[3]-Le fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative, l'acte réglementaire ou la décision de la Commission nationale de l'informatique et des libertés autorisant le traitement automatisé, ou par les déclarations préalables à la mise en oeuvre de ce traitement, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

يتحقق الركن المادي لهذه الجريمة عن طريق سلوك واحد، وهو المعالجة الإلكترونية للمعطيات لغرض آخر غير الغرض المحدد أو المسموح به قانونا، ويستوي لدى القانون أن يكون الشخص حائزا لهذه المعطيات بغرض تصنيفها أو نقلها أو علاجها تحت أي شكل. ويتحقق هذا الركن بمجرد الإنحراف عن الهدف، والغاية هي موضوع المعالجة الإلكترونية، أي الغرض المتوخى من علاج المعطيات الشخصية[1] .

هذا وقد نص المشرع التونسي على سبب إباحة، وهو موافقة المعني بموجب الفصل 12 كمايلي "**لا تجوز معالجة المعطيات...إلا بموافقة المعني...**"، والعلة في اعتبار ذلك ان هذا الرضا يزيل عن الفعل عنصر الإعتداء وينفي الضرر، ومن ثم ينفي عن الفعل الصفة غير المشروعة. أو في حالة تحقيق مصلحة حيوية للمعني، او لأغراض علمية ثابتة.

ب-الـــركـــن المـــعنـــوي

تعد هذه الجريمة من الجرائم العمدية التي يلزم لقيامها توافر القصد الجنائي بعنصريه العلم والإرادة، ومن ثم لا يعاقب عنها بموجب الخطأ غير العمدي.

ت-العقوبـــــة

ومتى قامت الجريمة بركنيها المادي والمعنوي، يعاقب الجاني في قانون العقوبات الفرنسي بالحبس خمس سنوات وغرامة ثلاثمئة الف يورو، بالإضافة الى العقوبة الإضافية المنصوص عليها في المادة 226-31 من قانون العقوبات، ومعاقبة الشخص المعنوي فضلا عن عقوبة الغرامة-بالعقوبات المنصوص عليها في المادة 131-39 عقوبات، طبقا للمادة 226-30 عقوبات، كما يمكن الحكم بمسح كل او بعض المعطيات التي كانت محلا للجريمة، وذلك طبقا للمادة 226-22-2 عقوبات.

اما عقوبة هذه الجريمة في القانون التونسي فهي طبقا للفصل 94 السجن مدة ثلاثة أشهر وبخطية قدرها الف دينار.

الفرع الثاني

الجرائم المتعلقة باستخدام المعطيـــات الشخصية

أصبحت نظم المعلومات بمثابة المكان الأمين والميسر لحفظ المعلومات، قد يستغله الجاني إلى إفشاءها إضرارا باصحابها ومن أجل الإنتقام منهم، وسواء كانت هذه المعلومات متحصلة من معالجة المعطيات أو عن طريق العاملين على النظم، هذا ما دفع المشرع الفرنسي الى تجريم السماح للغير بالإطلاع عليها وذلك بموجب المادة 226-22 عقوبات.

[1]-**د. أسامة عبد الله قايد**، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، بدون دار نشر، 1988, ص98.

ويقابل هذا النص الفصل 93 من القانون التونسي الذي جرم كل من يتعمد بمناسبة معالجة المعطيات الشخصية نشرها بطريقة تسيء لصاحبها أو لحياته الخاصة.

فضلا عن ذلك، منع المشرع الفرنسي بموجب القانون رقم 17-78 الشخص المسؤول عن معالجة المعطيات الشخصية من نقلها إلى دولة غير عضو في الإتحاد الأروبي، إذا كانت هذه الدولة لا توفر مستوى كافي من الحماية للحياة الخاصة والحريات فيما يتعلق بالمعالجة للمعطيات، وهو ما أكدت عليه المادة 226-22-1 عقوبات.

وفي سياق حظر نقل المعطيات الشخصية، جرم المشرع التونسي بموجب الفصل 86 احالة المعطيات الشخصية او نقلها إلى بلاد اجنبية إذا كان من شأن ذلك المساس بالأمن العام أو بالمصالح الحيوية للبلاد التونسية.

وعلى ذلك سنتناول فيمايلي الإفشاء غير المشروع للمعطيات الشخصية(أولا)، نقل المعطيات الشخصية إلى الخارج مع عدم مراعاة شروط النقل(ثانيا).

أولا- الإفشاء غير المشروع للمعطيات الشخصية

عرف المشرع الفرنسي مرتكب هذه الجريمة في مطلع المادة 226- 22[1] على أنه : من جمع معطيات شخصية بمناسبة تسجيلها أو تصنيفها أو نقلها أو أي شكل من المعالجة. كما عرفه المشرع التونسي بموجب الفصل 92 على انه "كل من تعمد بمناسبة معالجة المعطيات الشخصية..."

وتفترض هذه الجريمة إجتماع ركنين متميزين، وهما الركن المادي والركن المعنوي:

أ-الركــن المــادي

نص المشرع الفرنسي على فعلين تقوم بهما الجريمة هما فعل الحيازة والإفشاء للمعطيات الشخصية على نحو يضر باعتبار صاحب الشان أو حياته الخاصة.

فالبنسبة لفعل الحيازة فيستوي أن تكون حيازة المعطيات الشخصية بقصد تصنيفها أو نقلها أو معالجتها تحت أي شكل، فيجب لتحقق هذا الفعل ثبوت واقعة حيازة الجاني لهذه المعطيات القيام بأي إجراء من الإجراءات السابقة. دون إشتراط كون مصادر هده المعلومات صحيحة او مزورة.

[1]-Article 226-22 du CPfModifié par Loi n°2004-801 du 6 août 2004 - art. 14 JORF 7 août 2004 DISPOSE QUE:
Le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.
La divulgation prévue à l'alinéa précédent est punie de trois ans d'emprisonnement et de 100 000 euros d'amende lorsqu'elle a été commise par imprudence ou négligence.
Dans les cas prévus aux deux alinéas précédents, la poursuite ne peut être exercée que sur plainte de la victime, de son représentant légal ou de ses ayants droit.

أما المشرع التونسي فلم ينص على هذا الفعل بشكل صريح، إلا أنه إستخدم عبارات واسعة تضم في نطاقها فعل الحيازة حينما نص في الفصل 93 كما يلي"... ...**بمناسبة معالجة المعطيات الشخصية...**"و المعالجة حسب الفصل 6 يقصد بها تسجيل أو حفظ أو تنظيم أو تغيير أو إستعمال أو إرسال توزيع نشر اتلاف الإطلاع...، ومما لاشك فيه ان المعالجة على هذا النحو تستلزم بداية حيازة المعطيات.

أما إفشاء المعطيات فيتحقق بإطلاع الغير عليها لا صفة له في تلقي هذه المعلومات، مع انعدام رضا المجني عليه.

هذا وقد استخدم المشرع التونسي مصطلح "**النشر**"، ويفترض النشر شأنه شان الإفشاء انتقال المعطيات من حيازة الجاني إلى غيره من الأشخاص، حيث أنه يقوم بتقديم هذه المعطيات إلى غيره ولا يقصرها على نفسه.

ويتطلب المشرع لقيام الجريمة حدوث نتيجة إجرامية وهي أن يترتب على فعل الإفشاء او النشر ضرر للشخص، وقد حصر الضرر في السمعة والشرف والإعتبار وحرمة الحياة الخاصة[1].

وتجدرالإشارة إلى أن المشرع لم يحدد الوسيلة التي يمكن أن يصدر بها إفشاء لهذه المعطيات، مما يجعل الركن المادي لهذه الجريمة يتحقق بأي وسيلة[2]. وهذه الجريمة تختلف عن جريمة الدخول غير المشروع إلى النظم والحصول على معلومات شخصية يحميها القانون، ففي هذه الجريمة لايوجد إختراق، بل هنالك شخص ذي ثقة في تسجيل أو نقل بيان من البيانات الشخصية، ويقوم بتسريب هذه البيانات و إفشاءها[3]. كما تختلف عن جريمة افشاء الأسرار المعاقب عليها بالمادة 226-13[4] عقوبات فرنسي، إذ لا يتطلب المشرع في هذه الأخيرة ان يكون من طبيعة الإفشاء إحداث اعتداء على الشرف أو الإعتبار او الحياة الخاصة للمجني عليه، بخلاف جريمة إفشاء المعطيات الشخصية[5]، فضلا عن ذلك فإن الجريمة الأخيرة تشمل افشاء المعطيات الشخصية السرية وغير السرية، على خلاف جريمة افشاء الأسرار التي لا تشمل إلا المعطيات السرية[6].وعليه لا يعاقب الجاني إلا إذا كان عالم باسرار الغير بسبب مهنته أو وظيفته.

وتطلب المشرع الفرنسي شرط عدم رضا المجني عليه لقيام الجريمة المنصوص عليها في المادة 226-22 عقوبات، على خلاف جريمة إفشاء سر المهنة المنصوص عليها في المادة 226-13 عقوبات، إذ يجوز الإفشاء للمصلحة العامة بدون رضا المجني عليه. وخلافا للمادة 226-13 عقوبات يتطلب المشرع في

---

[1]-**د. أسامة عبد الله قايد**، المرجع السابق، ص146. د. **مدحت رمضان**، الحماية الجنائية للتجارة الإلكترونية، المرجع السابق، ص104، د. **أحمد حسام طه تمام**، المرجع السابق، ص329.

[2]-**يوسف بوهدون**، الحماية الجنائية للمستهلك في إطار عقود التجارة الإلكترونية، مجلة الملف، العدد 18، مطبعة النجاح الجديدة، الدار البيضاء، أكتوبر 2011، ص56.

[3]-**د. مدحت رمضان**، الحماية الجنائية للتجارة الإلكترونية، المرجع السابق، ص104

[4]-**Article 226-13** du CPF Modifié par Ordonnance n°2000-916 du 19 septembre 2000 - art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002 dispose que :" La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15 000 euros d'amende."

[5]- **د. محمد أمين الشوابكة**، المرجع السابق، ص103.

[6]-**د. حسام طه تمام**، المرجع السابق، ،ص329.

الجريمة المنصوص عليها في المادة 226-22 عقوبات ضرورة تقديم المجني عليه أو وكيله الخاص أو ممثله القانوني أو من ورثته شكوى لتحريك الدعوى العمومية.

بناء عليه، وإن كانت الجريمتان تتفقان في علة التجريم وهي حماية المعطيات، إلا أنهما تختلفان في الأركان، ومن ثم لا يمكن تمديد الحماية بموجب المادة 226-13 لتشمل المعطيات الشخصية التي قد يترتب عليها إعتداء على حرمة الحياة الخاصة إذا ما أسيء إستخدامها[1].

ب-الــركن المعنــوي

يأخذ الركن المعنوي لجريمة الإفشاء غير المشروع للمعطيات صورة القصد الجنائي أو الخطأ، و صورة القصد الجنائي مستفادة من تعريف الشارع لهذه الجريمة بأنها إعتداء على الشرف أو الإعتبار أو حرمة الحياة الخاصة، والإعتداء يفترض توافر القصد الجنائي لدى المعتدي[2].

أما صورة الخطأ فمستفادة من نص المشرع على عبارة "**الإهمال**" الواردة في الفقرة الثانية من المادة 226-22 . وهذا النص من شأنه أن يحفظ للتعاملات الإلكترونية جانبا من الثقة والأمان وحماية خاصة للمتعاملين الإلكترونيين.

وما قيل بخصوص المشرع الفرنسي يقال بالنسبة للمشرع التونسي، فبالرجوع للفصل 93 نجده قد تميز من ناحية البناء المعنوي بان المشرع قد استخدم فيه عبارة "**يتعمد**" وهو ما يستفاد منه ان هذه الجريمة مقصودة، كما استخدم عبارة "**دون قصد الإضرار**" وهو ما يستفاد منه ان هذه الجريمة قد تقع بطريق الخطأ.

ت-العقوبــة

متى قامت الجريمة بركنيها المادي والمعنوي، يعاقب الجاني بالحبس 5 سنوات و غرامة 300000 يورو فيما إذا كانت الجريمة عمدية، أما إذا كانت غير عمدية فيعاقب بالحبس 3 سنوات وغرامة 100000 يورو.

والحكم بمسح كل أو بعض المعطيات التي كانت محلا للجريمة في حضور الأفراد ووكلاء عن اللجنة الوطنية للمعلوماتية والحريات.[3]

اما العقوبة في القانون التونسي فهي السجن مدة ثلاثة أشهر وبخطية قدرها ثلاثة آلاف دينار طبقا للفقرة الأولى من الفصل 93 فيما إذا كانت الجريمة عمدية، أما إذا كانت غير عمدية فيعاقب بالسجن مدة شهر و بخطية قدرها الف دينار طبقا للفقرة 2 من نفس الفصل.

---

[1]- **د. اسامة عبد الله قايد**، المرجع السابق، ص152-153.

[2]- والملاحظ أن المشرع نص على سبب الإباحة، وهو رضا المجني عليه، والعلة أن هذا الرضا يزيل عن الفعل عنصر الإعتداء وينفي الضرر، ومن ثم ينفي عن الفعل الصفة غير المشروعة. وفي ذلك نصت المادة 8 في بندها 2 رقم 4 من قانون 2004 على أن المعالجة الآلية التي ترد على البيانات الإسمية تصبح عامة عن طريق رضا الشخص المعني.

[3]-Article 226-22-2 du CPfCréé par Loi n°2004-801 du 6 août 2004 - art. 14 JORF 7 août 2004.

ثانيا- نقل المعطيات إلى الخارج بدون مراعـــاة شـــروط النـــقل

يضـــع المشرع الفرنسي محددات أمام إنتقال المعطيات الشخصية إلى خارج الإتحاد الأروبي، بالنسبة للـــدول التي لا تضمن مستوى كاف للحماية في مجال نقل هذه المعطيات وذلك بموجب المادة 70[1] من القانون 78-17، ففي هذه الحالة تقوم اللجنة على الفور بابلاغ لجنة الإتحاد الأوربي في حالة علمها بان المعطيات الشخصية ستنقل الى هذه الدولة، كما توجه بيان للمسؤول عن المعالجة بتاجيل عملية النقل، إلى ان ترى لجنة الإتحاد الأروبي في مستوى الحماية المتوفرة.

وتكمن أهمية إحترام هذه الضوابط في أن مخالفتها يخضع صاحبه للمادة 226-22-1 [2]عقوبات.

أ-الركـــن المـــادي

يتحقق الركن المادي لهذه الجريمة بقيام الجاني بنقل أو السعي في نقل معطيات شخصية إلى دولة ليست عضوا في الإتحاد الأوربي بالمخالفة للإجراءات المتخذة من قبل لجنة الإتحاد الأروبي أو اللجنة الوطنية للمعلوماتية والحريات والمنصوص عليها في المادة 70 من القانون 78-17.

وإلى جانب المشرع الفرنسي، نجد المشرع التونسي يعاقب هو بدوره بموجب الفصل 86 فعل نقل المعطيات الشخصية الى بلاد اجنبية رابطا ذلك بضرورة المساس بالأمن العام او بالمصالح الحيوية للبلاد.

ب-الـــركن المـــعنوي

نقل المعطيات الشخصية جريمة عمدية يتخذ الركن المعنوي فيها صورة القصد الجرمي، بعنصريه العلم والإرادة. وعلم الجاني يجب أن يحيط بجميع الوقائع التي يتطلبها القانون لقيام الجريمة بكل أركانها، ومن ذلك علمه أن فعله ينصب على معطيات شخصية، وأن ما يفعله هو نقلا للمعطيات بالمخالفة للإجراءات المتخذة من قبل اللجنة بنوعها(حسب المادة 226-22-1 عقوبات فرنسي)، أو علمه أن هذا النقل من شأنه المساس بالأمن العام أو بالمصالح الحيوية للبلاد(حسب الفصل 86 من القانون التونسي) كما يجب أن تتجه إرادته إلى هذا الفعل والى تحقيق النتيـــجة.

ت-العقوبـــة

[1]-**Article 70** du loi 78-17 Créé par Loi n°2004-801 du 6 août 2004 - art. 12 JORF 7 août 2004.

[2]-**Article 226-22-1** du CPF Créé par Loi n°2004-801 du 6 août 2004 - art. 14 JORF 7 août 2004 dispose que: Le fait, hors les cas prévus par la loi, de procéder ou de faire procéder à un transfert de données à caractère personnel faisant l'objet ou destinées à faire l'objet d'un traitement vers un Etat n'appartenant pas à la Communauté européenne en violation des mesures prises par la Commission des Communautés européennes ou par la Commission nationale de l'informatique et des libertés mentionnées à l'article 70 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

وعقوبة هذه الجريمة في فرنسا طبقا للمادة 226-22-1 عقوبات هي الحبس من 5 سنوات وغرامة 300000 يورو، والحكم بمسح كل أو بعض المعطيات التي كانت محلا للجريمة في حضور الأفراد ووكلاء عن اللجنة الوطنية للمعلوماتية والحريات.[1]

أمـــا عقوبة هذه الجريمة في القانون التونسي فهي طبقا للفصل 86 السجن من عامين إلى خمسة اعوام وبخطية من خمسة الاف إلى خمسين الف دينار.

الفرع الثالث

جريمة إنتحـــال الهوية الرقمـــية

تتم التعاملات الإلكترونية على الأنترنت ضمن شبكة مفتوحة لا يعرف من خلالها هوية الأشخاص، وهو ما يؤدي إلى مخاطر عدة منها جمع معطيات شخصية عن المجني عليه، ثم إنتحال شخصيته من أجل إستخدامها في أعمال إحتيالية مالية أو جنائية لتحقيق نوع من الكسب المادي أو المعنوي، وبسبب إضطرار المتعامل الإلكتروني في كثير من الحالات إلى كشف بعض معطياته الشخصية كرقم الحساب أو رقم فيزا كارت للشراء عبر الأنترنت، فهذه الأمور سهلت إلى حد كبير سرقة الهوية الرقمية وإستخدامها في الشراء أو طلب القروض بإسم المجني عليه[2].وهو ما يستلزم في المقابل تأمين هذه الهوية عن طريق آليات قانونية تضفي الحماية عليها من أشكال الإعتداء.

إن إستحداث نص في فرنسا يجرم الإعتداءات الواقعة على الهوية الرقمية يمثل تقدما كبيرا في نظر القانون الجنائي لخصوصية التكنولوجيا الجديدة، فهذا التجريم الجديد جاء ليملأ فراغ قانوني في الوقت الذي أصبح فيه التشارك في الواب في تزايد مستمر. وقد جاءت هذه الفكرة لأول مرة سنة 2006 من قبل النائب ميشال دريفوس الذي أعرب عن أسفه عن الفراغ القانوني في هذا المجال، إلا أن الحكومة لم تعتمد هذا الإقتراح على أساس ان جريمة الإحتيال تسمح الإستجابة بفعالية لسرقة الهوية عبر الأنترنت[3]. وجاء هذا التجريم بموجب ***المادة 226-4-1*** عقوبات [4] المضافة بموجب المادة 2 من قانون الأمن الداخلي[5] حيث تنص على انه كل من يقوم بانتحال هوية الغير أو بإستخدام واحدة أو اكثر من معطيات من أي نوع، تسمح

---

[1]-Article 226-22-2 du CPFCréé par Loi n°2004-801 du 6 août 2004 - art. 14 JORF 7 août 2004.

[2]-http://www.assemblee-nationale.fr/13/propositions/pion2192.asp

[3]-Thibault Verbiest,Patrick Cuignet, La création d'un délit d'usurpation d'identité numérique, http://www.droit-technologie.org/actuality-1316/la-creation-d-un-delit-d-usurpation-d-identite-numerique.html

[4]-Article 226-4-1 du CPFCréé par LOI n°2011-267 du 14 mars 2011 - art. 2 disposeque: Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende. Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne.

[5]-Article 2 du LOI n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure

بتحديد هويته، وذلك بهدف إقلاق هدوئه أو هــدوء الآخرين، أو بــهدف المساس بشرفه أو اعتباره، ويعاقب بذات العقوبة عند ارتكابها من خلال شبكة الإتصالات المخصصة للعموم عن طريق خط الأنترنت.

و سنتناول هذه الجريمة من خلال بيان ركنها المادي والمعنوي كمايلــي:

اولا- الركــن المــادي

أ- محــل النشــاط الإجــرامي

إن المحل الذي ينصب عليه سلوك الجاني هو **الهوية الرقمية**، أو المعطيات التي تسمح بالتعرف على الشخص، وهوية الشخص هي مجموعة من المعلومات والتعريفات والمفردات التي تــدل على كينونته، ومن مكوناتها الإسم واللقب العائلي ومكان الميلاد وغيرها، ومع إستخــدام الأنترنت بدأ يظهر بقوة مفهوم جديد للهوية الشخصية هو الهوية الرقمية.

يقصد **بالهوية الرقمية** جميع العوامل والمفردات التي تعبر عن وجود المتعامل الإلكتروني في فضاء الأنترنت، مثل عنوان بروتوكول الأنترنت أو البريد الإلكتروني وكلمة السر أو الإسم المستعار الذي يعرف به بغرفة المحادثة أو إسم حسابه الإلكتروني على الفيس بوك[1]، كما عرفها البعض على أنها مجموعة من الآثار الرقمية يتركها الشخص وراءه، سواء كانت آثار عن محركات البحث بما تترجمه من تصرفات، أو تعلقت بأفكاره أو أقــواله[2].

وتظهر الهوية الرقمية أكثــر في نطاق التعاملات الإلكترونية من حيث إستخدام رقم بطاقات الإئتمان للشراء من الأنترنت.

فضلا عن ذلك، إستخدم المشرع عبارة "معطيات من أي نوع" لتحديد الهوية بدل إستخدام عبارة المعطيات الشخصية التي جاءت في الصياغة الأولى للنص، وهو ما يسمح باستيعاب الإعتداء الواقع على الهوية الرقمية ضمن مفهوم المعطيات على النحو الذي حدده قانون 1978 في المعنى الوارد في المادة 2 من هذا القانون.حين نصت على أن المعطيات الشخصية هي كل معلومات تسمح بالتعرف على الشخص عن طريق الإشارة إلى رقم الهوية أو إلى عنصر أو إلى عدة عناصر مميزة له.

ب-النشــاط الإجــرامـــي

إن السوك الإجرامي في هذه الجريمة يتحقق بارتكاب أحد الفعلين التي نصت عليهما المادة 226-4-1 وهما فعل انتحال هوية الغير وفعل إستخدام واحد أو أكثــر من المعطيات من أي نوع. وهاتان الصورتان

---

[1]-**زياد سويدان**، انتحال الهوية الرقمية، مقل منشور على الموقع التالي:
http://www.urdri.fdspt.rnu.tn/articles/colloque-internet-identite-numerique/zied-souiden-usurpation-identite.ppt

[2]- ***Olivier Ertzscheid***,QU'EST-CE QUE L'IDENTITÉ NUMÉRIQUE ?Collection : Encyclopédie numérique **:** Open Edition Press. Marseille2013P1.

هي على قدم المساواة في تحقيق النشاط الإجرامي المكون للجريمة، وهو مايستفاد من عبارة "أو" الواردة ضمن المادة الســـابقة.

1-انتحـــال هويـــة الغـــير

يقصد بانتحال الهوية الفعل القصدي الذي بموجبه يقوم الشخص بإستعمال أو إستغلال معطيات شخصية للغير لأهداف غير مشروعة. ويستوجب هذا الفعل قيام مرتكبه بفعليين متتاليين أولهما تجميع المعلومات والمعطيات الشخصية للغير، ثم القيام باستعمالها واستغلالها في ظل ما توفره شبكة الأنترنت من معلومات متدفقة وتجميع المعطيات الشخصية بطـــريقة فعـــالة[1].

في العالم الإفتراضي، من أكثر صور الإنتحال شيوعا هي التصيد phishing ، hameçonnage، حيث أصبح يشكل تهديدا متزايدا للمتعاملين الإلكترونيين عبر شبكة الأنترنت، وهو طريقة للحصول على المعلومات الخاصة بمستخدمي الأنترنت، سواء كانت شخصية او مالية، عن طريق الرسائل الإلكترونية أو **مواقع الأنترنت** التي تبدو كأنها مبعوثة من شركات موثوقة او مؤسسات مالية وحكومية كالبنوك الإلكترونية[2].

وهو ما حدث مع زبائن البنك الكندي، حيث قام المتهم دو الجنسية الجزائرية بعنابة بإنشاء موقع إلكتروني شبيه بالموقع الرسمي للبنك الكندي، وذلك للإحتيال على الأشخاص والحصول على هوياتهم الرقمية من خلال ارقامهم الحسابية والأرقـــام السرية، وإستعمالهـــا فيما بعد في الشراء عبر الأنترنت وتحويل الأموال على حساب أصـــحاب تلك البطـــاقات[3].

والى جانب التصيد، يوجد إلتقاط كلمة السرsniffing أو الإستدراج pharming أو رسائل البريد الإلكتروني المزعجة spam أو التخفي باستغلال بروتوكول الأنترنت ip spoofing وغيرها من اشكال انتحال الهوية.

2-إستخـــدام واحد أو أكثـــر من معطيات من أي نوع تسمح بتحديد الهوية: ومن ذلك كلمات السر والرسائل الإلكترونية، الصور[4] وعناوين المواقع adresse URL وعنوان بروتوكول الأنترنت adresse ip الخ

وتجدر الإشارة إلى أن المشرع يجرم هذان السلوكان متى تم إرتكابهما عن طريق الشبكات العامة المفتوحة للجمهور، ومن ثم يستثنى من تطبيق نص المادة السابقة حالات إستخدام الأنترانت.

---

[1]- **زياد سويدان**، انتحال الهوية الرقمية، مقل منشور على الموقع الإلكتروني السابق.

[2]- https://ar.wikipedia.org/wiki/%D8%AA%D8%B5%D9%8A%D8%AF,

[3]-محكمة عنابة، قسم الجنح،حكم رقم 07357/10 ، بتاريخ 28-06-2010، قضية جنحة تصميم وإدخال عمدا وعن طريق الغش لمعطيات للمعالجة الآلية والمتاجرة فيها أدت إلى تعديل معطيات تلك المنظومة وجنحة التقليد وجنحة السرقة، ضد (ف. محمد)، غير منشور.

[4] -*Tribunal de Grande Instance de Paris, 18 décembre 2014, n°12010064012,* Nicolás MelchiorLucie Robin l'usurpation d'identité numérique : en droit français et en droit espagnol, http://www.eurojuris.fr/fr/particuliers-informatique-et-internet-usurpation-d-identite-numerique#.VwcQ8JyLQSk

ثانيا- الركــن المعنــوي

كما لاحظنا من خلال دراستنا للمادة 226-4-1 التي تناولت تجريم الإعتداء على الهوية الرقمية، فإن هذه الأخيرة جريمة مقصودة، يتطلب القصد الجنائي العام فيها بأن يقــوم الجاني بإحدى الفعلين التي أوردهما النص القانوني، وأن من شأن أفعــاله هذه أن تؤدي نتيجة، وأن تتــجه إرادته إلى هذين الفعلين والى تحقيق النتيجة.

والى جانب تطلب القصد العام، فإن المشرع تطلب توافر القصد الخاص، يتمثل في نية إقلاق الغير أو المساس بشرفه وإعتباره، وهو ما يستفاد من البناء المعنوي لنص المادة السابقة حيث إستخدم فيه المشرع عبارة بنية en vue،

ثالثا- العــقوبــة

يعاقب المشرع الفرنسي على هذه الجريمة بالحبس سنة وغرامة 15 الف يورو، مع إمكانية قضاء القاضي بالعقوبات التكميلية المنصوص عليها في المادة 226-31، فضلا عن قيام مسؤولية الشخص المعنوي طبقا للمادة 226-7 عقوبات.

مما سبق، نخلص إلى أن المشرع الفرنسي لا يألو جهدا في محاولته لمواجهة الجرائم الواقعة في العالم الإفتراضي عامة، وعلى المعطيات الشخصية خاصة، فقد بدأ مبكرا في مواجهة هذه الجرائم، ولم يتأخر في إجراء التعديلات التشريعية عند الضرورة لمواكبة التطور في تقنية المعلومات، ولاندل على ذلك أكثر من التعديلات الصادرة بالقانون رقم 2014-1353 [1]والتي شدد فيها المشرع الفرنسي العقاب على الجرائم الماسة بنظم المعالجة الآلية في حالة ما إذا تم إرتكابها من طرف جماعة منظمة، وكان الإعتداء يمس نظام للمعالجة الآلية للمعطيات دات الطالع الشخصي التي تنفدها الدولة.

وبمقارنة النهج الصدار عن المشرع الفرنسي بما صدر عن المشرع التونسي يتضح التقارب الكبير في سياسة كلا منهما في حماية المعطيات ذات الطابع الشخصي.

وبعد هذا العرض لموضوع المعطيات ذات الطابع الشخصي وحمايتها في كل من فرنسا وتونس، نرصد فيما يلي لكيفية هذه الحماية في التشريع الجزائري وفي بعض التشريعات المقارنة الأخرى.

[1]-**LOI n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme,** JORF n°0263 du 14 novembre 2014

المطلب الثاني

الحماية الجزائية للمعطيات الشخصية في التشريع الجزائري وبعض التشريعات الأخرى

على خلاف الوضع في التشريع الفرنسي والتونسي، لم تحظ المعطيات الشخصية بالعناية الكافية في التشريع الجزائري، حيث خلت البنية لتشريعية من قانون خاص يحمي المعطيات الشخصية سواء للأفراد أو الشركات، رغم نص المشرع الدستوري الجزائري في المادة 46 إلى أن حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حق أساسي يضمنه القانون ويعاقب على إنتهاكه. وهو ما يدفعنا إلى محاولة إيجاد تلك الحماية في ثنايا هذا التشريع من خلال تطويع النصوص التقليدية الواردة في قانون العقوبات التي إستهدف بها المشرع حماية الحق في الحياة الخاصة(الفرع الأول)، أو من خلال الأحكام الخاصة التي سنها المشرع في نطاق قانون التوقيع الإلكتروني(الفرع الثاني). على أن تكون الدراسة بالمقارنة مع التشريع المصري، ولما كان المشرع التونسي قد نظم هو الآخر هذه الحماية بموجب قانون المبادلات الإلكترونية إلى جانب القانون رقم 63 لسنة 2004 المتعلق بحماية المعطيات الشخصية السابق دراسته، فراينا أن تشمل الدراسة نصوصه.

الفرع الأول

البحث عن حماية المعطيات الشخصية في قانون العقوبات

إذا إستقر الرأي لدى غالبية الفقه[1] حول حقيقة عدم إمكانية حماية المعطيات الشخصية بنصوص جريمة إفشاء الأسرار، فقد إتجه البحث في مدى تطبيق نصوص حماية حرمة الحياة الخاصة في نطاق حماية المعطيات الشخصية.

لقد كان قد أصدر كل من المشرع الجزائري والمصري مجموعة من النصوص التي إستهدفا بها حماية الحق في الحياة الخاصة تكريسا لما جاء في الدستور، ففي التشريع الجزائري نجد المادة 303 مكرر[2]

---

[1]-حيث إتجه الراي أن القصور الذي يشوب النصوص المتعلقة بجريمة إفشاء السر عن تحقيق الغرض المطلوب في حماية المعطيات الشخصية يرجع لسبب أن هذه الخيرة إن كانت تدخل ضمن مدلول السر، غلا أنها في أغلب الأحيان لا يمكن ان تأخذ وصف السر المهني الذي تاتي تلك النصوص على حمايته، فضلا عن ذلك فغن حماية المعطيات الشخصية بنوص جريمة إفشاء السر تتطلب ان يكون ما تم إفاشوه مما ينطبق عليه وصف السر و أن يكون مما ينطبق عليه وصف السر المهني، وما يزيد الأمر صعوبة في نطاق المعطيات الشخصية أن من غير المتصور حتى تشمل بحماية تلك النصوص ان تكون مقومات الحياة الخاصة للفرد كلها اسرار مهنية.**د. محمد حماد مرهج الهيتي**، البحث عن حماية جنائية للبيانات والمعلومات الشخصية المخزنة في الحاسب الآلي، مجلة الشريعة والقانون، العدد 27، جامعة الإمارات العربية المتحدة، جمادى الثانية، يوليو 2006، ص 481.

[2]– تنصالمادة 303 مكررعقوباتجزائري "يعاقببالحبسمنستةأشهرإلىثلاثسنواتوبغرامةمن 50000 دجإلى 300000 دجكلمنتعمد المساسبحرمةالحياة الخاصة للأشخاص بأية تقنية كانت وذلك :

1– بالتقاط ، أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية في غير إذن صاحبها أو رضاه.

من قانون العقوبات الجزائري المضافة بموجب القانون رقم 06-23 المقابلة للمادة 226-1 عقوبات فرنسي[1]، و في التشريع المصري المادة 309 مكرر[2] من قانون العقوبات والمضافة بالقانون رقم 37 لسنة 1972 والتي تم نقلها حرفيا من قانون العقوبات الفرنسي القديم، خاصة المادة 368 الموضوعة لأول مرة بموجب القانون 1810-02-17[3] الملغاة بموجب القانون 92-1336[4]. والتي حلت محلها المادة 226-1 عقوبات .

ولئن نادى البعض على إعتبار أن هذه الآلية القانـــونية المتوفرة كفيلة بإستيعاب هذه النوعية من المعطيات لكن الغلبة كانت للطرف المقابل، وحصلت القناعة لدى أغلب رجال القانون بضرورة إستنباط أطـــر قانونية جديدة في هذا المجـــال.

---

[2] – في التقاط ، أو تسجيل أ, نقل صورة لشخص في مكان خاص بغير إذن صاحبها أو رضاه.

يعاقب على الشروع في ارتكاب الجنحة المشار إليها في هذه المادة بالعقوبة ذاتها المقررة بالجريمة التامة .

إن صفح الضحية يضع حدا للمتابعة الجزائية .

[1]- **Article 226-1 du CPF**Modifié par Ordonnance n°2000-916 du 19 septembre 2000 - art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002**dispose que :**Est puni d'un an d'emprisonnement et de 45 000 euros d'amende le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui :

1° En captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ;

2° En fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé.

Lorsque les actes mentionnés au présent article ont été accomplis au vu et au su des intéressés sans qu'ils s'y soient opposés, alors qu'ils étaient en mesure de le faire, le consentement de ceux-ci est présumé.

[2]-تنص المادة 309 مكرراً يعاقب بالحبس مدة لا تزيد على سنة كل من اعتدي على حرمة الحياة الخاصة للمواطن، وذلك بأن ارتكب أحد الأفعال الآتية فى غير الأحوال المصرح بها قانوناً أو بغير رضاء المجني عليه.

أ) استرق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة أياً كان نوعه محادثات جرت فى مكان خاص أو عن طريق التليفون.

ب) التقط أو نقل بجهاز من الأجهزة أياً كان نوعه صورة شخص فى مكان خاص.

فإذا صدرت الأفعال المشار إليها فى الفقرتين السابقتين أثناء اجتماع على مسمع أو مرأى من الحاضرين فى ذلك الاجتماع ، فإن رضاء هؤلاء يكون مفترضاً.

ويعاقب بالحبس الموظف العام الذي يرتكب أحد الأفعال المبينة بهذه المادة اعتماداً على سلطة وظيفته .

ويحكم فى جميع الأحوال بمصادرة الأجهزة وغيرها مما يكون قد استخدام فى الجريمة أو تحصل عليه ، كما يحكم بمحو التسجيلات المتحصلة عن الجريمة أو إعدامها.

[3]-Article 368 du CPFCréé par Loi 1810-02-17 promulguée le 27 février 1810

[4]Art 368 du CPF Abrogé par -Loi n° 92-1336 du 16 décembre 1992 relative à l'entrée en vigueur du nouveau code pénal et à la modification de certaines dispositions de droit pénal et de procédure pénale rendue nécessaire par cette entrée en vigueur ,dispose que: "Sera puni d'un emprisonnement de deux mois à un an [*durée*] et d'une amende de 2.000 à 60.000 F [*taux résultant de la loi 77-1468 du 30 décembre 1977*], ou de l'une de ces deux peines seulement, quiconque aura volontairement porté atteinte à l'intimité de la vie privée d'autrui :
1° En écoutant, en enregistrant ou transmettant au moyen d'un appareil quelconque des paroles prononcées dans un lieu privé par une personne, sans le consentement de celle-ci ;
2° En fixant ou transmettant, au moyen d'un appareil quelconque, l'image d'une personne se trouvant dans un lieu privé, sans le consentement de celle-ci [*captation de paroles ou d'images*].
Lorsque les actes énoncés au présent article auront été accomplis au cours d'une réunion au vu et au su de ses participants, le consentement de ceux-ci sera présumé".

وعلى هدي ما تقدم، سنتناول بالدراسة أركان هذه الجريمة، ثم موقف الفقه حول مدى صلاحية النصوص التي تناولتها بالتنظيم لحماية هذه المعطيات.

أولا- أركان جريمة إلتقاط أو تسجيل أو نقل المكالمات أو الصور

أ-الــركن المــادي

يتخد السلوك الإجرامي في هذه الجريمة إحدى الصورتين:

الصورة الأولى:إلتقاط المكالمات الخاصة أو تسجيلها أو نقلها

يتحقق السلوك الإجرامي في هذه الصورة في فعل إلتقاط الحديث أو تسجيله أو نقله، ويفترض تسجيل الحديث حفظه على مادة أيا كانت طبيعتها للإستماع إليه فيما بعد، أما النقل فيفترض إرسال الحديث من مكان لآخر، وعلى غرار المشرع الفرنسي في المادة 226-1 يشترط المشرع الجزائري أن يكون الحديث خاصا أو سري سواء كان في مكان خاص أو عام، فالمعيار هنا ليس طبيعة المكان بل طبيعة الحديث موضع الجريمة، في حين إشترط المشرع المصري أن يكون الحديث في مكان خاص بغض النظر عن موضوع الحديث، سواء كان متعلقا بالحياة الخاصة أو العامة[1] أخدا بذلك صيغة نص المادة 368 عقوبات فرنسي الملغاة. مع الأخد في الإعتبار أن النص تصدرته عبارة إعتداء على الحياة الخاصة بمعنى أن يكون موضوع المحادثة متعلق بها، كما قــرر هذه الحمــاية للمحادثات التي تتم بطريق التلفون.

الصورة الثانية: إلتقاط صورة شخص أو تسجيلها أو نقلهــا

ويقصد بالإلتقاط تثبيت الصورة على مادة خاصة بحيث يمكن الإطلاع عليها في الحال أو فيما بعد، ويستوي في ذلك أن تكون الصورة في حالة ثبات أو حركة، أما التسجيل فيتحقق بآلة تصوير كاميرا، أو كاميرا فيديو المتواجدة في الهواتف أو اللوحات الرقمية، في حين النقل يفترض إطلاع الآخرين عليها سواء كانو في مكان خاص أو عام[2].

هذا وقد إشترطت التشريعات تواجد الشخص في مكان خاص، على خلاف جريمة إلتقاط أو تسجيل أو نقل المكالمات التي إعتد فيها كل من المشرع الفرنسي والجزائري بمعيار طبيعة الحديث بغض النظر عن المكان التي يجري فيه الحديث.

ويلاحظ أن التشريعات قد إشترطت تحقيق التجريم بوسيلة إرتكاب الفعل، حيث إشترط المشرع الجزائري والفرنسي" **بأي تقنية كانت**"، كما إشترط المشرع المصري أن يكون هذا السلوك قد تم عن طريق جهاز من الأجهزة أيا كان نوعه، دون تحديد منهم لنوع محدد، أو إشتراطه شروطا خاصة فيه، بل يكفي أن تكون صالحة لنقل الحديث أو الصورة، وهو مايسمح بإستيعاب أي تقنية أو جهاز قد يظهر بفعل التقدم العلمي، هذا من جهة.

---

[1]- أنظر:**د. مدحت رمضان**، جرائم الإعتداء على الأشخاص والأنترنت، دار النهضة العربية، 2000، ص114.

[2]-**د محمود نجيب حسني**، شرح قانون العقوبات، القسم الخاص، المرجع السابق، ص 794.

وم جهة أخرى، إشترطت التشريعات عنصر إنعدام رضا الضحية لقيام الجريمة، وإن كان إشتراط هذا الشرط يثير بعض المشاكل من ناحية الإثبات، ذهب كل من المشرع الفرنسي والمصري إلى إفتراض حالة الالتقاط الحاصل بمعرفة الشخص المعني دون الحاجة لإثبات هذا الرضا، حيث نصت الفقرة الأخيرة من المادة 226–1 عقوبات فرنسي وتقابلها المادة 309 مكرر مصري "عندما تتم الأفعال المشار إليها في هذه المادة على مرأى ومسمع من المعنيين دون أن يعترضو عليها رغم أنه كان في إمكانهم القيام بدلك فإن رضا هؤلاء يعد مفترضا".

أما محل الجريمة، فهو **المكالمات أو الأحاديث الخاصة أو سرية**، حسب المادة 303 مكرر جزائري والأحاديث التي جرت في **مكان خاص** حسب المادة 309 مكرر عقوبات مصري. وإن كان الحديث يعكس كل صوت له دلالة التعبير عن مجموعة من المعاني والأفكار المترابطة فإذا كان فاقدا للدلالة فلا يعتبر حديثا[1]. غير أن المسالة تبقى مطروحة بشأن متى يمكن إعتبار الحديث قد جرى بكيفية خاصة أو سرية؟

وفي تحديد مدلول عبارة خاصة أو سرية لم نجد كل من المشرع الفرنسي والجزائري قد ضبطا ذلك، وما دفع الفقه إلى البحث عن معيار يمكن من خلاله التمييز بين الحديث العام والخاص، وفي ذلك يرى البعض[2] أن الحديث يكون خاصا إدا تم عبر وسائل الإتصال الخاصة التي تحرص كافة التشريعات على كفالة سريتها (المادة 46 من دستور الجزائري) نظرا لأن الحديث في هده الحالة يتم في إطار من الخصوصية بعيدا عن العلانية وبالتالي فإن وجه السرية والحرمة فيه واضح. ويصدق ذلك على المحادثات التي يتبادلها الناس مع بعضهم من خلال وسائل الإتصال السلكية (كالتلفون الأرضي) أو اللاسلكية(التلفون المحمول) أو حتى عبر الأنترنت(البريد الإلكتروني)، وهو مايطلق عليه إصطلاحا **الحديث الخاص غير المباشر**، فمعيار الخصوصية هنا هو جريان المحادثة عبر وسيلة من هذه الوسائل[3].

بالإضافة إلى الحديث، يتخد محل الجريمة **الصورة الملتقطة لشخص في مكان خاص** التي تفسر على أنها عبارة عن إمتداد ضوئي لجسم الإنسان، ومن تم يخرج عن نطاق الحماية الأشياء أيا كانت أهميتها أو

---

[1]-**د. ياسر الأمير فاروق**، مراقبة الأحاديث الخاصة في الإجراءات الجنائية، دار المطبوعات الجامعية، الإسكندرية، ص146.

[2]– المرجع نفسه، ص522.

[3]–فقد أدانت محكمة إستئناف باريس في 5 مارس 1996 مديرالشركة بوصفه شريكا بالمساعدة في إرتكاب جريمة الإعتداء على الحياة الخاصة عندما قام هذا الأخير المكلف بأمن الأشخاص والأموال بتحريض أحد الموظفين للقيام بتسجيل مكالمات هاتفية لبعض رجال الأعمال من أجل الإطلاع على اسرار أعمالهم، وقد طعن المدير في هذا الحكم مستندا إلى إنتفاء عنصر الخصوصية وهو أحد عناصر الركن المادي لجريمة إنتهاك حرمة الحياة الخاصة، على إعتبار أن التنصت على المحادثات التلفونية الذي تم كان بغرض الحصول على معلومات عن الحياة المهنية، وهو لايعد فعلا معاقبا عليه. إلا أن محكمة النقض الفرنسية بتاريخ 7 اكتوبر 1997 رفضت الطعن المقدم وأكدت أن أركان الجريمة مستفادة من حكم الإدانة، وبالرجوع إلى تسبيب محكمة الإستئناف للحكم للتعرف على وجه الدقة على أركان الجريمة يتضح أن القضاة سجلوا الأسباب التالية: " **أيا كانت طبيعة المعلومات محل البحث، فان التوصيلات غير المشروعة من شأنها من حيث مفهومها وموضوعها ومدتها بحكم اللزوم إقحام الفاعلين في الحياة الخاصة للأشخاص الذي تم التنصت عليهم**".

...les juges énoncent que, quelle qu'ait été la nature des informations recherchées, les branchements clandestins ont, par leur conception, leur objet et leur durée, nécessairement conduit leur auteur à pénétrer dans la vie privée des personnes écoutées,

Cour de cassation .chambre criminelle, N° de pourvoi: 96-81485 Bulletin criminel 1997 N° 324 p. 1069, Décision attaquée : Cour d'appel de Paris , du 5 mars 1996

الضـــرر الناجم عن تصوريها، فضلا عن المستند مهما تضمن من معلومات وبيانات ذات خطورة على الحياة الخاصة[1].

ونرى أنه إذا رضي الشخص لغيره أن يصوره في موضع معين، فلإنه في الوقت ذاته لا يسمح لذات الشخص أن يعيد إستعمال ذات الصورة بأشخاصها في وضع آخر للتشهير بسمعة هذا الشخص[2].

وفي تحديد المقصود بالمكان الخاص، ذهب البعض من الفقه إلى تعريفه على أنه المكان الذي لا يعتبر مفتوح لأي شخص بدون تصريح ممن يشغله بطريقا دائمة أو مؤقتة[3].

وإذا كان الركن المادي للجريمة طبقا للنظرية العامة يتطلب سلوك ومحل ونتيجة إجرامية، فإنه بالرجوع إلى النصوص السابقة نجد تطلب التشريعات صراحة أن يؤدي فعل إلتقاط الحديث أو الصورة إلى نتيجة معينة وهي وجوب حدوث إنتهاك لحرمة الحياة الخاصة للغير، ولعل ما يؤكد رغبة المشرع في كون هذه الجريمة مادية أن رتب أثرا قانونيا معينا هو المعاقبة على الشروع.

ب-الركـــن المعنـــوي

هده الجريمة عمدية، يتخد الركن المعنوي فيها صورة القصد الجزائي العام بعنصريه العلم والإرادة. وهو ما يستفاد صراحة من البناء المعنوي لنص المادة 303 مكرر عقوبات جزائري والمادة 226-1 فرنسي "**كل من تعمد**".

وفضلا عن القصد الجنائي العام، يرى جانب من الفقه أن القصد المتطلب في هده الجريمة القصد الخاص المتمثل في نية الإعتداء على حرمة الحياة الخاصة، قياسا على القصد المتطلب لهده الجريمة في فرنسا من وجهة نظر هذا الرأي[4].

---

[1]- **عبد البديع آدم**، الحق في حرمة الحياة الخاصة ومدى الحماية التي يكفلها القانون الجنائي،رسالة دكتوراه،كلية الحقوق، جامعة القاهرة، 2005، ص547.

[2]- **د . نهاد فاروق عباس**، الحماية الجنائية الموضوعية للحياة الخاصة من جرائم الأنترنت في التشريع المصري، دورية الإدارة العامة، المجلس السادس والأربعون ، العدد الأول، فبراير 2006، ص117.

[3]-**Anthony Bem**, Le droit au respect de la vie privée : définition, conditions et sanctions; **http://www.legavox.fr/blog/maitre-anthony-bem/droit-respect-privee-definition-conditions-16644.htm#.V_Y0qtSLQSm**

CA Besançon, 5 janvier 1978; Question écrite n° 00425 de **Mme Esther Sittler** (Bas-Rhin - UMP) publiée dans le JO Sénat du 12/07/2012 - page 1562; https://www.senat.fr/questions/base/2012/qSEQ120700425.html

[4]-انظر: **د. عمر ابو الفتوح عبد العظيم الحمامي**، الحماية الجنائية للمعلومات المسجلة الكترونيا،دار النهضة العربية، القاهرة، 2010، ص837.

Dans un jugement du 23 octobre 1986 , la 17e chambre correctionnelle a défini que devait être qualifié de public : « *le lieu accessible à tous, sans autorisation spéciale de quiconque, que l'accès en soit permanent et inconditionnel ou subordonné à certaines conditions*. **Badinter (Robert)**, "La protection de la vie privée contre l'écoute électronique clandestine", *Semaine juridique* 1971, chronique 2435; cite par **Cordier François**, « L'atteinte à l'intimité de la vie privée en droit pénal et les médias », *LEGICOM* 4/1999 (N° 20) p1.

ثانيا–الإختلاف الفقهي حول مدى صلاحية نصوص حرمة الحياة الخاصة في توفير الحماية للمعطيات الشخصية

لقد إحتدم الخلاف بين الفقهاء لدى إجابتهم حول مدى صلاحية تلك النصوص في توفير حماية للمعطيات الشخصية الإكترونية من عــدمه:

إذ يرى البعض من الفقه المصري[1]**بفاعلية هذه النصوص** في توفير حماية للمعطيات الشخصية إذ بإمكانها أن تستوعب حالة الإعتداء الذي يتم بإختراق الأنظمة المعلوماتية المخزنة فيها هذه المعطيات، بسبب أن المشرع إستخدم عبارة ...عن طريق جهاز من الأجهزة أيا كان نوعه...". في نص المادة 309 مكرر عقوبات المقابلة لعبارة "باية تقنية كانت" الواردة في المادة 303 مكرر عقوبات جزائري، وهي نفس العبارة التي إستخدمها المشرع الفرنسي في المادة 226–1 عقوبات au moyen d'un procédé quelconque ، إد أن هذه العبارة من شأنها أن توفر حماية لحرمة الحياة الخاصة ضد مخاطر المعلوماتية، فتسمح بالعقاب على إلتقاط أو تسجيل أو نقل حديث جرى عبر الأنترنت، كما يسمح النص بالعقاب على إلتقــاط ونقل الصورة الشخصية التي أخدت في أماكن خاصة والتي تخزن على نظم المعلومات أو الموجودة في ملفات شخصية للأشخاص بالبريد الإلكتروني ولو كانت موجودة لدى موزع الأنترنت[2].

غير أن هناك من قال **بعدم صلاحية هذه النصوص** لتوفير حماية للمعطيات الشخصية الإلكترونية[3]، بسبب أن التجريم ينصب فيها حول الحصول على الصورة أو الحديث بطريقة غير مشروعة، إلا أن مقومات الحياة الخاصة للأفراد ليست فقط صوتا لحديث أو صورة، فالحياة الخاصة مقومات أكثر من ذلك بكثير ومن بينها المعطيات الشخصية المختزنة في أنظمة الحاسب الآلي أو المسجلة على الأنترنت.

ونحن من جانبنا نؤيد الرأي الثاني فيما ذهب إليه، من عدم صلاحية وكفاية النصوص السابقة في توفير الحماية الكاملة للمعطيات الشخصية، ذلك أن الرأي الأول وإن إرتكز على صيغة النص فيما يخص تقنيات الإعتداء، فقد أهمل جانبا مهما وهو محل الإعتداء الا وهو "المعطيات الشخصية **المكتوبة** و**المختزنة** بخاصة إدا كان مجال التخزين هو العالم الإفتراضي، في حين أن النص إقتصر على الحديث او الصورة او المكالمة، والقول بغير ذلك يسفر عن الخروج على مبدأ الشرعية، وإعمال القياس لحالات واقعية على الحالات المنصوص عليها، وهذا أمر محظور في نطاق نصوص التجريم.

---

[1]-انظر:**أسماء حسن سيد محمد رويعي**، الحق في حرمة الحياة الخاصة في مواجهة الجرائم المعلوماتية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 2013، ص561، **خالد محمد كدفور المهيري**، جرائم الكمبيوتر والأنترنت والتجارة الإلكترونية، الطبعة الثانية، دار الغريب للطباعة والنشر، دبي، بدون تاريخ نشر، ص626.

[2]– د.**مدحت عبد الحليم رمضان**، جرائم الإعتداء على الأشخاص والأنترنت، المرجع السابق، ص119.

[3]–**د. أسامة عبد الله قايد**، مرجع سابق، ص ص118، 119.**د. مدحت عبد الحليم رمضان**، الحماية الجنائية للتجارة الإلكترونية، المرجع السابق، ص 112، **د. عفيفي كامل عفيفي**، **فتوح الشادلي**، مرجع سابق، ص300.**ماشاء الله عثمان محمد الزوي**، المرجع السابق، ص259. **د. عمر أبــو الفتوح عبد العظيم الحمامي**، المرجع السابق، ص841.

كما أن هذه المواد لو كانت تكفي لحماية المعطيات الشخصية، لما كانت الحاجة دعت المشرع الفرنسي إلى إصدار نصوص جديدة خاصة بحماية المعطيات الشخصية.

بل وحتى على فرض التجريم على النحو السابق بيانه فإن الأمر لايخلو من القول من ضرورة تنظيم عملية المعالجة الآلية للمعطيات الشخصية، فيجب أن تكون عملية المعالجة من الدولة أو إنشاء هيئة مستقلة إدارية لذلك الغرض، والنص على تجريم أنشطة الإستخدام والتجميع غير المشروع لهذه المعطيات، إفشاءها ومخالفة قواعد حمايتها وغيرها من المخاطر التي تحملها المعالجة الآلية للمعطيات الشخصية على حق الأفراد في حماية حياتهم الخاصة.

الفرع الثاني

حماية المعطيات الشخصية في قانون التوقيع الإلكتروني

سبق القول بأن حماية المعطيات الشخصية والخصوصية في بيئة الأنترنت يولد الثقة في تعامل الأشخاص بالتعاملات الإلكترونية خاصة التجارية منها، التي تعد ركيزة أساسية من ركائز الإقتصاد في عالمنا اليوم، ولذلك تضمنت بعض الدساتير مبدأ ضمان حق حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، وهو ما أقره دستور الجزائر 1996 المعدل[1]في المادة 46 ونص على المعاقبة على إنتهاكه.

وجاء قانون التوقيع الإلكتروني رقم 15-04 ليقر حماية خصوصية المعلومات في نطاق التعاملات الإلكترونية وما يتعلق بها من معطيات ومعلومات يتم تداولها من خلال تجريم بعض الأفعال التي من شأنها المساس بها تحقيقا لمبدأ الردع العام والخاص في هذا المجال، وصور التجريم هذه منها ما تمثل حماية للمعطيات إبتداء قبل تسجيلها لدى الوسيط النظامي في التعامل الإلكتروني، وسبق أن رأينا أن الوسيط النظامي له أثرا في المركز القانوني للأطراف، والمقصود هنا مزود خدمة التصديق الإلكتروني، ومنها ما تمثل حماية بعد هذا التصديق، كما أنشأ المشرع سلطة إدارية لحماية التعاملات الإلكترونية التي تتم عبر التوقيع الإلكتروني، وفي هذا الإطار وضع المشرع مخطط هيكلي يضم سلطة وطنية للتصديق الإلكتروني وهيئتين تؤطران التصديق الالكتروني للفرعين الحكومي والاقتصـــادي.

وكذلك فعلت بعض التشريعات كما هو شأن المشرع المصري في قانون التوقيع الإلكتروني، كما أنشا من جهته هيئة تنمية صناعة تكنولوجيا المعلومات وهي تقدم حماية محدودة للخصوصية، حيث أنها تنصب وظيفتها على تنظيم نشاط خدمات التوقيع الإلكتروني وغيرها من الأنشطة في مجال التعاملات الإلكترونية و صناعة تكنولوجيا المعلومات.

[1]-بالقانون رقم 16-01 المؤرخ في 06 مارس 2016، الجريدة الرسمية،عدد 14 ، الصادرة في 7 مارس 2016 .

كذلك الأمر بالنسبة لتونس، حيث خصصت في قانونها المتعلق بالمبادلات والتجارة الإلكترونية الباب السادس لتنظيم مسالة حماية المعطيات الشخصية، كما أنشا لحماية المبادلات والتجارة الإلكترونية الوكالة الوطنية للمصادقة الإلكترونية.

وعلى ذلك سنحاول في هذا المطلب بحث هذه الحماية قبل التسجيل لدى مزود خدمة التصديق الإلكتروني(الفرع الأول) ثم بحث هذه الحماية بعد التسجيل لدى هذا المزود(الفرع الثاني) في كل من التشريع الجزائري والمصري والتونسي.

أولا- الحماية الجزائية قبل التسجيل لدى الوسيط النظامـــي في التعاملات الإلكترونية

القاعدة في معالجة المعطيات الشخصية وفق نظم المعالجة، أن هذه المعطيات لا يتم تخزينها أو معالجتها إلا بإذن صاحب الشان نفسه، ولدلك فعلى مزود خدمة التصديق أن يحصل على المعلومات الشخصية مباشرة من الشخص ذاته المعني بالشهادة الإلكترونية[1]، فهو الأقدر على الإدلاء بمعلومات تحدد وضعه ومركزه القانوني[2].

إلا أنه قد يحدث ويدلي هذا الشخص بتصريحات مغلوطة، مما قد يؤثرا سلبا على مصداقية الشهادة التي قد يقدمها مزود الخدمة، وهو ما تداركه المشرع الجزائري -على خلاف المشرع المصري -، حيث عاقبت المادة 66 من قانون التوقيع الإلكتروني**كل من يدلي باقرارات كاذبة للحصول على شهادة تصديق الكتروني موصوفة.** كما عاقب المشرع التونسي على ذات الفعل بمقتضى الفصل 47 كمايلي" **كل من صرح عمدا بمعطيات خاطئة لمزود خدمات المصادقة الإلكترونية ولكافة الأطراف التي طلب منها أن تـــثق بإمضائه...**"

وهذه الصورة من التجريم تمثل حماية جزائية للمعطيات الشخصية قبل تسجيلها لدى الجهة التي تمارس أعمال التوثيق.

أ- الركـــن المـــادي

يشترط حتى تتحقق جريمة الإدلاء العمدي بتصاريح كاذبة من طرف المستفيد، أن يكون قد صرح بمعلومات ما يميزها أنها كادبة أي مخالفة للحقيقة سواء تعلقت بهويته أو نشاطه أو أي معلومات لها أهمية. ولم يحدد المشرع من جانبه شكل هذه التصاريح، وعليه يستوي أن تكون يدوية أو معالجة بالنظام. وذلك لأن المشرع الجزائري عاقب على الإدلاء بهذه التصريحات للحصول على الشهادة، الأمر الذي يعني إمكانية الإدلاء بها قبل معالجتها. وكذلك فعل المشرع التونسي حين نص على إعطاء هده المعطيات لمزود الخدمة.

---

[1]-**الشهادة الإلكترونية** عبارة عن وثيقة في شكل إلكتروني صادرة عن جهة تصديق مختصة، تعتمد على تكنولوجيا رياضية معقدة وهي تقنية شفرة المفتاح العام والمفتاح الخاص، ويرجع ذلك إلى أن هذه التقنية من أقوى الوسائل الحديثة.

[2]- ومع ذلك أجاز المشرع التونسي بموجب الفصل 16 من قانون المبادلات و التجارة الإلكترونية لمزود الخدمة الحصول على هذه البيانات من الغيربعد الموافقة الكتابية أو الإلكترونية لهذا الشخص.

والملاحظ أن المشرع الجزائري إستخدم عبارة "**إقرارات**" بصيغة الجمع، وكذلك فعل الشرع التونسي من خلال عبارة "**معطيات**"، وهي صيغة من شانها تضييق نطاق التجريم واقصاء حالة الإدلاء بإقرار أو بيان واحد، فكان الأولى بالمشرع أن لا يحصر نطاق التجريم بعدد الإقرارات. فضلا عن ذلك فإن فعل الإدلاء أو التصريح فعل ايجابي، وهو ما يثير مسالة الكتمان وما إذا كان مشمولا بالنص أم لا؟ خصوصا متى كان عن عمـــد.

كما تجدر الإشارة إلى ان المشرع الجزائري لم يحدد الجهة التي يتم تقديم هذه التصاريح لها، وكذلك فعل المشرع التونسي حين نص "...**لمزود خدمات المصادقة الإلكترونية ولكافة الأطراف التي طلب منها** ...وعلى ذلك يستوي ان يتم تقديمها لمؤدي خدمات التصديق او إلى طرفي التعامل الإلكتروني او طرف اخر كالبنـــك.

ب- الـــركـــن المـــعنـــوي

جريمة الإدلاء العمدي بإقرارات كاذبة جريمة عمدية في التشريع الجزائري يشترط لقيامها توافر القصد الجنائي بعنصريه العلم والإرادة، فيجب أن يعلم الجاني بعدم صحة المعلومات المقدمة، وارادة تقديم تلك المعلومات بغية إصدار شهادة تصديق الكتروني موصوفة[1].وما قيل بخصوص المشرع الجزائري، يقال بخصوص المشرع التونسي.

ت- العقوبـــة

يعاقب المشرع التونسي على هذه الجريمة بموجب المادة 47 بالسجن لمدة تتراوح بين 6 أشهر وعامين وبخطية تتراوح بين 1000 و 10000 دينار أو بإحدى هاتين العقوبتين. أمـــا المشرع الجزائري فيعاقب عليها بموجب المادة 66 بالحبس من 3 أشهر إلى 3 سنوات وبغرامة من 20000 إلى 200000 أو بإحدى هاتين العقوبتنين.

ثانيا: الحماية الجزائية بعد التسجيل لدى الوسيط النظامي في التعاملات الإلكترونية

إذا كانت المعلومات الشخصية قد حضيت بحماية جزائية من فعل الأشخاص الذين يقدمونها بصورة غير صحيحة، فإن تلك المعلومات قد حظيت بحماية جنائية من فعل من يمتلك تلك المعلومات أو وضعت تحت بصره وعلمه بوصفه أمينا عليها، وسنحاول بيان ذلك من خلال مايلي:

أ- المعالجة دون تبصـــير ذوي الشـــأن

[1]- **صالح فايز الشراري**، الحماية التشريعية للأشخاص المتعاملين في التجارة الإلكترونية – دراسة مقارنة-، مجلة الفكر الشرطي، المجلد الثامن عشر، العدد 71، 2009، ص153.

ورد النص على هذه الجريمة في الفصل 38 من القانون التونسي التي منعت مزود خدمة المصادقة الإلكترونية من معالجة المعطيات الشخصية دون موافقة صاحب الشهادة المعني، في حين جرم المشرع الجزائري صورة واحدة من صور المعالجة ألا وهو "جمع المعطيات الشخصية" دون موافقة المعني وذلك بموجب المادة 71 التي أحالت للمادة 43 من قانون التوقيع الإلكتروني، في حين لا نجد لهذه الصورة ذكرا في القانون المصري.

1-الركـــن المـــادي

يتحقق الركن المادي لهذه الجريمة بقيام الجاني بمعالجة المعطيات الشخصية، ولم يحدد المشرع التونسي من جانبه المقصود بالمعالجة في قانون المبادلات، وبالرجوع لقانون حماية المعطيات الشخصية نجده يعرف المعالجة في الفقرة الأولى من المادة 6 على أنها العمليات المنجزة سواء بطريقة آلية أو يدوية من شخص طبيعي أو معنوي، والتي تهدف خاصة الى جمع معطيات شخصية أو تسجيلها أو حفظها أو تنظيمها أو تغييرها او استغلالها او استعمالها او ارسالها او توزيعها او نشرها او اتلافها او الإطلاع عليها وكذلك جميع العمليات المتعلقة باستغلال قواعد البيانات او الفهارس او السجلات او البطاقات او بالربط البيني. على ان تتم هذه المعالجة دون موافقة الشخص المعني.

ويتحقق الركن المادي للجريمة بمجرد إجراء معالجة للمعطيات حتى ولو لم يترتب على الفعل أي نتيجة، فالجريمة سلوكية يكتفي المشرع فيها بتحقق السلوك الإجرامي دون اشتراط تحقق نتيـــجة.

2- الركـــن المعنـــوي

تعد هذه الجريمة من الجرائم العمدية التي يلزم لقيامها توافر القصد الجنائي بعنصريه العلم والإرادة، حيث يجب أن ينصرف علمه إلى عناصر الركن المادي للجريمة، بان يعلم بانه يقوم بمعالجة معطيات شخصية دون موافقة صاحب الشهادة، ويجب أن تتجه إرادته إلى إجراء المعالجة في أي صورة من صورها المختلفة.

3- العقوبـــة

يعاقب المشرع التونسي على هذه الجريمة بموجب الفصل 51 من قانون المبادلات بخطية تتراوح بين 1000 و 10000 دينار.اما المشرع الجزائري فيعاقب عليها بالحبس من 6 اشهر الى 3 سنوات، وبغرامة من 200000 دينار إلى 1000000 دج او باحداهما.

ب- جريمة جمع المعطيات الشخصية او استعمالها بشكل غير مشروع

يتطلب المشرع أن تتم عملية جمع المعطيات الشخصية بشكل مشروع، وتكون هذه العملية كـــذلك متـــى تمت بموافقة صاحب الشهادة، وهو ما أكده المشرع الجزائري صراحة في الفقرة الأولى من المادة 43 مـــن قانون التوقيع الإلكتروني، وتبعا لذلك الزم مؤدي خدمات التصـــديق الإلكترونـــي ان يجمـــع إلا المعطيـــات

الشخصية الضرورية لمنح وحفظ شهادة التصديق الإلكتروني، ولا يمكن استعمال هذه المعطيات لأغـــراض أخرى. ومخالفة ذلك يعرض صاحبه للعقوبة المنصوص عليها في المادة 71.

وإلى جانب المشرع الجزائري نجد المشرع التونسي ينص على ذلك بموجب الفصل 39 من قانون المبادلات على أنه"باستثناء حالة موافقة صاحب الشهادة ، لا يمكن لمزود خدمات المصادقة الالكترونية او أحد أعوانه جمع المعلومات الخاصة بصاحب الشهادة الا ما كان منها ضروريا لابرام العقد وتحديد محتواه و تنفيذ واعداد واصدار الفاتورة.

لا يمكن استعمال المعطيات المجمعة طبقا للفقرة الاولى من هذا الفصل لغير الغاية المذكورة اعلاه من قبل المزود او غيره الا اذا تم اعلام صاحب الشهادة بذلك ولم يعارضه."

كما حظر المشرع المصري من جانبه وبموجب المادة 21 من قانون التوقيع الإلكتروني استخدام المعطيات التي تقدم الى الجهة المرخص لها باصدار شهادات التصديق الإلكتروني في غير الغرض الذي قدمت من اجله. ايمانا منه أن هذه المعطيات وإن كانت ضرورية لإصدار الشهادة إلا أنها تمس خصوصية الشخص نفسه، وقد تمتد لعائلته.

إذا يستفاد من خلال النصوص السابقة الذكر أن جريمة جمع المعطيات الشخصية أو إستعمالها بشكل غير مشروع تقوم على أركان محددة، فلا بد من توافر الركن المادي المتمثل في فعل الجمع أو الإستعمـــال، وركـــن معنوي متمثل في القصد الجنائي، سنتناولـــهما كمايـــلي:

1-الركـــن المـــادي

يتمثل الركن المادي في هذه الجريمة في سلوك يتخده الجاني قد يأخذ صورة الجمع او الإستعمال ينصب على محل معين هو المعطيات الشخصية.

تتمثل الصورة الأولى من النشاط الإجرامي في جمع المعطيات الشخصـــية، علـــى أن تكـــون غيـــر ضرورية لمنح وحفظ شهادة التصديق الإلكتروني حسب المادة 43 من قانون التوقيع الإلكتروني الجزائري. أو غير ضرورية لإبرام العقد أو تحديد محتواه أو تنفيذه او إعداده أو إصدار الفاتورة من قبل مزود خدمـــة المصادقة أو أحد أعوانه ودون موافقة صاحب الشهادة حسب المادة 39 من قانون المبادلات التونسي.

أما الصورة الثانية للسلوك الذي جرمه المشرع هو الإستعمال(المادة 43 من القانون الجزائري-المـــادة 39 من القانون التونسي) أو الإستخدام(المادة 21 من القانون المصري)، ويقصد به في هذا المجال استعمال المعطيات الشخصية لغير الغرض الذي جمعت من أجله، وقد أورد المشرع التونسي استناء وهو حالة ما إدا تم اعلام صاحب الشهادة بذلك و لم يعترض.

هذا وقد وسع المشرع من دائرة التجريم الى كل استعمال للمعلومات دون تحديد منه لعدد المرات اللازمة لقيام الجريمة، كما انه لم يحدد نوعه وهو ما يستفاد بوضوح من عبارة "**لا يمكـــن اســـتعمال... لأغـــراض اخرى**" الواردة في المادة 43 من قانون التوقيع الإكتروني الجزائري. وعبارة "**...لا يمكن استعمل...لغيـــر الغاية المدكورة اعلاه...**" الواردة في المادة 39 مبادلات تونسي، وعبارة"**...استخدامها في غير الغرض...**"

الواردة في المادة 21 من قانون التوقيع الإلكتروني المصري، وربما هدفه من ذلك هو غلق كل باب أمام من يريد إستعمال هده المعلومات.

2-الركـــن المـــعنـــوي

تعد هذه الجريمة من الجرائم العمدية التي يلزم لقيامها توافر القصد الجنائي بعنصريه العلم والإرادة، اي يجب أن يعلم الشخص بأنه يقوم بجمع غير مشروع للمعطيات الشخصية او انه يستعملها لغير الغايـــة مـــن جمعها، وان تجه ارادته الى تحقيق ذلك، هذا ولم يشترط المشرع قصد جنائي خاص لتقوم الجريمة.

3- العقـــوبـــة

يعاقب المشرع الجزائري على هذه الجريمة بموجب المادة 71 من قانون التوقيع الإلكتروني بالحبس من 6 اشهر الى 3 سنوات، وبغرامة من 200000 دينار إلى 1000000 دج او باحداهما. أما المشرع التونسي فيعاقب عليها بموجب الفصل 51 من قانون المبادلات بخطية تتراوح بين 1000 و 10000 دينار.

أمـــا المشرع المصري فقد جعل من مخالفة أحكام المادة 21 الحبس والغرامة التي لا تقل عـــن عشـــرة آلاف جنيه ولا تجاوز مائة الف جنيه او باحدى هاتين العقوبتين وذلك بمقتضى الفقرة د من المادة 23 مـــن القانون.

ث- الإفشاء غير المشروع للمعطيات الشخصية

إهتم المشرع الجزائري بسرية المعطيات الشخصية واحترام الحق في الخصوصية، وجعل مـــن قيـــد السرية من الإلتزامات الواقعة على العاملين في معالجة المعطيـــات الشخصـــية فـــي مواجهـــة المتعـــاملين الإلكترونيين، ومن ذلك مؤدي خدمات التصديق وهذا ما نصت عليه صراحة المادة 42 من قـــانون التوقيـــع الإلكتروني، وبناء عليه جرم بموجب المادة 70 اي انتهاك او إخلال لهذا القيد من قبل مؤدي الخدمات. والى جانب المشرع الجزائري نجد المشرع التونسي في نص المادة 52 اكثر تحديدا حـــين نـــص علـــى تجـــريم الإعتداء على السرية بافشاء معلومات عهدت الى مزود خدمات المصادقة الالكترونية واعوانه فـــي اطـــار تعاطي نشاطاتهم باستثناء تلك التي رخص صاحب الشهادة كتابيا او الكترونيا في نشرها او الاعلام بها.

كما قضت المادة 21 من قانون التوقيع الإلكتروني المصري رقم 15 لســـنة 2004 بســـرية معطيـــات التوقيع الإلكتروني والوسائط الإلكترونية والمعلومات التي تقدم إلى الجهة المرخص لها بإصـــدار شـــهادات التصديق الإلكتروني، ولا يجوز لمن قدمت إليه أو إتصل بها بحكم عمله إفشاؤها للغير أو إستخدامها في غير الغرض الذي قدمت من أجلـــه.

سنتناول هذه الجريمة من خلال دراسة ركنها المادي والمعنوي كما يلي:

1 -الركـــن المـــادي

انطلاقا من نص المادة 52 من القانون التونسي والمادة 21 من القانون المصري، يتضـــح ان الـــركن المادي لهذه الجريمة يتلخص في أن الجاني في نطاق التعاملات الإلكترونية قد اطلع على معلومـــات بحكـــم وظيفته ثم قام عامدا بافشاءها، ويفترض فعل الإفشاء انتقال المعطيات من حيازة شخص توصل اليها بحكم

عمله في النظام الذي تتداول فيه هذه المعطيات واذاعتها واطلاع شخص لا علاقة لـــه بهـــذه المعطيـــات ، وخروجها من حيز الكتمان أو السرية بعد ان كان العلم بها قاصرا على اصحابها أو الذين إئتمنوا عليها بحكم وظيفتهم[1]، وهم مزودي خدمة المصادقة الإلكترونية ومعاونيهم دون علم ورضا صاحبها.

وإذا كان كل من المشرع التونسي والمصري آثرا مصطلح الإفشاء، أورد المشرع الجزائري نص عاما وهو نص المادة 70 من قانون التوقيع الجزائري، حيث تجرم هذه المادة أي إخلال بواجب الحفاظ على سرية البيانات من قبل مؤدي خدمات التصديق.

ونظرا لسهولة إرتكاب تلك الجريمة ممن يكون مكلف بالتدقيق بغرض مراقبة مؤدي خـــدمات التصـــديق الإلكتروني من قبل السلطة الإقتصادية، فإن المشرع الجزائري عاقب بموجب المادة 73 كل شخص مكلـــف بالتدقيق يقوم بكشف معلومات سرية إطلع عليها أثناء قيامه بالتدقيق. اكثر من ذلك جرم المشرع الجزائـــري بموجب المادة 68 كل من يقوم بإفشاء بيانات إنشاء التوقيع الكتروني موصوف خاصة بالغير والمعبر عنهـــا بمفتاح التشفير الخاص الذي يحوزه الموقع حصريا والذي يجب أن يكون **سريا**، دون تحديد منه للقائم علـــى اتيان النشاط الإجرامي. فالذي يقوم بفعل الإفشاء هنا ليس شخصا مؤتمنا على هده المعطيـــات، فهـــو لـــيس ملتزما بكتمان هده المعطيات بمقتضى وظيفة أو عقد ما.

ورغبة من المشرع التونسي في تحقيق حماية جنائية فعالة للمعطيات الشخصية، عاقـــب علـــى إفشـــاء المعلومات أو المشاركة في عملية الإفشاء أو التحريض عليها.

والملاحظ ان المشرع التونسي لم يحدد المعلومات او الوقائع التي يتوجـــب علـــى مـــزود الخدمـــة او معاونوه المحافظة على سريتها بل جعلها عامة، مما يمكن إدخال ضمنها المعطيات الشخصية، وكذلك فعـــل المشرع الجزائري في المادة 73 من قانون التوقيع الإلكتروني، إلا ان المادة 42 التي احالت اليها المادة 70 قد حصرتها في المعلومات المتعلقة بشهادات التصديق الإلكتروني. ويستوي في ذلك أن تكون مسجلة علـــى دعامة الكترونية على شريط مرن او قرص مدمج، او تكون مخزنة ضمن برنامج معلوماتي في جهاز حاسب آلي[2].

وكذلك هو الشان بالنسبة للمشرع المصري، ذلك أنه وإن كان قد حصر المعلومـــات الواجـــب الحفـــاظ سريتها في بيانات التوقيع الإلكتروني والتي تعد من **المعطيات الشخصية**، والوسائط الإلكترونية إلا أنه عـــاد وأضاف عبارة "**...والعلومات التي تقدم الى الجهة...**" هذا من جهة.

ومن جهة أخرى، نلاحظ عدم تحديد المشرع للوسيلة التي يمكن ان يصدر بها افشاء لهذه المعلومات مما يجعل الركن المادي لهذه الجريمة يتحقق باي وسيلة.

---

[1]- **د.أحمد حسام طه تمام**، المرجع السابق، ص325. **د. عبد الفتاح بيومي حجازي**، النظام القانوني للتوقيع الإلكتروني، –دراسة تاصيلية مقارنة، دار الكتب القانونية، مصر، 2007، ص508.

[2]- **د. عبد الفتاح بيومي حجازي**، النظام القانوني للتوقيع الإلكتروني، المرجع السابق، ص508.

في الأخير تجدر الإشارة إلى أن هذه الجريمة من جرائم الخطر يكتفي فيها المشرع بتحقق السلوك الإجرامي دون اشتراط تحقق نتيجة لأن الغرض من التجريم هو الحفاظ على سرية و خصوصية المعطيات[1].

2-الركن المعنوي

هذه الجريمة من الجرائم العمدية التي تقوم على القصد الجنائي العام بعنصريه العلم والإرادة، فالجاني هنا يسعى بإرادته إلى إفشاء المعطيات او المشاركة فيه او التحريض عليه والمساعدة فيه، وذلك مع علمه التام بماديات الواقعة المؤثمة قانونا. وقد اورد المشرع التونسي سببا للإباحة في حالة إذا كان الجاني قد قام بإفشاء هذه المعطيات الشخصية بناء على ترخيص من صاحب الشأن أو في أحد الفروض التي يوجب عليه القانون ذلك، كا في حالة صدور إذن قضائي بتقديم هذه المعلومات و المعطيات.

3-العقوبة

متى تحقق الركن المادي والمعنوي وجب انزال العقوبة على الجاني، وهي حسب المادة 254 من المجلة الجزائية التونسية السجن لمدة تتراوح بين شهرين و3 سنوات وغرامة تتراوح بين 1000 و10000 دينار او باحدى هاتين العقوبيتين، اما المشرع الجزائري فعاقب على إخلال مؤدي خدمات التصديق الإلكتروني بسرية البيانات المتعلقة بشهادات التصديق الإلكتروني الممنوحة بالحبس من 3 اشهر إلى سنتين، وبغرامة من 200000 إلى مليون دينار او باحدى هاتين العقوبتين. وهي نفس العقوبة المقررة لمن يكشف البيانات الشخصية اطلع عليها اثناء قيامه بالتدقيق ماعدى الغرامة، فالغرامة المفروضة هنا هي من 20000 إلى 200000 دينار. اما عقوبة من يقوم بافشاء بينات انشاء التوقيع الإلمتروني موصوف خاصة بالغير هي السجن 3 اشهر الى 3 سنوات و بغرامة من مليون دينار إلى خمسة ملايين دينار.مع امكانية معاقبة الشخص المعنوي في جميع الجرائم السابقة بغرامة تعادل 5 مرات الحد الأقصى للغرامة المفروضة على الشخص الطبيعي.

أما المشرع المصري فقد جعل من مخالفة أحكام المادة 21 الحبس والغرامة التي لا تقل عن عشرة الاف جنيه ولا تجاوز مائة الف جنيه او باحدى هاتين العقوبتين وذلك بمقتضى الفقرة د من المادة 23 من القانون.

مما سبق نلاحظ أن التجربة الفرنسية في حقل أمن المعلومات و الخصوصية هي التجربة الأكثر نضجا في العالم، ففرنسا من اوائل الدول التي تعاملت مع الظاهرة تعاملا واقعيا عبر دراسات معمقة للواقع، ولطبيعة المشكلات، وللحلول والتدابير الأفضل، فلم تكن تجربة متسرعة لكنها لم تكن بطيئة أيضا من حيث الإستجابات، بل كانت إستجابات مبكرة في حدود متطلبات الواقع، ولأن فهم الظاهرة اساسا وأخد التدابير على ضوء هذا الفهم المعمق هو أهم ضمانات النجاح.

وعلى خلاف ذلك، فقد تبين أثناء الدراسة أن هناك نقصا لدى الدول العربية في إصدار تشريعات أو تنظيمات قانونية تتعلق بكيفية معالجة المعطيات الشخصية وحمايتها، وأن هناك فقط بعض الدول التي اصدرت تشريعا خاصا بذلك كما هو الحال في تونس، أما الوضع في الجزائر ومصر فلم تكن مسالة الحماية

---

[1]-**د. جلال ثروت**، نظم القسم الخاص-جرائم الإعتداء على المال المنقول، الجزء الثاني، دار المطبوعات الجامعية، الإسكندرية، 1995، ص5 .**د. عوض محمد عوض**، شرح قانون العقوبات -القسم العام-دار المطبوعات الجامعية، الإسكندرية، 1991، ص55.

على نفس المستوى المطلوب، صحيح أنهما قد خطتا خطوة ايجابية نحـــو حمايـــة المعطيـــات ذات الطـــابع الشخصي من مخاطر المعالجة غير المشروعة في قانون التوقيع الإلكتروني، إلا ان تدخلهما كان قاصرا في الإحاطة بجميع الجوانب سواء تعلق منها بالمحل أو بالأفعال، ولا ندل على ذلك أكثر من عدم تطرقهما إلـــى إنشاء سلطة الرقابة الرسمية المختصة بالسهر على حماية المعطيات الشخصية وصـــلاحية ســـلطة الرقابـــة التحقيقية مثل جمع المعلومات والوصول إلى المعطيات، ومسالة نقل المعطيات دات الطابع الشخصـــي إلـــى دول أجنبية والمعايير المفروضة لتقويم مستوى حماية معالجة المعطيات الشخصية.

ومن ثم نهيب بالمشرع الجزائري والمصري التدخل لتوفير الحماية الجزائية للمعطيات الشخصية، وذلك بإقرار تشريع يضع تنظيما دقيقا لكيفية معالجة هذه المعطيات وحمايتها مع مراعاة المعاهدات والإتفاقيات الدولية المبرمة في هذا المجال، نظرا لطبيعة تقنية المعلومات الشمولية ذات الصيغة الدولية ولمنع التناقض بين التنظيم الداخلي والدولي لمعالجة هذه النوعية من المعطيات.

الفصـــل الثـــاني

الحماية الجزائية لمضمون التعاملات الإلكترونية

إن فحوى مضمون التعاملات الإلكترونية، إرتبط بشكل عام بالتحول من المستندات التقليدية العادية إلى الدعامات المعلوماتية التي تحتوي على تلك المعلومات التي كانت متواجدة بالمستندات التقليدية، مما اقتضى ظهور التوقيع الإلكتروني كمحور تأكيد على وجود علاقات تمت عن بعد بين الأشخاص، كعلامة مميزة لإتفاقهم والتزاماتهم من جهة.

ولمواكبة مقتضيات التعاملات الإلكترونية متطلبات نظام التجارة الدولية، ووضع أسس تضمن موثوقية التعاملات، وثقة المتعاملين بها في مرحلة إبـــرام التعاملات الإلكترونية، وإتمامها من جهة أخرى، وذلك بإستخدام وسائل الدفع الإلكترونية، مخففا بذلك من التعامل النقدي، خاصة بطاقات الإئتمان.

ولذلك فإن أهم الدراسات التي ناقشت الحماية الجزائية لمضمون التعاملات الإلكترونية، قد أسفرت على ضرورة تركيز الأنظمة القانونية على 3 مواضيع أساسية، يشكل كل واحد منها مقوم من مقوات الحماية القانونية بشكل عام لمضمون هذه التعاملات:

الأول: يتعلق **بالإعتراف بالأدواتالخاصة بتبادل الأعمال:** ونعني بذلك الإعتراف بالمستندات الإلكترونية ومساواتها بالمستندات الكتابية التقليدية، والإعتراف بالتوقيع الإلكتروني ومعادلته بالتوقيع اليدوي العادي.

الثاني: يتعلق بوضع تنظيم قانوني لوسائل دفع جديدة تكون ملائمة لطبيعة ومتطلبات التعاملات الإلكترونية، تعتمد على الركيزة الإلكترونية.

الثالث : بث الثقة والأمان في أدوات تبادل الأعمال وأدوات نظـــم الدفع خاصة بطاقات الإئتمان، بإعتبارهما من مقدمة الضمانات التي ينبغي توافرها لإزدهار التعاملات الإلكترونية، سواء كانت تجارة إلكترونية أو حكومة الكترونية أو غيرها من التعاملات التي أفرزتها ضرورة الحياة كنتيجة للتطور المتزايد لوسائل التكنولوجيا وهيمنتها على كافة جوانب الحياة، وذلك بوضع قواعد للتاكد منها، ومن تلك القواعد إقامة المسؤوليات وفرض الجزاءات لمواجهة الأنماط المتعددة من السلوك والأفعال التي تمثل إعتداء على مجمل محتوى التعامل الإلكتروني، سواء كان مرتكب الإعتداء طرفا في التعامل الإلكتروني، أو كان من خارجه. إذ أن أثر ذلك ليس فقط أثر علاجي بل هو أيضا وقائي يولد الحرص لدى جميع الأطراف.

إذن ترتبط التعاملات الإلكترونية عضويا بثلاثة مفاهيم أساسية، المستند الإلكتروني والتوقيع الإلكتروني والدفع الإلكتروني خاصة من خلال بطاقة الإئتمان، وعلى الرغم من ان إسباغ الحماية الجزائية على المستند الإلكتروني تهدف إلى حماية التوقيع وتضمن أدائه لدوره الإجتماعي، إلا أن العالم الرقمي فرض تكريس صور من الحماية الخاصة تختلف عن الحماية المقررة للمستند بصفة عامة.

وعلى ضوء ذلك، فإننا سنبحث الحماية الجزائية لكل مقوم على حدى نظرا لخصوصية كل منهم في مجال المعلوماتية، من خلال ثلاثة مباحث كمايلـــي:

المبحث الأول: الحماية الجزائية للمستند الإلكتروني

المبحث الثاني: الحماية الجزائية للتوقيع الإلكتروني

المبحث الثالث: الحماية الجزائية لبطـــــاقة الإئتمان

المبحث الأول

الحماية الجزائية للمستند الإلكتروني

مع إزدياد التقدم في مجالي الإعلام والإتصال، أصبح إجراء التعاملات عبر مختلف الوسائط الإلكترونية ، حيث يقوم أحد طرفي التعاملات الإلكترونية بإرسال المعلومات التي يريدها، من خلال قاعدة معطيات تكون مربوطة على الشبكة، وذلك عن طريق إدخال بعض المعلومات كتلك المتعلقة بالمرسل إليه[1]، والمعلومات المتعلقة بالخدمة أو السلعة، ليكون لدينا في الأخير ما يسمى بـــ: "**المستند الإكتـــروني**".

إن المستند الإلكتروني يعتبر من الأدوات المهمة في تنفيذ فكرة التعاملات الإلكترونية إدارية كانت أو تجارية أو مدنية أو مالية، التي تمتد لتشمل الدولة والأفراد على حد سواء، حيث أن له صلة بنشاط الهيئات التي تعمل في مجال البنوك والتأمين والخدمات الطبية وغيرها، ومن خلاله يمكن إنجاز المعاملات وإبرام التصرفات والصفقات التي تقتضيها التجارة الإلكترونية.

وغني عن البيان أن الحماية الجزائية للمستند الإلكتروني أهمية كبيرة تكمن في أهمية هذا المستند في حد ذاته، كونه يلعبا دورا مناظرا للدور الذي يلعبه المستند التقليدي، وهو ما يحقق في المقابل سهولة التعاملات الإلكترونية وسرعة إنجازها وما توفره من نفقات، كما أن هذه الحماية تؤدي الى تحقيق الإستقرار والأمان القانوني، فحماية المستند الإلكتروني وصيانته من المساس بسريته وكشف محتواه يكفل للمتعاملين الطمأنينة وزرع الأمان في هذه الوثيقة، ومن ثم إستقرار التعاملات، كما يؤدي الى أن يصبح هذا المستند دليلا في الإثبات يقف على قدم المساواة مع المستند الورقي، مما يؤدي إلى إستقرار النظام القانوني والحد من المنازعات.

على هدي ماتقدم، فإن دراسة الحماية الجزائية للمستند الإلكتروني تقتضي منا الوقوف أولا على مفهومه، مرورا بتبيان أوجه الحماية الجزائية له بشكل عام، ونظرا لكون جرائم تزوير المستند الإلكتروني تعد من ضمن أهم الإعتداءات التي تطاله، بل من أهم جرائم تقنية المعلومات، والتي أخذت في الإنتشار في الآونة الأخيرة، وزادت خطورتها، خاصة مع التغيير في بعض المفاهيم القانونية الخاصة بجريمة التزوير عند تطبيقها على التزوير في المجال المعلوماتي. فاننا سنخصص لها مطلب مستقل.

وعلى ذلك سنقسم هذا المبحث إلى ثلاثة مطالب على النحـــو التالـــي:

المطلب الأول: نطاق الحماية الجزائية(المستند الإلكتروني)

المطلب الثاني:الحماية الجزائية للمستند الإلكتروني بشكل عام

المطلب الثالث::الحماية الجزائية للمستند الإلكتروني من التزوير

[1]-**د. عبيدات محمد لورانس**، إثبات المحرر الإلكتروني، الطبعة الأولى، دارالثقافة للنشر والتوزيع ، عمان، 2009، ص77.

المطلب الأول

نطاق الحماية الجزائية(المستند الإلكتروني)

إن الإعتماد على التعاملات الإلكترونية يعني بالضرورة أن المستند الإلكتروني سيصبح هو **السند القانوني** المعتمد بين الأطراف، بل قد لا نبالغ إن قلنا أن هذه التعاملات ترتبط وجودا وعدما بوجود هذا المستند أو إنعدامه.

ومع إختلاف التشريعات في تسميته وتعريفه سواء عند تنظيمه بقانون خاص أو عند تنظيمه بإعتباره دليل إثبات في القانون المدني أو قانون الإثبات، ولتجنب الوقوع باللبس ارتاينا تحديد مفهومه حتى يتسنى لنا تحديد نطاقه وإستظهار الأفعال الماسة به، وذلك بتعريفه(الفرع الأول)، وتبيان شروط صحته لإمكانية التعامل به(الفرع الثاني)، وتمييزه عما يلتبس به من مفاهيم(الفرع الثالث).

الفرع الأول

تعريف المستند الإلكتروني

نشير في البداية إلى أنه لا يوجد مصطلح موحد في بين التشريعات والفقهاء للدلالة على هذا المفهوم، إذ نجد مصطلح "رسالة معلومات" أو بيانات،" المحرر لإلكتروني" الوثيقة الإلكترونية""الوثيقة المبرمجة""الوثيقة الرقمية" وغيرها، إلا أننا آثرنا ترجيح مصطلح **المستند الإلكتروني**[1] على إعتبار أن مصطلح المستند يتسع ليشمل كل طريقة يتم بها تدوين أو تسجيل ما يتعلق بالحقوق، والمراكز القانونية للأشخاص الطبيعية، و المعنوية، كما أنه مصطلح قانوني على عكس المصطلحات الأخرى ذات دلالة تقنية محضة.

ولتحديد مدلول المستند الإلكتروني، لا بد من إستعراض الآراء الفقهية في مفهومه والرجوع إلى مجموع التشريعات المقارنة التي نظمت التعامل به من خلال النصوص التي تضمنتها في المعاملات القانونية المختلفة.

أولا- التعريـــف الفقـــهي

عرف الفقه المحرر بصفة عامة بأنه "كل كتابة تدل على معنى مفهوم ويمكن نسبتها إلى شخص محدد[2] من خلال توقيعه عليها"، ويعد الورق هو الدعامة السائدة في مجال إستعمال الكتابة وفي مختلف الميادين.

---

[1]- أنظر في الإتفاق حول ذلك: **د. أيمن عبد الله فكري**، المرجع السابق، ص404. د. **أشرف توفيق شمس الدين** ، الحماية الجنائية للمستند الإلكتروني –دراسة مقارنة–، الطبعة الأولى، دارالنهضة العربية، القاهرة، 2006، ص334 وما بعدها.

[2]– أنظر في صدد تعريف المحرر بالتفصيل لدى: **د.فتوح عبد الله الشادلي**، شرح قانون العقوبات، القسم الخاص، دار المطبوعات الجامعية، الإسكندرية، 2001، ص385.

أما عن المستند الإلكتروني فيعرفه جانب من الفقه من خلال مصطلح الوثيقة المبرمجة على أنه" **كل دعامة معلوماتية يتم الحصول عليها بوسائل معلوماتية أي ناشئة على جهاز الكتروني أو كهرومغناطيسي أو طبع ممغنط**"[1]، كما عرف بمصطلح الوثيقة المعلومتية على أنه "**رسالة بيانات تتضمن معلومات تنشأ أو ترسل أو تستلم أو تخزن باستخدام وسائل الكترونية**"[2] كما عرف على أنه" **معلومات يتم إنشاؤها أو إرسالها أو تخزينها أو إستلامها بوسيلة الكترونية أو ضوئية أو رقمية أو صوتية مادامت تتضمن إثبات واقعة أو تصلرف قانوني محدد وتتضمن توقيع الكتروني ينسب هذه الواقعة أو التصرف لشخص محدد**"[3]

إن المتأمل للتعريفات السابقة يجد أنها إعتنقت مبدأ الحياد التقني، حيث حددت طبيعة الوسيط الحامل للمعلومات كونه إلكتروني دون تحديد منها لوسيلة الكترونية بعينها، وهو ما يسمح باستيعاب أي وسائل إلكترونية قد تظهر حاضرا ومستقبلا، كما أنها ألقت الضوء على عنصر واحد من عناصر المستند الإلكتروني، وهو عنصر الكتابة دون الإشارة إلى العنصر الآخر وهو التوقيع، على الرغم –على حد قول بعضهم[4]– من أن الكتابة والتوقيع هما للمستند كالجناحين للطائر. ضف إلى ذلك إغفالها لعنصر مهم ألا وهو الوظيفة التي يقوم بها هذا المستند كونه وسيلة لإثبات حق أو مركز قانوني أو له أثر قانوني معين.

ثانيا–التعريـــف التشريعـــي

لتحديد مفهوم المستند الإلكتروني، لا بد من الرجوع إلى التشريعات التي نظمت التعامل به، سواء على المستوى الوطني أو الدولي. ولذلك سنحاول التركيز على أهم القوانين الدولية والداخلية التي وضعت إطارا قانونيا للتعامل بالمستند الإلكتروني.

فعلى المستوى الدولي، نجد مثلا قانون الأونسترال النموذجي بشأن التجارة الإلكترونية الذي أشار للمستند الإلكتروني باستخدام مصطلح "رسالة البيانات"، بمقتضى المادة 2 منه ويقصد بها:"**المعلومات التي يتم إنشاؤها أو إرسالها أو إستلامها أو تخزينها بوسائل الكترونية أو صوتية أو بوسائل مشابهة، بما في ذلك على سبيل المثال لا الحصر تبادل البيانات الإلكترونية أو البريد الإلكتروني، أو البرق، أو النسخ الورقي**" وهو ذات التعريف الوارد بالمادة 2 فقرة ت من قانون الأونسترال بشأن التوقيعات الإلكترونية[5].

أما على المستوى الوطني، فلم تضع الكثير من التشريعات نصوصا تحدد بموجبها فكرة المستند الإلكتروني، إلا أنها في المقابل أدخلت تعديلات تشريعية على قواعد الإثبات التقليدية من شأنها النهوض بالكتابة الإلكترونية إلى مستوى موثوقية الكتابة العادية، وإعطاءها مفهوما موسعا تستوعب الكتابة

---

[1]– **د. محمد سامي الشوا**المرجع السابق، ص168.

[2]– د. **ناهد فتحي الحموري**، الأوراق التجارية الإلكترونية، الطبعة الأولى، دار الثقافة، عمان، 2009، ص36.

[3]–**د. محمد أمين الرومي**، المستند الإلكتروني، دار الفكر الجامعي، الإسكندرية، 2007، ص55.

[4]– **نور خالد عبد المحسن العبد الرزاق**، حجية المحررات والتوقيع الإلكتروني في الإثبات عبر شبكة الأنترنت، رسالة دكتوراه، جامعة عين شمس، 2009، ص385.

[5]- Article 2 alinéa c dispose que "Le terme “message de données” désigne l’information créée, envoyée, reçue ou conservée par des moyens électroniques ou optiques ou des moyens analogues, notamment, mais non exclusivement, l’échange de données informatisées (EDI), la messagerie électronique, le télégraphe, le télex et la télécopie;"

والمستندات الورقية والإلكترونية وغيرها، كما هو حال المشرع الفرنسي، فتماشيا مع التوجيهات الأروبية بشأن الإعتراف بالوسائط غير الورقية في إثبات مختلف التعاملات عن بعد، قام بإجراء تعديلات على قواعد الإثبات السائدة، ومن بين ما مسه التعديل المادة 1316 مدني وذلك بموجب القانون رقم 230-2000 الخاص بتكبيف قواعد الإثبات مع تكنولوجيا المعلومات[1]، حيث أورد فيها تعريفا عاما للدليل الكتابي أدرج فيه مصطلحات لغوية واسعة تتيح ضم المستندات التقليدية والإلكترونية في آن واحد، حيث نصت على أنه *"الدليل الكتابي او الدليل المكتوب يستنتج من الحروف أو العلامات أو الأرقام أو أي رمز أو أي إشارة أخرى ذات دلالة تعبيرية واضحة ومفهومة أيا كانت دعامتها أو طرق نقلها"*[2]. وقد تم نقل مضمون هده المادة ضمن المادة 1365 بموجب الأمر رقم 2016-131 المتعلق بإصلاح قانون العقد، واثبات الإلتزامات[3]، مع حدف العبارة الأولى والثانية، وتعويضها بعابرة الكتابةL'écrit consiste*، فضلا عن حدف طرق نقلها.*

وعلى غرار المشرع الفرنسي، نجد المشرع الجزائري هو بدوره لم يضع تعريف خاص بالمستند الإلكتروني بل أورد تعريف عام للدليل الكتابي ، حيث نصت المادة 323 مكرر مدني " **ينتج الإثبات بالكتابة من تسلسل حروف أو أوصاف أو أرقام أو أية علامات أو رموز ذات معنى مفهوم، مهما كانت الوسيلة التي تتضمنها وكذا طرق إرسالها**"[4].

أما المشرع المصري فقد تبنى صراحة مفهوم المستند الإلكتروني من خلال مصطلح المحرر الإلكتروني، بموجب المادة 1 من القانون الخاص بالتوقيع الإلكتروني، حيث عرفته على أنه "**رسالة بيانات تتضمن معلومات تنشأ أو تدمج أو تخزن أو ترسل أو تستقبل كليا أو جزئيا بوسيلة الكترونية أو رقمية أوضوئية أو أي وسيلة أخرى مشابهة**".

بعد إستعراضنا للتعريفات السابقة، نلاحظ أنها حاولت تحديد هذا المفهوم المستحدث، إلا أننا نسجل بعض الملاحظات نوردهـــا فيمايلي:

– ركزت أغلب هذه التشريعات في تعريفها على الجانب الفني للمستند وليس القانوني، وهو ما جعل المستند يشمل كل البيانات والمعلومات حتى **تلك التي ليس لها أهمية قانونية**. والتي تكون كذلك عندما تتوافر لها

---

[1]- Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.

[2]- **Article 1316 du CCF** Modifié par Loi n°2000-230 du 13 mars 2000 - art. 1 JORF 14 mars 2000 **dispose que "** La preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission.

[3]Ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations

حيث جاء هذا الأمر بغرض تحديث وتبسيط وتحسين وإمكانية الوصول إلى قانون عام للعقود، ونظام الإلتزامات وقانون الإثبات وذلك لضمان فعالية القاعدة القانونية. وقد دخل هذا الأمر حيز التنفيد في أكتوبر 2016. تفصيل أكثر حول المبادي التي جاء بها هذا الأمر أنظر:

Bérengère Peyrat, LA RÉFORME DU DROIT DES OBLIGATIONS. Article disponible:http://www.village-justice.com/articles/JeSuis1382-reforme-droit-des,21553.html

[4]- تجدر الإشارة الى أن المشرع الجزائري قد أشار الى المستند الإلكتروني بعبارة "**بيانات الكترونية اخرى**" الواردة ضمن المادة 2 –1 من القانون 15–04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، حين تعريفها للتوقيع الإلكتروني.

الحجية في إثبات شيء معين أو نفـــيه، ضف إلى ذلك أن يكون لهذا الشيء أو الواقعة قيمة يعترف بها الشارع ويقـــرها[1].

– إتبعت التشريعات نهج مرن فيما يتعلق بالتقنيات المستخدمة في الكتابة ودعامتها، وهو ما يسمى **بمبدأ الحياد بين الوســـائط** [2].

– أدرجت بعض التعريفات في تعريفها للمستند الإلكتروني عنصر **التـــداول**، كمـــا هو شأن المشرع الفرنسي، وهو عنصر جديد من عناصر التعريف حيث يعطي هذا العنصر شكلا حركيا للتعريف الساكن للمحرر التقليدي.

– إستعملت بعض التشريعات عبارة " **الوسيلة الإلكترونية وما في حكمها**"،فضلا عن إستخدامها لفظ" **أو**" فيما يخص عملية المعالجة، وهو ما يعني أن المستند الإلكتروني وفق التعريفات السابقة، قد يبدأ بطريقة غير إلكترونية، وينتهي بوصفه مستندا إلكترونيا، فالتعريفات من الإتساع ما يشمل جميع مدخلات ومخرجات الوسائط الإلكترونية، فالمستند قد يكون مكتوبا على دعامة ورقية ثم يجري إدخـــاله إلى الحاسب الآلي عن طريق تقنية المسح الضوئي، ثم يرسل إلى شخص آخرعن طريق شبكة الأنترنت، ثم يخزن على قاعدة بيانات الحاسب للمرسل اليه أو ينسخ على شريط ممغنط أو قرص ضوئي أو يرسل بالفاكس[3].

–حصرت البعض من هذه التشريعات المستند في مدلول "**الرسالة**" كما هو حال التشريع المصري ، إلا أن نطاق المستند يتعدى مفهوم الرسالة التي تنطوي على إيجاب وقبول، إذ يمكن أن يكون معلومات **مخزنة في سجلات إلكترونية**[4] كشهادات الميلاد[5] والبطاقات الرمادية للسيارات، أو بطاقة إلكترونية للضمان الإجتماعي كبطاقة الشفا في الجزائر، والبطاقات المغناطيسية التي تصدرها البنوك، ففي هذه الحالة فإن هذه المعلومات لا تنطوي على أية رسالة موجهة لأحد[6].

–قصور جميع التعريفات السابقة في تحديدها مدلول المستند الإلكتروني، لعنصر مهم إذا غاب أصبح المستند كتابة الكترونية فقط، ألا وهو التوقيع الإلكتروني، فهو أحد العناصر المهمة لتمتع المستند الإلكتروني بالحجية، ومن ثم إضفاء الحماية القانونية عليه.

---

[1]– **د. رايس محمد**، الحماية الجنائية للسند الإلكتروني في القانون الجزائري، مجلة الدراسات القانونية، العدد الأول، كلية الحقوق، بيروت، 2006–2008، ص80.

[2]– دليل تشريع[اشتراع] قانون الاونسيترال النموذجي بشان التوقيعات الالكترونية لسنة 2001، بند 67، ص 32.

[3]–**د. عبد الفتاح بيومي حجازي**، النظام القانوني للتوقيع الإلكتروني ، المرجع السابق، ص 50.

[4]– يشبه **السجل الإلكتروني** السجل الورقي الذي يحفظ فيه الأشخاص تصرفاتهم اليومية مثل سجلات التجار، سجلات الأحوال المدنية، سجلات قيد الصحائف الدعاوى القضائية: **عيسى غسان الريضي**، القواعد الخاصة بالتوقيع الإلكتروني، دار الثقافة للنشر والتوزيع، عمان، 2012، ص189.

[5]– ففي الجزائر تم تأسيس **السجل الوطني الآلي للحالة المدنية**، بموجب القانون رقم 08/14 المؤرخ في 2014/08/09 الذي يعدل ويتمم الأمر رقم 20/70 المؤرخ في 1970/02/19 و المتعلق بالحالة المدنية، جريدة رسمية ، عدد 49، صادرة في 20 غشت 2014.

وهو يضم عقود الحالة المدنية الرقمية للمواليد والوفيات والزواج، لكل بلديات الوطن، وهي عقود ممسوحة و محجوزة ابتداء من سجلات الحالة المدنية للبلديات و ترسل إلى مصلحة السجل الوطني الآلي للحالة المدنية بوزارة الداخلية عبر الأنظمة المعلوماتية والشبكات التي وضعت لهذا الغرض. يهدف السجل الوطني الآلي للحالة المدنية إلى تكوين قاعدة معطيات مركزية شاملة، تستغل عبر كافة بلديات الوطن لإصدار عقود الحالة المدنية للمواليد و الوفيات و الزواج لأي شخص و من أية بلدية ،مجنبا المواطن عناء التنقل إلى البلدية التي سجلت بها عقوده.

[6]– **د. رايس محمد**، المرجع السابق، ص80. **د. اشرف توفيق شمس الدين**، الحماية الجنائية للمستند الإلكتروني، المرجع السابق، ص ص32–35.

بناء على الملاحظات السابقة، يمكننا تعريف المستند الإلكتروني على أنه" ***معلومات لها اهمية أو قيمة قانونية يتم نشاءها أو إرسالها أو إستلامها أو تخزينها أو غير ذلك من العمليات المتصلة بها بطريقة إلكترونية أو بأية وسيلة أخرى مشابهة، مصحوبة بتوقيع الكتروني***".

وللمستند الإلكتروني على النحو السابق بيانه نماذج كثيرة، يتم تداولها في التعاملات الإلكترونية سواء عند إتمامها في شكل **عقود إلكترونية**، أو عند تنفيدها عن طريق البطاقات الإلكترونية سواء صدرت عن جهات حكومية كبطاقة التعريف البيومترية الإلكترونية أو عن مؤسسات مالية خاصة كالبطاقات المصرفية."

الفرع الثاني

شروط صحـــة المستند الإلكتـــروني

لقد حرصت أغلب التشريعات على الإعتداد بالكتابة والمستند الإلكتروني الموقع إلكترونيا، وصاحب ذلك إقرار مبدأ التكافؤ بين المستندات الإلكترونية والمحررات الورقية من حيث قبولها وحجيتها في الإثبات. وكانت النتيجة المترتبة أن المساس بهذه المستندات يشكل **فعـل مـجرم** .

ويرجع الفضل في هذه المساواة، إلى القانون النموذجي بشأن التجارة الإلكترونية، حيث نجده يؤكد في المادة 5 منه على أنه لا يجوز رفض الأثر القانوني للمعلومات أو قيمتها أو قابليتها للتنفيذ لأسباب تقتصر على كونها إتخدت شكلا الكترونيا[1].

وقد سار المشرع الفرنسي على خطى القانون النموذجي، وإعترف بذلك صراحة بمقتضى المادة 1366 [2]من القانون المدني المعدل بموجب الأمر رقم 2016–131 المتعلق بإصلاح قانون العقد، واثبات الإلتزامات، حيث نصت على انه **للكتابة الإلكترونية[3]نفس القوة في الإثبات التي تكون للكتابة على دعامة ورقية بشرط أن يكون في الإمكان تحديد هوية الشخص الذي صدرت منه كما ينبغي وأن تعد وتحفظ في ظروف من طبيعتها ضمان سلامتها**". هذا ويبرر الفقه الدور الهام والحيوي الذي يجب أن تكفله التقنية من ثقة في المستندات الإلكترونية حيث تقوم بإعطاء الثقة والأمان في الوسيلة المستخدمة[4].

---

[1]- L'effet juridique, la validité ou la force exécutoire d'une information ne sont pas déniés au seul motif que cette information est sous forme de message de données.

[2]-Article 1366 du CCF dispose que" L'écrit électronique a la même force probante que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité".

وتجدر الإشارة إلى أن المادة 1365 و1366 أخدت تعريف الكتابة و الكتابة الإلكترونية من المادة 1316 و1316–1 من القانون المدني.

[3] – ذهب جانب من الفقه الفرنسي إلى تفضيل إستخدام تعبير كتابة على دعامة الكترونية عن تعبير كتابة الكترونية حيث ان استخدام هذه المصطلحات يدل على ان دعامات الكتابة هي التي تتغير وليس طبيعتها، في هذا الخصوص أنظـــر:

Eric CAPRIOLI, Le juge et la preuve électronique, colloque de Strasbourg, "Le commerce électronique : vers un nouveau droit", 8-9 octobre 1999. Revue de droit des technologies de linformation , n10 , 2000.P3

[4]-**د. أيمن عبد الله فكري**، المرجع السابق، ص352.

وعلى ذات النهج سار المشرع الجزائري في اقراره هده المساواة بمقتضى المادة 323 مكرر 1 من القانون المدنيحيث نصت"**يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق ، بشرط امكانية التاكد من هوية الشخص الذي اصدرها و ان تكون معدة ومحفوظة في ظروف تضمن سلامتها**".

كذلك الأمر بالنسبة للمشرع المصري، حيث أقر بدوره المساواة الكاملة بين الكتابة والمستندات الإلكترونية في الإثبات ومنحهما ذات الحجية المقررة للكتابة والمحررات التقليدية بمقتضى المادة 15 و18 من قانون التوقيع الإلكتروني، مع إحالته بموجب المادة 17 بشأن إثبات صحة المستندات الإلكترونية الرسمية والعرفية فيما لم يرد بشأنه نص في هذا القانون أو في لائحته التنفيدية، إلى الأحكام المنصوص عليها في قانون الإثبات في المواد المدنية والتجارية.

إن اعمـــال مبدأ التكافؤ السابق بيانه، متوقــف على استيفاء ضوابط وشروط معينة نتعرض لها فيمايلي.

أولا-الكتـــابة الإلكـــترونية

تتربع الكتابة على الهرم الذي يضم طرق الإثبات، فهي الوسيلة الأفضل والأكمل للإثبات، لذلك يجب أن يكون المحرر مكتوبا، ومن أجل تحديد شروط الكتابة الإلكترونية حتى تؤدي الوظيفة التي تؤديها الكتابة على الورق، إستوجب تحديد مفهومها بإعتبارها مرتبطة ببيئة الكترونية، وهو ما سعت إليه مختلف التشريعات التي نظمت التعامل بالمستند الإلكتروني، سنحاول فيما يلي إستقراء نصوصها في تحديد مفهوم الكتابة الإلكترونية.

إن معنى الكتابة لا يرتبط بالضرورة بتدوين الأفكارعلى الورق، وبالتالي يكفي أن يكون هناك وسيط قادر على نقل الرموز والأشكال وما تضمنته الوثيقة أي كان الوسيط المستعمل لنقل هذه التعابير المتعلقة بحق أو مركز قانوني معين. وبالتالي ينعدم الإرتباط بين الكتابة والوسيط الورقي، حيث أي دعامة قادرة على عكس مضمون الكتابة فإنه من الممكن أن يأخد بها في الإثبات. وبذلك تم الفصل بين شرط الكتابة الورقية وحماية المستند الإلكتروني[1] ، وهو ما كرسه قانون الأونسترال النموذجي بشان التجارة الإلكترونية في المادة 6-1 على أنه عندما يشترط القانون أن تكون المعلومات مكتوبة، تستوفي رسالة البيانات ذلك الشرط إذا تيسر الإطلاع على البيانات الواردة فيها على نحو يتيح إستخدامها بالرجوع إليها لاحقا، وقد عرفت المادة 2-أ رسالة البيانات بأنها المعلومات التي يتم انشاؤها أو إرسالها أو إستلامها أو تخزينها بوسائل الكترونية أو صوتية أو بوسائل مشابهة، بما في ذلك على سبيل المثال لا الحصر تبادل البيانات الإلكترونية أو البريد الإلكتروني، أو البرق، أو النسخ الورقي". ويلاحظ تأكيد هذه المادة على عدم الإعتداد بنوع الوسيط الحامل للبيانات المكتوبة في الإثبات.

[1]-**ناهد فتحي الحموري**، المرجع السابق، ص ص66،67، **براهمي حنان**، جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2014، ص129.

وإذا كان هذا هو موقف قانون الأونسترال النموذجي، فإن الموقف الفرنسي كان أكثر وضوحا، وذلك من خلال المادة 1365 من القانون المدني التي نصت على أن الكتابة هي نتيجة تسلسل حروف أو علامات أو أرقام أو أي رمز أو أي إشارة أخرى ذات دلالة تعبيرية واضحة ومفهومة أيا كانت الدعامة.

ويفهم من عباره "**واضحة ومفهومة**" الواردة في نص المادة السابقة، أن الرموز التي لا يستوعبها الإنسان ولو بواسطة جهاز الحاسوب لا تصلح لتكون كتابة إلكتـــرونية تشكل المستند الإلكتروني.

كما أخضعت المادة 1366 مدني مقبولية الكتابة في الشكل الإلكتروني كدليل في الإثبات لشرطين: تحديد هوية الشخص الذي صدرت منه، وأن تنشا وتحفظ في ظروف من شأنها ضمان سلامتها.

وبذلك ألغى المشرع الفرنسي التدرج بين الوثائق على أساس الدعامة التي يتم الكتابة عليها، فلافرق بين المستند الورقي والمستند الإلكتروني من حيث القيمة الثبوتية إذا توافرت الشروط المطلوبة قانونا[1]. مع إعتناقه لمبدأ الحياد التقني وذلك بعدم تفضيله تقنية معينة في الكتابة، وهو مسلك حسن يسمح لجميع التقنيات بنيل فرصة إستيفاء الشروط اللازمة للإعتراف بها.

لم يكن المشرع الجزائري بمنأى عن التطور الذي مس أدلة الإثبات، حيث نجده وسع من مفهوم الكتابة أثناء تعريفه للدليل الكتابي ليشمل الكتابة الإلكترونية، وذلك بموجب المادة 323 مكرر من القانون المدني، ليكرس بموجب المادة 323 مكرر 1 مبدأ التعادل الوظيفي بين كل من الكتابة الإلكترونية والكتابة التقليدية.طالما كان من الممكن التأكد من هوية الشخص الذي أصدرها وأن تكون محفوظة في ظروف تضمن سلامتها.

كما نجد قانون التوقيع الإلكتروني المصري، قد عرف الكتابة الإلكترونية بموجب الفقرة أ من المادة 1 على أنها كل حروف أو أرقام أو رموز أو علامات أخرى تثبت على دعامة الكترونية أو رقيمة أو ضوئية أو أية وسيلة أخرى مشابهة وتعطي دلالة قابلة للإدراك". كما نصت المادة 15 منه على إصباغ الحجية الكاملة للكتابة الإلكترونية سواء في المعاملات المدنية أو التجارية أو الإدارية، متى إستوفت الشروط التي حددتها المادة 18 ، وبتحليل نص المادة المشار إليها نخلص إلى أن المشرع المصري **يعول في المقام الأول على التوقيع الإلكتروني** في مجال منح الحجية للكتابة والمحررات الإلكترونية، أي أن التوقيع الإلكتروني هو مفتاح تحقيق الموثوقية للكتابة والمستندات الإلكترونية، كما أحال المشرع إلى الضوابط الفنية والتقنية اللازمة لتحقق هذه الحجية للائحة التنفيذية[2] (المواد 8،9،10،11). أما المشرع الفرنسي دهب إلى أبعد من ذلك حينما أنشأ قرينة تفيد موثوقية التوقيع الإلكتروني الذي يستوفي شروط وضوابط محددة من أجل إفتراض صحة المستند الإلكتروني العرفي.

---

[1]–**د. سامح عبد الواحد التهامي**، التعاقد عبر الأنترنت–دراسة مقارنة– دار الكتب القانونية، القاهرة، 2008، ص552.

[2]-قرار رقم 109 لسنة 2005، بتاريخ 15–5–2005 بإصدار اللائحة التنفيذية لقانون التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات.

وعلى العموم، وبتحليل النصوص السابقة، نجدها متقاربة في ما بينها من حيث شروط قبول الكتابة الإلكترونية، إلا من حيث طريقة التعرض لها وهي: 1-أن تكون ذات دلالة تعبيرية واضحة، 2-أن تمكن من تحديد الشخص مصدرها 3-أن تكون معدة ومحفوظة في ظروف تضمن سلامتها[1].

وفي كل الأحوال فإن الكتابة أمر لازم في المستند الإلكتروني رسمي كان أو عرفي، ومناط رسمية المستند وفقا للقواعد العامة في الإثبات أن يكون صادرا عن **موظف أو ضابط عمومي أو شخص مكلف بخدمة عامة** في حدود سلطته وإختصاصه حسب الأوضاع المقررة قانونا[2]، في حين أن المستند العرفي التقليدي هو المستند الذي يتم بمعزل عن الموظف العام، أي يستقل الأفراد بتحريره، ولا يختلف الأمر في نطاق العالم اللامادي، وإن كان مسألة التفكير في تطويع فكرة الرسمية الموجه ناحية المستند الإلكتروني بشكل يسمح بتلبية المتطلبات الإجتماعية والإقتصادية للتعاملات الإلكترونية يصاحبه حرص دائم على حماية مجمل الإمتيازات القانونية للمستند الرسمي.

والحقيقة أن فكرة المستند الرسمي الإلكتروني وثيق الصلة بما يسمى **التعاملات الإلكترونية الحكومية** حيث تشمل إختصاصات الحكومة الإلكترونية المعاملات الإدارية الحكومية وخدمات المواطنين بشكل عام، ومنها التصاريح المختلفة والخدمات التي تقدمها الجمارك والضرائب ومصلحة الأحوال المدنية، وكذلك كل ما يقدم إلى الجهات الحكومية من طلبات والتي من الممكن ووفقا لهذا القانون أن تتم عن طريق المستندات الإلكترونية التي تصدرها الجهات المشار إليها، ويتم توقيعها من قبل الموظفين العموميين في هذه الجهات مما يضفي على تلك المستندات الإلكترونية صفة المستندات الرسمية[3]، وتنبع اهمية اصباغ صفة الرسمية على المستند الإلكتروني، أن الإعتداء عليه يدخله في مصاف الإعتداء على **الأموال العامة**، وكذا تزويره يرتفع به إلى مصـــاف **الجنايات**.

ومجارات للمشرع الفرنسي للمستند الرسمي التطور التقني في مجال تقنيات المعلومات والإتصال، كرس مبدأ الإعتراف بالمستند الرسمي الإلكتروني بموجب المادة 1369[4] من القانون المدني إدا أمكن حفظه في الشروط المطلوبة قانونا، وتطبيقا لدلك صدر المرسوم رقم 972-2005 في 10 اغسطس 2005 الذي يحدد شروط إنشاء وحفظ المستندات الرسمية على دعامة الكترونية وصورها بالنسبة للمحضرين القضائيين[5]، وفي ذات الوقت صدر المرسوم رقم 973-2005 في 10 اغسطس 2005 الذي يحدد شروط إنشاء وحفظ المستندات الإلكترونية على دعامة الكترونية وصورها بالنسبة للموثقين[6].

---

[1]- ويقابل هذا الشرط شرطي تدوينها على وسيط يسمح بثباتها عليه وإستمرارها وعدم قابليتها للتعديـــل .

[2]- **د. أنور سلطان**، قواعد الإثبات في المواد المدنية والتجارية، دار الجامعة الجديدة للنشر،الإسكندرية، 2005 ، ص57.

[3]-**د. أحمد حسام طه تمام**، المرجع السابق، ص51.

[4]- **Article 1369 DU CCF** Modifié par Ordonnance n°2016-131 du 10 février 2016 - art. 4 dispose que "L'acte authentique est celui qui a été reçu, avec les solennités requises, par un officier public ayant compétence et qualité pour instrumenter.

Il peut être dressé sur support électronique s'il est établi et conservé dans des conditions fixées par décret en Conseil d'État. Lorsqu'il est reçu par un notaire, il est dispensé de toute mention manuscrite exigée par la loi."

[5]-**Décret n°2005-972 du 10 août 2005 modifiant le décret n° 56-222 du 29 février 1956 pris pour l'application de l'ordonnance du 2 novembre 1945 relative au statut des huissiers de justice** ;

[6]-**Décret n° 2005-973 du 10 août 2005 modifiant le décret n° 71-941 du 26 novembre 1971 relatif aux actes établis par les notaires** , JORF n°186 du 11 août 2005.

أما في مصر كان المشرع أقل وضوحا حين أشار للمحررات الرسمية الإلكترونية في قانون التوقيع الإلكتروني ولم يفردها بنص خاص، حيث إكتفى بمجرد ترديد القاعدة العامة في الإعتراف بالمساواة بين المستندات الرسمية الإلكترونية والمستندات الرسمية الورقية(المادة 15 من قانون التوقيع الإلكتروني)، دون تحديد منه للمسائل الخاصة بإنشاءه وحفظه.

أما الوضع في التشريع الجزائري، فرغم أنه ساوى في الحجية بين الكتابة الخطية والإلكترونية، إلا أنه لم يبين حدود هذه المساواة إن كانت تشمل المستندات الرسمية أم لا. إلا أنه وتماشيا ومبادرة الجزائر بإرساء معالم الحكومة الإلكترونية، بدأت العديد من الوزارت إعتمادها، مثل وزارة العدل عن طريق القانون رقم15-03 الذي إحدث بموجبه منظومة معلوماتية مركزية تتعلق بنشاط وزارة العدل والمؤسسات التابعة لها وكذا الجهات القضائية للنظام القضائي، مع امكانية مهر الوثائق والمحررات التي تسلمها الوزارة بتوقيع إلكتروني تضمن الوزارة على التصديق عليه بواسطة ترتيب إلكتروني مؤمن، وقد بين هذا القانون في إطار التطبيق العملي للمستندات الرسمية الإلكترونية، شروط تمتع المستند الإلكتروني المرسل بالطريق الإلكتروني بصحة وفعالية الوثيقة الأصلية في المادة 10 منه، حيث إشترطت أن تضمن الوسائل التقنية المستعملة في الإرسال:

-التعرف الموثوق على أطراف التراسل الإلكتروني.

-سلامة الوثائق المرسلة.

-امن وسرية التراسل .

-حفظ المعطيات بما يسمح بتحديد تاريخ الإرسال والإستلام من طرف المرسل إليه بصفة أكيدة.

فضلا عن ذلك، تم إستحداث سلطة تصديق حكومية تتولى تأطير تسيير الشهادات الإلكترونية المستعملة في التعاملات الإلكترونية التي تكون الإدارة طرفا فيها، والتي يقدمها الطرف الثالث الموثوق.

ثانيا- التوقيع الإلكتروني:

كي يكون للمستند الحجية الكاملة فإنه لابد أن يشتمل على توقيع من صدر عنه، وشرط التوقيع شرط بديهي كونه يعني نسبة ماورد في المستند لأطرافه. وإذا كان المستند رسمي فإن التوقيع فيه ليس توقيع ذوي الشأن، بل توقيع الموظف العام المختص الذي يحرر هذه الورقة الرسمية وفقا للأوضاع والشروط التي نص عليها القانون، ثم يوقع على هذه الورقة بما يفيد تمام شروط صحتها ومن تم إكتسابها صفة الرسمية.

وبما أن المستند الإلكتروني يتكون من كتابة وتوقيع، فمن غير المتصور أن يبقى شكل التوقيع على المستند الإلكتروني تقليديا، بل يجب ان يكون من نفس تقنية المستند الإلكتروني أي أن يكون إلكترونيا. وقد سعت التشريعات إلى الأخد بهذا المفهوم وذلك من خلال تبني الأحكام الواردة في القوانين النموذجية الصادرة عن الأمم المتحدة والإتحاد الأروبي، حتى يتسنى لها مواكبة هذه الطفرة المعلوماتية.

وحيث أن التوقيع الإلكتروني سيكون موضوع دراسة مفصلة في المبحث الثاني من هذا الفصل فإننا سنقوم بتفصيل ما يتعلق به لاحقـــا.

ثالثا– كشف هوية الشخص مصدر المستند الإلكتروني:

وهو ماعبرت عنه صراحة المادة 1366 من القانون المدني الفرنسي، والمادة 323 مكرر 1 من القانون المدني الجزائري، وتجدر الإشارة إلى أن تحديد هوية الشخص في التشريع الفرنسي يجري بواسطة تحقق مسبق عن طريق **التوقيع**، وهو ما يستفاد من دلالة عبارة" كما ينبغي أو بحسب الأصول "dument الواردة في المادة السابقة[1].

وعلى خلاف مسلك المشرع الفرنسي والجزائري، لم يتطلب المشرع المصري ضرورة تحديد هوية منشيء المستند الإلكتروني، بل إتجه إلى تحديد شروط تمتع التوقيع الإلكتروني والكتابة الإلكترونية والمحررات الإلكترونية بالحجية في الإثبات. مركزا في ذلك–كما مر معنا–على دور التوقيع الإلكتروني في الإثبات، ولعل أن مسلكه هذا مبرر من كون أن هذا الشرط بديهي وضروري في التعاملات الإلكترونية لتحقيقه عنصر الأمان والثقة فيها، فضلا عن ذلك فإن التوقيع الإلكتروني متى توافرت عناصر موثوقيته يكفل تحديد هوية الشخص المنسوب إليه المستند[2].

وفي الغالب يتم التحقق من نسبة المستند لمن صدر عنه عن طريق إستخدام التوقيع الرقمي المعتمد على التشفير اللامتماثل، وعن طريق شهادة التصديق الإلكتروني على النحو الذي سنبينه في الموضع المناسب في هدا الفصل.

رابعا– حفظ المستند الإلكتروني بطريقة تضمن سلامته:

تتميز الدعامات الإلكترونية على إختلاف أشكالها بسهولة إجراء تعديلات في المعطيات المدونة عليها، ذلك أنه بإمكان أي شخص يملك خبرة في معالجة المعطيات إجراء أي تعديل سواء بمسح أو بإضافة معطيات إلى المستند دون ترك أي أثــر مــادي، ماعدا البيان الذي يسجله الحاسوب والمتعلق بزمن وتاريخ التغيير، بل حتى هذا البيان قابل للتغيير إذ أن الجهاز يمكن أن نبرمجه وفق أي تاريخ نرغب فيه قبل القيام بتغيير المستند، وبالتالي يسجل التاريخ الذي وقع فيه التغيير ويكون موافقا لتاريخ كتابة المستند[3]. أكثر من ذلك، يمكن أن تتعرض هذه المعطيات أثناء بثها من المرسل إلى المرسل إليه عبر الأنترنت، إلى الاختراق أو الإتلاف أو حتى الاستيلاء، وهو ما قلل في المقابل من الثقة في المستند الإلكتروني. وقد تم حل هذه المشكلة

---

[1] ويرى بعض الفقه الفرنسي أن تحديد هوية الشخص الذي صدرت منه الكتابة يشكل وظيفة أساسية يؤديها التوقيع وليس الكتابة، وبناء عليه فإن إشارة القانون الفرنسي إلى إشتراط تحديد الهوية وشرط السلامة في المادة المخصصة للكتابة (1366) ثم تعرضه لهما مرة أخرى في المادة المتعلقة بالتوقيع، يعتبر بلا شك نوعا من التكرار:

Eric CAPRIOLI,op.cit. P4

[2] **–د. تامر محمد سليمان الدمياطي**، المرجع السابق، ص537.

[3] **–سليمان المقداد**، ضوابط الإعتراف بالمحررات الإلكترونية في الإثبات، الندوة العلمية حول المعاملات الإلكترونية : التطبيق المخاطر والحماية ، مركز الدراسات والبحوث الإنسانية والإجتماعية، وجدة، 14–05–2015، ص3.

عن طريق إعتماد التوقيع الإلكتروني المشفر الرقمي الذي هو مزيج من تحليل الشفرات والتشفير[1]، لتجنب تحريف مضـــمون المستند.

ولقد عبرت عن ذلك بعض التشريعات صراحة، فقانون الأونسترال النموجي بشأن التجارة الإلكترونية نص بمادته 8 على ذلك الشرط باعتماده مصطلح في شكلها الأصلي كمايلي"...تقديم المعلومات أو الإحتفاظ بها في شكلها **الأصلي**..." ، هذا وقد إشترط هذا القانون بموجب المادة 10 منه مراعاة الشروط التالية:

– تيسير الإطلاع على المعلومات الوارد فيها على نحو يتيح استخدامها في الرجوع إليها لاحقا.

– الإحتفاظ برسالة البيانات بالشكل الذي أنشات أو أرسلت أو أستلمت به أو بشكل يمكن إثبات أنه يمثل بدقة المعلومات التي أنشات أو أرسلت أو أستلمت .

– الإحتفاظ بالمعلومات إن وجدت التي تمكن من إستبانة منشأ رسالة البيانات وجهة وصولها وتاريخ ووقت إرسالها وإستلامها.

هذا وأوجب المشرع الفرنسي من جهته تحقق شرط حفظ المستند الإلكتروني بصفة تمنع تغيير محتواه لتضاهي قيمة المحرر الورقي[2]، وكذلك فعل المشرع الجزائري في القانون المدني بموجب المادة 323 مكرر، وفي قانون التوقيع الإلكتروني بموجب المادة 4 منه حيث إشترط وجوب أن تحفظ الوثيقة الموقعة إلكترونيا في شكلها **الأصلي**، ومعنى ذلك هو وجوب حفظ هذه الوثيقة في الشكل الأخير الذي إتفق عليه أطرافها بجعلـــها في مأمن من كل تغيير أو تحوير، سواء كان ذلك بطريقة مقصودة أو غير مقصودة.

كما حرص المشرع المصري على أن يدرج ضمن شروط تحقق حجية المستند الإلكتروني، شرطا يفيد ضرورة الحفاظ على سلامة مضمونه يتمثل في" إمكانية كشف التعديل أو التبديل في بيانات المستند الإلكتروني أو التوقيع الإلكتروني وفقا للضوابط التي تحددها اللائحة التنفيدية لقانون التوقيع الإلكتروني، وحسب المادة 11 من هذه اللائحة يتم ذلك عن طريق إستخدام تقنية شفرة المفتاحين العام والخاص، وبمضاهاة شهادة التصديق الإلكتروني وبيانات إنشاء التوقيع الإلكتروني بأصل هذه الشهادة وتلك البيانات، أو بأية وسيلة مشاهبة، وهو الشرط الذي أدرجه المشرع الجزائري ضمن شروط تحقق التوقيع الإلكتروني الموصوف كما سنرى.

ولكن معنى الحفظ الذي قصدته التشريعات لا يقتصر على حفظ المعلومات المتصلة بالمستند الإلكتروني من التحريف والتغيير فحسب، وإنما يشمل حماية ذلك المستند في حد ذاته من التلف والإضمحلال أيضا.

---

[1]-**Karima MOUSTAID,** Solutions pour prévenir les modifications non autorisées **,disponible en lingne á l'adresse suivante** http://karimamoustaid.over-blog.com/article-solutions-pour-prevenir-les-modifications-non-autorisees-84767396.html

[2]-Voir article 1366 du CCF .

خامسا-إمكانية إسترجاع المستند الإلكتروني المحفوظ:

أشارت بعض التشريعات صراحة إلى هذا الشرط، كما هو حال قانون الأونسترال النموذجي بشان التجارة الإلكترونية في المادة 10-1-أ "**...الرجوع اليها لاحقا...**"، كما تطلبه القانون المدني الفرنسي ضمنا من خلال عبارة " **... ومحفوظة...**" الواردة في المادة 1366 ، وسار على نهجه المشرع الجزائري من خلال المادة 323 مكرر 1، على إعتبار أن الهدف من الحفظ هو إمكـــانية الرجوع إليها في أي وقت.

إن إشتراط التشريعات هذا الشرط مهم جدا في الإثبات الإلكتروني، إذ أن إمكانية إسترجاع المستند المحفوظ توازي وتعادل قيمة المستند الورقي، فالإحتجاج بهذا المستند يتحقق بامكانية الرجوع إليه وإسترجاعه.

هذا ولم تشأ التشريعات الخوض في الوسائل المعتمدة لتحقيق الحفظ المادي للمستند الإلكتروني، غير أن عدم بيان ذلك لا يمنع من ذكر بعض الطرق والآليات التي أفرزتها تطبيقات المعلوماتية في هذا المجال من ذلك ندكر الأقراص المغناطيسية الرقمية، الأقراص المغناطيسية البصرية، البطاقات الليزرية....

الفرع الثالث

تمييز المستند الإلكتروني عن غيره من المستندات

لقد توصلنا من خلال دراستنا إلى أن المستند الإلكتروني معلومات لها أهمية أو قيمة قانونية يتم إنشـــاءها أو إرسالها أو إستلامها أو تخزينها عبر وسائط الكترونية أو بأية وسيلة أخرى مشابهة، مصحوبة بتوقيع صاحب الإرادة، وهو ما يميزه عن المستند التقليدي، ويميزه عما يختلط به في البيئة الإلكترونية.

أولا_ تمييز المستند الإلكتروني عن المستند التقليدي

رغم التشابه بين المستند الورقي، والمستند الإلكتروني في إحتواء كل منهما على حقيقة يريد المشرع حمايتها، وأن كل منهما ينطوي على مجموعة من الرموز التي تعبر عن مجوعة مترابطة من الأفكار والمعاني الإنسانية، ويتماثل كل منهما في إنطوائهما على فكرة الضرر التي هي علة تجريم المساس بهما، فإن بينهما فوارق يمكن أن نستخلصها من العناصر الأساسية التي يقوم عليها المستند التقليدي وهي: ***الكـــتابة، الدعامـــة، التوقـــيع.***

أ-من حيث الدعامة:

إن الكتابة التقليدية ترد دائما على دعامات تقليدية تتصف بطابعها الملموس كالأوراق أو ما شابهها، وما يميزها أنها تتسم بقدر كبير من الثبات، إذ يصعب تعديل الكتابة الواردة في المستند دون ترك أثر مادي واضح لهذا التعديل، أما المستند الإلكتروني فيرد على دعامة الكترونية تمتاز في الغالب الأعم بسهولة إجراء

تغييرات أو إدخال تعديلات على البيانات المدونة عليها، ومثال ذلك الأقراص المضغوطة القرص الوميض، القرص الصلب.

فضلا عن ذلك، فإن دعامات المستندات التقليدية تثبت البيانات المدونة عليها لفترة زمينة قد تصل عشرات السنين، بما يكفل قبولها كوسيلة إثبات أمام القضاء، أما الوسيط الإلكتروني فإنه معرض للتلف السريع عند أدنى اختلاف في قوة التيار الكهربائي، أو تعرضه للفيروسات مما يجعلها أقل قدرة في الاحتفاظ بالمعلومات لمدة طويلة[1].

ب–من حيث الكتابة:

تتمثل الكتابة العادية في كيان مادي مرئي، يسهل قراءتها بالعين المجردة، كما أنها ترتبط بكاتب المستند وتعكس شخصيته وبالتالي يمكن إحالتها إلى خبير لمعرفة مدى صحة نسبتها إليه، أما الكتابة الإلكترونية تتكون من نبضات الكترونية حيث لا قلم أو حبر، لا يمكن الإطلاع على محتواها إلا باستعمال وسيط الكتروني كجهاز الحاسوب، فهي كتابة قابلة للقراءة ولكنها غير ظاهرة للعين بشكل مباشر، كما أنها لا تختلف في حروفها بحسب من قام بكتابتها[2].

ت– من حيث التوقيع:

يختلف التوقيع الإلكتروني عن التوقيع الكتابي، فهذا الأخير يتحقق بالإمضاء الخطي أو بوضع بصمة الأصبع ، في حين أن التوقيع الإلكتروني كما سنرى قد يكون بوضع أرقام أو إشارات أو رموز أو حتى صورة ما، بالقدر الذي يميز صاحب التوقيع عن غيره و يعبر عن إرادته تعبيرا قانونيا[3].

ثانيا– تمييز المستند الإلكتروني عما يختلط به في البيئة الإلكترونية

إن المستند الإلكتروني ليس هو المكون الوحيد الذي يسبح في الفضاء الرقمي أو البيئة الإلكترونية، بل يوجد العديد من الكيانات التي تتخذ من هذا الفضاء بيئة لها، كمنتديات المناقشة والمجموعات الإخبارية وغيرهـــا، إلا أننا سنقصر الدراسة على منتديات المناقشة لإعتبارها الأقرب إلى الإختلاط بالمستند الإلكتروني.

تعرف منتديات المناقشة الإلكترونية بأنها إحدى البرمجيات الاجتماعية التي تسمح للمستخدمين بإرسال موضوعات للأعضاء كى يتناقشون فيها ويعلقون عليها، إما بطريقة خطية متعاقبةLinear ، أو بطريقة

---

[1]- **نور خالد عبد المحسن العبد الرزاق** ، حجية المحررات والتوقيع الإلكتروني في الإثبات عبر شبكة الأنترنت، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 2009، ص406–407. **عيسى غسان الربضي**، المرجع السابق، ص199.

[2]-**د.شيماء عبد الغني**، المرجع السابق، ص81. د. **محمد رايس**، المرجع السابق، ص82.

[3]– **د. محمد رايس**، المرجع السابق، ص83.

خطية متداخلةThreaded ، ويشتمل المنتدى الواحد أحياناً على أبواب مختلفة يتخصص كل منها في موضـــوع بعينه.[1]

ويزداد عدد منتديات المناقشة المشهورة ليفوق خمسين ألف منتدى تنهمر عليها يوميا مئات الألاف من الرسائل الإلكترونية، وتتضمن هذه المنتديات عشرات الموضوعات التي يجري تبادل الآراء و الأفكار حولها في المجالات المختلفة مما يثير **مسالة طبيعة الرسائل الإلكترونية التي تنساب بين مرتادي هذه المنتديات وهل يمكن إعتبارها مستند الكتروني؟**

لو تأملنا في الرسائل هذه لوجدناها تنطوي على عنصرين فقط من عناصر المستند الإلكتروني وهما: الكتابة الإلكترونية لأنها تتم بوسيلة الكترونية هي جهاز الحاسوب ، والدعامة التي ترد عليها هذه الكتابة وهي دعامة الكترونية، تنتقل عن طريق شبكة الأنترنت، إلا أنها تفتقد إلى عنصر مهم ألا وهو التوقيع الإلكتروني، وهو مادفع البعض –وبحق[2]–إلى إستبعادها من نطاق المستندات الإلكترونية.

المطلب الثاني

الحماية الجزائية للمستند الإلكتروني بشكـــل عام

لا شك أن تحقيق الحماية للمستند الإلكتروني من المخاطر التي تتهدده يؤدي إلى تحقيق الإستقرار والأمان القانوني للمعاملات المبرمة عن طريق الوسائل الإلكترنية، ونظرا لإنتشار الإعتداءات المرتكبة عن طريق الأنترنت، أخذت العديد من الهيئات الدولية والإقليمية في الإعتبار المشكلات التي تواجه سلامة المستندات الإلكترونية، فقد أخذت إتفاقية بودابست بعين الإعتبار لنوعين من الجرائم الماسة بسلامة المستند الإلكتروني، وذلك من خلال تجريم التزوير المتعمد باستخدام الكمبيوتر، ومنع الأعمال التدليسية في شان المعلومات. وكذلك فعلت الإتفاقية العربية لمكافحة جرائم تقنية المعلومات.

وحرصا من التشريعات الوطنية على حماية المستند الإلكتروني من المخاطر التي تهدده في إطار البيئة الإلكترونية التي يجري في فلكها، فقد حرصت على النص على تجريم الأفعال الماسة به. إلا أنها اختلفت خطتها في موضع النص على هذه الحماية[3]، وأيا كان السبيل المنتهج لتوفير هذه الحماية، فإن المتفق عليه هو ضرورة هذه الحماية.

---

[1]- **محمد جابر خلف الله**، التعليم بالمنتديات الإلكترونية، مقـــال منشـــور على الموقـــع التـــالي:
http://kenanaonline.com/users/azhar-gaper/posts/511728

[2]- **نور خالد عبد المحسن العبد الرزاق**، المرجع السابق، ص414.

[3]- **الإتجاه الأول:** يرى إصدار قوانين خاصة يعاقب فيها على الجرائم الإلكترونية بكافة صورها ومن ضمنها الجرائم الماسة بالمستند الإلكتروني، و تقترن هذه الخطة في تجريم هذه الأفعال بإصدار تشريعات تنص على صورة معينة من المستند الإلكتروني مثل السجلات والتوقيع الإلكتروني، ومن أمثلة هذه التشريعات تشريعات الولايات المتحدة الأمريكية.

الإتجاه الثاني: يرى تعديل التشريعات القائمة حتى تستوعب الصور المستحدثة من الجرائم الإلكترونية، ومن بينها صور الإعتداء على المستند الإلكتروني، مع إصدار قوانين خاصة ببعض الموضوعات مثل التوقيع الإلكتروني والتي تتضمن نصوصا تتصل بتجريم الإعتداء على المستند الإلكتروني، ومن امثلة هذه التشريعات القانون الفرنسي.

وعلى العموم، تتنوع صور المساس بالمستند الإلكتروني وتختلف فيما بينها، غير أنه يمكن تأصيلها في طائفتين: الأولـــى تتضمن الأفعال الماسة بسرية المستند الإلكتروني(الفرع الأول)، والثانية تشمل الأفعال الماسة بحجيتة(الفرع الثاني).

الفرع الأول

الحماية الجزائية لسرية المستند الإلكتروني

عمدت العديد من التشريعات إلى حماية سرية المستند الإلكتروني، فجرمت بذلك الدخول غير المصرح به إلى نظام المعالجة الآلية بأي وسيلة، حيث يمكن تصور دخول الجاني إلى النظام وينفد بدوره إلى المستند الإلكتروني سواء خلال تبادله أو أثنـــاء حفظه. والسبب وراء سهولة إختراق الأجهزة والأنظمة هو ضعف الوسائل الأمنية المستخدمة في حماية الشبكات الخاصة بالمؤسسات والهيئات وإعتمادها على وسائل حماية من إنتاج شركات أجنبية يعرف معظم خبراء الشبكات والمعلومات ادق جوانبها الأمنية.

وفي حالة إستطاع المخترق إختراق النظام الإلكتروني حكومي كان أو غيره، والخاص بحفظ المستندات الإلكترونية، فحينها يستطيع أن يعمل على الدخول إلى المستندات الأخرى والعبث بمحتوياتهـــا.

لذلك نجد المشرع الفرنسي قد إتخذ موقفا واضحا في حماية السرية، وكان ذلك بموجب المادة 323–1 عقوبات التي عاقبت على مجرد الدخول او البقاء بغش داخل نظام المعالجة الآلية بصفة عامة، هادفا بتدخله حماية سرية المعلومات، وهو ما يمكن تطبيقه على النظام الذي يحوي المستند الإلكتروني، كما نص من خلال المواد 226–16 إلى المادة 226–24 من قانون العقوبات، على تجريم المعالجة الإلكترونية للمعطيات ذات الطابع الشخصي في حالة اعتراض الشخص المعني على تلك المعالجة، كما حضر تجميع أو معالجة المعطيات الحساسة كتلك المتعلقة بالأراء السياسية أو الفلسفية أو الدينية أو غيرها، كما جرم إفشاء المعطيات على نحو يضر باعتبار صاحب الشأن أو حياته الخاصة. فضلا عن تجريم مختلف العمليات التي ترد على هذه المعطيات من جمعها وتخزينها بشكل غير مشروع.

وإلى جانب المشرع الفرنسي، نجد المشرع الجزائري الذي عاقب بموجب المادة 394 مكرر عقوبات على مجرد الدخول أو البقاء بطريق الغش في كل أو جزء من نظام المعالجة الآلية. فإذا نتج عن ذلك الدخول أو البقاء حذف أو تغيير لمعطيات المنظومة كانت العقوبة مضاعفة، أما إذا ترتب عن الأفعال السابقة تخريب نظام إشتغال المنظومة تكون العقوبة مضاعفة فيما يخص الحبس أما الغرامة فتصل في حدها الأقصى إلى غاية 150000 دج .

الإتجاه الثالث: هو الذي لم يفرد بعد تجريما خاصا للجرائم الإلكترونية، ومازال يكتفي بالنصوص التقليدية التي ينص عليها في التشريعات المختلفة ومن أهمها قانون العقوبات، غير أنه يقصر الحماية الجزائية على بعض صور المستند الإلكتروني ومن أمثلة هذا الإتجاه غالبية الدول العربية. أنظر: **د. توفيق شمس الدين**، الحماية الجنائية للمستند الإلكتروني، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، الجزء الثاني، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ماي 2003 ، ص 547.

ويجب لتوافر الظرف المشدد أن تتوافر علاقة السببية بين فعل الدخول أو البقاء غير المشروع وبين حذف أو تغيير المعطيات أو تخريب نظام تشغيل المنظومة. ولعل فعل الحذف أو التغيير يرد على المعلومات باعتبارها أموالا إلكترونية معنوية، و باعتبارها محررا إلكتــرونيا يشكل سندا ذو صبغة الكترونية.[1]

وكما سبق وأن أشرنا في الباب الأول من هده الدراسة، أن هذه الجريمة لا تتطلب صفة خاصة في فاعلها، كما يستوي أن يتم الدخول أو البقاء في كل أو جزء من النظام كما لو تمكن الجاني من كسر شفرة بعض قواعد المعطيات أو مواقع المعلومات دون أن يتمكن من إختــراق كل الموقع.

وهده الجريمة شكلية، لا تفترض تحقق نتيجة من أي نوع بل تقوم بمجرد قيام الجاني بالإتصال الكترونيا بالنظام المخزن به المستند الإلكتروني، وهو ما يتطلبه الحق في السرية الذي يتحقق المساس به بمجرد قيام الجاني بالإتصال غير المشروع. كما أنها جريمة عمدية، يتخد الركن المعنوي فيها صورة القصد الجنائي بعنصريه العلم و الإرادة.

ويحمي المشرع الجزائري كدلك سرية المستند من خلال تجريم التعامل في المعلومات المتحصلة من الأفعال الماسة بالنظام من خلال المادة 394 مكرر2، سواء بحيازته أو إفشاءه أو نشره وإستعماله.

وإلى جانب المشرع الفرنسي والجزائري، نجد المشرع المصري يعاقب بموجب المادة 23 فقرة ه من قانون التوقيع الإلكتروني على: **كل من توصل بأي وسيلة إلى الحصول بغير حق على... وسيط او محرر الكتروني.أو اختراق هذا الوسيط او اعتراضه او عطله عن اداء وظيفته.**

ومناط التجريم في الصورة الأولى هو أن يكون الحصول على المحرر بغير حق، ولا يشترط في ذلك أن تكون الوسيلة مشروعة أم لا.

ولم يشترط المشرع في الصورة الثانية وسيلة معينة لحدوث الإختراق أو الاعتراض، كما أنه لم يشترط أن يترتب عليها نتيجة معينة، وهو مايعني أن هذه الجريمة شكليــة.

وما يلاحظ على نص المادة السابقة، أن المشرع أشار في البداية إلى تجريم الحصول بغير حق على وسيط أو محرر الكتروني، ثم قصر أفعال الإختراق والتعييب على الوسيط الإلكتروني، ما يعني أنها تتعلق بما يرد منها على الوسيط فقط، والوسيط حسب الفقرة د من المادة 1 على انه أداة أو أدوات أو أنظمة إنشاء التوقيع الإلكتروني.

ومع ذلك يرى البعض –وبحق[2]–أن مدلول الوسيط يمكن أن يتسع ليشمل الوسيط الإلكتروني بمعناه الواسع الذي يستخدم لحفظ وتداول المستندات الإلكترونية، ومن ثم فإن الإعتداءات المنصبة على الوسيط تكون الحماية مقررة في هذه الحالة للوسيط بصفة عامة، غير أنها تمتد بطريق التبعية إلى المستند الإلكتروني الذي يتضــمنه.

---

[1]– **د. محمد رايس**، المرجع السابق، ص97.

[2]-**د. تامر محمد سليمان الدمياطي**، المرجع السابق، ص648.

والملاحظ أن المشـــرع إستخدم في الصورة الأولى مصطلح "**توصل**"، وهو مصطلح يفيد السعي إلى الحصول، مما يعني أن هذه الجريمة عمدية، يتخذ الركن المعنوي فيها صورة القصد الجنائي. كما يتحقق في الصورة الثانية بعلم الجاني بأنـــه يخترق الوسيط الإلكتروني أو يعترضـــه وتتجه إرادته الى ذلك.

الفرع الثـــاني

الحماية الجزائية لحجيـــة المستند الإلكتروني

تتعدد صور المساس بمحتوى المستند الإلكتروني وتختلف فيما بينها، فقد يرتبط السلوك المادي لجرائم الإعتداء على المستند الإلكتروني بإتلاف نظام معالجة المعلومات أوالتلاعبه، وهو سلوك من شأنه المساس بحجية ما تضمنه من وقائع التي أعد لإثباتها، كما أنه من المتصور أن يكون محل الجريمة هو المساس بحجية المستند الإلكتروني في الإثبات في صورة أخرى كما هو الحال في جريمة التزوير.

وحيث أن تزوير المستد الإلكتروني من أخطر صور الغش المعلوماتي بصفة عامة، بإعتباره يمس بوثيقة ذات قيمة قانونية، معبرة في نظر الناس عن الحقيقة، والا فقدو ثقتهم فيها واحجموا عن الإعتماد عليها في معاملاتهم، وهو ما يؤدي الى إضطراب التعاملات الإلكترونية ، فإننا سنـــفرد له مطلبا مستقلا.

لقد إختلفت التشريعات فيما بينها حول طريقة تجريم إتلاف المستند الإلكتروني، ففي حين حرصت بعض التشريعات على النص على ذلك بصورة مباشرة، كما هو حال المشرع المصري في قانون التوقيع الإلكتروني، لم تفرد أغلبية التشريعات نصوصا خاصة تجرم فيها هذا السلوك بشكل مباشر، كما هو حال التشريع الفرنسي والجزائري، بل يمكن تمديد الحماية له بصورة تبعية من خلال بسط الحماية على نظام التشغيل ومعطياته، فالإتلاف المنصب على نظام التشغيل الذي يحتوي المستند الإلكتروني يؤدي بالتبعية إلى إتـــلاف هذا المستند، كما أن الإتلاف المنصب على المعطيات التي يحتويها المستند تكون الحماية مقررة في هده الحالة للمعلومات الإلكترونية بصفة عامة، غير أنها تمتد بطريق التبعية إلى المستند الإلكتروني بمعناه الدقيق[1]، وهذا ما سنراه من خلال النقاط التالية:

أولا– إتلاف المســـتند الإلكـــتروني ذاتـــه

ذهب المشرع المصري إلى تجريم أفعال الإتلاف والتعييب التي ترد على المستند الإلكتروني بموجب المادة 23 –ب من قانون التوقيع الإلكتروني حيث نصت: "...**أتلف أو عيب.... أو وسيطا أو محررا الكترونيا...**" وقد كان هذا النص محل إنتقاد من جانب الفقه[2]، الذي ذهب –بحق– إلى أن تعبير التعييب

---

[1]– **د. أشرف توفيق شمس الدين**، الحماية الجنائية للمستند الإلكتروني، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون،المرجع السابق، ص543.

[2]- **د. أشرف توفيق شمس الدين**، الحماية الجنائية للمستند الإلكتروني –دراسة مقارنة–، المرجع السابق، ص117–118. أنظر في تأييد ذلك: د. **تامر محمد سليمان الدمياطي**، المرجع السابق، ص642.

يدخل في الإتلاف، ذلك أن الإتلاف قد يكون كليا أوجزئيا، ومن ثم فإن لحق التعييب المستند صار إتلافا جزئيا، ولذا كان من الأولى بالمشرع أن يقتصر على النص على فعل الإتلاف.
وإتلاف المستند الإلكتروني على النحو السابق، يتحقق بأية وسيلة تؤدي إلى عدم اللإنتفاع به، ويمكن تصور ذلك عن طريق فيروس أو طمس بعض الأسطر المكتوبة عليه بطريقـــة إلكتـــرونية.

ونرى أن المشرع المصري قد جانبه الصواب في النص على محل جريمة الإتلاف حين نص على الوسيط الإلكتروني، إذ أن من شأن إتلاف هذا الأخير أن يلحق الوصف المستند الإلكتروني.

هذا وقد نص المشرع المصري من جانبه على استعمال المستند المزور والمعيب مع العلم بذلك، إلا أنه لم يشر إلى إستعمال التالف منه، إدراكا منه إلى أن المستند التالف لا أثر له من الناحية القانونية، ويمكن إعتباره والعدم سواء، ويمكن تشبيه المستند الإلكتروني التالف بحالة التزوير المفضوح غير المتقن الذي لا عقاب عليه لأنه لا يمكن ان ينخدع به أي شخص[1].اما فعل التعييب فهو بحسب طبيعته لا يفقد المستند وظيفته بصفة كلية، لكنه يؤدي تلك الوظيفة بصورة غير كاملـــة[2].

ثانيا- إتلاف نظام المعالجة الآلية للمعطيات

إستقرت غالبية التشريعات المقارنة على تجريم هذا السلوك بما فيها المشرع الفرنسي في نص المادة 323-2 عقوبات كما يلي:"... *كل من قام* ***بتعطيل*** *أو* ***إفساد*** *نشاط نظام المعالجة الآلية يعاقب...*".. اما المشرع الجزائري فقد استغنى عن وضع نص خاص له، واكتفى بنتيجة إفساد النظام كظرف مشدد لجريمة الدخول أو البقاء غير المشروع.

ينصرف فعل تعطيل أو إفساد نشاط النظام إلى كل عمل من شأنه إرباك عمل نظام المعالجة الآلية، ويستوي أن يكون من شأن نشاط الجاني تعطيل أو إفساد نظام التشغيل أو الإرسال أو أن يؤدي إلى توقف النظام عن العمل بصورة دائمة أو مؤقتة[3].

إن إتلاف النظام في هذه الصورة لا يمس المعلومات التي يحويها بل ينال النظام نفسه، وعلى ذلك فالحماية التي توفرها النصوص المقررة له على نحو أصيل، تمتد إلى المستند على **نحو تبعـــي**.
وحيث أن إتلاف نظام المعالجة الآية كان محل دراستنا في الفصل الأول من هذا الباب فنحيل إليه منعا للتكـــرار.

ثالثا-إتـــلاف المعلومات التي يحويها نظام المعالجة الآلية

---

[1]- أنظر: د. **عبد الفتاح بيومي حجازي**، التوقيع الإلكتروني في النظم القانونية المقارنة، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2005، ص545.

[2]-**د. تامر محمد سليمان الدمياطي**، المرجع السابق، ص644.

[3]-**د. مدحت رمضان**، الحماية الجنائية للتجارة الإلكترونية، المرجع السابق، ص45.

لا تحمي التشريعات في هذه الصورة النظام نفسه، بل المعلومات التي يتضمنها من أي نشاط اجرامي، حيث نص المشرع الفرنسي في المادة 323-3 على عقاب كل من يدخل معلومات بطريق الغش في نظام المعالجة الآلية أو يمحو أو يعدل المعلومات التي يحتوي عليها بطريق الغش، كما عاقب على ذات الأفعال المشرع الجزائري بموجب المادة 394 مكرر 1 من قانون العقوبات.

وواضح من خلال النصوص السابقة، أن النشاط الإجرامي محصور في فعل: الإدخال أو الإزالة أو التعديل، ولا يشترط إجتماعها جميعا بل يكفي أن ياتي الفاعل فعل واحد، ونستدل على ذلك بلفظ " **أو**" الواردة في النصوص السابقة، هذا من جهة.

ومن جهة أخرى، فإن محل الجريمة هو المعطيات المعالجة إلكترونيا، دون أن يفرق المشرع بين المعلومات الخاصة بتشغيل النظام التي تتالف من البرامج، وبين المعطيات التي تمت معالجتها إلكترونيا و التي يحتويها النظام، ومن أمثلتها المعطيات الواردة في المستندات الإلكترونية[1].

المطلب الثالث

الحماية الجزائية للمستنـــد الإلكتروني من التـــزوير

فرضت التشريعات المقارنة نصوص عقابية للحماية من التزوير الذي يقع على المحررات بانواعها المختلفة، وذلك حماية للثقة التي يعطيها الناس لها في اكتساب الحقوق أو تحمل الإلتزامات، فهي وسيلة السلطة العامة لمباشرة اختصاصاتها، ووسيلة الأفراد لإثبات علاقاتهم، وإثبات حقوقهـــم المتنازع عليها[2].

إلا أنه نتيجة الثورة المعلوماتية وظهور المستندات الإلكترونية العرفية والرسمية، ظهر التزوير المعلوماتي بوصفه أحد أنماط الغش المعلوماتي تزايدا سريعا في الآونة الأخيرة، ويعتبر من أخطر الجرائم التي تؤثر على التعاملات الإلكترونية، لأن الوسائل الإلكترونية أصبحت تقوم بكافة العمليات في مجال التعاملات الإلكترونية تجارية كانت أو حكومية أو غيرها، مثل عمليات الدفع وطلبات البضائع وتحويل الأموال من بنك إلى بنك وإرسال الوثائق والمحررات القضائية، ومما يزيد من خطورة التزوير هو صعوبة إكتشاف وإثبات التزوير الذي يقع في هذا المجـــال.

ويشير التزوير في النطاق المعلوماتي إلى تغيير الحقيقة في معلومات لها قيمة قانونية مخزنة بالنظام المعلوماتي أو على الدعامة المعلوماتية إضرارا بالغير[3].

لقد أخذت بعض الدول على عاتقها مواجهة التزوير المعلوماتي، مساهما كل من الفقه والقضاء فيها بدور كبير. الا انها اختلفت في طرق المواجهة ما بين ايجاد نص عام يتم من خلاله مواجهة تغيير الحقيقة

---

[1]– **د. رايس محمد**، المرجع السابق، ص97.

[2]–**د. محمود نجيب حسني**، شرح قانون العقوبات القسم الخاص، الجرائم المضرة بالمصلحة العامة، دار النهضة العربية، 1988، ص244.

[3]– أنظر في تعريف التزوير المعلوماتي لدى: **د.على عبد القادر القهوجي**، الحماية الجنائية للبيانات المعالجة الكترونيا، المرجع السابق، ص63. **د. احمد حسام طه تمام**، المرجع السابق، ص407.

في نطاق المعلوماتية، أو افراد تشريع خاص، وبين هاته وتلك لازالت بعض الدول تدرس الأمر سواء من خلال النصوص القائمة أو محاولة وضع نصوص خاصة تكفل تلك الحماية، وهو ما سنحاول دراسته فيمايلي، لكن قبل الخوض في ذلك وجدنا أنه من المستحسن والمناسب أن نستهل هذا المطلب بدراسة القواعد التقليدية ومدى إنطباقها على التزوير المعلوماتي، لأن من شأن ذلك فهم سببية فشل النظام السابق في توفير الحماية لهذا المستند.

الفـــرع الأول

القواعد التقليدية والتزويرالمـــعلوماتي

بظهور المستند الإلكتروني تغيرت بعض المفاهيم القانونية الخاصة بجرائم التزوير عند تطبيقها على التزوير المعلوماتي، الأمر الذي أثار جـــدل في الفقه الجنائي بشأن هذا التطبيق، وإنقسم الى اتجاهين: أحدهما يرى إمكانية هذا التطبيق والآخر يرفضه ولكل منهما أسانيده ومبرراته التي يستند إليها في دعم وجهة نظره حيال تلك المســـالة.

ولتحليل ذلك، لا بد لنا أن نشير إلى أهم الطرق التي تستخدم في عملية التزوير التي تقع على المستند الإلكتروني، وبيان الأحكام العامة لجريمة التزوير في المحررات الواردة في القوانين الجزائية، لننطلق من خلالها لتحليل مدى توافق إنطباق هذه الجريمة على ما يحدث في المستند الإلكتروني.

أولا- طرق وأساليب تزوير المســـتند الإلكتروني[1]

يرجع خبراء الكشف عن التزوير طرق وأساليب تزوير المستند الإلكتروني رغم تنوعها إلى طائفتين:

الأولى: طرق التزوير التقليدية: والتي تتم وفقا للطرق المحددة بالنص القانوني **بالطرق المادية والمعنوية:**

ومن قبيل الطرق الماديةوضع إمضاءات أو أختام مزورة، ويتم ذلك من خلال وضع التوقيع أو الختم الذي تم سحبه الكترونيا من خلال وحدة الإدخال scanner بواسطة وحدة معالجة المدخلات للنظام، ووضعها على المستند الذي يهدف الجاني إلى تغيير الحقيقة في محتواه ليخرج في صورة مخرجات ورقية. كما قد يتم عن طريق **التغيير** في المحررات والأختام والتوقيعات او زيادة كلمات، ويتم ذلك متى تمكن الجاني من الدخول الى النظام وتغيير المعلومات المخزنة فيه المكونة للمستند، كما قد يتم من خلال التقليد من خلال الإمكانيات

[1]-د. **عبد الفتاح بيومي حجازي**، الدليل الجنائي والتزوير في جرائم الكمبيوتر والأنترنت، المرجع السابق، ص181 وما بعدها. **د. أيمن عبد الله فكري**، المرجع السابق، ص377 ومابعدها.

الهائلة التي يملكها النظام المعلوماتي بحيث يصعب التفرقة بين الأصل والتقليد، كما يتم بالإصطناع من خلال استخدام جهاز scanner.

فضلا عن الطرق المادية السابق تناولها، يمكن أن يقع التزوير **بالطرق المعنوية** وإن كان يرى البعض[1] أنه لا يمكن أن تقع، إلا أننا نرى أن الواقع العملي يشهد بإمكانية تحقق التزوير بالطرق المعنوية، **كتغيير إقرارت أولى الشأن** من قبل المسؤول عن النظام المعلوماتي الذي يتعامل مع الجمهور على خلاف الحقيقة بما يريد إثباته بالمخالفة لإقرار ذوي الشان. أو قيام الموظف القائم على عمليات التسويات المالية بالنسبة لعمليات دفع الفواتير الخاصة بالمياه أو الكهرباء أو الإتصالات بإثبات على غير حقيقة ما تم من إجراء من قبل العميل بالدفع أو الإنقاص أو الزيادة في المطلوب منه سدادها للجهة التي يعمل فيها الموظف، أو عن طريق قيام القائم على التحقيق الإلكتروني **بنسبة واقعة غير صحيحة** إلى الجاني فيضيف أو ينقص من أقواله بالتحقيق ويثبت ذلك من خلال النظام المعلوماتي.

الثانية: طرق التزوير المستحدثة: لقد ارتبط مفهوم تزوير المستند الإلكتروني في صورته المستحدثة بالإعتماد على التلاعـــب في المعلومات داخل النظام المعلوماتي بصرف النظر عن وجودها على دعامة مستقلة[2]، عن طريق المحو أو الإضافة أو الإعاقة، سواء من خلال عمليات الإدخال المعلوماتي سواء كان من الأشخاص المسموح لهم التعامل بالنظام أولا، أو في مرحلة المعالجة للمعلومات أو في مرحلة الإخراج المعلوماتي كنتيجة لما وقع من تلاعب في المرحلتين السابقتين، سواء كان الإخراج على ورقة أو في شرائط أو أسطوانات معلوماتية. ويتحقق ذلك متى كان من الممكن إستخدام المستند أو الوسيط الذي تمت عليه عملية التزوير لممارسة حق أو تصرفان يصلح لإثبات حق او تصرف له اثار قانونية.

ومن الصور الشائعة للتزوير المعلوماتي هو انتحال الشخصية في التعامل عبر النظم المعلوماتية من خلال الإستيلاء على اداة التعريف الشخصي المعبرة عن هوية المستخدم الشرعي والتي يمثلها غالبا التوقيع الإلكتروني خاصة من خلال الدفع والتسويات المالية من خلال الأنترنت، ومن الصور الشائعة كدلك انتحال المواقع الإلكترونية عبر شبكة المعلومات[3] من خلال الإستيلاء على الموقع الإلكتروني الذي يريده وتحويل الإتصالات المختلفة والمحررات والمعلومات من الموقع الأصلي، على اساس ان موقع الجاني الإلكتروني هو الموقع الأصلي.

---

[1]-**د. علي عبد القادر القهوجي**، الحماية الجنائية للبيانات المعالجة إلكترونيا، المرجع السابق، ص63.

[2]- **د. نائلة عادل فريد قورة**، المرجع السابق، ص436.

[3]-**د. أيمن عبد الله فكري**، المرجع السابق، ص378.

ثانيا– جريـــمة التـــزوير وفق القـــواعد التقلـــيدية

التزوير بصفة عامة هو تغيير الحقيقة في محرر بإحدى الطرق التي نص عليها القانون تغييرا من شأنه إحداث ضرر ومقترنا بنية إستعمال المحرر المزور فيما أعد له[1].

وقد عالجته أغلب التشريعات في قانون العقوبات في باب الجرائم المرتكبة ضد الشيء العمومي وليس في باب الجرائم المرتكبة ضد الأفراد، للدلالة على خطورتها بالنسبة لكيان الدولة كله، كما هو حال قانون العقوبات الجزائري بموجب المادة 214 ومابعدها، والمصري بموجب المادة 211 وما بعدها، والفرنسي بموجب المادة 441–1 وما بعدها، وأعطتها تكييفات مختلفة تتراوح بين الجنح والجنايـــات.

هذا ولم تحدد أغلب التشريعات مدلول جريمة التزوير، ذلك هو وضع القوانين العربية والقانون الفرنسي القديم[2]، في حين قانون العقوبات الفرنسي الحالي نص في المادة 441–1[3] منه "***يشكل تزويرا كل تغيير بغش للحقيقة، من شأنه إحداث ضرر، وينجز بأية وسيلة كانت، وينصب على محرر أو على أية دعامة للتعبير عن الأفكار يكون موضوعها او يكون من اثارها اقامة الدليل على حق او على واقعة دات نتائج قانونية***"[4].

والعلة في تجريم التزوير في المحررات هو تغيير الحقيقة في المحررات على نحو يزعزع الثقة في المحررات الرسمية أو يؤدي للمساس بحقوق الأفراد في المحررات العرفية[5].

تشترط النصوص العقابية[6] المنظمة لجرائم التزوير في المحررات على إختلاف أطيافها مثلها مثل أي جريمة أخرى توافر أركانـــها القانونية، والأركان القانونية لجريمة التزوير ركنان أولهما الركن المادي وثانيهما الركن المعنوي.

قوام **الركن المادي** في جريمة التزوير هو تغيير الحقيقة في محرر بإحدى الطرق التي حددها القانون تغييرا من شأنه أن يسبب ضررا للغير.

ويعني **تغيير الحقيقة** إستبدالها بما يخالفها[1]، فإذا لم يكن هناك تغيير للحقيقة فلا يوجد ثمة تزوير[2]، سواء كان هذا التغيير كليا أو جزئيا، ويراد بالحقيقة في هذا الإطار الحقيقة القانونية النسبية وليس الواقعية

---

[1]–**د. محمود نجيب حسني**، شرح قانون العقوبات، القسم الخاص المرجع السابق، ص 215، انظر في تعريف التزوير: **د. محمد عقاد**، جريمة التزوير في في المحررات للحاسب الآلي، دراسة مقارنة، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون، القاهرة، 1993، ص394. د. **رمسيس بهنام**، قانون العقوبات جرائم القسم الخاص، منشاة المعارف بالإسكندرية، 2005، 437.

[2]– المادة 145 وما بعدها من قانون العقوبات الفرنسي القديـــم.

[3]-Article 441-1 du CPf Modifié par Ordonnance n°2000-916 du 19 septembre 2000 - art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002 dispose que "Constitue un faux toute altération frauduleuse de la vérité, de nature à causer un préjudice et accomplie par quelque moyen que ce soit, dans un écrit ou tout autre support d'expression de la pensée qui a pour objet ou qui peut avoir pour effet d'établir la preuve d'un droit ou d'un fait ayant des conséquences juridiques.
Le faux et l'usage de faux sont punis de trois ans d'emprisonnement et de 45000 euros d'amende.

[4]- وهو تعريف مأخذومن اجتهاد محكمة النقض الفرنسية:
Cour de cassation-chambre criminelle-8 juin 1994-**N° de pourvoi: 93-83360** , publication : bulletin criminal 1994 n228 ,Attendu que constitue un faux pénalement punissable l'altération frauduleuse de la vérité, préjudiciable à autrui, accomplie dans un document faisant titre ; p554

[5]-**Louis Garron**, "L'incrimination du faux et du Mensonge en droit Pénal" 20 juin 2011, (irc – gov – mu), p .1

[6]- انظر المواد: 214 ،115 ، 216 من قانون العقوبات الجزائري، 262 من قانون العقوبات الأردني، المادة 211 وما بعدها من قانون العقوبات المصري.

المطلقة[3]. أي أن جريمة التزوير تقع إذا ثبت في المحرر ما يخالف إرادة صاحب الشأن، الذي يعبر المحرر عن إرادته، ولو كان تعبيرا صـــادقا عن الـــواقع[4].

ويرتبط تغيير الحقيقة في جريمة التزوير بالمحرر[5]، وعليه لا يعد تغيير الحقيقة بالقول، أو الفعل دون الكتابة تزويرا وإن كانت هذه الأفعال من الممكن أن تكون ضمن جرائم أخرى كشهادة الزور.

وقد اقترنت كلمة محرر بكلمة الكتابة وبالذات بالكتابة على الورق، وقيمة المحرر تكمن في دلالة الكتابة أو الرموز والعلامات التي يتضمنها ومعرفة مصدره، أي نسبته إلى شخص أو جهة ما، فضلا عن تعبيرها عن فكرة ما وإمتيازها بشيء من الثبـــات لمدة غير محددة.

وقوانين العقوبات في اغلب الدول العربية على غرار قانون العقوبات الفرنسي القديم، قد حددت جصريا طرق التزوير، كما هو شأن قانون العقوبات في الجزائر ومصر، وقد درج الفقه على تقسيمها إلى قسمين مادي ومعنوي.

فاما المادي فتدركه الحواس وتثبته الخبرة، ومن طرقه المحو أو الشطب أو إضافة كلمات أو أختام او تواقيع مزورة[6]، وضع أسماء وصور اشخاص أخرين مزورة، الإ صطناع والتقـــليد[7].

أما طـــرق التزوير المعنوي فيتحقق بتغيير مضمون المحرر أوظروفه أوملاباسته دون المساس بمادته او شكله، فلا تتحلف عنه آثار ظاهرة يدركها الحس كتغيير اقرارات أولى الشان وجعل واقعة مزورة في صورة واقعة صحيحة.

إن تحديد طرق التزوير من طرف المشرع قد لاقت معارضة البعض من الفقه، ذلك ان القاعدة العامة في باب التجريم والعقاب أن المشرع إذا جرم فعلا ما فإنه لا يهتم بتحديد طرق ارتكابه، والأخد بعكس ذلك يجعل من الفعل مباحا في كثير من الحالات، وهدا ما يرفضه المنطق السليم.

ونحن نتفق فيما دهب اليه هذا الإتجاه، ولعل ما يدعم راينا هدا هو مسلك المشرع الفرنسي في هذه المسألة في قانون العقوبات الجديد، إد نصت المادة 441-1 "...***تزويرا كل تغيير إحتيالي للحقيقة، من شأنه إحداث ضرر، وينجز بأية وسيلة كانت***..."فكما هو واضح فإن المشرع جاء بتعبير عام يشمل كل طرق التزوير.

والتزوير بالمعنى السابق، يجب أن يتسبب **بضرر للغير**، وهو ما أشـــار اليه قانون العقوبات الفرنسي صراحة في نص المادة 441-1 "...، ***من شأنه إحداث ضرر***..."[1].،ولا يشترط وقوع ضرر بالفعل بل يكفي إحتمال وقوعه، ويستوي أن يكون الضرر ماديا أو معنويا فرديا أو اجتماعيا.

---

[1]– د. **فتوح الشادلي، عفيفي كامل عفيفي**، المرجع السابق، ص236.

[2]– قرار المحكمة العليا الصادربتاريخ 07-10-2010، غرفة الجنح والمخالفات– فصلا في الطعن رقم 618867 المرفوع في 25-10-2008، مجلس قضاء بلعباس ، مشار اليه لدى: د. **نجمي جمال**، جرائم التزوير في قانون العقوبات الجزائري ، دار هومة، الجزائر، 2013، ص 445.

[3]–د. **محمود نجيب حسني**، شرح قانون العقوبات، القسم الخاص، المرجع السابق، ص219.

[4]–د. **فوزية عبد الستار**، شرح قانون العقوبات، القسم الخاص، دار النهضة العربية، القاهرة، 1990، ص 247 .

[5]-La conception du document est large, comme l'a précisé la Cour de cassation (v. p. ex. Crim. 16 nov. 1967 : Bull. crim. N° 296 ; 19 déc. 1974 : Bull. crim. N°378 ; 13 juill. 1889 : D. 1903. I. 164; 18 mai 1960: Bull. Crim. N°272).

[6]- Cassation criminelle 21/05/1963 Bulletin criminel n° 180)

[7]- voir: **Michel Véron**, droit pénal spécial ,2 éme édition, masson, paris, 1982 ;p68.

وإذا كان هذا هو حال قانون العقوبات الفرنسي، فإن الأمر يختلف في قوانين أخرى، كما هو شأن قانون العقوبات الجزائري حيث لم نجد ما يشير إلى أهمية الضرر في البنيان القانوني لجريمة التزوير، ومع ذلك فقد استقر الفقه[2] والإجتهاد القضائي[3] على اشتراط هذا العنصر لقيام الجريمة، بحيث إستوجب أن يكون هناك ضرر حاصل أو محتمل الحصول. خاصة المحررات العرفية والتجارية، ذلك أن المحررات العمومية و الرسمية فإن الضرر مفترض وقوعه بمجرد تزويرها لما يترتب على ذلك من مساس بالمصداقية والثقة العامة التي تتميز بها هده المحررات[4].

وجريمة التزوير جريمة عمدية، يتخذ **الركن المعنوي** فيها صورة القصد الجنائي، الذي يتحقق يتوافر عنصرين هما العلم و الإرادة، إذ يجب ان يعلم الجاني أن فعله ينطوي على تغيير الحقيقة في محرر بإحدى الطرق التي نص عليها القانون حصرا، وأن يعلم أن من شأن هذا التغيير أن يسبب ضررا فعليا أو محتملا، وأن تتجه إرادته إلى تحقيقه[5]. إلى جانب ذلك يشترط المشرع قصدا خاصا يتجسد في نية الجاني استعمال المحرر المزور في الحال أو في المآل فيما أعد له.

من خلال إستعراضنا لأساليب التي يتم بها تزوير المستند الإلكتروني، ومن خلال تبيان أركان جريمة تزوير في المحرر التقليدي بصفة عامة، يتبين لنا أن العنصر الهام الذي يثير إشكالا قانونيا في تطبيقه على فعل تزوير المعلومات دات القيمة القانونية، هو عنصر **المستند، *فإلى أي مدى يمكن إعتبار المعلومات المخزنة في النظام المعلوماتي او على الدعامة المعلوماتية التي يقع عيها فعل تغييرالحقيقة محررا؟***

ثالثا– نطاق تطبيق أحكام جريمة التزوير على المستند الإلكتروني

مما لا شك فيه أن النصوص الخاصة بالتزوير اهمية كبيرة في حماية ما تضمنه هده المحررات من وقائع، ومناط الحماية تلك الثقة المنبعة منها، إلا أن تطبيقها على تزوير المستند الإلكتروني قد أثار جدل واسع في مجال الفقه، وانقسم على إثره الى اتجـــاهين أحدهما يؤيد والثـــاني يعارض:

أ– الإتجاه المؤيد لتطبيق نصوص التزوير التقليدية على التزوير الإلكتروني

---

[1]-Crim. 15 juin 1962 : D. 1962. 505 cité par Pierre Lebriquir, Présentation synthétique de l'infraction de faux , article disponible http://www.legavox.fr/blog/plebriquir/presentation-synthetique-infraction-faux-code 6295.htm#.V0yXqdSLQSk

[2]-أنظر: **د.رمسيس بهنام**، المرجع السابق، ص459 ومابعدها، **د.محمود نجيب حسني**، شرح قانون العقوبات القسم الخاص، المرجع السابق، ص250. انظر على خلاف ذلك: **د. علي عبد القادر القهوجي**، شرح قانون العقوبات القسم الخاص، منشورات الحلبي الحقوقية، بيروت، 2002، ص149.

[3]–قرار صادر يوم 8–12–1987، القسم الأول للغرفة الجنائية الثانية في الطعن رقم 47575، المجلة القضائية للمحكمة العليا، العدد 4 لسنة 1990 ص243، مشار اليه لدى **جيلالي بغدادي**، الإجتهاد القضائي في المواد الجزائية، الطبعة الأولى، الديوان الوطني للأشغال التربوية بالجزائر، 2002، ص140. نقض بتاريخ 15–2–1965 الطعن رقم 1816 لسنة 34 ق، مشار اليه لدى**نجيمي جمال**، المرجع السابق، ص518.

[4]–**د.أشرف شمس الدين**، الحماية الجنائية للمستند الإلكتروني، مؤتمر الأعمال المصرفية الإلكترونية، المرجع السابق، ص 501.

[5]-Cassation criminelle 24/2/1972 – Bulletin Criminel n° 78 11/12/1974 Bulletin criminel n° 366.

يرى هذا الإتجاه أنه لا يوجد سبب يمنع قبول تطبيق نصوص التزوير التقليدية على تزوير المستند الإلكتروني الذي يحدث عند التلاعب في المعلومات المتواجدة بالنظام الرقمي أو على دعامة معلوماتية، وحججهم في ذلك مايلي[1]:

-عدم تحديد المشرع لمفهوم التزوير، الأمر الذي يزيل عقبة من أمام عدم تطبيقه على التزوير المعلوماتي.

- إن امكانية او عدم إمكانية الإطلاع مباشرة على المعلومات المخزنة بالمستند الإلكتروني وبالتالي خروجها من نطاق مفهوم المحرر لعدم إمكانية الإدراك المباشر لمحتواه هي عملية نسبية، حيث يمكن رؤيتها باستخدام أجهزة خاصة، ويمكن تطبيق روح النص عليها وليس منطوقه.

- نظرا لتمتع المستند الإلكتروني بقيمة ثبوتية بمقتضى قوانين الإثبات من جهة، ولكون العلاقة قائمة بين جريمة التزوير وتمتع هذا المستند بهذه القيمة من جهة اخرى، أمكن مد النص الجنائي التقليدي ليشمل تزوير المستند الإلكتروني.

-لا يوجد تلازم بين فكرة الكتابة والورق، بل يمكن أن تكون الكتابة واردة على دعامة ورقية أو غير ورقية كالخشب ، وكدلك على دعامات معلوماتية، فالمشرع كل ما اشترطه هو تحقيق وظائف معــينة.

وقد انتهى القضاء الفرنسي[2]– قبل تدخل المشرع بنص صريح– إلى توافر وصف التزوير في هذا الفرض، باضفائه على الكتابة الإلكترونية وصف المحرر في مفهوم جريمة التزوير.

ب– الإتجاه الرافض لتطبيق نصوص التزوير التقليدية على التزوير الإلكتروني

على عكس الإتجاه السابق، يعبر هذا الإتجاه عن رفضه لتطبيق نصوص التزوير التقليدية على التزوير الإلكتروني، بالقول أن تزوير المعلومات بطريقة الكترونية لا يمكن ان ينطوي تحت النصوص التقليدية وذلك لوجود تعارض بين المفهوم المستقر للتزوير ومايحدث في البيئة الرقمية من تلاعب في المعلومات الموجودة بالنظام الرقمي أو على الدعامة، ويمكن ابراز أهــم الحجج التي إستندوا عليها فيمايــلي:

- أن المشرع لم يعرف الكثيرمن المفاهيم، بل ترك هذه المهمة للفقه والقضاء، والفقه قد عرف المحرر بأنه كل مسطور يتضمن علامات ينتقل بها الفكر لدى النظر اليها من شخص إلى آخر، والبصر واللمس هي الحاسة التي تكشف الفكرة التي يعبر عنها المحرر[3].

- مدلول المحرر الذي تعاقب عليها التشريعات على المساس به يتصل على وجه اللزوم "بالسندات والأوراق"[4].

---

[1]- أنظرفي عرض هذه الحجج: **عبد الناصر محمد محمود فرغلي**، الإثبات العلمي لجرائم تزييف وتزوير المحررات التقليدية والإلكترونية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 2010، ص56، **براهمي حنان**، المرجع السابق، ص176، د. **ايمن عبد الله فكري**، المرجع السابق، ص370 وما بعدها، **محمد سليم العوا**، التحكيم في المعاملات المصرفية والإلكترونية، دراسة مقدمة إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، الجزءالخامس، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ماي 2003، ص2384–2385.

[2]-TGI paris,12 oct,1998,lamy,avr,1989,p24

مشار إليه لدى:**د. شيماء عبد الغني**، المرجع السابق، ص82.

[3]–**د. ايمن عبد الله فكري**، هامش رقم 2، المرجع السابق، ، ص370.

[4]–**د. ايمن عبد الحفيظ**، استراتيجية مكافحة جرائم استخدام الحاسب الآلي، المرجع السابق، ص93 وما بعدها.

– كما يرى البعض[1] أن المعلومات المبرمجة لا تعتبر محرر من حيث أنه لا يمكن مشاهدة المعلومات المخزنة على وسائط التخزين الخاصة بها عن طريق النظر، وبالتالي فهي ليست مقروءة ولا يمكن للمعنى الذي تحمله أن ينتقل عن طريق العين، أما عن إمكانية الإطلاع عليها بإتباع طرق وإجراءات خاصة – يضيف البعض الآخر[2]– أن المحرر هو أداة للتفاهم وتبادل الأفكار يجب أن يكون مقروءا بمجرد الإطلاع عليه بالعين المجردة أو ما يقوم محلها.

كما أن الكتابة فيها تتميز بعدم الثبات والإستقرار، مما يعني فقدان شرط من أهـــم الشروط الوظيفية للكتابة، وبالتالي فإن تغيير الحقيقة في المعلومات المخزنة على الدعامة الرقمية لا يعتبر تزويرا لإنتفاء هذا الشـــرط.

وذهبوا إلى أن طـــرق التزوير واردة في القانون على سبيل الحصر، وليس من بينها التزوير الواقع على المستندات الإلكترونية، وأنه لا يكفي أن يتم تغيير الحقيقة بطريقة ما، بل بإحدى الطرق التي حددها المشرع، ذلك أنه ليـــس كل كدب مكتوب تزوير[3].

ويضيف البعض[4] الآخر أن فكرة المستند الإلكتروني ونظم حمايته وتأمينه مازالت عرضة للتطور التقني، ذلك أن الأخد بفكرة التوقيع الإلكتروني على سبيل المثال يجب أن يصاحبه تنظيم تشريعي دقيق يحدد طرق هذا التوقيع وصوره واثاره في الإثبات والوسائل والضمانات اللازمة لحمايته، و أنه يترتب على الأخد بالتوسع في فكرة المحرر دون وجود تنظيم تشريعي إلى إثارة مشكلات عديدة تتعلق بالإثبات وهو ما يهدد إستقرار المعاملات. ومن المقرر أنه إذا تعارض إستقرار المعاملات مع تسهيل المعاملات وسرعة إنجازها فلا يجوز التضحية بإستقرار المعاملات في سبيل ذلك.

يتبين لنا من خلال اسانيد الإتجاه السابق، أنه يجري تلازم بين جريمة التزوير والطبيعة الورقية للمستند، فلا يمكن ان يتفق التزوير في المستند الإلكتروني مع مفهوم التزوير المستقر إلا أذا إتخدت المعلومات الناتجة عن النظام الإلكتروني صورة المخـــرجات التقلـــيدية.

ومن جهتنا، نحن لا نأخد بهذه الأراء على إطلاقها، إذ نرى إمكانية إنطباق جريمة التزوير في المحررات على فعل تغير الحقيقة على المستندات الإلكترونية وذلك في التشريعات التي اضفت حجية على المعلومات في الإثبات، ونستند في ذلك إلى الحجج التالية:

– إن عدم إمكانية القراءة البصرية لمحتويات المستند لا يعني عدم إمكانية تغيير هذه المعلومات، لأنه من الممكن قراءتها وفقا لإجراءات خاصة، والقاضي المطروح أمامه واقعة التزوير لا يقوم هو بإثباته بحاسة البصر، بل يحيل ذلك لأصحاب الإختصاص من الخبراء، فضلا عن ذلك فإن بعض التشريعات حسمت المســـألة من خلالها قوانينها، فالمشرع الجزائري نص في الفقرة 1 من المادة 2 على تعريف التوقيع الإلكتروني بأنه : **بيانات** في شكل الكتروني، مرفقة أو مرتبطة منطقيا ببيانات الكترونية اخرى، تستعمل

---

[1]–**د. نائلة عادل فريد قورة**، المرجع السابق، ص584–585. **د. هشام محمد فريد رستم**، المرجع السابق، ص326.

[2]– أنظر: د.**أيمن عبد الله فكري**، هامش رقم2، المرجع السابق، ص370.

[3]– انظر: **د. السيد عتيق**، المرجع السابق، ص120.

[4]–**د. اشرف توفيق شمس الدين**، الحماية الجنائية للمستند الإلكتروني، مؤتمر الأعمال المصرفية الإلكترونية، المرجع السابق، ص501.

كوسيلة توثيق. وقد عرفت الفقرة ب من المادة 2 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال البيانات على انها عملية عرض الوقائع او المعلومات او المفاهيم في شكل جاهز للمعالجة داخل المنظومة.

كما نصت المادة 323 مكرر 1 على إعتبار الكتابة الإلكترونية المثبة على دعائم غير ورقية كالكتابة على الورق، كما اقرت المادة 8 من قانون التوقيع الإلكتروني على أن التوقيع الإلكتروني منتجا لأثاره القانونية داتها المترتبة على التوقيع المكتوب، كما نصت الفقرة أ من المادة 2 من القانون رقم 09-04 في تعريفها للجريمة الإلكترونية على أنها جرائم المساس بانظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات و أي جريمة أخرى ترتكب او يسهل ارتكابها عن طريق منظومة معلوماتية او نظام للإتصالات الإلكترونية.

فمن خلال إستقراء النصوص السابقة، نجد أن المشرع الجزائري قد حسم المسالة عندما عرف المعلومات والكتابة الإلكترونية والتوقيع الإلكتروني وعدها منتجة لأثار القانونية داتها المترتبة على الكتابة التقليدية والتوقيع المكتوب، وبذلك منحها قوة في الإثبات الموجودة في المستندات العادية، وبالتالي فإن المشرع عد البيانات الإلكترونية ضمن المستندات العادية. وعليه تكون المستندات الإلكترونية محلا لجريمة التزوير وتلتقي مع المستندات العادية من حيث التعريف وقوة الإثبات، وحمايتها من التزوير.

فضلا عن ذلك، لو رجعنا إلى بعض المواد كالمادة 222 الخاصة بالتزوير في بعض الوثائق الإدارية والشهادات –وتقابلها المادة 441-2 عقوبات فرنسي–، نجدها لم تحـــدد الوثائـــق الإدارية تعدادا حصريا، ونستدل على دلك من عبارة "... أوغيرها من الوثائق" التي تسلمها الإدارة العمومية من أجل إثبات حق أو هوية أو صفة أو منح رخصة، وهو ما يسمح باستيعاب البطاقة الإلكترونية ضمن اطارها، كبطاقة التعريف البيومترية وسند السفر البيومتري، حيث يستطيع النظام المعلوماتي من خلال الإمكانيات الهائلة التي يملكها ان يقوم بتقليد أي مستند بصورة يصعب فيها التفرقة بين الأصل والتقليد، بالنظر لما يتميز به من امكانيات وتجهيزات وبرامج مخصصة للقيام بمثل تلك الأعمال. وهو ما تؤكده المادة 17 من القانون رقم 14-03 المتعلق بالسندات ووثائق السفر[1]، حيث أحالت في ذلك إلى العقوبات المنصوص عليها في قانون العقوبات في حق كل من يزور أو يقلد سند سفر بيومتري، وإذا مست الأفعال المذكورة أعلاه البيانات المخزنة في النظام البيومتري الإلكتروني، فتطبق العقوبات خاصة المنصوص عليها في المواد 394 مكرر إلى 394 مكرر. مع احالة المادة 18 منه الى احكام المادة 222 و 223 حالة اتخاد جواز السفر البيومتري تحت حالة مدنية غير صحيحة.

لكن هل يكفي الإعتراف التشريعي بحجية المستند الإلكتروني في الإثبات لكي نخضع التلاعب فيه لجرائم التزوير؟على ضوء صعوبة التفرقة بين المستند الأصلي والمزور في النطاق المعلوماتي، فانه يلزم ان يكون

[1]- قانون رقم 14-03 مؤرخ في 24 ربيع الثاني 1435 الموافق لـــ 24 فيفري سنة 2014، المتعلق بسندات ووثائق السفر.

هنالك ارتباط بين اتخاذ **اجراءات التوثيق أو التصديق**[1]، والإعتراف بحجية المستند المعلوماتي، حتى يمكن الرجوع إليها في حالة وقوع التلاعب في المعلومات المتعلقة بالمستند داخل النظام.

ومع ذلك، وإن كنا نرى إمكانية تطبيق مقتضيات هذه الجريمة على المستند المعلوماتي، للأسباب المتقدمة، إلا أن التردد حول إمكانية تطبيقها على المستندات الإلكترونية بإختلاف أنواعها، يجعل من الأفضل تدخل المشرع لتجريمها بنص خاص مع التدرج في العقوبة حسب طبيعتها(رسمية أو عرفية) مع إنتهاج طريقة أكثر مرونة بإستبعاد التعداد الحصري لطرق التغيير فيها نظرا لطبيعتها الخاصة.

الفرع الثاني

تجريم تزوير المستند الإلكتروني بين النصوص العامة والنصوص الخاصة

في سبيل حل المعادلة الصعبة التي تتطلب تحقيق هدفين أساسيين: عدم تفويت الفرصة من الإستفادة من تطور التقنية المعلوماتية، وضرورة حماية الثقة اللازمة في المحررات الناتجة عن النظم المعلوماتية بأشكالها الحديثة، أخذت التشريعات على عاتقها مواجهة التزوير المعلوماتي.

ونظرا للإختلاف في تحديد مفهوم المستند الإلكتروني سواء من خلال توسيع مفهوم المحرر الورقي، أو من خلال إدراج مفهوم خاص له، انعكس ذلك على الصيغ التشريعية عند تجريم تزوير هذا المستند، فمن التشريعات من عالجها بنصوص عامة عن طريق تبنيها تعديلا تشريعيا على نصوص التزوير في قانون العقوبات على نحو يسمح بامتدادها إلى المستندات الإلكترونية كما هو شان المشرع الفرنسي، ومنها من عالجها بموجب نصوص خاصة كما هو شأن المشرع المصري.

أولا- تجريم تزوير المستند الإلكتروني بنصوص عامة

عمد المشرع الفرنسي بموجب المادة 441 -1 عقوبات التي تتضمن **القاعدة العامة لأحكام التزوير** و تشمل تزوير المحررات التجارية والمصرفية والعرفية، إلى التوسع في تجريم التزوير ليستوعب حالات التزوير العادي في المحررات إلى جانب تزوير المستند الإلكتروني، فنصت على مايلي: "***يشكل تزويرا كل تغيير إحتيالي للحقيقة، من شأنه إحداث ضرر، وينجز بأية وسيلة كانت، وينصب على محرر أو على أية دعامة للتعبير عن الأفكار يكون موضوعها او يكون من اثارها اقامة الدليل على حق او على واقعة دات نتائج قانونية***".

لم تكن جريمة التزوير في المستندات المعلوماتية كما هي عليه الآن، ففي ظل قانون العقوبات الفرنسي القديم تباينت آراء الفقه[2] حول تطبيق نص المادة 145 ومالياها على التزوير المعلوماتي، ليتقدم بعدها النائب

---

[1]- أنــظر في التأكيد على هدا الأمر بالقانون 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين. وعلى العموم ستكون اجراءات التصديق محل دراسة مفصلة في المبحث الثاني من هذا الفصل.

[2]- أنظر في ذلك: **د. أيمن عبد الله فكري**، المرجع السابق، ص394 وما بعدها.

الفرنسي godfrain بمقترح في 5 لغسطس 1986 يهدف الى ادخال تعديل في جريمة التزوير في المحررات لتشمل التزوير المعلوماتي، إلا أن هذا الإقتراح لم يؤخذ به وأصدر المجلس القانون رقم 88–19 المؤرخ في 5 يناير 1988، الذي تضمن المادة 462–4 التي كانت تعاقب على التلاعب بالمعلومات، والمادة 462 –5 كانت تنص على عقاب كل من يقوم بارتكاب أفعال تؤدي الى تزوير المستندات المعالجة آليا أيا كان شكلها و باية طريقة تؤدي إلى إحداث ضرر يعاقب..."في حين المادة 462–6 كانت تعاقب على كل من يستخدم مستندات معالجة مزورة[1].

وكما هو ملاحظ، فإن المشرع أدرج جريمة تزوير المستندات المعالجة ضمن الجرائم المعلوماتية، مكملا في ذلك النص الخاص بتزوير المحررات، وإعتبارها جريمـــة مستقلة[2].

وقد لاقت هاتين المادتين إعتراض في مجلس الشيوخ عند مناقشة هذا القانون، لما يترتب عليهما من مساواة بين المعطيات المعلوماتية بصفة عامة، وبين المحررات من حيث القيمة القانونية[3].

على أساس ذلك قام المشرع الفرنسي في خطوة تشريعية أخرى بإدماج المادة 462–6 ،5 المتعلقة بتزوير المستندات المعالجة آليا واستعمالها داخل إطار النص العام للتزوير بعد إجراء تعديلات عليه في المادة 441–1 عقوبات. مخرجا بدلك جريمتي تزوير المستندات المعالجة آليا من بين جرائم الاعتداء على نظم المعالجة الآلية، وذلك أمر منطقي يجد مبرره في اختلاف **المصلحة** التي يحميها القانون في جريمة التزوير في المستندات وهي حماية الثقة العامة فيها، عن المصلحة المحمية في جرائم المساس بنظم المعالجة الآلية ومعطياتها[4].

ويستفاد من نص المادة المشار إليها، ان جريمة التزوير تقوم على أركان محددة، فلا بد من توافر الركن المادي وركن معنوي سنتطرق لدراستهما من خلال مايلـــي:

أ– الـــركـــن المـــادي

---

[1]– **المستندات المعالجة آليا** هي مستندات تم بالفعل خضوعها لمعالجة آلية، أي تم صياغتها بإحدى لغات الحاسوب، أما **المستندات المعلوماتية**"فهي تلك الوثيقة غير المعالجة، وتعتبر مستندات معلوماتية الأوراق المعدة لتسطير المعلومات عليها، والأقراص الممغنطة التي لم يسجل عليها أي شيء بعد و الملاحظات التي تكون على شكل كتب أو نشرة متعلقة بطريقة إستخدام البرنامج وكذلك البطاقات البنكية التي لم تدخل الخدمة بعد، وهذه وإن كان مسجلا عليها معلومات مكتوبة بخط اليد أو مطبوعة أو محفورة إلا أنه لم يتم معالجتها بعد إذ أنها مازالت في مرحلة الإعداد فقط أنظر: **آمال قارة**، المرجع السابق، ص134.**د. عفيفي كامل عفيفي**، **فتوح الشاذلي**،المرجع السابق، ص150.

[2]–**د. نائلة عادل فريد قورة**، المرجع السابق، ص587.

[3]– أنظر: د. **أيمن عبد الله فكري**، المرجع السابق، ص398.

[4]– أنظر في ذلك:**د. عبد الفتاح بيومي حجازي**، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، المرجع السابق، ص142 وما بعدها، و د. **عفيفي كامل عفيفي** ، **فتوح الشاذلي**، المرجع السابق، ص246 وما بعدها. و **د. أحمد حسام طه تمام**، المرجع السابق, ص407 وما بعدها، و **د. مفيد تركي**، إشكالية المحل في جريمة التزوير المعلوماتي، مجلة كلية الحقوق، العدد 16، كلية الحقوق والشريعة، جامعة النهرين، أيار، 2006، ص161 و ما بعدها.

يتمثل الركن المادي في هذه الجريمة في تغيير الحقيقة في محرر أو أي دعامة للتعبير عن الفكر، وصياغة المادة على النحو السابق يسمح بإستيعاب كل صور التعبيرعن الفكر التي تكون في شكل إلكتروني، بل وحتى تلك التي لم يتوصل اليها العلم بعد.

ونتيجة للتطورات التكنولوجية التي تداخلت مع الأنشطة الحياتية وإرتكاب الأفعال غير المشروعة من خلالها، جعل المشرع من مدلول تغيير الحقيقة من الإتساع ما يشمل جميع الطرق التي يتم بها هذا التغيير دون تحديد لطريقة بعينها، وهو ما يستفاد صراحة من البناء المادي الذي صيغت به المادة 441-1 كمايلي:..."***يشكل تزويرا كل تغيير إحتيالي للحقيقة...***"

وتغيير الحقيقة في المستند الإلكتروني يمكن تصوره بطرق كثيرة، سواء كانت طرق مادية أو معنوية. ينصب هذا النشاط على محل محدد وهو المحرر أو أي وعاء آخر للتعبير عن فكرة أو معاني معينة، والمقصود بذلك أي دعـــامة أخرى غير المحرر، حيث أن الدعامة الأخرى تنصرف إلى كافة الأشكال المتصورة التي يمكن أن تكون وعاء للتعبير عن فكر، مثل البطاقات والأشرطة الممغنطة[1]، ميكروفيلم، الشرائح أو القرص الصلب للكمبيوتر.[2]وبالتالي لم تشمل هذه المادة ما كان منصوصا عليه في المواد 462-5 و 462-6 المتعلق بالغش المعلوماتي في شأن التزوير الواقع على الوثيقة المعالجة معلوماتيا فحسب بل امتدت الحماية إلى المستندات المعلوماتية سواء كانت تخضع لهذه المعالجة أم لا. مادام انها تحوي تعبير عن فكر ينتج أو يمكن أن ينتج عنه دليل على حق أو واقعة ذات آثار قانونية، أو كما عبر عنها البعض[3] ذات قيمة ثبوتية.

وعليه فتعريف التزوير الوارد في المادة 441-1 عقوبات ينطبق دون شك على المستندات المعلوماتية بعد صدور القانون رقم 2000-230 ، مما يضفي حماية عليها بشكل يؤدي إلى كفـــالة الثقة فيـــها.

ولايكفي في جريمة التزوير تغيير الحقيقة في المستند المعلوماتي، بل يجب أن يترتب عليه ضررا للغير.

وتجدر الإشارة، إلى أنه يجب التمييز بين التلاعب بالمعلومات وهو الفعل المنصوص والمعاقب عليه بموجب المادة 323-1 (المساس بسلامة المعلومات) والتزوير في المستند الإلكتروني المنصوص عليه في المادة 441-1 (الاعتداء على أصالة المعلومات) ، وذلك من حيث المحل ونتيجة السلوك المادي فيها، حيث في جريمة التلاعب بالمعلومات يتم الاعتداء على المال المعلوماتي المعنوي أي المعطيات الموجودة داخل النظام أوالمنقولة عبره ويترتب على ذلك تغيير حالتها من خلال الأفعال المتمثلة للنشاط الجرمي في هذه الجريمة، دون أن يكون قصد الجاني متجها الى إستـــخدام تلك المعلومات في شيء مـــا.

في حين أن جريمة التزوير المعلوماتي هي تغيير الحقيقة في معلومات تشكلا مستندا كون لها قيمة في الإثبات، هادفا الجاني من خلاله الإستفادة منه واستخدامه.

---

[1]-CA Paris, 6 mai 1997 cite par: **Charlène WANPOUILLE**, Le faux, l'usage de faux et le faux en écriture publique Comparaison de l'état du droit et de la jurisprudence en France et à Maurice,2015 articledisponible en lingne á l'adresse suivante: www.ijls.mu/index.php/lecture-notes?download=94:expose-sur-**le-faux**

[2]-**د. عبد الفتاح بيومي حجازي**، الدليل الجنائي والتزوير في جرائم الكمبيوتر والأنترنت، المرجع السابق، ص144.

[3]- **Charlène WANPOUILLE**, op,cit, p4.

ومع ذلك فانه من الممكن أن يجتمع في النشاط الإجرامي الوصفين الجنائيين معا كما لو قام الجاني بالتلاعب بمعلومات لها قيمة في الإثبات بقصد إستخراج مستند معلوماتي تم النشاط عليه بصورة غير صحيحة[1].

ب- الـــركـــن المـــعنـــوي

تميز نص المادة 441-1 عقوبات من ناحية البناء المعنوي بأن المشرع إستخدم فيه عبارة "**غش**"، كما تطلب أن يكون غرض الجاني من التزوير إثبات حق أو واقعة ذات آثار قانونية، وهو ما يستفاد معه أن هذه الجريمة تقوم على توافر القصد العام بعنصريه العلم والإرادة، فضلا عن القصد الخاص[2].

ت- العقوبـــــة

عاقب المشرع الفرنسي عن هده الجريمة بالحبس من 3 سنوات وغرامة 45000 أورو.

ذلك كان عن المستندات الإلكترونية التجارية والمصرفية والعرفية، أما المستندات الإلكترونية الرسمية فتتفاوت العقوبات المقررة لها، بحسب إدا ماكانت صادرة عن إدارة عامة(441-2 فقرة 1 عقوبات) أو وثيقة صادرة عن جهات حكومية وكدا الوثائق القضائية(المادة 441-4 فقرة 1 عقوبات) ، أو وقع التزوير من قبل شخص يملك سلطة عامة أو مكلف بتأدية خدمة عامة (المادة 441 -4 فقرة 3 عقوبات).

ثانيا: تجريم تزوير المستند الإلكتروني بنصوص خاصة

من بين التشريعات التي واجهت التزوير المعلوماتي بنصوص خاصة نجد المشرع الجزائري والمشرع المصري، سنحاول ان نعرض فيمايلي كل تجربة على حـــدى.

أ- تجريم تزوير المستند الإلكتروني في التشريع الجزائري

لإرساء جو من الثقة وتامين التعاملات الإلكترونية، اتجه المشرع الجزائري مستفيدا من قانون الأونسترال النموذجي للتجارة والتوقيع الإلكترونيين إلى إصدار القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكتروني، وباستقراء نصوصه نجد أنه قد أرسى من خلاله ثلاث مبادىء أساسية هي: ***التوثيق السلامة، عدم الإنكار***. وفي ذات الوقت نص على مساواة التوقيع الإلكتروني بالتوقيع العادي في انتاج كافة الاثار القانونية الناشئة عن استخدامه في المعاملات القانونية المختلفة.

وإن كان الأمر كذلك، فإنه لم يعالج بشكل كافي التزوير الواقع على المستند الإلكتروني، بل جاءت معالجته للأمر جزئية من خلال القانون السالف الدكر، حيث نجده يعاقب بموجب المادة 66 من هذا القانون على إعطاء معلومات مزورة فنص" **يعاقب بالحبس من 3 اشهر إلى 3 سنوات و بغرامة من عشرين الف**

[1]- **د.أحمد حسام طه تمام**، المرجع السابق، ص ص357 358، **د. أيمن عبد الله فكري**، المرجع السابق، ص252.

[2] **Françoise SIBAUD**, DU DROIT PENAL DES AFFAIRES DU FAUX , Sources Editions Jurisclasseur 2002, http://webcache.googleusercontent.com/search?q=cache:http://lexilis.free.fr/notesjur/note56.htm

دينار إلى 200000 دج أو بإحدى هاتين العقوبتين فقط، كل من أدلى بإقرارات كاذبة للحصول على شهادة تصديق الكتروني موصوفة".

وهــذه الجريمة تقترب نوعا ما من التزوير التقليدي، فقد ينتحل الجاني هوية غيره أو يبدل شخصيته، لإنشاء شهادة تصديق غيرصحيحة.

كما عاقب بموجب المادة 68 بالحبس من 3 اشهر إلى 3 سنوات و بغرامة من مليون دينار إلى خمسة ملايين دينار او باحدى هاتين العقوبتين فقط، كل من يقوم **باستعمال بيانات إنشاء توقيــع الكتروني** موصوف خاصة بالغير، والمعبر عنها عموما بمفتاح التشفير الخاص، إلى جانب ذلك نجد المشرع يعاقب بموجب المادة 17 من قانون عصرنة العدالة كل شخص يستعمل بطريقة غير قانونية العناصر الشخصية المتصلة بإنشاء التوقيع الإلكتروني يتعلق بتوقيع شخص أخر". في كلا النصين فإن التوقيع الإلكتروني سليم و لم يجر عليه أي تعديل، و إنما تم إستعماله من شخص غير مخول بدلك، والتوقيع بإسمه مما يشكل تزويرا.

وإلى جانب ذلك، تناول المشرع المنهج الخاص بوضع نص عام يتم من خلاله مكافحة الطريق المؤدي و الموصل للتزوير المعلوماتي بجميع أشكاله وصوره، و يتمثل هذا النص في تجريم الدخول غير المشروع للنظام المعلوماتي بموجب المادة 394 مكرر عقوبات، بإعتباره الطريق الأساسي الذي من خلاله يتم فيما بعد التزوير المعلوماتي وسائر الأنشطة غير المشروعة في مجال المعلوماتية، ويرى البعض من الفقه[1] بأنه يمكن تكييف نشاط الدخول غير المشروع على أنه **انتحال للشخصية**، ويعد بدلك من صور وقوع جريمة التزوير أو بإعتباره توقيعا إلكترونيا مزورا كما ذهــب إلى ذلك بعضهم الآخر[2].

بالإضافة إلى ماسبق، تضمن قانون العقوبات السالف الذكر جريمة التلاعب بالمعطيات التي يحتويها نظام المعالجة الآلية، وهنا يمكن القول بامكانية إعتبار أن هذا التلاعب تزويرا في مستند عرفي، ويمكن تصور ذلك في حالة ما إذا كانت هذه المعطيات تمثل **قيمة في الإثبات**، وتوافر لدى الجاني نية إستعمال المستند المزور فيما زور من أجله، إلا أن هذه الشروط لا تتوافر دائما، ذلك أنه يمكن أن نتصور جريمة التلاعب بالمعلومات دون أن يشكل ذلك جريمة التزوير في المستند إذا لم يتوافر ركن أو شرط في هذه الجريمة كما لو كانت هده المعطيات من قبيل الأوراق الداخلية في الشركة[3]، كما يمكن أن نتصور جريمة تزوير في مستند دون أن يشكل ذلك جريمة تلاعب كما لو تعلق الأمر بالتزوير في المستندات الرسمية التي ترتفع إلى مصاف الجنايات، وهو ما يستوجب في المقابل الحاجة إلى وجود نصين، نص يعاقب على التلاعب في المعلومات، ونص عام يعاقب على التزوير في المستندات.

من خلال ماسبق نخلص إلى أن المشرع الجزائري لم يكفل حماية كاملة وشاملة للمستند الإلكتروني ضد تزويره بكافة صوره، بل جاءت حمايتة قاصرة نوعا ما، ولذلك نهيب بالمشرع التدخل لحفظ هذا السلوك المستحدث في قالب تجريمي مستحدث، يبين تدرج العقوبة حسب طبيعة المستند الإلكتروني المــزور.

---

[1]-انظر: **د.كامل السعيد**، بحث جرائم الكمبيوتر والجرائم الأخرى في مجال التكنولوجيا، المؤتمر السادس للجمعية المصرية للقانون الجنائي حول جرائم المعلوماتية وجرائم البيئة ، المنعقد في القاهرة في الفترة من 25 إلى 28 أكتوبر 1993.، دار النهضة العربية، ص 331 وما بعدها

[2]– **د. ايمن عبد الله فكري**، المرجع السابق، ص425.

[3]–**د.شيماءعبد الغني**، المرجع السابق، ص137.

ب- تجريم تزوير المستند الإلكتروني في التشريع المصري

لقد تطور الوضع في القانون المصري من قصر تجريم التزوير على تزوير السجلات الإلكترونية الخاصة بالأحوال المدنية، وفقا لقانون الأحوال المدنية رقم 143 لسنة 1994 إلى تجريم الصور المختلفة للمساس بالمستند ومن بينها جريمة التزوير، وفقا لقانون التوقيع الإلكتروني رقم 15 لسنة 2004.

نصت المادة 72 " في تطبيق أحكام هذا القانون وقانون العقوبات تعتبر البيانات المسجلة بالحاسبات اللآلية وملحقاتها بمراكز معلومات الأحوال المدنية ومحطات الإصدار الخاصة بها المستخدمة في إصدارالوثائق وبطاقات تحقيق الشخصية بيانات واردة في محررات رسمية، فإذا وقع تزوير في المحررات السابقة أو غيرها من المحررات الرسمية تكون العقوبة الأشغال الشاقة المؤقتة أو السجن لمدة لا تقل عن خمس سنوات".

كما نصت المادة 74 "مع عدم الإخلال بأي عقوبة أشد منصوص عليها في قانون العقوبات أو في غيره من القوانين يعاقب بالحبس ...كل من إطلع أو شرع...في الحصول على البيانات او المعلومات التي تحتويها السجلات او الحاسبات الآلية أو وسائط التخزين الملحقة بها أو **قام بتغييرها بالإضافة أو بالحذف أو بالإلغاء أو بالتدمير أو بالمساس بها** بأي صورة من الصور...".

رغم أهمية هذه النصوص في حماية المعلومات التي تتضمنها الكمبيوترات الخاصة بمصلحة الأحوال المدنية، إلا أنه لا يجوز ان يقاس عليها أي مستندات اخرى ايا كان نوعها، ولدلك فهذا النص يعد قاصرا في نطاق الحماية.

أمـــا قانون التوقيع الإلكتروني فقد نص في المادة 23 منه على انه "**مع عدم الإخلال باي عقوبة أشـــد منصوص عليها في قانون العقوبات أو في أي قانون آخر، يعاقب بالحبس....كل من أتلف أو عيب توقيعا أو وسيطا أو محررا إلكترونيا، أو زور شيئا من ذلك بطريق الإصطناع أو التعديل أو التحوير أو بأي طريق آخر، إستعمل توقيعا أو وسيطا أو محررا إلكترونيا معيبا أو مزورا مع علمه بدلك.**

سنحاول فيما يلي تحليل هذه الجريمة من خلال ركنيها المادي والمعنوي على النحو التالي:

1-الركـــن المـــادي

قوام الركن المادي في جريمة تزوير المستند الإلكتروني هو تغيير الحقيقة، وقد حدد المشرع المصري صور هذا التزوير، بأن نص على وقوعه عن طريق الإصطناع أو التعديل في معلومات موجودة أو التحوير.

ونظرا لإدراك المشرع كون حصر هذه الطرق يعد أمرا غير ممكن لتعدد صور تغيير الحقيقة وإختلافها وتجددها بما لا يمكن معه حصرها، فقد ترك الباب مفتوحا لما قد يستجد من وسائل أخرى للتزوير، مما يضفي على النص طابع المرونة، وهو ما يستفاد صراحة من دلالة عبارة" ....**أو بـــأي طريق آخر**"الواردة بنص المـــادة 23.

و من جهة أخرى، نجده قد إستخدم مصطلح المعيب بالإضافة للمزور، بما يوحي أن المشرع قد سلك منهجا موسعا لمفهوم تغيير الحقيقة في مجال المستندات الإلكترونية.

كما أنـــه إستخدم مصطلح **التعديل والتحوير**، قد يبدو للوهلة الأولى من وجود ترادف بينهما، إلا ان مدلول كل منهما يختلف عن الآخر، فالتحوير يرتبط بصفة مباشرة بمضمون المستند، اما التعديل فيمكن ان يرد على صلب المستند كما قد يرد ايضا على مضمونه، فالتحوير يندرج ضمن التعديل[1]، لكن ليس كل تعديل هو تحوير.

ولما كان مناط التجريم مرتبط بتمتع المستند بقيمة في الإثبات، فقد اضفى صراحة بموجب المادة 15 من قانون التوقيع الإلكتروني على المسنتد الإلكتروني حجية في الإثبات في نطاق التعاملات الإلكترونية المدنية و التجارية والإدارية، وهي ذات الحجية التي تتمتع بها المحررات الرسمية والعرفية في أحكام قانون الإثبات. ومع ذلك لم يشر إلى هذا العنصر صراحة في صلب المادة 23 –أي اهمية البيان الدي ينصب عليه التزوير–، وهو ما جعله محل إنتقاد من طرف البعض من الفقه[2]، إلا اننا نرى أن المشرع مادام اضفى على المستند الإلكتروني دات الحجية المقررة في الإثبات للمستند الورقي بموجب المادة 14 و 15 بما يعني له قيمة قانونية يعتد بها القانون، وأن من شـــأن التزوير الذي يرد عليه أن يؤثر على إثبـــات واقعة أونفيها، فقد تجنب التكرار باعادة النص على ذلك في المادة 23 من نفس القانون[3].

ولا يكفي لإكتمال الركن المادي لجريمة التزوير أن يقع تغيير الحقيقة في مستند، بل ينبغي أن يكون من شانه أن يسبب ضررا للغير، وإذا إنـــعدم الضرر تكون الجريمة غير قائمة، إلا أنه بالرجوع لنص المادة 23 لم نجده يشير إلى هذا العـــنصر.

2–الركـــن المعنـــوي

جريمة التزوير بصفة عامة ومنها التزوير المعلوماتي، هي جريمة عمدية، ومن ثم يتخذ الركن المعنوي فيها صورة القصد الجنائي وهو تعمد تغيير الحقيقة في محرر تغييرا من شأنه أن يسبب ضررا وبنية إستعمـــال المحـــرر فيما غيرت الحقيقة من أجله.

إلا أنه وبالرجوع إلى المادة 23 نجده قد تميزمن ناحية البناء المعنوي بان المشرع لم يستخدم فيه من العبارات الدالة على سوء النية أو الخداع أو الغش، كما أنه لم يحدد الغاية التي يريد الجاني الوصول اليها من القيام بالتزوير، ومع ذلك فالقضاء المصري يتطلب في جريمة تزوير المحررات المكتوبة توافر قصد خاص

---

[1]- أنظر: **د. تامر محمد سليمان الدمياطي**، المرجع السابق، ص639.

[2]– **د. اشرف توفيق شمس الدين**، المرجع السابق، ص 113.

[3]– ويرى البعض من الفقه أن عدم تحديد البيان الذي يقع عليه التزوير في المستند الإلكتروني لايعني ذلك الإحالة للقواعد العامة لأن ذلك يتطلب وجود نص يلزم بذلك، كما ان الإحالة في المسائل الجزائية تستوجب صدور نص، فضلا عن استخدامه مدلولات جديدة تختلف عن السائد في القواعد العامة، **د. ايمن عبد الله فكري**، المرجع السابق، ص439.

لدى الجاني، هونية استعمال المحرر المزور فيما زور من اجله وهو ما يعتبر استكمالا لتحديد مدلول القصد الجنائي[1].

3- العقوبـــة

وقد عاقب المشرع على هذه الجريمة بموجب المادة 23 بالحبس وبغرامة لا تقل عن 10000 جنيه ولاتجاوز مائة الف جنيه أو بإحدى هاتين العقوبتين، مع عدم الإخلال باية عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون آخر، ومؤدى ذلك ان عقوبة تزوير المستند الإلكتروني تختلف حسب طبيعة المستند المزور، **فالتزوير في المستندات الرسمية الإلكترونية يعاقب عليها بعقوبة أشد.**

المبحث الثاني

الحماية الجزائية للتوقيـــع الإلكتروني

بظهور الدعامات الإلكترونية التي تحمل عليها الكتابة الإلكترونية باعتبارها دليل كامل لإثبات التعاملات الإلكترونية المختلفة، ولتعذر إستخدام التوقيع التقليدي في هذه الركيزة الجديدة، إتجه الواقع العملي لإيجاد نظير يتوائم مع هذه الوسائل الإلكترونية، ويحقق الأمن والثقة للمتعاملين الإلكترونيين باعتبارهما من أهم الأسس التي يقوم عليها التعامل الإلكتروني، هذا النظير إصطلح عليه بـــ" **التوقيع الإلكتروني**"[2].

على أنه إذا كان التوقيع الإلكتروني هو البديل العملي للتوقيع التقليدي، **فهل يعتبر أيضا بديـــلا قانـــونيا؟**

لقد تنبهت الدول المتقدمة مبكرا إلى غياب القوانين التي تنظم التواقيع الإلكترونية، فنظمته من حيث النص على قيمته الثبوتية ووضع مبدأ التكافؤ الوظيفي بينه وبين التوقيع التقليدي من جهة. كما حمته جزائيا من الإعتداءات التي يمكن أن يتعرض لها، مما يكفل في المقابل حماية جزائية للمستند الإلكتروني.

ولم تكن الدول العربية في منأى عن هذا التطور، بل أن البعض منها عمد إلى سن قوانين خاصة حددت من خلالها القواعد العامة المتعلقة به وبالتصديق عليه، قصد التكفل بالمتطلبات القانونية والتنظيمية والتقنيات التي ستسمح بإحداث جو من الثقة الملائمة لتعميم وتطوير التعاملات الإلكترونية.

رغم إختلاف التشريعات في موضع النص على هذه الحماية، الا انه كان هناك اتفاق على ضرورة هده الحماية. **وعليه: كيف تم تنظيم مثل هاته الوسيلة؟ وماهي حدود الحماية الجزائية التي أتى بها المشرعون**

---

[1]- نقض 21 فبراير 1942 مجموعة القواعد القانونية جـــ 7 رقم 817 ص 773، 2 فبراير 1956، 24 ديسمبر 1972 س 23 رقم 322 ص 1431، 16 مايو 1971 س 28 رقم 129 ص 609.

[2]- تجدر الإشارة إلى أن البعض يطلق عليه تسمية التوقيع الإجرائي حيث يعرفه أنه التوقيع الناتج عن إتباع إجراءات محددة تؤدي في النهاية إلى صحة نتيجة معروفة مقدما.**محمد مرسي زهرة**، الدليل الكتابي وحجية مخرجات الكمبيوتر في الإثبات في المواد المدنية والتجارية، مؤتمر القانون والكمبيوتر والأنترنت ،الجزء الثالث، الطبعة الثالثة، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ماي 2000.،ص814.

إلا أن هذه التسمية لا محل لها في الوقت الراهن في ضوء الإستقرار الفقهي والقضائي والتشريعي على إطلاق تسمية التوقيع الإلكتروني على هذا الشكل الحديث من التوقيعات.

لصون التوقيع الإلكتروني ذاته عبر تجريمهم للأفعال غير المشروعة الماسة به سواء من قبل أطراف التعامل الإلكتروني أو من الغير؟

للإجابة على هده الأسئلة وغيرها وتماشيا مع تسلسل الأفكار على النحو الذيسبق ذكره يقتضي منا تقسيم هذا المبحث إلى ثلاثة مطالب كمايلي:

المطلب الأول: نطاق الحماية الجزائية(التوقيع الإلكتروني)

المطلب الثاني:المسؤولية الجزائيةعن الأفعال غير المشروعة من قبل أطراف التعامل الإلكتروني

المطلب الثالث:المسؤولية الجزائية عن الأفعال غير المشروعة من قبل الغيــر

المطلــب الأول

نطــاق الحماية الجزائية(التوقيع الإلكتروني)

إستمرت فكرة التوقيع–بمفهوها التقليدي– وصمدت إلى حد كبير في وجه المتغيرات التي استجدت في التعامل باعتباره الطريق الرئيسي لإسباغ الحجية على المحررات، وفي ظل هذه الظروف لم يجد التوقيع التقليدي بأشكاله المعروفة له مكانا أمام إنتشار نظم المعالجة الآلية. فاتجه الواقع إلى البحث عن نظير له يستطيع أن يؤدي وظائــفه.

ولا شك أن التوقيع التقليدي والإلكتروني يتشابه مع الآخر في بعض الخصائص ويختلف في بعضها الآخر كما تتعدد صوره بحسب الطريقة التي يتم بها هذا التوقيع، وتتباين من حيث درجة الثقة ومستوى ما تقدمه من ضمان، بحسب الإجراءات المتبعة في إصداره وتامينه والتقنيات التي تتيحها.

إلا أن التوقيع الإلكتروني لا يكفي وحده للتحقق من هوية المتعامل الكترونيا، فليس من العسير أن يدلي أحد الطرفين بمعلومات غير حقيقية عن هويته، الأمر الذي تطلب أن يتم الربط بين التوقيع الإلكتروني وبين شخص معين، وهذا الدور هو الذي يقوم به مزود خدمة التصديق على التوقيع الإلكتروني من خلال إصدار شهادة مصادقة تؤكد هوية الشخص وصحة توقيعه الإلكتروني.

وفقا لما تقدم من أفكار رئيسية، قسمنا هدا المطلب إلى فرعين، خصصنا الفرع الأول لبحث مفهوم التوقيع الإلكتروني، والفرع الثاني لدراسة مسالة التصديق الإلكتروني عليه.

الفــرع الأول

مفهوم التوقيــع الإلكتروني

يفترض بيان مفهوم التوقيع الإلكتروني تعريفه وتمييزه عن التوقيع التقليدي، فضلا عن بيان شروط صحته والتطرق لأهم صوره.

أولا–تعريف التوقيع الإلكتروني وتمييزه عن التوقيع التقليدي

سنتناول في هذا العنصر مسالة تعريف التوقيع الإلكتروني ثم نبرز أهم نقاط الاختلاف والتشابه بينه وبين التوقيع العادي.

أ- تعريف التوقيع الإلكتروني

يعتبر التوقيع ظاهرة إجتماعية، بل هو ظاهرة ضرورية يحميها القانون، ومع ذلك لم تتعرض التشريعات لتعريفها، ولربما يمكن تبرير ذلك كون أن التوقيع فكــرة جوهرية مألوفة وفطرية. وهوما دفع الفقه في محاولة منه ايجاد تعريف له[1]، ومهما تعددت التعريفات[2] التي قيلت بشأنه إلا أنها في الغالب تتجه إلى إبراز الوظائف التي يؤديها التوقيع في الإثبات، وهي أن يحدد هوية الموقع وأن يعبر عن إرادته في قبول التصرف.

وإذا كان هذا هو شان التوقيع التقليدي، فإن التوقيع الإلكتروني كان اوفر حظ منه، فنظرا لتطور الآلية التي يتم بها، وكونه واقعة مستجدة تحتاج إلى البحث والإقناع، عمدت العديد من الدول الى تحديد مفهومه في خطوة الهدف منها بث الثقة والأمان في نفوس المتعاملين الإلكترونيين، وهما من الأسس التي يقوم عليها التعامل الإلكتروني.

لقد حظي التوقيع الإلكتروني بإعتباره جوهر المستندات الإلكترونية بل عنصر مهم لإثبات صحته، باهتمام كبير من قبل العديد من المشرعين بل وفقهاء القانون.

فعلى النطاق الفقهي، تعددت التعاريف التي رصدت له،فقد عرفه[3]البعض على أنه: "***مجموعة من الإجراءات التقنية التي تسمح بتحديد شخصية من تصدر عنه هذه الإجراءات، وقبوله بمضمون التصرف الذي يصدر التوقيع بمناسبته***"، كما عرفه البعض[4] على أنه"***مجموعة من المعلومات مدرجة بشكل الكتروني في رسالة البيانات أو مضافا عليها أو مرتبطا بها إرتباطا منطقيا تستخدم لتحديد هوية الموقع وإثبات موافقته على فحوى الرسالة وتؤكد سلامتها***".

أما على النطاق التشريعي، فقد عمدت الدول التي نظمت التعاملات الإلكترونية على وضع تعريف له لإزالة الغموض عنه، وقد تعددت نطاقها.

فعلى الصعيد الدولي نجد**المادة 7-1**-أ من قانون الأونسترال النموذجي بشان التجارة الإلكترونية لعام 1996 **تعترف بوجود توقيع الكتروني من الأطراف بالنسبة لرسالة البيانات إذا إستخدمت بطريقة لتعيين**

---

[1]– أنظــر: **د.محمد مرسي زهرة**، المرجع السابق، ص807.

[2]- انظر في هذه التعريفات لدى:

Lamberterie Isabelle, « La valeur juridique de la signature, pe rspective de longue durée », revue; *Hypothèsets*; Publications de la Sorbonne 1/2006 (9) , p. 361.

[3]–**د. حسن عبد الباسط جميعي**، إثبات التصرفات القانونية التي يتم إبرامها عن طريق الانترنت، دار النهضة العربية، القاهرة، 2000، ص 34.

[4]-Rosenoer, **Jonathan,** CyberLaw, The Law of the Internet, Springer, 1997, p237

هوية ذلك الشخص والتدليل على موافقة ذلك الشخص على المعلومات الواردة في رسالة البيانات[1]، لتعرف المادة الثانية من الفقرة أ من قانون الأونيسترال النموذجي بشان التوقيعات الإلكترونية لعام 2001التوقيع الإلكتروني على أنه"**بيانات في شكل الكتروني مدرجة في رسالة بيانات أو مضافة إليها أو مرتبطة بها منطقيا، يجوز أن تستخدم لتعيين هوية الموقع بالنسبة إلى رسالة البيانات، ولبيان موافقة الموقع على المعلومات الواردة في رسالة البيانات**"[2].

يستفاد من هذا التعريف، أن المشرع الدولي قد ركز على إستخدام التوقيع الإلكتروني كنظير وظيفي للتوقيع التقليدي، وفي هذا الإطار إستند على وظيفة التوقيع الأساسية وهي تحديد هوية محرر رسالة البيانات والتاكيد على موافقته على مضمونها. آخذا بذلك بمبدأ الحياد التكنولوجي، وذلك بعدم تمييزه بين أي من تقينيات التوقيع الإلكتروني.

كما تولى مشرع الإتحاد الأروبي في سياق حثه جميع الدول الأروبية المكونة للإتحاد على الإعتراف بالتوقيع الإلكتروني واعطاء تعريف له، فاصدر في 13 ديسمبر 1999 التوجيه الأروبي رقم 93 / 1999 الخاص بالتوقيعات الإلكترونية[3]؛

وقد ميز بين نوعين من التوقيعات الإلكترونية، التوقيع الإلكتروني البسيط والتوقيع الإلكتروني المتقدم، فعرف الأول بموجب الفقرة الأولى من المادة الثانية على أنه عبارة عن" **بيانات في شكل الكتروني متصلة أو مرتبطة منطقيا ببيانات الكترونية أخرى وتستخدم كوسيلة للتوثيق**"،[4]أما التوقيع المتقدم فعرفه في الفقرة الثانية من نفس المادة على أنه **ذلك التوقيع الإلكتروني الذي يشترط فيه أن يكون مرتبط ارتباطا فريدا من نوعه مع صاحب التوقيع، وأن يكون قادرا على تحديد صاحب التوقيع والتعرف عليه باستخدامه، وأن يكون قد تم إيجاده باستخدام وسائل يضمن فيها صاحبه السرية التامة، وأن يكون مرتبط مع المعلومات المحتواة في الرسالةحيث أنه يكشف أي تغيير في المعلومات** ".

من خلال إستقراء المادتين السابقتين، يتبين لنا أن التوجيه الأروبي قد إعتمد على أداء التوقيع وظيفتين أساسيتين الأولى هي الربط بين الموقع والمستند الذي وقع عليه والثانية: وظيفة **التوثيق**[5]. والتوثيق كخاصية

---

[1]-Si une méthode est utilisée pour identifier la personne en question et pour indiquer qu'elle approuve l'information contenue dans le message de données; et

[2]-Le terme "signature électronique" désigne des données sous formeélectronique contenues dans un message de données ou jointes ou logiquementassociées audit message, pouvant être utilisées pour identifier le signataire dans le cadre du message de données et indiquer qu'il approuve l'information qui y estcontenue;

[3]- Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques, j.o nº l013 du 19-01-2000.

[4] -Art 2-1(D 1999/93/CE du PEC , du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques, j.o nº l013 du 19-01-2000) dispose que "signature électronique"، une donnée sous forme électronique، qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification;

[5]- يقصد بالتوثيق التحقق من هوية أطراف العقد تحديدا مميزا لهم عن غيرهم وان المستند الموقع منهم ينسب اليهم، أنظر: **د.إبراهيم الدوسقي**، توثيق التعاملات الإلكترونية ومسؤولية جهة التوثيق تجاه الغير المتضرر، المرجع السابق، ص1859. ويمكن أن يتحقق ذلك بتدخل **وسيط محايد للتصديق** على توقيع صاحب المستند.

يتمتع بها التوقيع الإلكتروني يرتبط بمجموعة من العناصر إما بأصل البيانات أو بسلامتها فضلا عن إرتباطه بعناصر أخرى[1].

وإن كان قد ألغى المشرع الأروبي التوجيه السابق، بإصداره النظام رقم 910-2014 الصادر عن البرلمان الأروبي المتعلق بتحديد الهوية الإلكتروني وبث الثقة في التعاملات الإلكترونية في السوق الداخلية[2]، فإنه ميز بين التوقيع إلكتروني والتوقيع الإلكتروني المتقدم محتفظا بنفس التعريف وفق التوجيه السابق، والتوقيع الإلكتروني الموصوف والذي عرفه بموجب الفقرة 12 من المادة 3 على أنه التوقيع الإلكتروني المتقدم الذي يتم إنشاءه وفق اداة إنشاء توقيع إلكتروني موصوف، و ينشأ على أساس شهادة تصديق إلكتروني موصوفة. وبالرغم من هذا التقسيم، فإنه لم يحد عن المبادىء التي إعتنقها في التوجيه الســـابق.

هذا وقد أكد المشرع الأروبي على مبدأ الحياد التقني، وذلك بعدم تمييزه بين تقنيات التوقيع الإلكتروني، ذلك هو الوضع في التوقيع الإلكتروني العادي، ذلك أن الفقرة 11 من المادة 3 التي احالت للمادة 25 تعتبر التوقيع الإلكتروني متقدم بقدر تلبيته لبعض المقتضيات، بعضها يتعلق **بعدم الإنكار** ، والثاني **بتحديد الهوية** والآخر **بسلامة المعطيات.**

أما على الصعيد الوطني، فلم تتأخر التشريعات الوطنية عن وضع تعريف للتوقيع الإلكتروني، وإن إختلفت في موضع النص عليه ما بين تحديث نصوصها القانونية القائمة من أجل الإعتداد بالتوقيع الإلكتروني وبين وضع قانون خاص بـــه.

ففرنسا ونتيجة للتطور الحاصل في المعاملات الإلكترونية من جهة، وإلتزاماتها بالتوجيهات الأوربية الخاصة بالتوقيع الإلكتروني من جهة أخرى، حتم عليها إدخال تعديلات على مواد القانون المدني الخاصة بالإثبات، وقد كان ذلك بموجب القانون رقم 2000-230 الصادر في 13 مارس 2000 المتعلق بتطويع قانون الإثبات لتكنولوجيا المعلومات والتوقيع الإلكتروني[3]، حيث تم إضافة المادة 1316-4 في القانون المدني لتعتبر بذلك مقدمة لتعريف التوقيع التقليدي[4]، وإن تـــم إلغاءها بموجب المادة 3 من الأمر رقم 2016-131[5] ، إلا أن المشرع إحتفظ بنفس المضمون بموجب المادة 1367، حيث نصت فقرتها الأولى:"**التوقيع ضروري لإتمام عقد قانوني يكشف عن هوية الشخص الذي وضع التوقيع، كما يعلن عن رضا الأطراف بالالتزام الناجم عن هذا العقد، وإذا ما وضع التوقيع بواسطة موظف عام، فإن هذا التوقيع يضفي على العقد الطابع الرسمي**".

---

[1] -**Voir** **Zahi Younes** L' incidence des nouvelles technologies sur le droit traditionnel des actes juridiques Thèse de doctorat : Droit privé : Université Panthéon-Sorbonne Paris 1 : 2002; p 304

[2] -RÈGLEMENT (UE) N° 910/2014 DU PARLEMENT EUROPÉEN ET DU CONSEILK .du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE

[3] -Loi n° 2000-230 du 13 mars 2000, portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, J.O.R.F numéro 62, 14 mars 2000.

[4] - **Eric caprioli**, Le juge et la preuve électronique.op, cit . P5.

[5] - **Ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations**

ويتضح من هذا النص أن المشرع الفرنسي قد أخذ **بالتعريف الوظيفي للتوقيع**، أيا كان شكله أو طريقة تحريره أو الوسيط الذي يستخدم في ذلك.

أما التوقيع الإلكتروني فقد نصت عليه الفقرة الثانية من نفس المادة، على أنه ومتى كان إلكترونيا فانه يتمثل في إستعمال وسيلة تحقق موثوقة تؤكد إرتباط التوقيع بالتصرف المعني، تفترض الموثوقية في وسيلة التصديق إلى غاية إثبات العكس، متى أنشيء التوقيع الإلكتروني وكانت هوية الموقع أكيدة وسلامة العقد مضمونة" ضمن الشروط المحددة بمرسوم مجلس الدولة[1].

يتضح من نص المادة أن المشرع إعتبر التوقيع الإلكتروني **وسيلة للتوثيق**[2] يسمح بتحديد هوية الموقع وسلامة الوثيقة. متخذا في ذلك مبدأ الحياد التقني، حيث تسمح عمومية العبارات الموظفة في النص مسايرتها لأي تطور تكنولوجي. ويكون بدلك المشرع الفرنسي قد سار على نهج التوجيه الأروبي.

ليأتي بعد ذلك المرسوم رقم 2001-272[3] الصادر في 30 مارس 2001 ليحدد آليات تطبيق أحكام المادة 1316-4 من القانون المدني المستخلفة بالمادة 1367. وقد ميز بموجب الفقرة الثانية منه بين التوقيع الإلكتروني العادي والتوقيع الإلكتروني المؤمن، حيث إشترط في هذا الأخير مجموعة من المتطلبات بأن يكون خاصا بصاحب التوقيع، وأن ينشا بوسائل يمكن لصاحب التوقيع أن يضعها تحت رقابته الخاصة، وأن يرتبط هذا التوقيع بالعقد اللازم له، بحيث أن كل تعديل لاحق للعقد يمكن فصله. وهو نفس التعريف الذي جاء به التوجيه الأروبي حيث عرفه كما سبق وأشرنا على مستويين.

وإلى جانب المشرع الفرنسي، نجد المشرع الجزائري قد خطا خطوة إيجابية في هذا الإتجاه، وذلك من خلال مروره بمرحلتين، المرحلة الأولى تتعلق بتعديل القانون المدني بموجب القانون رقم 05-10[4] ثم صدور المرسوم التنفيدي 07-162[5]، والثانية تتعلق بتطبيق القانون رقم 15-04[1] المتعلق بالتوقيع والتصديق الإلكترونيين.

---

[1]- **Article 1367 du CCF** Modifié par Ordonnance n°2016-131 du 10 février 2016 - art. 4**dispose que "** La signature nécessaire à la perfection d'un acte juridique identifie son auteur. Elle manifeste son consentement aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte. Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'État."

جاءت هده المادة لتؤكد المادة 25 من التوجيه الأروبي رقم 910-2014 المتعلق بتحديد الهوية الإلكتروني وبث الثقة في التعاملاتالإلكترونية في السوق الداخلية.

[2]- **Christiane Féral-Schul**, Cyberdroit, le droit à l'épreuve de l'internet, Paris, Dalloz, 6ème éd., 2010, v. n°92.11., **Eric A. CAPRIOLI**, « De l'authentification à la signature électronique : quel cadre juridique pour la confiance dans les communications électroniques internationales ? » articledisponible en ligne a l'adresse suivante: https://www.uncitral.org/pdf/english/colloquia/EC/Caprioli_Article.pdf

[3]-**Décret n°2001-272 du 30 mars 2001, pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique**, J.O. numéro 77 ,31 mars 2001

[4]– أمر رقم75-58 المؤرخ في 20 رمضان عام 1395الموافق لـــ 26 سبتمبر 1975، المتضمن القانون المدني،الجريدة الرسمية، العدد78،الصادرة في 30 سبتمبر 1975، المعدل والمتمم بموجبالقانون رقم 05-10 المؤرخ في 13 جمادى الأولى عام 1426الموافق لـــ20 يونيو 2005، الجريدة الرسمية، العدد 44، الصادرة في 26 يونيو 2005.

[5]– مرسومتنفيذيرقم 07 - 162 مؤرخفي 13 جمادى الأولىعام 1428 الموافق 30 مايوسنة 2007 يعدل ويتمّمالمرسومالتنفيذيرقم 01 - 123 المؤرخ في 15 صفرعام 1422 الموافق 9 مايوسنة 2001 والمتعلقبنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية،الجريدة الرسمية، العدد 37، الصادرة في 7 يونيو 2007.

ففي المرحلة الأولى، نظم المشرع الجزائري لأول مرة التوقيع الإلكتروني، وذلك بموجب التعديل الذي أجراه على القانون المدني رقم 05-10، دون أن يورد تعريفا له، بل إكتفى بالإعتراف بحجيتة رابطا دلك بتوفر نفس الشروط المتطلبة في الكتابة العادية، حيث نصت المادة 2/327 المعدلة بموجب القانون المذكور على أنه"... **يعتد بالتوقيع الإلكتروني وفق الشروط المذكورة في المادة 323 مكرر أعلاه..**"ونصت المادة 323 مكرر على أنه "**يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق، بشرط إمكانيةالتأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها**".

ليتدخل بعد ذلك عام 2007 بموجب المرسوم التنفيذي 07-162ليميز بين التوقيع الإلكتروني[2] والتوقيع الإلكتروني المؤمن.

وحسب ما تضمنته المادة 3 مكرر من هذا المرسوم، **فإنه يشترط في التوقيع الإلكتروني ليوصف بالتوقيع المؤمن أن يستوفي المقتضيات التـــالية:** أن يكون خاصا بالموقع. يتم بوسائل يمكن أن يحتفظ بها الموقع تحت مراقبته الحصرية. يضمن مع الفعل المرتبط به صلة ببحث يكون كل تعديل لاحق للفعل قابلا للكشف عنه.

أما المرحلة الثانية، فقد كانت بصدور القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين، ووفقا لما ورد في هذا القانون فإن للتوقيع الإلكتروني مستويين أو نوعين وهما التوقيع الإلكتروني البسيط والتوقيع الإلكتروني الموصوف ووضع لكل نوع تعريفا محددا.

فالتوقيع الإلكتروني البسيط عرفه بموجب الفقرة الأولى من المادة الثانية من القانون رقم 15-04 على أنه "**بيانات في شكل الكتروني مرفقة أو مرتبطة منطقيا ببيانات الكترونية أخرى كوسيلة توثيق**". وقد عرف هذه البيانات بموجب الفقرة 3 من نفس المادة على أنها **بيانات فريدة، مثل الرموز او مفاتيح التشفير الخاصة، التي يستعملها الموقع لإنشاء التوقيع الإلكتروني.**

من خلال هاتين المادتين، يتبين لنا أن التوقيع الإلكتروني هو جزء من الوثيقة المذيلة به لكن لا يعتبر من محتواها، يؤدي وظيفة أساسية ألا وهـــي **التوثيق**، وهو ما أكدته المادة 6 "يستعمل التوقيع الإلكتروني لتوثيق هوية الموقع وإثبات قبوله مضمون الكتابة في الشكل الإلكتروني"، دون أن يدقق في شكل التوقيع وهو توجه سليم في تقديرنا نظرا لصعوبة الإلمام بمختلف أشكال التوقيعات الإلكترونية التي تشهد تطورا يكاد يكون

---

[1] – القانون رقم 15-04 المؤرخ في 1 فبراير 2015،المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية، العدد 06، الصادرة في 10 فيفري2015 .

[2] – حيث نصت المادة 3 مكرر من المرسوم 07-162 والمتعلق بنظام الاستغلال المطبق على الشبكات، على أن التوقيع الإلكتروني هو أسلوب عمل يستجيب للشروط المحددة في المادتين 323 مكرر و323 مكرر 1 من القانون المدني

يوميا. ويظهر من ذلك تأثر المشرع الجزائري بمبدأ الحياد التكنولوجي الذي أقرته المادة الثالثة من قانون الأونسترال النموذجي الخاص بالتوقيعات الإلكترونية تحت عنوان المعاملة المتكافئة لتكنولوجيات التوقيع.

أما التوقيع الإلكتروني الموصوف: فلم يعرفه وإنما ذكر الشروط التي يجب توافرها في التوقيع حتى يكتسي وصف الموصوف، حددتها المـــادة 7 كمايلي:

أ- أن ينشأ على أساس شهادة تصديق الكترونية موصوفة

ب-أن يرتبط بالموقع دون سواه

ت-أن يتمكن من تحديد هوية الموقع

ث-أن يكون مصمما بواسطة آلية مؤمنة خاصة بإنشاء التوقيع الإلكتروني

ج- أن يكون منشأ بواسطة وسائل تكون تحت التحكم الحصري للموقع

ح- أن يكون مرتبطا بالبيانات الخاصة به بحيث يمكن الكشف عن التغييرات اللاحقة بهذه البيانات.

وتضيف المادة 8 أنه يعتبر التوقيع الإلكتروني الموصوف وحده مماثلا للتوقيع المكتوب.

يتضح من خلال ماسبق، أن المشرع يهدف إلى تحقيق مساواة قانونية بين التوقيع التقليدي والتوقيع الإلكتروني الموصوف الذي تتوفر فيه الشروط الخاصة بضمان الأمان والموثوقية، والتي لا تعتبر مطلوبة في التوقيع الإلكتروني البسيط.

ولم يكن التشريع المصري هو الآخر بمعزل عن مسايرة التطور التكنولوجي ودعم التحول إلى العالم الإلكتروني، وكان ذلك بوجب الفقرة ج من المادة 1 من القانون" **مايوضع على محرر الكتروني ويتخد شكل حروف او ارقام او رموز او اشارات او غيرها و يكون له طابع متفرد يسمح بتحديد شخص الموقع و يميزه عن غيره**"

وكما هو ملاحظ، فإن المشرع لم يحدد الأشكال التي يتخدها التوقيع الإلكتروني، بل أوردها على سبيل الحصر وهو ما يستفاد من عبارة" **أو غيرها** " الواردة في المادة السابقة، وهو مايفتح المجال أمامالإعتراف بجميع صور التواقيع الإلكترونية التي تتمتع بالثقة الكافية وتحقيق وظائف التوقيع، كما أنه أخد بنهج **النظير الوظيفي** على غرار التشريعات السابقة، حين نص "... **يسمح بتحديد شخص الموقع ويميزه عن غيره**"، لكن ما يؤخد عليه أنه أغفل الوظيفة الثانية للتوقيع ألا وهي قبوله بمضمون التصرف الذي يصدر التوقيع بمناسبته.

كما ينتقد البعض[1] نهج المشرع المصري باستخدامه في مطلع المادة "**ما يوضع على**"، على أساس أنها عبارة توحي بمادية الشكل الذي يتخذه ذلك التوقيع وهو ما لا يتماشى وطبيعة التوقيع الإلكتروني.

من خلال ما سبق، يتضح ان التشريعات الحديثة قد حررت النظرة القديمة للتوقيع التي أبقته تحت مظلة الأشكال التي يتخدها رغم ظهور التقنيات الحديثة، واتجهت صوب التعويل على الوظائف التي يؤديها

[1]- د.**تامر محمد سليمان الدمياطي**، المرجع السابق، ص 422.

التوقيع، والتوقيع الإلكتروني بدلك يحقق نفس وظائف التوقيع التقليدي، كل ما هنالك أنه ينشا عبر وسيط الكتروني، وذلك استجابة لنوعية المعاملات التي تتم الكترونيا مدنية كانت أو تجارية أو إدارية[1].

ب-تمييزالتوقيـــع الإلكتروني عن التوقيع التقلـــيدي

رغم كون التوقيع الإلكتروني والتوقيع التقليدي من أهم الآليات المعتد بها في إثبات التصرفات القانونية، إلا أنهما يختلفان من عدة نواح أهمها:

1-من حيث الوسيط الذي يوضع عليه التوقيع: في حين يتم التوقيع التقليدي على وسيط مادي هو في الغالب دعامة ورقية، نجد أن التوقيع الإلكتروني يتم كليا أو جزئيا عبر وسيط الكتروني غير محسوس، وعند إرتباطه بالكتابة يتحول إلى مستند صالح للإثبات.

2-من حيث الوظائف التي يؤديها التوقيع: في حين يؤدي التوقيع التقليدي دور ثنائي الأبعاد، فهو وسيلة لتحديد هوية الموقع وتمييز شخصيته، وتعبير عن إرادته في الإلتزام بمضمون الورقة، فإن التوقيع الإلكتروني يناط به فضلا عن الوظيفتين السابقتين انه يسمح بالتعاقد عن بعد، ويحقق قدرا من الأمن والثقة في صحة التوقيع وانتسابه لصاحبه والتحقق من سلامة مضمون المستند وتامينه من التعديل بحيث يختلط بالمستند على نحو لا يمكن فصـــله[2].

3-من حيث مدى حرية الشخص في إختـــيار شكل توقيعه:فبينما يتمتع الشخص في التوقيع التقليدي بإختيار الصورة التي ستفرغ فيها توقيعه سواء بالبصمة أو بالختم، أو قد يجمع بين أكثر من صورة، فإنه لا خيار للمتعاقدين في الصوة التي سيفرغ فيها التوقيع الإلكتروني، إذ القائم بإصدار التوقيع سلطة مقدمي خدمات التصديق وفقا لشرائط تقنية تتم بالسرية والخصوصية والأمـــان[3].

4- من حيث الأطراف: في التوقيع التقليدي طرفين فقط، المنشيء والمرسال إليه، أما في التوقيع الإلكتروني ثلاثة أطراف المنشيء والمرسل إليه ومزود خدمة التصديق أو الطرف الثالث الموثوق حسب نوع المتدخلين.

5-من حيث ترك الأثـــر: إن الإعتداء على التوقيع التقليدي كتزويره يترك أثرا في كثير من الأحوال يدل عليه، ولا يفرض على صاحبه عند اكتشاف التقليد أو التزوير تغيير شكل توقيعه، على عكس التوقيع

---

[1]- فالتصرفات القانونية المدنية كعقود البيع والإيجار بين الأشخاص العاديين، والإقرار أو الوقف أو الوصية، كل هذه معاملات مدنية تتطلب توقيع ذوي الشان، ويمكن توقيعها الكترونيا.

كما أن التوقيع الإلكتروني يساعد الإدارة على سرعة إنجاز معاملاتها سواء تعلقت بالعقود الإدارية أو القرارات الإدارية، نظرا للسرعة والدقة و صعوبة تزويره، وذلك في ظل تحول جهات الإدارة في معظم بلدان العالم إلى "**الحكومة الإلكترونية**" .

أما بالنسبة للمعاملات التجارية الإلكترونية فقد أصبح التوقيع الإلكتروني يحقق الغاية المقصودة من هذه المعاملات وهو سرعة الحركة وحسن المبادرة وحسم الموقف وإتخاذ القرار دون تردد، إذ يمكن لمستورد في الجزائر و بعد معاينة البضاعة عبرالأنترنت ان يتعاقد على شراءها من مورد في كندا في ساعات معدودة عن طريق التعاقد عبر الأنترنت وبعد تأكده من صحة التوقيعات الخاصة بالطرف الآخر عن طريق مزود الخدمة، وهي عملية قد لا تتجاوز ساعات محدودة.**د. عبد الفتاح بيومي حجازي**، النظام القانوني للتوقيع الإلكتروني، المرجع السابق، ص370.

[2]- د. **ممدوح على مبروك**، مدى حجية التوقيع الإلكتروني في الإثبات، دار النهضة العربيـــة، القـــاهرة، 2005، ص 47، **د. تـــامر محمـــد ســـليمان الدمياطي**، المرجع السابق، ص375.

[3]-**د. ممدوح على مبروك**، المرجع السابق، ص46.

الإلكتروني فإنه يصعب إكتشافه والوقوف على مرتكب التزوير كون هذا التوقيع قد يتألف من شفرة تحدد هوية الموقع وهذه الشفرة يمكن التدخل فيها أو محوها، وتبعا لذلك يفرض على صاحبه تغيير توقيعه إن اكتشف توصل الغير إلى المنظومة التي تنشئه[1].

6-من حيث نطاق الحماية الجزائية: بينما يتصور إنطباق كافة النصوص المتعلقة بحماية التوقيع التقليدي كجرائم إختلاس التوقيع و الإكراه بالتوقيع على سند وتزوير التوقيع، فإن نطاق الحماية الجزائية للتوقيع الإلكتروني أكثر إتساعا، بحيث تشمل فوق ذلك، الدخول غيرالمشروع على قاعدة معطيات تتعلق بالتوقيع الإلكتروني وفض مفاتيح الشتفير وغيرها من الجرائم التي لا تنطبق إلا في البيئة الإلكترونية[2]

ثانيا- صور التوقيـــع الإلكـــتروني

لم تحدد أغلب التشريعات نوعا معينا من التواقيع الإلكترونية، بل تركت المجال مفتوحا كي يتسع لإستيعاب ما يستجد من تقنيات تفرز تواقيع جديدة، وعمليا فإن التوقيع الإلكتروني يتخذ ما يعرف بالتوقيع الرقمي، كما يظهر بصور أخرى بحسب الطريقة التي يتم بها، كما تختلف هذه الصور فيما بينها من حيث درجة الثقة ومستوى ما تقدمه من ضمان بحسب الإجراءات المتبعة في إصدارها وتأمينها، وهذا ما سنراه من خلال النقاط المتقدمة من هذا العنصر.

أ- التوقيع الرقـــمي

ويسمى أيضا التوقيع بواسطة المفتاح، وسمي رقميا لأنه يحتوي على رقم سري لا يعرفه سوى صاحبه، ووفقا لمعيار الإيزو رقم ISO 7498-2 المتعلق ببنية الأمان للأنظمة المفتوحة الصادر عن المنظمة الدولية لتوحيد المقاييس، يقصد بالتوقيع الرقمي بيان يتصل بوحدة معطيات أو تحويل تشفيري لوحدة من المعطيات، على نحو يسمح للمرسل إليه بإثبات مصدر وحدة المعطيات وسلامة مضمونها وتأمينها ضد أي تعديل أو تحريف[3]. كما عرفه البعض على أنه عبارة عن مجموعة أرقام أوحروف يختارها صاحب التوقيع، ويتم تركيبها أو ترتيبها في شكل غير مقروء، ويتم عن طريقه تحديد شخصية صاحبه، بحيث لايكون معلوما إلا له فقط[4].

---

[1]- **عيسى غسان ربضي**، المرجع السابق، ص87. **د. اشرف توفيق شمس الـــدين**، الحماية الجنائية للمستند الإلكتروني ، مؤتمر الأعمـــال المصـــرفية الإلكترونية، المرجع السابق، ص537،

[2]- **أيمن رمضان محمد أحمد**، الحماية الجنائية للتوقيع الإلكتروني، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 2010، ص36.

[3] -**signature numérique** Données ajoutées à une unité de données, ou transformation cryptographique (voir **cryptographie**) d'une unité de données, permettant à un destinataire de prouver la source et l'intégrité de l'unité de données et protégeant contre la contrefaçon (par le destinataire, par exemple).
Voir ISO 7498-2:1989(fr);Systèmes de traitement de l'information — Interconnexion de systèmes ouverts — Modèle de référence de base — Partie 2: Architecture de sécurité disponible
https://www.iso.org/obp/ui/fr/#iso:std:iso:7498:-2:ed-1:v1:fr

[4]- **د. إبراهيم الدوسقي أبو الليل**، توثيق المعاملات الإلكترونية ومسؤولية جهة التوثيق اتجاه الغير المتضرر، المرجع السابق، ص1853.

من السمات الرئيسية للتوقيعات الرقمية هو إستخدام التشفير[1]، إذ يعتمد على اللوغرتميات أو المعادلات الرياضية حيث تتحول الكتابة العادية المقروءة إلى لغة الأرقام وهي لغة خاصة غير مقروءة[2].وقد تعرض القانون الفرنسي رقم 575-2004 المتعلق بالثقة في الإقتصاد الرقمي في المادة 29 منه الى تعريف طريقة التشفير بأنها **أي أداة أو برنامج يتم تصميمه أو تعديله لأجل تحويل المعطيات سواء كانت تتعلق بمعلومات او رموز، وذلك عن طريق الإستعانة باتفاقات سرية، أو لإجل انجاز عملية عكسية باتفاق سري او بدونه، وغرض طرق التشفير المشار اليها هو ضمان سلامة تخزين المعطيات أو تحويلها من خلال إتاحة ضمان سريتها، وتوثيقها أو التحقق من سلامتها**" **كما تشير ذات المادة الى أنه يقصد بخدمة التشفير أية عملية تهدف الى بدء تنفيذ طرق تشفير لحساب الغير**".

وتستخدم التوقيعات الرقمية في الغالب ما يعرف باسم **التشفير غير المتماثل** ، وهو تشفير يقوم على استخدام خوارزمية وحيدة ومفتاحين مختلفين أحدهما يستخدم للتشفير والآخرلفك التشفير، بحيث كل مستخدم يملك مفتاحين مرتبطين رياضياً: **مفتاح عام ومفتاح خاص،** ونظرا لأهمية التشفير في مجال التعاملات الإلكترونية ، فقد اهتمت بعض التشريعات بوضع تعريف توضيحي لهده المفاتيح، حيث قرر المشرع الجزائري بموجب الفقرة 8 من المادة 2 من قانون التوقيع الإلكتروني ان مفتاح التشفير الخاص هو **عبارة عن سلسلة من الأعداد يحوزها حصريا الموقع فقط، وتستخدم لإنشاء التوقيع الإلكروني و يرتبط هدا المفتاح بمفتاح تشفير عمومي،** اما مفتاح التشفير العمومي فقد عرفه بموجب الفقرة 9 من ذات المادة على أنه **عبارة عن سلسلة من الأعداد تكون موضعة في متناول الجمهور بهدف تمكينهم من التحقق من الإمضاء الإلكتروني و تدرج في شهادة التصديق الإلكتروني.**

وفي ذات الإتجاه تشير المادة 1-12 من اللائحة التنفيدية لقانون التوقيع الإلكتروني المصري أن المفتاح الخاص هو **أداة الكترونية خاصة بصاحبها تنشا بواسطة عملية حسابية خاصة و تستخدم في وضع التوقيع الإلكتروني على المحررات الإلكترونية، ويتم الإحتفاظ بها على بطاقة ذكية مؤمنة**" أما المفتاح العام فتعرفه المادة1-11 من اللائحة التنفيدية على أنه أداة إلكترونية متاحة للكافة ، تنشأ بواسطة عملية حسابية خاصة ، وتستخدم فى التحقق من شخصية الموقع على المحور الإلكترونى، والتأكد من صحة وسلامة محتوى المحرر الإلكترونى الأصلى.

يتضح من خلال التعريفات السابقة، أن المشرع الجزائري كان أكثر توفيقا من نظيره المصري فيما يخص المصطلحات التي وظفها، ذلك أن هدا الأخير إستخدم لفظ" **أداة**"، وهو لفظ يوحي بالطبيعة المادية الذي يتشابه مع لفظ الوسيلة، وهو مالا يتماشى ونصه" **تنشا بواسطة عملية حسابية خاصة**"، ليرجع ويضيف" **الإحتفاظ بها على بطاقة دكية مؤمنة**"، فيستخلص بدلك أن هذا المفتاح عبارة عن مجموعة من الرموز و الأرقام[3]. هذا من جهة.

---

[1]- **Dominique Mougenot**, droit des obligations la preuve ; 3 edition; larcier, s,abruxelles, 2002, p 170

[2]-**د. عبد الفتاح بيومي حجازي**، النظام القانوني للتوقيع الإلكتروني، المرجع السابق، ص400.

[3]- ويتم التوصل للرموز والأرقام المكونة للمفتاح الخاص عن طريق الرقم الشخصي لصاحب المفتاح، أنظر:

من جهة أخرى، نلاحظ أن المشرع المصري حصر وسيلة الإحتفاظ بالأداة الإلكترونية في **بطاقة ذكية مؤمنة**، وهو ما يتعارض ومبدأ الحياد التقني الذي صار عليه المشرع، فكان الأولى أن يترك الباب مفتوحا أمام ما يظهر من تقنيات حديثة يمكنها أداء ذات الوظيفة[1].

وعموما، ينشر المستخدم مفتاحه العام ويحتفظ بالمفتاح الخاص بشكل سري. يقوم المرسل بتشفير الرسالة باستخدام المفتاح العام للمرسل إليه ويستخدم المستلم مفتاحه الخاص للتشفير ولا يمكن فك تشفير النص بغير هذا المفتاح. وعادة ما يتم تخزين المفتاح الخاص ضمن البطاقات الذكـية[2].

والتشفير على النحو السابق، لا يحقق السرية للمستند أو للمعطيات بصفة عامة فحسب، بل يحـافظ على سلامتها ويسمح بتحديد مصدر التغييرات، غير المصرح بها، كما يثبت هوية الأطراف، بل أنه يضمن عدم الإنكار من الموقع على أساس أن التوقيع تم إنشاءه وفق بيانات فريدة[3].

الشيء الرئيسي الذي يتعلق بالمفاتيح العامة هو موثوقية المفتاح العام، بالتالي هناك مشكلة توليد مفاتيح عامة مزورة ونشرها, وهذا ما يعرف باسم (man in the middle attack), تم حل هذه المشكلة بشكل نموذجي باستخدام معلومة تحقق من الهوية وتبعية المفتاح تسمى **الشهادة الرقمية** وهي تزود من قبل طـرف ثالـث موثوق، الشهادة الرقمية كانت الحل النموذجي لتغطية مثل هذه الثغرات، كما كانت الوسيلة النموذجية لنقـل المفاتيح العامة عبر الإنترنت[4].

ب- بعض التوقيـعات الإلكترونيـة الأخـرى

1- التوقيـع البيومتـري

هو إمضاء يعتمد على الصفات الجسدية للشخص، ومن بينها بصمات أصابع اليد أو الإبهـام أو قزحيـة العين،وهي الأكثر إستعمالا في التطبيق، وتعتمد هذه الطريقة عمليا على خـزن الصـورة بصـفة رقميـة ومضغوطة في الذاكرة الصلبة للحاسوب – أو في البطاقة الذكيةـ وعندما يتولى الشخص إدخال بطاقته في

---

[3]**Pierre BreeseK Gautier Kaufman**, Guide juridique de l'Internet et du commerce électronique ; vuibert;paris,2000, p320,321.

[1]-د. **تامر محمد سليمان الدمياطي**، المرجع السابق، ص439.

[2]– والبطاقات الذكية ينظر إليها بإعتبارها مكانا لتخزين المفتاح الخاص للتوقيع، وبها وحدة معالجة مركزية داخل البطاقة، ويمكن للمفتاح الخاص أن يستقل عن البطاقة الذكية، ويمكن أن يبرمج بحيث لا ينفصل عنها، وهذا يؤكد على وجود نسخة واحدة فقط من المفتاح الخاص، والوصول إلى هذا المفتاح يحقق مزيدا من الحماية من خلال رقم PIN أو كلمة المرور، وعلى ذلك فإن التوقيع الرقمي يمكن أن ينتج عن البطاقة الذكية نفسها من أجل التأكد من وجود مستوى عال جدا من الأمن. **أمين عزان**، الحماية الجنائية للتجارة الإلكترونية، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، ص265.

[3]**Maxime Wack, Nathanael Cottin, Bernard Mignot, Abdellah ElMoudni**, CERTIFICATION ET ARCHIVAGE LÉGAL DE DOSSIERS NUMÉRIQUES.*revue Document numérique*. Lavoisier. 1/2002 .Vol. 6. P150

[4]- **نسرين هاني علم الدين**، دراسة الحل الأمثل لبناء نظام مركز لتوليد الشهادات الرقمية المستخدمة في أمن المعلومات، رسالة دكتوراه، جامعة دمشق، كلية العلوم، دون تاريخ، ص25.

-**Dominique Mougenot**, op;cit**,** p172 et s

الآلة القارئة للموزع الإلكتروني للأوراق النقدية، تقوم تلك الآلة بالتقاط صورة حينية لقزحية العين مثلا تدرج اليا في سجل رقمي و تقع مقارنته بالسجل الرقمي الموجود على البطاقة او على حاسوب المنظومة[1].

ويعيب على طرق التوقيع البيومترية إمكانية مهاجمتها أو نسخها من قراصنة الحاسب الآلي عن طريق فك شفرتها، كما نسب إليها أنها تفتقر إلى الأمن والسرية، حيث تعمل الشركات المنتجة للطرق البيومترية على توحيد نظم عملها كما أنها لا تقدم نتائج كاملة الصحة[2].

2- التوقيع بالقلـــم الإلكتـــروني

يعتبر التوقيع بالقلم الإلكتروني صورة من صور التوقيع البيومتري لأنه يعتمد على التوقيع الشخصي، حيث يقوم المتعامل بكتابة توقيعه الشخصي باستخدام قلم الكتروني خاص على شاشة جهاز الحاسب الآلـــي، وهذا يستوجب جهاز حاسب الي ذا مواصفات خاصة تمكنه من أداء مهمته في التقاط التوقيع من شاشته[3].

يتم التأكد من صحة هذا التوقيع بمضاهاة التوقيع الخطي المرسل بهذا القلم الإلكتروني الخاص بالتوقيع المخزن في ذاكرة الكمبيوتر، وذلك من خلال الإستناد على حركة القلم الإلكتروني والأشكال التي يتخدها من إنحناءات أو التواءات وغيرها من السمات الخاصة بالتوقيع الخـــاص بالموقع[4].

3-**التوقيع باستخدام البطاقة الممغنطة المقترنة بالرقم السرى**(P.I.N) وهى الطريق الاكثر شيوعاً خاصة فى المعاملات البنكية، ونظرا لكون هذه البطاقة ستكون محل دراسة معمقة في المبحث الثالث من هذا الفصل فنحيل إليها حرصا على عدم التكرار.

ثالثا- شروط صحـــة التوقيع الإلكترونـــي

تستلزم دراسة الحماية الجنائية للتوقيع الإلكتروني الوقوف على حماية حجيته، دلك ان المساس بهده الحجية يؤثرعلى اقتصاد مؤسسات كبرى الدول فضلا عن فقدان الثقة فيه.

ولكي يتمتع التوقيع الإلكتروني بالحجية القانونية في الإثبات، فلا بد أن يتوفر فيه شروط يمكن ردها إلى الوظيفة التي يؤديها، وهي تحديد هوية الموقع والتعبير عن إرادته في الإلتزام بما وقع علي،إلا أنه ونظرا لكون العديد من تطبيقاته تتم الكترونيا ومن تم إمكان تقليده وتزويره، فقد خلق مشكلة الثقة فيه والتعويل عليه، فكان من الضروري البحث عن أمـــور **تعزز** هذه الثقة. وهو ماكرسته العديد من التشريعات التي أضفت عليه الحجية طالما توافرت فيه الشروط التي توفـــر هذه الثقة.

---

[1]- **Dominique Mougenot**, op;cit , P 169

[2]- **عادل محمود شرف، عبد الله إسماعيل عبد الله،** ضمانات الأمن والتامين في شبكة الأنترنت، مؤتمر القانون والكمبيوتر والأنترنت، الإمارات العربية المتحدة، مايو ، ص3، مشار إليه لدى: **د. إبراهيم الدوسقي أبو الليل**،توثيق المعاملات الإلكترونية ومسؤولية جهة التوثيق اتجاه الغير المتضرر، المرجع السابق، ص1855.

[3]- **د. إبراهيم الدوسقيأبو الليل،** الجوانب القانونية للتعاملات الإلكترونية، المرجع السابق، ص161.

[4]-**Article 2 du Décret n°2001-272 dispose que "** La fiabilité d'un procédé de signature électronique est présumée jusqu'à preuve contraire lorsque ce procédé met en oeuvre une signature électronique sécurisée, établie grâce à un dispositif sécurisé de création de signature électronique et que la vérification de cette signature repose sur l'utilisation d'un certificat électronique qualifié".

فالمشرع الفرنسي حدد شروط تحقق التوقيع الإلكتروني المؤمن،ومن تم تمتعه بالحجية في الإثبات بموجب أحكام المرسوم رقم 2001-272،علاوة على ما جاء في الفقرة 2 من المادة 1367 من القانون المدني، والملاحظ من خلال الفقرة 2 من المادة 1 من المرسوم السابق، أن المشـــرع حدد خصائص التوقيع الإلكتروني المؤمن دون تحديد منه على وجه الدقة كيفية تعيين كل من هذه الخصائص على حدة. وانما أشار فقط في المادة 2[1] منه إلى إفتراض **موثوقية** وسيلة التوقيع المستخدمة متى كانت تنشيء توقيعا الكترونيا مؤمنا، وأن هذا الأخير ينشأ بفضل منظومة انشاء توقيع الكتروني مؤمنة، وان يعتمد التحقق من صحة هذا التوقيع على إستخدام شهادة تصديق الكتروني مؤهلة.

وعلى نفس النهج سار المشرع الجزائري في قانون التوقيع الإلكتروني، حيث ميز بين التوقيع الإلكترني وبين التوقيع الإلكتروني الموصوف، واشترط لمعادلة التوقيع الإلكتروني بالتوقيع المكتوب أن يكون هذا الأخير موصوفا بأن تتطلب فيه جملة من الشروط التي حددتها المادة 7، دون تحديد منه بصورة مباشرة كيفية تحقق خصائص التوقيع الإلكتروني الموصوف من الناحية الفنية والتقنية، وذلك على خلاف بعض التشريعات التي تولت ذلك كما هو حال المشرع المصري، من خلال اللائحة التنفيذية لقانون التوقيع الإلكتروني.

وبوجه عام، فإن كافة المسائل المرتبطة بتحقق حجية التوقيع الإلكتروني في الإثبات ترتبط في مجملها **بموثوقية** ذلك التوقيع من الناحية الفنية، وهو ما سنعمل على تحليله فيمايلي مستثنين بدلك الشرط المتعلق بضرورة إنشاءه على أساس شهادة تصديق الكتروني موصوفة، كوننا سنتعرض له بالدراسة في المكان المخصص لدراسة التصديق على التوقيع الإلكتروني.

أ-أن يرتبط بالموقع دون سواه:

ومؤدى ذلك من الناحية القانونية أن يسمح التوقيع بتحديد هوية الموقع فقط دون غيره، وذلك بإســتخدام بياناته المتعلقة بتحديد الهوية. فللاعتداد بالتوقيع في ترتيب آثاره القانونية ينبغي أن يتيح هذا التوقيع لإطراف العلاقة القانونية الآخرين تحديد هوية الموقع ، أما إذا لم يكشف التوقيع هوية صاحبه، ولم يكن محدداً لذاتيته فإنه لا يعتد به في إضفاء الحجية القانونية على المستند لتعذر نسبة التصرف الوارد به لشخص معين، وهــو ما نصت عليه صراحة المادة 1367 مدني فرنسي في فقرتها الثانية ..."ومتى كان الكترونيا فانه يتمثل في إستعمال وسيلة تحقق موثوقة تؤكد ارتباط التوقيع بالتصرف المعني..."، وكذلك فعل المشرع الجزائري فــي الفقرة 3 من المادة 7 والمادة 323 من القانون المدني التي احالت الى المادة 323 مكرر 1، ولعل من أكثــر التوقيعات التي تحقق هذه الخاصية دونما منازع هو التوقيع القائم على التشفير، فمثلا بواسطة المفتاح العــام

[1]-Article 2 dispose que" La fiabilité d'un procédé de signature électronique est présumée jusqu'à preuve contraire lorsque ce procédé met en oeuvre une signature électronique sécurisée, établie grâce à un dispositif sécurisé de création de signature électronique et que la vérification de cette signature repose sur l'utilisation d'un certificat électronique qualifié."

يستطيع المرسل إليه التحقق من هوية الشخص الموقع وذلك من خـــلال الرجـــوع إلـــى شـــهادة التصـــديق الإلكتروني المبعوثة مع المستند الإلكتروني أو المنشورة على الموقع الإلكترونـــي الخـــاص بالجهـــة التـــي اصدرتها[1].

فضلا عن تعبيره عن إرادة الموقع في الإلتزام بالتصرف القانوني الذي يتضمنه المستند الإلكتروني، ويدل على رضائه به وإقراره له[2].

هذا وقد حدد المشرع المصري كيفية تحقق هذا الشرط من الناحية الفنية والتقنية، بموجب المادة 9 من اللائحة التنفيذية، حيث وضح ذلك من خلال الإستناد إلى منظومة تكوين بيانات إنشاء توقيع الكتروني مؤمنة، وهي منظومة يتم بواسطتها تكوين بيانات إنشاء التوقيع الإلكتروني إستوفت جملة من الشروط والضوابط الفنية والتقنية، وتوافرت إحدى الحالتين الأتيتين: ان يكون هذا التوقيع مرتبط بشهادة تصديق الكتروني معتمدة ونافذة، وان يتم التحقق من صحة التوقيع الإلكتروني.

ب-أن يكون مصمما بواسطة آلية مؤمنة خاصة بانشاء التوقيع الإلكتروني:

تعد منظومة إنشاء التوقيع الإلكتروني حسب المرسوم الفرنسي رقم 272-2001 وقانون التوقيع الإلكتروني الجزائري معدات أو برامج حاسوبية تختص بوضع بيانات إنشاء التوقيع الإلكتروني موضع التطبيق، ولم يحدد كلا القانونين بأي شكل من الأشكال دورها في إنشاء التوقيع ذاته حسبما يشير اليه عنوانها، أمـــا المشرع المصري فقد كان أكثر دقة حيث فرق بموجب الفقرة 18 و19 من اللائحة التنفيذية بين منظومة تكوين بيانات إنشاء التوقيع الإلكتروني والتي يتم بواسطتها تكوين بيانات الإنشاء _والتي توازي منظومة الإنشاء حسبما عرفها المشرع الفرنسي والجزائري- وبين منظومة انشاء التوقيع التي يتم بواسطتها التوقيع الكترونيا على المستند باستخدام بيانات الإنشاء وشهادة التصديق الإلكتروني. ويتم بواسطتها وضع وتثبيت المستند الموقع الكترونيا على دعامة الكترونية.

إلا أنـــه ولكي يكون التوقيع الإلكتروني موصوفا، يجب أن يكـــون مصمم بواسطة منظومة إنشاء **مؤمنة**، وقد حددت التشريعات المختلفة ضمن قوانينها الشروط والضوابط اللازمة لإعتبارها كدلك، حيث نصت المادة 3 [3]من المرسوم الفرنسي 30 مارس 2001 على هذه الشروط، وهي أن تتضمن بوسائل تقنية

---

[1]- **عيسى غسان ربضي**، المرجع السابق، ص181.

[2]- **د.ممدوح محمد على مبروك**، المرجع السابق، ص140.

[3]- Article 3 du**Décret n°2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique** Modifié par Décret n°2002-535 du 18 avril 2002 - art. 20 JORF 19 avril 2002dispose que " Un dispositif de création de signature électronique ne peut être regardé comme sécurisé que s'il satisfait aux exigences définies au I et que s'il est certifié conforme à ces exigences dans les conditions prévues au II.
I. - Un dispositif sécurisé de création de signature électronique doit :
1. Garantir par des moyens techniques et des procédures appropriés que les données de création de signature électronique :
a) Ne peuvent être établies plus d'une fois et que leur confidentialité est assurée ;

وإجراءات ملائمة، أن بيانات إنشاء التوقيع الإلكتروني لا يجوز إنشاؤها أكثر من مرة وأن تكون سريتها مكفولة. فضلا عن عدم جواز الإهتداء إليها عن طريق الإستنتاج، وأن يكون التوقيع الإلكتروني محميا ضد أي تزويـــر.

فضلا على إمكانية حمايتها بصورة مقبولة من جانب الموقع إزاء كل إستخدام من قبل الغير، وألا تؤدي إلى أي تحريف في مضمون المستند المراد توقيعه، وألا تشكل عقبة تحول دون علم الموقع علما تاما بذلك المضمون قبل توقيعه لـــه.

وقد نقل المشرع الجزائري نص المادة السابقة حرفيا من المشرع الفرنسي بمقتضى المادة 11 ، كما حددت اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري إيضاح هده الشروط في المادة 2 منها، لتأتي متطابقة في ذلك مع مضمون المادة 3 من المرسوم الفرنسي والمادة 11 من قانون التوقيع الإلكتروني الجزائري، مع إختلاف نوعا ما في الصياغة.

ت-أن يكون منشأ بواسطة وسائل تكون تحت التحكم الحصري للموقع:

وهو ما يعني ضرورة أن تتحقق سيطرة الموقع المنفردة على وسائل إنشاء التوقيع الإلكتروني، وهذا ما نصت عليه الفقرة 2 من المادة 1[1] من المرسوم الفرنسي 272-2001، والفقرة 5 من المادة 7 من قانون التوقيع الإلكتروني الجزائري، والفقرة ب من المادة 18 من قانون التوقيع الإلكتروني المصري. ووسائل إنشاء التوقيع تعني مفاتيح التشفير الخاصة أو السرية أو أي عناصر أخرى يمكن أن تستخدم في عملية إنشاء توقيع الكتروني. ويمكن تخزين المفتاح الخاص اللازم لإنشاء التوقيع الإلكتروني المؤمن على قرص صلب للحاسوب أو على دعامة خارجية خاصة كالبطاقة الذكية[2]، وتبين المادة 1-5 من المرسوم الفرنسي منظومة إنشاء التوقيع الإلكتروني على أنها عبارة عن معدات أو برامج حاسوبية مخصصة لتطبيق بيانات إنشاء التوقيع الإلكتروني، وهو نفس التعريف الذي أخد به المشرع الجزائري.

هدا وقد حددت المادة 19 من اللائحة التنفيذية للقانون الأخير الضوابط الفنية والتقنية اللازمة لتحقق ذلك، وذلك عن طريق حيازة الموقع لأداة حفظ المفتاح الشفري الخاص متضمنة البطاقة الدكية المؤمنة والكود الســـري المقترن بها.

والجدير بالذكر أنه بمجرد حصول هذه السيطرة المباشرة والحصريه يترتب علـــى ذلـــك بشـــكل قـــاطع ومباشر، أنه إذا وضع التوقيع الالكتروني على مستند ما، فإنه يجعل التصرف القانوني المرتبط به ثابتاً فـــي مواجهة المنسوب إليه الـــتوقيع .

---

b) Ne peuvent être trouvées par déduction et que la signature électronique est protégée contre toute falsification ;
c) Peuvent être protégées de manière satisfaisante par le signataire contre toute utilisation par des tiers.
2. N'entraîner aucune altération du contenu de l'acte à signer et ne pas faire obstacle à ce que le signataire en ait une connaissance exacte avant de le signer".

[1]Article 1-2 du **Décret n°2001-272** être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ;-

[2]- **د. تامر محمد سليمان الدمياطي**، المرجع السابق، ص598.

ث- أن يكون مرتبط بالبيانات الخاصة به بحيث يمكن الكشف عن التغييرات اللاحقة بهذه البيانات:

وقد حدد المشرع المصري بموجب المادة 11 من اللائحة التنفيذية طريقة كشف هذا التعديل باستخدام تقنية شفرة المفتاحين العام والخاص، وبمضاهاة شهادة التصديق الإلكتروني وبيانات إنشاء التوقيع الإلكتروني بأصل هذه الشهادة وتلك البيانات، أو بأي وسيلة مشابهة، وهو ما فعله المشرع الجزائري، كما أغفل تحديد المكلف بعبء الإثبات، سيما وأن الجرائم التي يكون التوقيع الإلكتروني محلا لها ترتكب عن بعد، ويتعذر على الدائن أن يثبت عكس ذلك في غياب إمتلاكه التقنية اللازمة[1].

ومن جانب آخر، يجب التفرقة في محل التوقيع الإلكتروني، فإذا كان مستند رسمي إكتسب التوقيع ما للمستندات الرسمية من حجية، أما إذا كان عرفي فإن التوقيع يكتسب ذات الحجية للمحررات العرفية ويخضع لنفس قواعده في الإثبات.

يتضح مما سبق، أن التوقيع الإلكتروني يتمتع بالحجية في الإثبات، و يرتبط إرتباطا وثيقا بدرجة الأمان والثقة التي يوفرها التوقيع الإلكتروني لدى المتعاملين به.

وتجدر الإشارة إلى أن المشرع الفرنسي قد رتب على تحقق هذه الشروط ، قرينة قانونية بسيطة على صحة هذا التوقيع تفيد بتحقق حجيته وجدارته لإداء دوره في الإثبات. وهو ما نصت عليه الفقرة 2 من المادة 1367 من القانون المدني، والمادة 2 من المرسوم 272-2001.[2]

وعلى خلاف الوضع في فرنسا، نجد أن كل من المشرع الجزائري والمصري، لم يقرا صراحة وجود قرينة على **موثوقية** وسيلة التوقيع الإلكتروني المستخدمة رغم إشارتهما إلى ضوابط تحقق شروط الحجية.

إلا أنه في المقابل، نجد أن المشرع الجزائري قد نقل حرفيا الفقرة 2 من المادة 1367 (المادة 1316-4 سابقا) من القانون المدني الفرنسي بموجب المادة 5 من قانون عصرنة العدالة، حيث نصت "**تفترض الموثوقية في وسيلة التصديق إلى غاية إثبات العكس متى أنشيء التوقيع الإلكتروني وكانت هوية الموقع أكيدة وسلامة العقد مضمونة**". ومن ثم نخلص من هذه المادة أن موثوقية التوقيع الإلكتروني أصبحت عنصرا أساسيا في المنظومة التشريعية المعمول بها حاليا في الجزائر والمنظمة لأنشطة وزارة العدل والمؤسسات التابعة لها وكذا الجهات القضائية، وذلك على خلاف المشرع الفرنسي الذي جعل من نطاق التطبيق عاما.

فضلا عما سبق، تطلبت التشريعات شرط تعزيز التوقيع بشهادة تصدر من طرف محايد يصادق على صحة هوية المرسل لكي يتساوى مع التوقيع المكتوب، ونظرا لأهمية هذا الشرط كون التعامل يتم عن بعد وعبر وسائل الكترونية مما يثير مسالة الجهالة بالطرف الأخر، فضلنا دراسته من جوانب عديدة، فضلا عن الإشكالية التي يثيرها في حالة تخلفه من ناحية حجية التوقيع الإلكتروني وآلية حلها.

---

[1]-**ايمن رمضان محمد أحمد**، المرجع السابق، ص70.

[2]-اكثر تفاصيل، انظر.**د. تامر محمد سليمان الدمياطي**، المرجع السابق، ص603 وما بعدها.

الفرع الثـــاني

التصـــديق[1] على التوقيـــع الإلكـــتروني

يحتاج التوقيع الإلكتروني لكي يكون مصدقا إلى **صدور شهادة تصديق خاصة به** من قبل **جهة معينة** تتولى تلك المهمة، وهو ما أشارت إليه بعض التشريعات صراحة كما هو حال المشرع الفرنسي، حيث ربط الإعتراف بموثوقية وسيلة التوقيع بتقديم هذه الشهادة، وذلك بموجب الفقرة 2[2] من المرسوم 2001-272 repose sur l'utilisation d'un certificat électronique qualifié."، وكذلك فعل المشرع الجزائري بموجب المادة 7 من قانون التوقيع الإلكتروني حينما نص "**أن ينشأ على أساس شهادة تصديق الكتروني موصوفة**"، مع الإشارة إلى أن المشرع أخضع التصديق والتوقيع الإلكترونيين للوثائق والمحررات الصادرة عن قطاع العدالة لأحكام القانون 15-03 المتعلق بعصرنة العدالة.

وكون التصديق على هذا النحو يقوم دليلا على صحة التوقيع الإلكتروني، ويدفع الغير إلى إعتماد الوثائق المرفقة بهذا التوقيع ومن ثم التعامل الكترونيا مع صاحب التوقيع، فإن الأمر يتطلب إبتداء تحقق الثقة في الجهة التي تصدق على التوقيع الإلكتروني، ولهذا حرصت القوانين على إختلافها على تنظيم المركز القانوني لمزود خدمة التصديق على التوقيع الإلكتروني وفرض شروط معينة في من يقدم هذه الخدمة، فلا شك أن دلك يعد **أحد أهمعناصر الحماية للتوقيع الإلكتروني**، فبقدر التزامه بقدر ما تتضاءل المخاطر الناجمة عنه.

إن الإحاطة بالأفكار المتقدمة يوضح مفهوم التصديق على التوقيع الإلكتروني، كونه وسيلة لدرء المنازعات مستقبلا في صحة هذا التوقيع، ولبيان تلك الأفكار تفصيلا قسمنا هذا الفرع إلى ثلاثة عناصر كمايلي :

أولا- التعريف بمزود خدمـــة التصـــديق الإلكتـــروني

يندرج هذا الوسيط ضمن القسم الثاني من الوسطاء في التعامل الإلكتروني وهو "**الوسيط النظامي**"[3]، بسبب أن لـــه أثر في المركز القانوني للأفراد، وقد تنوعت التسميات التي أطلقت عليه[1]، كما تعددت

---

[1]- يختلف مفهوم التوقيع الإلكتروني المصدق عن التوقيع الإلكتروني من ناحية التصديق، والتصديق الإلكتروني[1] يعد من الخدمات الإلكترونية المستحدثة أفرزته مقتضيات المعلوماتية، إرتبط ظهوره بالتوقيع الإلكتروني واستخدامه كرديف مهم للتوقيع التقليدي في المعاملات القانونية، ليمثل بذلك إحدى خصوصيات مجتمع المعلومات على مستوى المفاهيم القانونية المعتمدة. لم تتولى غالبية التشريعات المنظمة للتعاملات الإلكترونية وضع تعريف توضيحي للمقصود بالتصديق الإلكتروني، غير أن الفقه تصدى لهذه المهمة، ومهما تعددت التعاريف التي قيلت في ذلك إلا أنها تدور حول مفهوم واحد هو أن التصديق أو التوثيق الإلكتروني وسيلة فنية آمنة تم إبتكارها بهدف إضفاء المصداقية على عمليات التبادل الإلكتروني للمعطيات لما توفره من إمكانيات لا يستهان بها من حيث التعريف بأطراف المعاملة وتحديد عناصر هوياتهم ونسبة التوقيع الإلكتروني لصاحبه دون غيره من المتعاملين عبر جهة موثوق بها يطلق عليها اسم مقدم خدمة التصديق.**أسامة بن غانم العبيدي**، التصديق الإلكتروني وتطبيقاته في النظام السعودي، مجلة القضائية، العدد الرابع، وزارة العدل، المملكة العربية السعودية، 1433، ص179.

[2]-Article 2 du **Décret**272-2001 dispose que "... repose sur l'utilisation d'un certificat électronique qualifié ... .

[3]-**سعيد بن محمد الغامدي**، المرجع السابق، ص145

التعريفات التي قيلت بشأنه وإن كان يجمعها إتفاقها في المضمون الذي يدل عليه المصطلح وهو تقديم خدمات التصديق الإلكتروني.

في هذا الإطار، يشير قانون الأونسترال النموذجي بشأن التوقيعات الإلكترونية في فقره ه من المادة 2 إلى أنه يقصد بمقدم خدمة التصديق **شخص يصدر شهادات ويجوز أن يقدم خدمات أخرى ذات صلة بالتوقيعات الإلكترونية**، وفي ذات الإتجاه عرفه التوجيه الأروبي رقم 910-2014 بموجب الفقرة 19 من المادة 3 تحت مسمى مزود خدمة الثقة، أنه **كل شخص طبيعي أو معنوي يقوم بتقديم خدمة أو أكثر متعلقة بالثقة سواء كان موصوف او لا**"[2]، وعرفه المرسوم الفرنسي الصادر في 30 مارس بشان تطبيق المادة 1367 (1316-4 سابقا) من القانون المدني بمقتضى المادة 1 فقرة 11 بأنه **كل شخص يصدر شهادات تصديق الكتروني أو يقدم خدمات أخرى تتعلق بالتوقيعات الإلكترونية.**

وكذلك فعل المشرع الجزائري في قانون التوقيع الإلكتروني، وإن كان قد جسد مناخ الثقة بموجب **مخطط ثقة وطني**[3]، ومن بين النماذج الموجودة في العالم إختار مخططا هيكليا يضم سلطة وطنية للتصديق الإلكتروني وهيئتين تؤطران التصديق الإلكتروني للفرعين الحكومي والإقتصادي، ويعتمد هذا النموجد التنظيمي على هيئات فرعية مكلفة بالتدقيق والمعادلة. تكلف السلطة الوطنية بترقية إستعمال التوقيع والتصديق الإلكترونيين وتطويرهما وضمان موثوقية إستعمالها[4]، أما سلطة التصديق الحكومية فهي تؤطر تسيير الشهادات المستعملة في التعاملات الإلكترونية بين الإدارات (المراسلات بين الوزارات) وبين الإدارة والمؤسسات(كالسجل التجاري الإلكتروني) وبين الإدارة والمواطنين (السجل الوطني الآلي للحالة المدنية)، وتشرف **أطراف موثوقة أخرىعلى تسليم شهادات أو تقديم خدمات أخرى متعلقة بالتصديق الإلكتروني لفائدة المتدخلين في الفرع الحكومي على أن تصادق عليها السلطة الحكومية**[5]، في حين سلطة التصديق الإقتصادية فهي مكلفة بتسيير الشهادات المستعملة في التعاملات الإلكترونية بين المؤسسات (كالعقود الإلكترونية) وبين المؤسسة والمواطن(كالمعاملات التجارية الإلكترونية) وبين المواطنين (كتبادل البريد الإلكتروني الموقع والمصدق عليه)، ويضمن تسليم الشهادات في هذا الفرع **مؤدي خدمة التصديق الإلكتروني** ، وقد عرفه المشرع بموجب الفقرة 12 ن المادة 2 من قانون التوقيع الإلكتروني على انه **شخص طبيعي او**

---

[1]- بين جهة التصديق إلى مقدم أو مزود خدمات التصديق إلى سلطة المصادقة على التواقيع الإلكترونية، إلى مقدم خدمة الثقة.

[2]- وتتمثل **خدمة الثقة** حسب الفقرة 16 من المادة 3 من التوجيه الأروبي910-2014 في: إنشاء و التثبت من التوقيعات الإلكترونية والأختام الإلكترونية والطوابع الإلكترونية والخدمات البريدية الإلكترونية الموصى بها، والشهادات المتعلقة بهذه الخدمات.

إنشاء والتحقق من صلاحية الشهادة من أجل توثيق المواقع الإلكترونية.

الحفاظ على التواقيع الإلكترونية والأختام الإلكترونية والشهادات المتعلقة بهذه الخدمات.

[3]- حديث الوزيرة زهرة دردوري لوكالة الأنباء الجزائرية متاح على الموقع الإلكتروني التالي:

http://www.pfln.org.dz/?p=6223

[4]- مرسوم تنفيدي رقم 16-134 مؤرخ في 17 رجب عام 1437 الموافق ل25 أبريل 2016، يحدد تنظيم المصالح التقنية والإدارية للسلطة الوطنية للتصديق الإلكتروني وسيرها ومهامها، جريدة رسمية، عدد 26، صادرة في 28 أبريل 2016.

[5]- أنظر المرسوم التنفيدي رقم 16-135 مؤرخ في 17 رجب 1437 الموافق ل 25 أبريل 2016، يحدد طبيعة السلطة الحكومية للتصديق الإلكتروني وتشكيلها وتنظيمها وسيرها، جريدة رسمية، عدد 26، مؤرخة في 28 أبريل 2016.

معنوي يقوم بمنح شهادات التصديق الكتروني موصوفة و قد يقدم خدمات أخرى في مجال التصديق الإلكتروني".

ومن تم نخلص إلى أن امشرع الجزائري اتبع الإزدواجية في جهة التصديق الإلكتروني حسب طبيعة المتعاملين الإلكترونيين.

كما عرفه المشرع المصري بموجب المادة 1 من اللائحة التنفيذية لقانون التوقيع الإلكتروني "**الجهات المرخص لها بإصدار شهادة التصديق الإلكتروني وتقديم خدمات تتعلق بالتوقيع الإلكتروني**".

يتضح من التعريفات السابقة، أنها تكاد تتطابق فيما بينها بصدد تحديد مدلوله، فيمكن أن يكون شخص طبيعي أو معنوي، وإن كان عمليا لا يمكن تصور ان يكون شخص طبيعي نظرا لما يتطلبه من امكانيات فنية و تكنولوجية واجهزة متطورة وكيانات بشرية ومعدات لا تتوافر إلا للشخص المعنوي، هذا الأخير الذي إشترطه المشرع الجزائري في الطرف الثالث الموثوق. كما قامت التشريعات بتوسيع الدور المنوط به، ففضلا عن إصدار شهادة تصديق إلكترونية تربط بين شخص طبيعي أو معنوي والمفتاح العام ، فانه يناط به خدمات أخرى ترتبط مجملها بالتوقيع الإلكتروني بصفة عامة.

وبالنظر للخدمات التي يقدمها مزود خدمة التصديق وتعزيزه للثقة في التعامل الإلكتروني، فإن القوانين فرضت شروطا ترمي في مجملها إلى التأكد من تحقق الثقة المطلوبة في مزود الخدمة.وهذا ما نتبينه فيمايـــلي.

ثانيا– شـــروط تأديـــة خدمـــة التصـــديق على التوقيع الإلكتـــروني.

إشترطت غالبية التشريعات بعض الشروط والمتطلبات لتأدية خدمات التصديق الإلكتروني، بين أن هذه الشروط ليست من طبيعة واحدة، فهناك من القواعد التي تتسم بالطابع التنظيمي أو الإداري، وشروط أخرى ذات طابع الشخصي وأخرى تتميز بطابع فني وتقني ومـــالي.

ففي فرنسا، يقدم طلب القيام بمهمة المكلف بخدمات التوثيق إلى أي مركز من مراكز التقييم والتوثيق، وبعد ذلك يكتب المركز تقارير فنية عن المتقدمين يبادر على أساسها الوزير الأول باصدار شهادة تؤكد إلتزام مقدم الطلب بالمقتضيات الواردة في المرسوم 30 مارس 2001 أو يرفض طلبه.

أشارت المادة 6–2 من المرسوم الصادر 30 مارس 2001 إلى الشروط الواجب توافرها في مقدم خدمة التصديق حينما تطلبت ضرورة إستفائه جملة من المتطلبات من بينهما إستخدام الكوادر التي تتوفر لديها المعرفة والخبرة والمؤهلات اللازمة لتقديم خدمات التصديق، تطبيق إجراءات الأمان الواجب إتباعها وأن تقوم كذلك باستخدام أنظمة وبرامج تحقق الأمان التقني. إقامة الدليل على موثوقية خدمات التصديق الإلكتروني التي يقدمها ، كفالة الأداء الوظيفي لخدمة إعداد دليل سنوي يحصي شهادات التصديق الإلكتروني التي يجري طلبها، وذلك لصالح الأشخاص الصادرة لهم الشهادات.

ثم صدر المرسوم رقم 535-2002 الصادر في 18 افريل 2002 المتعلق بتقييم مستوى الأمان الذي توفره منتجات وانظمة تكنولوجيا المعلومات[1] الذي يعد امتدادا للمرسوم 30 مارس 2001، ليدخل في المنظومة التشريعية الفرنسية تقييم أمان تكنولوجيا المعلومات والتصديق عليه[2]. وقد أناط هذا المرسوم اللجنة الرئيسية للتصديق إصدار الأراء بشأن القواعد والمعايير المستخدمة في إجراء التقييم وإبداء الرأي بقبول أو سحب قبول مراكز التقييم والتوثيق. فضلا عن فحص كل نزاع يعرضه عليها الأطراف يتعلق باجراءات التقييم التي نظمها المرسوم للفصل فيها[3].

أما ما يتعلق بالمشرع الجزائري فقد إشترط من جانبه جملة من الشروط، البعض جاءت بها المادة 34 من قانون التوقيع الإلكتروني، وهي شروط ليست من طبيعة واحدة. ففيما يخص الشروط الشخصية تطلب المشرع أن يكون الشخص الذي يقدم خدمات التصديق سواء كان شخص طبيعي أو معنوي. خاضع للقانون الجزائري للشخص المعنوي أو الجنسية الجزائرية للشخص الطبيعي وأن لا يكون قد سبق الحكم عليه في جناية أو جنحة تتنافى مع نشاط تأدية خدمات التصديق الإلكتروني.

وفضلا عن ذلك، تطلب المشرع **متطلبات فنية وتقنية** بأن تكون له مؤهلات وخبرة ثابتة في ميدان تكنولوجيا الإعلام والإتصال للشخص الطبيعي أو المسير للشخص المعنوي، فضلا عن الضمانات المالية، لضمان إمكانية تعويض المتعاملين الإلكترونيين مع مؤدي هاته الخدمات، وهو من الشروط الجوهرية لتحقيق عنصري الثقة والأمان بين الجهات التي تقوم بالتصديق على التوقيع الإلكتروني والأطراف المتعاملين الكترونيا.

وحتى عند توافر جملة الشروط في الشخص الطالب، فإن هذا الأخير لا يمكنه ممارسة نشاط مزود خدمات المصادقة الا اذا تحصل على **ترخيص مسبق**[4] –يخضع لدفع مقابل مالي[5] –بذلك من السلطة الإقتصادية للتصديق الإلكتروني، وقبل الحصول على الترخيص، تمنح **شهادة التاهيل** لمدة سنة قابلة للتجديد مرة واحدة لتهيئة كل الوسائل اللازمة لتأدية خدمات التصديق الإلكتروني.غير أن منح ذلك الترخيص لا يعني أن مزود خدمة التصديق أصبح بإمكانه إسداء خدماته دونما تقيد بأية ضوابط بل أوجبت عليه المادة 40 تعاطي نشاطه وفق لدفتر الأعباء الذي يحدد شروط وكيفيات تأدية خدمات التصديق الإلكتروني.

---

[1]-**Décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information**: JORF n°92 du 19 avril 2002 .

[2]- حيث إهتم بتنظيم سياسة اعتماد مقدمي خدمات التصديق وتحديد اجراء التقييم والتصديق عليه (الباب الأول) وقبول مراكز التقييم (الباب الثانب) واللجنة الرئيسية للتصديق في شان امان تكنولوجيا المعلومات (الباب الثالث) والأحكام المتنوعة والوقتية (الباب الرابع).

[3]-Voir article 15 du Décret n°2002-535 du 18 avril 2002.

وهي لجنة يرأسها الأمين العام للدفاع الوطني أو من يمثله، وتتضمن في عضويتـــها ممثلـــين عن الـــوزارات المختلفة. اكثر تفاصي حول قواعد ممارسة خدمات التصديق فب التشريع الفرنسي انظر: **د. تامر محمد سليمان الدمياطي**، المرجع السابق ص 465 وما بعدها.

[4]–يقصد بالترخيص حسب الفقرة 10 من المادة 2 من قانون التوقيع الإلكتروني"نظام إستغلال خدمات التصديق الإلكتروني الذي يتجسد في الوثيقة الرسمية الممنوحة لمؤدي الخدمات،بطريقة شخصية تسمح له بالبدء الفعلي في توفير خدماته.

[5]– أنظر المادة 40 من قانون التوقيع الإلكتروني الجزائري.

والجدير بالملاحظة، هو أن المشرع لم يكتف بوضع شروط قانونية مدققة للترخيص في تعاطي نشاط خدمات المصادقة الإلكترونية، وانما أوجب على مزود تلك الخدمة الذي يرغب في إيقاف نشاطه كليا او جزئيا اعلام السلطة الإقتصادية للتصديق الإلكتروني في الأجال المحددة في سياسة التصديق لهذه السلطة[1]، والى جانب صورة الإيقاف الإرادي للنشاط ادرج المشرع صور اخرى يترتب على مخالفتها جزاء اداري، يتمثل في سحب الترخيص من مزود خدمات المصادقة وايقاف نشاطه، كحالة انتهاكه للمقتضيات التي يتطلبها الدفاع الوطني والأمن العمومي[2]، وحالة عدم احترامه احكام دفتر الأعباء او سياسة التصديق الإلكتروني الخاصة به[3].

والوضع في مصر غير مختلف كثيرا عما هو عليه في الجزائر، حيث ينبغي لمزاول نشاط خدمات التصديق الحصول على ترخيص مسبق من هيئة تنمية صناعة تكنولوجيا المعلومات[4]، بل هو وضع معظم الدول حيث تفرض قوانينها التي نظم المعاملات الإلكترونية بشكل عام في من يمارس تقديم خدمات التصديق أن يكون حاصلا على الترخيص المسبق[5]، والهدف من الترخيص ضمان الرقابة المسبقة للدولة على النشاط الذي يمارسه المزود والتحقق من توافر الشروط اللازمة لممارسة هذه المهنة[6]. إلا أنه في المقابل لم يتعرض في القانون أو لائحته التنفيذية للشروط الشخصية، وهي تعد لازمة لقيام مقدم الخدمة بدوره كون خدماته تتعلق بمصالح الأفراد وحقوقهم، وهو أمـــر يمثل خطورة شديدة إذا لم يتم تنظيم كافـــة جوانبه.

كما إشترط المشرع المصري شأنه شان المشرع الجزائري والفرنسي متطلبات فنية وتقنية ليتكمن من أداء عمله على أكمل وجه، وذلك بمقتضى المادة 12 ،أ من اللائحة التنفيذية لقانون التوقيع الإلكتروني[7] وعلى غرار المشرع الجزائري، تطرق المشرع المصري بموجب المادة 14 إلى المتطلبات المالية التي يجب أن تتوافر في مزود خدمة التصديق[8]؛

---

[1]–المادة 58 من قانون التوقيع الإلكتروني الجزائري

[2]- المادة 65 من قانون التوقيع الإلكتروني الجزائري

[3]– المادة 64 من قانون التوقيع الإلكتروني الجزائري

[4]–وهو ماأشارت إليه صراحة المادة 19 من قانون التوقيع الإلكتروني" **لا يجوز مزاولة نشاط اصدار شهادات التصديق الإلكتروني إلا بترخيص...**"، وتختص هذه الجهة بمنح الترخيص لمقدم خدمات التصديق وتملك سحبه أو تعديله أو إلغاءه في أي وقت وفقا للقانون.

[5]–أنظر مثلا الفصل الأول من قانون المبادلات والتجارة الإلكترونية التونسية، المادة 33 من قانون المعاملات الإلكترونية الأردني.

[6]– **آلاء يعقوب النعيمي**، التصديق على التوقيع الرقمي، مفهومه والعلاقات القانونية الناشئة عنه ، مجلة الحقوق للبحوث القانونية والإقتصادية، العدد الأول، كلية الحقوق، جامعة الإسكندرية، 2011، ص223.

[7]– حيث نصت صراحة"**يجب أن يتوافر لدى طالب الحصول على الترخيص بإصدار شهادات التصديق الإلكترونى المتطلبات التالية: أ) نظام تأمين للمعلومات وحماية البيانات وخصوصيتها بمستوى حماية لايقل عن المستوى المذكور فى المعايير والقواعد المشار إليها فى الفقرة (د) من الملحق الفنى والتقنى للائحة**"، كما نصت الفقرة و" **المتخصصون من ذوى الخبرة الحاصلين على المؤهلات الضرورية لأداء الخدمات المرخص بها**".

[8]– حيث نص في المادة 14 من اللائحة التنفيذية للقانون" **على طالب الترخص بإصدار شهادات التصديق الإلكترونى أن يقدم الضمانات والتأمينات التى يحددها مجلس إدارة الهيئة لتغطية أى أضرار أو أخطار تتعلق بذوى الشأن ، وذلك فى حالة إنهاء الترخيص لأى سبب ، أو لتغطية أى إخلال من جانبه لالتزاماته الواردة فى الترخيص.**

ومن جانبيا نرى، أن أغلب الشروط المطلوب توافرها في مقدم خدمة التصديق تدور حول كفالة المهمة الأساسية المعهودة اليه وهي إنشاء وإصدار شهادات التصديق الإلكتروني على التوقيعات الإلكترونية.

ثالثا–مهام الجهة المختصة بالتصديق على التوقيـــع الإلكـــتروني

من خلال البحث في مقتضيات نصوص التشريعات المقارنة التي نظمت هذه الجهة، نلاحظ أنها أسندت لمزود خدمة التصديق صلاحيات واسعة لإضفاء المصداقية على التعامل الإلكتروني بشكل عام، وعهدت إليه بمهام متنوعة تولى المشرع ضبطها وتحديدها تفعيلا لنجاعة المصادقة الإلكترونية، وهو ما فعله المشرع الفرنسي بمقتضى المرسوم رقم 272–2001 الصادر في 30 مارس 2001 بموجب المادة 6 منه، وكذلك المشرع الجزائري بموجب الفرع الثاني من القسم الأول من الفصل الثالث من قانون التوقيع الإلكتروني تحت عنوان **تادية خدمات التصديق الإلكتروني**، والفرع الأول من القسم الثاني من نفس الفصل تحت عنوان"**واجبات مؤدي خدمات التصديق الإلكتروني**"، أما بعض التشريعات كما هو حال المشرع المصري، فلم يتعرض لهذه الإلتزامات في قانون التوقيع الإلكتروني، كما إقتصرت اللائحة التنفيذية لهذا القانون على بيان القواعد المنظمة للحصول على الترخيص بإصدار شهادة التصديق دونما تحديد واضح لإلتزاماته، على الرغم من أهمية تحديد هذه المسالة، ذلك أنه بقدر إلتزامه بقدر ما تتضاءل المخاطر الناجـــمة عن التوقيع الإلكتـــروني.

على العموم، تتنوع الإلتزامات الملقاة على عاتق مقدم خدمات التصديق، البعض منها رئيسي متعلق أساسا بشهادة التصديق الإلكتروني التي عهد إليه التصرف فيها، والبعض الآخر تبعـــي، وهدا ما سنتناوله من خلال العناصر التالية:

أ– الإلتزام بإصـــدار شهادة التصـــديق الإلكـــتروني

يتمثل الإلتزام الرئيسي للقائم بخدمة التصديق **في إصدار** شهادات التصديق الإلكتروني، لإثبات نسبة التوقيع الإلكتروني لصاحبه، وصحة هذا التوقيع، وتأكيد أن البيانات الموقع عليها بيانات صحيحة صادرة عن الموقع.

وايمانا من المشرعين بدور هده الشهادة الفعالة في إبـــرام التصرفات عبر الوسائل الإلكترونية، إرتأو وضع تعريف ايضاحي لها، فقد عرفها قانون الأونسترال النموذجي بشان التوقيعات الإلكترونية بموجب المادة 2–ببانها" **رسالة بيانات او سجل يؤكدان الإرتباط بين الموقع و بيانات انشاء التوقيع**"[1].

الملاحظ من خلال هذا التعريف، أن الشهادة الغرض منها وجود صلة ما بين شخصية الموقع والمفتاح الخاص والمعبر عنه بيانات انشاء التوقيع. قد يخمن البعض للوهلة الأولى بعدم صحة هذا الربط، كون أن المفتاح الخاص يبقى سرا مع صاحبه ولا يدرج كبيان في شهادة التصديق، على عكس المفتاح العام. لكن

[1]-Le terme "certificat" désigne un message de données ou un autreenregistrement confirmant le lien entre un signataire et des données afférentes à lacréation de signature;

سرعان ما يتاكد لنا صحة هذا الربط إدا ما علمنا أن مقدم خدمة التصديق وعند قيامه بإصدار شهادة التصديق فإنه يعمل على التاكد من ان بيانات التحقق من التوقيع قد تم إنشاؤها عن طريق بيانات إنشاء التوقـــيع.

أما النظـــام الأروبـــي رقم 910-2014 فقد ميز في المادة 3 بين شهادة التوقيع الإلكتروني والشهادة الموصوفة للتوقيع الإلكتروني، فعرف الأولى بموجب الفقرة 14 بأنها **الشهادة الإلكترونية التي تربط البيانات الخاصة بصحة التوقيع الإلكتروني للشخص الطبيعي وتؤكد على الأقل الإسم أو الإسم المستعار له.** اما الشهادة الثانية فقد عرفها بموجب الفقرة 15 بأنـــها" **الشهادة التي يتم إصدارها بواسطة مقدم خدمة الثقة المؤهل وتلبي المتطلبات المنصوص عليها في الملحق 2**" ونجد أن الهدف من شهادة التوثيق في التوجيه الأروبي هو ربط المفتاح العام بصاحب التوقيع، وتحديد هويته، حتى يستطيع المرسل إليه التأكد من شخصية وهوية الموقع.

وعلى نفس النهج سارالمشرع الفرنسي عندما ميز بموجب الفقرة 9 و10 من المادة 1 من المرسوم رقم 2001-272 بين الشهادة الإلكترونية والشهادة الإلكترونية الموصوفة، حيث عرف الأولى بأنها"**مستند إلكتـــروني يؤكد الإتصال بين بيانات التحقق من التوقيع الإلكتروني وصاحب التوقيع،** وبيانات التحقق معبر عنها عموما حسب الفقرة 7 من نفس المادة بالمفتاح العام، أما الثانية فقد عرفها بأنها **الشهادة المستوفية للمتطلبات المنصوص عليها في المادة 6 من هذا المرسوم.**

وفي نفس الإتجاه ميز المشرع الجزائري بدوره بين شهادة التصديق الإلكتروني وشهادة التصديق الإلكتروني الموصوفة، التي نظم المشرع مسؤولية وواجبات الجهة التي تصدرها، ناقلا بدلك نفس تعريف المشرع الفرنسي[1].

كما نجد المشرع المصري قد عرف بدوره شهادة التصديق بموجب الفقرة و من المادة 1 من قانون التوقيع الإلكتروني بانها **الشهادة التي تصدر من الجهة المرخص لها بالتصديق وتثبت الإرتباط بين الموقع وبيانات انشاء التوقيع.** وقد عرفت اللائحة التنفيدية بيانات إنشاء التوقيع بموجب المادة 1-8 على أنها" **عناصر متفردة خاصة بالموقع و تميزه عن غيره، ومنها على الأخص مفاتيح الشفرة الخاصة به، والتي تستخدم في انشاء التوقيع الإلكتروني.** والملاحظ أن المشرع المصري قد حدد الجهة المختصة بإصدار الشهادة، فضلا على بيان الدور الذي تؤديه، بربط الموقع على الشهادة والمفتاح الخاص، ونرى أن الملاحظة نفسها الموجهة لتعريف قانون الأونسترال النموجي تنطبق أيضا على هذا التعريف.

---

[1]- حيث عرف شهادة التصديق الإلكتروني بموجب الفقرة 7 من المادة 2 على أنها "**وثيقة في شكل الكتروني تثبت الصلة بين بيانات التحقق من التوقيع الإلكتروني والموقع**" وعرف بيانات التحقق من التوقيع بموجب الفقرة 5 من نفس المادة على أنها **رموز أو مفاتيح التشفير العمومية أو أي بيانات أخرى مستعملة من أجل التحقق من التوقيع الإلكتروني.** أما شهادة التصديق الإلكتروني الموصوفة فقد عرفها بموجب المادة 15 على أنها **تلك التي تستوفي جملة من المتطلبات والتي يقدمها طرف ثالث موثوق أو مؤدي خدمات التصديق الإكتروني.**

بعد إستعراض التعريفات السابقة، يمكن القول أن شهادة التصديق الإلكتروني عبارة عن وثيقة في شكل إلكتروني صادرة عن جهة تصديق مختصة، تعتمد على تكنولوجيا رياضية معقدة وهي تقنية شفرة المفتاح العام والمفتاح الخاص، ويرجع ذلك إلى أن هذه التقنية من أقوى الوسائل الحديثة[1]. لا تقتصر على أداء وظائف حماية البيانات فقط، بل تمتد كذلك إلى المساهمة في تدعيم وسيلة الإثبات الإلكتروني من خلال تحديد هوية مرسل المستند والموافقة على مضمونه وعلى توقيع ذوي الشأن إلكترونيا، والتأكد من سلامته، ومن ثم ضمـــان عدم قابليته للإنكـــار.

وشهادة التصديق على النحو السابق بيانه، لا بد أن تتضمن بيانات معينة، حتى تتمكن من أداء مهمتها بتأكيد صدور التوقيع الإلكتروني ونسبته إلى أصحابه، وهو ما حددته التشريعات صراحة كما هو حال المرسوم الفرنسي رقم 2001–272 بموجب المادة 6 منه، وقانون التوقيع الإلكتروني الجزائري بموجب المادة 15 منه، مع الإشارة إلى أن هذين التشريعين قد أقرا هده البيانات للشهادة الإلكترونية الموصوفة، أما قانون التوقيع الإلكتروني المصري فقد أحال للائحة التنفيذية، وبالرجوع إلى هذه الأخيرة نجدها نظمتها من خلال المادة 20.

ويمكننا أن نجمع تلك البيانات في 3 طوائف رئيسية: **الطائفة الأولى** تتعلق بالبيانات الخاصة بشهادة التصديق[2] **الطائفة الثانية** وتتضمن البيانات المتعلقة بصاحب التوقيع[3]، **الطائفة الثالثة:** وتتضمن البيانات المتعلقة بمقدم خدمة التصديق[4].

ومهمة إصدار شهادة التصديق تتلخص عمليا في قيام المزود حال توصله بطلب في الحصول على الشهادة سواء كان الطلب يدويا أو إلكترونيا احداث الوثيقة بناء على المعلومات الضرورية ذات الصبغة الشخصية التي يكون قد استقاها من طالب الشهادة، وذلك بعد التحقق من هويته وعند الإقتضاء التحقق من صفاته.
وبعد احداث شهادة المصادقة، يتولى المزود تسليمها لصاحبها الكترونيا ليقوم هدا الأخير بادراجها ضمن مراسلاته للتعريف بنفسه لدى المرسل إليه الذي يريد انجاز تعامل الكتروني معه، اما إدا كان طالب الشهادة شخصا معنويا، فيحتفظ مؤدي خدمات التصديق بسجل يدون فيه هوية وصفة الممثل القانوني للشخص

---

[1]–أنظر: **د. ميشال عيسى طوني**، التنظيم القانوني لشبكة الأنترنت، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2001، ص19.

[2]- **وتتضمن:** إشارة واضحة تفيد بأن هذه الشهادة صادرة بصفة شهادة موصوفة، بيان يحدد بداية ونهـــاية صلاحية الشهادة الإلكترونية، تحديد إستعمال شهادة التصديق الإلكتروني وقيمة المعاملات التي قد تستعمـــل من أجلها.

[3]- **المتمثلة في** إسم الموقع أو الإسم المستعار الذي يسمح بتحديد هويته. بيانات تتعلق بالتحقق من التوقيع الإلكتروني، وتكون موافقة لبيانات إنشاء التوقيع الإلكتروني ويتمثل هذا البيان في المفتاح العام لصاحب الشهادة.

[4]- **والمتمثلة في :** هوية الجهة التي أصدرت الشهادة، والبلد التابعة له إن وجد. التوقيع الإلكتروني للجهة التي أصدرت الشهادة.
وإلى جانب هذه البيانات التي نص عليها كل من التشريع الفرنسي والجزائري، هناك بعض البيانات التي أضافها المشرع المصري منها: عنوان الموقع الإلكتروني المخصص لقائمة الشهادات الموقوفة أو الملغاة، موضوع الترخيص الصادر للمرخص له، موضحا فيه نطاقه ورقمـــه وتاريخ إصداره وفترة سريـــانه.

المعنوي المستعمل للتوقيع المتعلق بشهادة التصديق الإلكترونية، بحيث يمكن تحديد هوية الشخص الطبيعي عند كل استعمـــال لهذا التوقيـــع[1].

ب-الإلتزام بالتحقق من صحة المعلومات التي تم المصادقة عليها[2]:

أولى الأمور التي يضمنها مقدم خدمة التصديق هي صحة المعلومات التي تم المصادقة عليها وتم تضمينها في الشهادة في التاريخ الذي منحت فيه. ويعتبر هذا الإلتزام أكثر الإلتزامات دقة وصعوبة بالنسبة لعمل جهات التصديق الإلكتروني، يحتاج لكادر وظيفي وفني ملائم للتحقق من البيانات المقدمة وأهلـــية الشخص الصادرة له الشهادة. والبيانات المقدمة تستخلص عادة من الأوراق المقدمة كالهوية الشخصية وجواز الـــسفر.

وهناك التزام شديد الصلة بهذا الإلتزام، يتمثل في التحقق من تكامل بيانات الإنشاء مع بيانات التحقق من التوقيع[3]، وسبق أن وضحنا أن بيانات الإنشاء يعبر عنها عموما مفاتيح التشفير الخاصة أما بيانات التحقق بمفاتيح التشفير العمومية.

ت-الإلتزام بالمحـــافظة على السرية:

علاوة على ماسبق، فان مزود الخدمة مدعو بحكم القانون بالمحافظة على سرية البيانات التي قدمت إليه أو إتصـــل بها بحكم عمله وعدم إفشائها، تحت طائلة المسؤولية، كل ذلك دعما للثقة بين المتعاملين بالوسائل الإلكترونية، وهو ما نص عليه المشرع الجزائري صراحة في المادة 42 "**يجب...الحفاظ على سرية البيانات والمعلومات...**"، كما نص على ذلك القانون المصري" في المادة **21**"**بيانات التوقيع الإلكتروني...سرية**". وفي ذات الإتجاه، يلتزم مقدم الخدمة بالغرض الذي يجمع من أجله البيانات الشخصية، ويحظر أن يجمع منها الا ما يتفق ومنح وحفظ شهادة التصديق الإلكتروني.

ث-الإلتزام بإلغاء العمـــل بشهادة التصديق الإلكترونـــي أو إيقافها:

فضلا عن مهمة **إصدار ومنح** شهادة التصديق، عهدت معظم التشريعات الى مزود الخدمة الالتزام **بالغاء** العمل بالشهادة التي سبق أن أصدرها تحت طائلة المسؤولية، وايمانا منها بالآثار الخطيرة التي ترتبها الشهادات المشكوك فيها أو غير الصحيحة، فقد فصلت أحكامها بشكل دقيق كما هو حال المشرع الجزائري، وذلك بموجب المادة 45 من قانون التوقيع الإلكتروني، فبمقتضى هذه المادة فإن مزود الخدمة مدعو بحكم القانون الى إلغـــاء شهادة التصديق الإلكتروني الموصوفة تماما بصفة نهائية بحسب الحالات بناء على طلب

---

[1]- الفقرة 3 من المادة 44 من قانون التوقيع الإلكتروني الجـــزائـــري.

[2]-المـــادة 4 من الملحق الثاني للتوجيه الأروبي، المادة 6-2- ض- ص من المرسوم الفرنسي رقم 272-2001، المادة 53-1 من قانون التوقيع الإلكتروني الجزائري

[3]-المادة 6-2 -د من المرسوم الفرنسي رقم 272-2001، المادة 44 من قانون التوقيع الإلكتروني الجزائري.

صاحب الشهادة أو عندما يتبين له وجود بعض الأمور التي من شأنها أن تفقد الشهادة قيمتها ومصداقيتها، كأن يتبين له أنه قد تم منحها بناء على معلومات **خاطئة أو مزورة**، كتزوير بطاقته الشخصية او شهادة ميلاده. أو تم انتهاك سرية بيانات انشاء التوقيع. او عندما يتم اعلامه بوفاة الشخص الطبيعي أو بـــحل الشخص المعنوي[1]...

أما بخصوص بعض التشريعات كما هو حال المشرع المصري، فلم يتطرق إلى حالات الإلغاء، إلا أنه في المقابل نظم حالات **الإيقاف**[2] وهي الحالات التي خلى منها قانون التوقيع الإلكتروني الجزائري، ووفقا للمادة 12 من اللائحة التنفيذية فإن حالات ايقاف العمل بالشهادة قد وردت على سبيل الحصر، وذلك في حالة العبث ببيانات الشهادة أو إنتهاء مدة صلاحيتها،أو في حالة عدم التزام صاحب الشهادة ببنود العقد المبرم مع جهة التوثيق، أو في حالة سرقة أو فقد المفتاح الشفري الخاص أو البطاقة الدكية أو عند الشك في حدوث ذلك.

لكن: ماهـــي الآثار المترتبة على التصـــديق على التوقيـــع الإلكتروني؟

يترتب على التوقيع الإلكتروني المصدق إذا ما توفرت فيه الشروط القانونية[3] أن يصبح موثوقا، أومؤمنا كما سمي في المرسوم الفرنسي 272-2001أو موصوفا كما نعته المشرع الجزائري، مع ملاحظة أن هذا الأخير قد أدرج شرط التصديق على التوقيع الإلكتروني مع باقي الشروط القانونية في مادة واحدة وهي المادة 7. ومن تم متمتعا بالحجية في الإثبات أمام القضاء في كافة المعاملات متساويا في ذلك مع التوقيع التقليدي، وهو ما أشـــار إليه المشرع الجزائري صراحة في المادة 8 "**يعتبر التوقيع الإلكروني الموصوف وحده مماثلا للتوقيع المكتوب، سواء كان لشخص طبيعي أو معنوي**".ويتضح من ذلك أن المشرع أقر مساواه قانونية بين التوقيع الإكتروني الموصوف والتوقيع التقليدي متاثرا بدلك بمبدأ النظير الوظيفي الذي نصت عليه المادة 7 من قانون الأونسترال النموجي الخاص بالتجارة الإلكترونية.

وتجدرالإشارة إلى أن التوقيع الإلكتروني الذي لا يستند إلى شهادة تصديق الكتروني موصوفة صادرة من جهة تصديق مرخص لها، لا تنعدم قوته الثبوتية،وهو ما نص عليه المشرع الجزائري صراحة في المادة 9، ويمكن في هذه الحالة ترك تقدير حجية هدا النوع من التوقيعات وما يتوافر فيها من عناصر أمان لسلطة القاضي التقديرية في ضوء ظروف كل حالة.

---

[1]- بسبب أن عقد شهادة التوثيق من العقود المؤسسة على الإعتبار الشخصي. وقرار الإلغاء الذي يتخده مزود الخدمة لا يحتج به تجاه الغير إلا إبتداء من تاريخ النشر مع تحميل مزود الخدمة واجب إخطار صاحب الشهادة بقرار الإلغاء مع تسبيب ذلك.

[2]- ويقصد بايقاف الشهادة تعطيل العمل بالأثر القانوني المترتب عليها، تمهيدا لإلغائها أو إستئناف سريانها متى ثبت عدم صحة السبب الذي تم بناء عليه وقف هذه الشهادة: **د. عبد الفتاح بيومي حجازي**، النظام القانوني للتوقيع الإلكتروني، المرجع السابق، ص174.

[3]- وتتمثل تلك الشروط في:أن يرتبط بالموقع وحده، أن يمكن من تحديد هوية الموقع، ان يكون مصمم بواسطة الية مؤمنة خاصة بانشاء التوقيع الإلكتروني، ومنشا بوسائل تحت التحكم الحصري للموقع، وان يرتبط بالبيانات الخاصة به بحيث يمكن كشف عن التغييرات اللاحقة بهذه البيانات، أنظر المادة 1316-4 من القانون المدني الفرنسي فضلا عن المادة 1-2 من المرسوم 272-2001 التي تطابق المادة 2-2 من التوجيه الأروبي، والمادة 7 من قانون التوقيع الإلكتروني الجزائري،

والواقع هناك سؤالا يتبادر إلى الأذهان أثناء دراسة التصديق الإلكتروني وهو أنه: إذا كان التصديق على التوقيع العرفي من طرف موظف عام مختص، يرفع به إلى مصاف الرسمية، كون أن المحرر وإن كان عرفيا فإنه مايخص التوقيع كاحد بياناته لحقته الرسمية،**فهل التصديق الإلكتروني يضفي الرسمية على التوقيع الإلكتروني؟**

نعتقد أن الإجابة على هذا السؤال تكون بالسلب، وذلك كون جهة التصديق الإلكتروني كما سبق و درسناها قد تكون أفراد أو شركات، ونشاطها في هذا الإطار نشاط خاص تنافسي في الفرع الإقتصادي، يقوم بناء على ترخيص. وبناء عليه فإن شهادة التصديق الإلكتروني لا تضفي الرسمية على التوقيع الإلكتروني، لأنها ليست شهادة رسمية، كما أن التصديق الإلكتروني لا يعد عملا صادرا من موظف عام مختص، وعليه فإن التصديق على التوقيع الإلكتروني لا يضفي عليه الرسمية.

المطلب الثـــاني

المسؤولية الجزائية عن الأفعال غير المشروعة من قبل أطراف التعامل الإلكتروني

لما كان التوقيع الإلكتروني من الأوضاع الجديدة التي تحتاج إلى تنظيم، فلا يتم ذلك إلا بقواعد قانونية جديدة تواجه هذا التطور السريع، لذا نجد الكثير من التشريعات قد أظهرت إستجابة لهذا التطور، وتمكنت من إضفاء الحماية الجزائية للتوقيع الإلكتروني بمقتضى قوانين خاصة به، كما هو حال التشريع الجزائري والمصري. فبالرجوع لهاذين القانونين نجد أن المشرعين قاما بتحرير مجموعة من الأفعال الماسة بالتوقيع الإلكتروني سواء **بصورة مباشرة** أو **غير مباشرة**، سواء منها المرتكبة من طرف الوسيط النظامي(الفرع الأول)، أو المستفيد من خدمات التصديق الإلكتروني(الفرع الثاني).

الفـــرع الأول

مسؤولية مقـــدم خدمة التصديق الإلكتروني

خول المشرع الجزائري للسلطة الإقتصادية للتصديق الإلكتروني بمتابعة ومراقبة مؤدي خدمات التصديق الإلكتروني الذين يقدمون خدمات التوقيع والتصديق الإلكترونيين لصالح الجمهور، وفي هذا الإطار تتولى منح التراخيص لمؤدي خدمات التصديق ومراقبة نشاطهم، ومنه نجد أن الترخيص يمنح لمن تتوفر فيه الشروط التي حددتها المادة 34. ويترتب على هذا المنح آثار يستلزم إحترامها ويترتب على خرقها توقيع عقوبات، ولعل من أهمها الإلتزام بالحفاظ على سرية المعلومات المتعلقة بشهادات التصديق الممنوحة المقرر بموجب المادة 42 من قانون التوقيع الإلكتروني، وبناء عليه عاقب بموجب المادة 70 كل مؤدي خدمات التصديق الإلكتروني الذي أخل بأحكام المادة 42 من هـــذا القانون.

كما نجد المشرع المصري ينص بموجب المادة 21 من قانون التوقيع الإلكتروني على أن بيانات التوقيع الإلكتروني والوسائط الإلكترونية والمعلومات التي تقدم إلى الجهة المرخص لها بإصدار شهادات التصديق الإلكتروني سرية ولا يجوز لمن قدمت إليه أو إتصل بها بحكم عمله إفشاؤها للغير أو إستخدامها في غير الغرض الذي قدمت من أجله. فضلا عن ذلك، عاقب كلا المشرعين على مزوالة نشاط التصديق دون ترخيص أو بعد سحبـــه.

أولا- الركـــن المـــادي

إنطلاقا من النصوص القانونية السابقة، يتضح أن الركن المادي في هذه الجريمة يتم بسلوك يرتكبه الجاني يتخد صورة **إفشاء** المعلومات، ويقصد بالإفشاء النشر على كثيرين على نحو تتحقق به العلانية، كما قد يتحقق بالإستخدام في غرض آخـــر.

هذا هو الوضع في قانون التوقيع الإلكتروني المصري، ذلك أن المشرع الجزائري وإن نص على ضرورة الإلتزام بالحفاظ من جانب مزود الخدمة بسرية البياناتالمتعلقة بشهادات التصديق الممنوحة ، إلا أنه لم يعمد الى تجريم سلوكات محددة حماية لهذه السرية، بل الحظر جاء عاما مطلق. ومن ثم يدخل في التجريم جميع الحالات التي تنطوي على إعتـــداء على السرية.

لكن في مقابل ذلك، قام المشرع الجزائري بالحد من هذا التوسع عندما تطلب أن يكون محل هذا الإخلال هو البيانات المتعلقة بشهادات التصديق الممنوحة، وبذلك يختلف المشرع الجزائري عن المشرع المصري الذي وسعها بصريح العبارة جين نص في المادة 21 كما يلي" **بيانات التوقيع الإلكتروني والوسائط الإلكترونية و <u>المعلومات</u>...**". وعلى ذلك فإن الحظر هنا عام ومطلق يشمل كل المعلومـــات المقدمة.

إلا أنه في المقابل حصر المشرع المصري نطاق التجريم في الجهة التي تصدر شهادات التصديق وكل من قدمت إليه تلك المعلومات بحكم عمله، وكذلك فعل المشرع الجزائري وإن كان هذا الأخير قد نص فضلا عن ذلك على معاقبة المكلف بالتدقيق الذي يقوم بكشف معلومات سرية إطلع عليها أثناء قيامه بالتدقيق[1] بموجب نص خاص.

ثانيا- الركـــن المعنـــوي

إدا توافر الركن المادي للجريمة على النحو السابق بيانه، تعين أن يقوم القصد الجنائي لدى الجاني بوصفها جريمة عمدية يلزم لقيامها إتجاه إرادة الجاني إلى الفعل المجرم مع علمه بذلك وقبول النتائج المترتبة على هذا السلوك الإجرامي الذي لا يتصور وقوعه بطريق الخطأ.

ثالثا_العقوبـــة

[1]- المادة 73 من قانون التوقيع الإلكتروني الجزائري.

هذه الجريمة جنحة عاقب عليها المشرع الجزائري بالحبس من ثلاثة أشهر إلى سنتين وبغرامة من 200000 دج إلى مليون دينار أو بإحدى هاتين العقوبتين، أما المشرع المصري فقد عاقب عليها بموجب المادة 23 بالحبس وبغرامة لا تقل عن 10000 جنيه و لا تجاوز مائة الف جنيه او باحدة هاتين العقوبتين، مع عدم الإخلال باي عقوبة اشد منصوص عليها في قانون العقوبات أو في قانون آخر.

الفـــرع الثـــاني

المسؤوليـــة الجزائيـــة للمستفيد

جرم كل من المشرع الجزائري والمصري مجموعة من الأفعال التي قد يرتكبها المستفيد من خدمات التصديق الإلكتروني والماسة بالتوقـــيع الإلكـــتروني وهـــي:

أولا– الإدلاء العمدي بتصاريح كاذبة

نص المشرع الجزائري على هذه الجريمة في المادة 66 "**كل من أدلى بإقرارات كاذبة للحصول على شهادة تصديق الكتروني موصوفة**"، إلا اننا لم نجد نص مماثل في القانون المصري.

وهذه الجريمة التي إنفـــرد بها المشرع الجزائري من الجرائم التي تقع على بيانات التعاملات الإلكترونية و كدلك التوقيع الإلكتروني الذي يعد أساس التعامل الإلكتروني عبر الوسائط الإلكترونية.

أ – الركـــن المـــادي

يتحقق الركن المادي بسلوك يرتكبه الجاني يتخد صورة "**الإدلاء**" بإقرارات، أي اعلان تصريحات، ما يميزها أنها **كاذبة**، إنطوت على **تغيير الحقيقة**، والذي يشكل السلوك الإجرامي لجريمة النصب وكذلك جريمة التزوير، إلا أن هذا التغيير للحقيقة لم يتم لغرض الحصول على منقول له قيمة لسلب ثروة الغير أو بعضها، على العكس من جريمة التزوير التي ترد على مستند أو توقيع، وبناء عليه يرى البعض من الفقه[1] أن هذه الجريمة تقترب من التزوير في مفهومه التقليدي، فقد ينتحل الشخص هوية غيره أو إبدال شخصيته.

هذا ولم يحدد المشرع موضوع هذه الإقرارات، وسواء تعلقت بهوية صاحب الشهادة أو نشاطه أو غيرها. ويستوي أن يتم هذا الإدلاء الى مزود خدمة التصديق، أو إلى أطراف التعاقد[2]. ويكون الغرض من ذلك إستصدار شهادة تصديق إلكتروني موصوفة.

---

[1]– **د. هدى حامد قشقوش**، الحماية الجنائية للتوقيع الإلكتروني، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، الجزء الثاني، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ماي 2003 ، ص589.

[2]– **د. هدى حامد قشقوش**، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة، ص 45.

ب-الركـــن المعنـــوي

جريمة الإدلاء باقرارات كاذبة جريمة عمدية يتخد الركن المعنوي فيها صورة القصد الجنائي، بعنصريه العلم والإرادة، فيجب أن يعلم الجاني بحقيقة سلوكه الإجرامي، وأن يدلي بمعلومات كاذبة بهدف الحصول على شهادة التصديق، ويعلم بمخالفة ذلك للقانون، ومع ذلك تتجه ارادته الى هدا الفعل ويقبل الاثار المترتبة عليه.

ت-العقوبـــــة

ومتى قامت الجريمة بركنيها المادي والمعنوي في حق الجاني، فانه يعاقببموجب المادة 66 بالحبس من 3 أشهر إلى 3 سنوات وبغرامة من 20000 إلى 200000 أو بإحدى هاتين العقوبتين.

ثانيا- إستعمال شهادة التصديق الإلكتروني

سبق القول أن الشهادة الإلكترونية بشكل عام يجب أن تتضمن جملة من البيانات، من بينها إشارة إلى بداية و نهاية مدة صلاحية الشهادة، وفي المقابل فإنه من الإلتزامات الرئيسية المشتركة بين التشريعات إلتزام مقدم خدمة التصديق بإلغاء العمل بالشهادة عند حدوث سبب يقيني يحتم ذلك، كما لو تم منحها بناء على معلومات مزورة أو خاطئة. وعلى ذلك يحدث أن يقوم الحائز على هذه الشهادة بمواصلة إستعمالها بعد إنتهاء مدة صلاحيتها أو إلغائها، وذلك بتوقيعه على معاملاته بالتوقيع الإلكتروني المصدق بشهادة الكترونية. ورغم خطورة هذا الفعل كون أن الشخص يمكن أن يعقد صفقات أو يجري تحويلات نقدية أو يسحب أموال بشهادات الكترونية مشكوك فيها أو غير صحيحة، أو إنتهت مدة صلاحيتها فإن القليل النادر من التشريعات قد تناول بالتجريم الإستمرار في إستعمال هذا النوع من الشهادات بشكل صريح وانزاله منزلة العناية ما يتناسب مع خطورته، إذ لا نجد لهذا السلوك ذكرا لا في قانون التوقيع الإلكتروني الجزائري ولا في المصري.

ذلك هو الوضع في قانون التوقيع الإلكتروني، ذلك أن المشرع الجزائري وبموجب المادة 18 من قانون عصرنة العدالة نص على معاقبة كل شخص حائز شهادة الكترونية يواصل استعمالها رغم علمه بانتهاء مدة صلاحيتها أو إلغائها. فضلا عن الصورة السابقة، جرم المشرع صورة أخرى للإستعمال غير المشروع للشهادة بمقتضى المادة 74 من قانون التوقيع الإلكتروني، متى كان ذلك لغير الأغراض التي منحت من أجلها، وهدا ما سنتناوله فيمايلي:

أ- الركـــن المـــادي

1-إستعمال شهادة إلكترونية منتهية الصلاحية أو تم إلغائها

يتحقق السلوك الجرمي بفعل يرتكبه الجاني وهو الإستمرار في إستعمال الشهادة الإلكترونية التي تصدرها وزارة العدل، على الرغم من علمه بانتهاء مدة صلاحيتها أو إلغائها، هذا وقد وسع المشرع دائرة التجريم الى كل استعمال مهما كان الهدف منه ومهما كان نوعه، اكثر من ذلك فان نص المادة السابقة بصيغته المطلقة يكفي ليطبق على الإستعمال ولو تم لمرة واحدة.

وينصب هذا السلوك على شهادة الكترونية منتهية الصلاحية أو تم إلغائها. والملاحظ أن نص المادة 18 من قانون عصرنة العدالة قد جاء مطلقا إذ لم يحدد نوع أو صفة الشهادة الإلكترونية، سواء كانت موصوفة أم لا، إلا أنه يمكن استخلاص ذلك من دلالة المادة 6 التي تنص" يتم إثبات العلاقة بين معطيات التحقق من التوقيع الإلكتروني وصاحب التوقيع عن طريق **شهادة الكترونية موصوفة** تصدرها وزارة العدل".

اما المواصلة في استعمال الشهادة بعد الغائها، فلم يحدد المشرع في قانون عصرنة العدالة حالات الإلغاء، على عكس ما انتهجه في قانون التوقيع الإلكتروني، حيث يتحقق باخطار مؤدي خدمات التصديق صاحب شهادة التصديق الإلكترونية الموصوفة مع تسبيب دلك وهو ما أشارت إليه المادة 45 .

2-الإنحراف عن الغرض الذي منحت من أجله الشهادة

إن شهادات التصديق التي تصدر من مزود الخدمة كثيرة، حسب الغرض منها، فيمكن أن تتمثل في التصديق على منظومة إنشاء التوقيع الإلكتروني، أو التصديق على صحة هذا التوقيع، كما أن مجالات إستخدامها كثيرة، فبإمكان مزود الخدمة أن يحصر إستخدامها على مجالات معينة، ومن ثم يجب على المستفيد أن يتقيد بذلك، ومن ثم فإن قام المستفيد الذي تحصل على هذه الشهادة باستعمالها لغرض أو هدف آخر غير الغرض الذي منحت من أجله، فيكون قد وقع سلوكه تحت حكم المادة 74.

ب-الركــن المعــنوي

جريمة استعمال الشهادة الإلكترونية بعد انتهاء صلاحيتها أو الغائها جريمة عمدية، يتخذ الركن المعنوي فيها صورة القصد الجنائي، بان يعلم الجاني انه يقوم باستعمال شهادة منتهية الصلاحية او تم الغائها، وان تتجه ارادته الى ارتكابه هذا الفعل.

والقول نفسه يسري على الجريمة التانية، فهي من الجرائم العمدية، فيجب أن يعلم الشخص أن فعله من شأنه الإنحراف عن الغرض الذي منحت من أجله الشهادة، واتجاه إرادته إلى تحقيق ذلك.

ت-العقوبــة

عقوبة الجريمة في صورتها الأولى فهي الحبس من سنة إلى خمس سنوات وبغرامة تتراوح بين 100000 دج إلى 500000 دج. حسب المادة 18 من قانون عصرنة العدالة، اما في صورتها التانية فقد أخضع المشرع مرتكبها لعقوبة الغرامة دون الحبس، من ألفي دينار إلى مائتي ألف دينار حسب المادة 74.

المطلب الثالث

المسؤولية الجزائية عن الأفعال غير مشروعة من قبل الغير

لتهيئة البيئة الآمنة لإنجاز التعاملات الإلكترونية من جهة، وحماية التوقيع الإلكتروني باعتباره الأداة الفعالة لإنجازها بأمان من جهة أخرى، جرم كل من المشرع الجزائري والمصري من خلال قانونيهماللتوقيع الإلكتروني، مجموعة من الأفعال التي يرتكبها الغير، سواء إرتبط السلوك المادي بالتعامل غير المشروع في نشاط التصديق الإلكتروني(الفرع الأول)،أو بالمساس بحجية التوقيع الإلكتروني في الإثبات(الفرع الثاني).

الفــرع الأول

التعامل غير المشروع في نشاط التصــديق الإلكتروني

تتعدد صور التعامل غير المشروع في نشاط التصديق الإلكترونـــي، ذلـــك ان مباشـــرة نشـــاط التصـــديق الإلكتروني لا يكون إلا ممن خوله المشرع تلك السلطة، كما أن بيانات شهادة التصـــديق الإلكترونـــي لهـــا خصوصية بما يوجب المحافظة على سريتها، ومن جهة أخرى فإن التعامل فـــي بيانـــات إنشـــاء التوقيـــع الإلكتروني أو الحصول على هذا التوقيع أو وسيطه يجب أن يكون ممن هو مخـــول قانونـــا. وعلـــى ذلـــك سنتناول فيمايلي لتلك الصور من الحماية الجزائية على النحو التالي:

أولا– تقديم خدمة المصادقة الإلكترونية بدون ترخيص أو بعد سحبه

سبق أن رأينا أن نشاط التصديق الإلكتروني لا يجوز مباشرته إلا ممن خوله المشرع تلك السلطةتحت طائلة المسؤوية، حيث نص المشرع الجزائري بموجب المادة 72 "يعاقب ...**كل من يؤدي خدمات التدصيق الإلكتروني للجمهور دون ترخيص أو كل مؤدي خدمات التصديق الإلكتروني يستأنف أو يواصل نشاطه بالرغم من سحب ترخيصه.**

كما ورد النص على هذه الجريمة في المادة 23_د من القانون التوقيع الإلكتروني المصري والتي عاقبت كل من يخالف أحكام المادتين 19 و 21 من هذا القانون، وما يعنينا في هذا المقام هو مخالفة أحكام المادة 19، التي نصت على أن مزاولة نشاط إصدار شهادات التصديق الإلكتروني لا يتم إلا بترخيص من الهيئة".

إنطلاقا من النصوص السابقة، يتضح أن هذه الجريمة تقوم على ركن مادي وركن معنوي، سنتناولها على النحـــو التالي.

أ-الركـــن المـــادي

يتحقق الركن المادي لهده الجريمة بسلوك اجرامي يرتكبه الجاني يتخد صورة تقديم خدمة التصديق الإلكتروني دون الحصول على الترخيص، وهو أمر بديهي ومنطقي، كون التشريعات قد اشترطت لتأدية خدمة المصادقة الإلكترونية الحصول على ترخيص من جهة خاصة، وهي السلطة الإقتصادية للتصديق الإلكتروني في التشريع الجزائري، وهيئة تنمية صناعة تكنولوجيا المعلومات في التشريع المصري. وأن هناك شروط محددة نصت عليها التشريعات لمن يمنح رخصة مزاولة هذا العمل.

والملاحظ أن المشرع الجزائري كان أكثر توسعا من المشرع المصري من حيث نطاق السلوك المجرم حين وسعه لكل خدمات التصديق الإلكتروني، على العكس المشرع المصري الذي حصره في إصدار شهادات التصديق الإلكتروني فقط.

أكثر من ذلك، وسع المشرع الجزائري من دائرة الأعمال التي تدخل في نطاق التجريم، حيث لم يقتصر على تجريم مزاولة النشاط دون الحصول على ترخيص، بل نص على إعتبار الأفعال التي يمارسها رغم سحب الترخيص فعلا جرميا كذلك. حين نص"...**يستأنف أو يواصل نشاطه...**" ذلك ان مقدم خدمة التصديق قد يرغب في وقف نشاطه المتعلق بتادية خدمة التصديق، فهنا يجب عليه اعلام السلطة الإقتصادية للتصديق في الآجال المحددة في سياسة التصديق لهذه السلطة بهذه الرغبة، ويترتب على وقف النشاط سحب الترخيص.وهو **بذلك يأخـــذ حكـــم الغير**، على أساس أن السحب قد جرده من صفته كمزود خدمة.

والجرائم التي نحن بصددها من جرائم السلوك المجرد، إذ لم يتطلب المشرع لقيامها حدوث نتيجة مادية منفصلة عن النشاط الإجرامي الصادر من الجاني، وذلك سعيا من المشرع من خلال تجريم هدا الفعل من وقف آثاره عند مرحلة الخطر لكي لا تتطور لمرحلة الضرر.

ب-الركـــن المعنـــوي

جريمة مزاولة نشاط خدمة التصديق أو إستئنافه رغم سحبه جريمة عمدية، يتخد الركن المعنوي فيها صورة القصد الجرمي العام بعنصريه العلم والإرادة، ذلك أنه يكفي لمعاقبة مزود الخدمة أن يعلم بأنه غير مرخص له في ممارسة نشاط التصديق ومع ذلك يقدم عليه، وتنصرف إرادته إليه، ويقبل النتائج المترتبة على ذلك.

ت-العقوبـــــــة

يعاقب المشرع على هذه الجريمة بالحبس من سنة الى 3 سنوات وبغرامة من 200000 الى مليوني دينار أو باحدى هاتين العقوبتين بموجب المادة 72 من قانونالتوقيع الإلكتروني الجزائري. كعقوبة اصلية، وبمصادرة التجهيزات التي استعملت لإرتكاب الجريمة كعقوبة تكميلية.

ويعاقب بموجب المادة 23 من قانون التوقيع المصري بالحبس وبالغرامة التي لا تقل عن عشرة الاف جنيه ولا تجاوز مائة الف جنيه او باحدى هاتين العقوبتين، وذلك مع عدم الإخلال باية عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون اخر.

ثانيا- إصدار شهادات التصديق الإلكتروني بدون ترخيص

ورد النص على هذه الجريمة في المادة 23-1 من قانون التوقيع الإلكتروني المصري التي عاقبت كل من أصدر شهادة تصديق الكتروني دون الحصول على ترخيص بمزاولة النشاط من الهيئة المختصة. وذلك على خلاف المشرع الجزائري الذي جاء خاليا من الإشارة الى هذا الفعل. وتاتي هذه الجريمة متسقة مع ما قررته المادة 19 السابقة الذكــر من عدم جواز مزاولة نشاط إصدار شهادات التصديق الإلكتروني إلا بترخيص من الهيئة.

وهذه الصورة التي إنفرد بها المشرع المصري تعد من أحد أهم التجريمات، وتتبع أهمية هذا التجريم من كونه يشكل الإطار القانوني الرادع الذي يضمن عدم إصدار الشهادات دون ترخيص، بسبب الآثار الخطيرة التي تترتب على هذه الشهادة في حق الغير[1]، حيث يكون مضمونها التسليم بصحة بيانات التوقيع أو بيانات المعاملة المطلوب صدور شهادة التصديق عنها، ومما لا شك فيه أن هذا السلوك يشكك في الثقة التي يجب توافرها في التعاملات الإلكترونية، والتي لأجلها صدر تشريع مثل التوقيع الإلكتروني.

أ-الــركن المــادي

تتمثل هذه الجريمة في فعل إصدار الشهادة دون ترخيص، بأن ينتحل الجاني صفة مزود الخدمة. ولايكفي مجرد اعلان النية عن إصدار الشهادات، لكي تقوم الجريمة، بل لا بد أن يكون الجاني قد زاوله فعلا .بأن أصدر الشهادة التي تعد دليلا مباشرا على مباشرة هذا الفعل.

غير أن المشرع لم يكن دقيقا في حصر الأفعال التي قد تمس الثقة في التعاملات الإلكترونية، إذا ما قورن مع بعض التشريعات كما هو حال المشرع الإماراتي الذي جرم بموجب المادة 29 كل من أنشا شهادة تتضمن أو تشير إلى بيانات غير صحيحة مع علمه بذلك، والإنشاء هو نوع من الإصطناع الذي يعد إحدى طرق التزوير المنصوص عليه قانونا، بالإضافة إلى فعل النشر والتــقديم[2].

ب-الركــن المعنــوي

[1]-**ايمن رمضان محمد احمد**، المرجع السابق، ص 132.

[2]-أكثــر تفاصيل: أنظر **محمد أمين الخرشة، نايف عبد الجليل الحمايدة**، الحماية الجنائية للتوقيع الإلكتروني في التشريع الإماراتي والبحريني، مجلة جامعة الأزهر، المجلد 16، العدد 1، سلسلة العلوم الإنسانية، غــزة، 2014، ص 339.

تميز نص المادة 23–أ من ناحية البناء المعنوي بأن المشرع استخدم فيه عبارة "أصدر، وهو مايفيد أن هذه الجريمة عمدية[1]، يتخد الركن المعنوي فيها صورة القصد الجرمي بعنصريه العلم والإرادة، وذلك بأن يعلم الجاني بأن سلوكه المتمثل في إصدار الشهادة دون ترخيص هو سلوك مجرم، وان تتجه إرادته للقيام بهذا الســـلوك.

ت–العقوبـــــــة

أخضع المشرع المصري بموجب المادة 23 كل من يصدر الشهادة دون ترخيص إلى عقوبة الحبس و الغرامة التي لا تقل عن عشرة الاف جنيه ولاتجاوز مائة الف جنيه أو بأحدى هاتين العقوبتين، وفي حالة العود تزداد بمقدار المثل، العقوبة المقررة لهذه الجرائم في حديها الأدنى والأقصى.

وفي جميع الأحوال يحكم بنشر حكم الإدانة في جريدتين يوميتين واسعتي الإنتشار، وعلى شبكات المعلومات الإلكترونية المفتوحة على نفقة المحـــكوم عليه.

ثالثا– التعامل في بيانات إنشاء توقيع إلكتروني موصوف خاصة بالغير

رأينا فيما سبق أن التوقيع الإلكتروني لكي يكون موصوفا يجب أن يتم انشاؤه بواسطة أدوات تكون خاصة بالشخص الموقع، وأن تكون خاضعة لسيطرته وحده دون غيره من ذلك المفتاح الشفري الخاص، وعادة ما يتم إصدارهذا النوع من المفاتيح فضلا عن المفتاح التشفيرالعام من جهة التصديق، إلا أنه في المقابل لا يجوز لهدا الأخير أن يحتفظ بها أو ينسخها، وذلك كون المفتاح الشفري الخاص يجب أن يكون سريا، و إذا كان من الواجب على الموقع فور توقيعه على شهادة التصديق الإلتزام بالحفاظ على سرية بيانات انشاء التوقيع الإلكتروني وتجنب تسلم أي شخص غير مأدون له لهذه البيانات وإستخدامها في التوقيع ، ويتعين عليه استخدام آليات مادية ذات نوعية خاصة مؤمنة بكود سري كالبطاقة الذكية، فان الأمر لا يخلو من القول بامكانية إنتهاك سرية هذه البيانات.

ومن مظاهر إدراك المشرع الجزائري للأضرار الي يمكن ان تترتب جراء تسريب هذه البيانات، ان نص في المادة 68 من قانون التوقيع الإلكتروني على أنه "**يعاقب...كل من يقوم بحيازة أو إفشاء أو إستعمال بيانات إنشاء توقيع الكتروني موصوف خاصة بالغير**". غير أن القانون المصري قد صدر خاليا من أي نص مماثل مكتفيا في ذلك بالفقرة ج من المادة 23 التي عاقبت على مخافة احكام المادة 21، والتي نصت على كون بيانات التوقيع الإلكتروني والوسائط الإلكترونية سرية ولا يجوز لمن قدمت اليه أو اتصل بها بحكم عمله افشاؤها للغير او إستخدامها في غير الغرض الذي قدمت من أجله.كما عاقب في المادة 23 –ه **.كل من توصل باية وسيلة إلى الحصول بغير حق على توقيع الكتروني.**

[1]- د. **محمد عبيد الكعبي**، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة، 2010، ص664، **د.عبد الفتاح بيومي حجازي**، النظام القانوني للتوقيع الإلكتروني، المرجع السابق، ص541.

انطلاقا مما سبق، يتضح لنا ان النشاط الإجرامي في جريمة التعامل غير المشروع في بيانات انشاء التوقيع الإلكتروني يتمثل في فعل حيازة أو إفشاء أو إستعمال، تنصب هذه الأفعال على محل محدد وهو بيانات إنشاء التوقيع الإلكتروني الموصوف الخاصة بالغير.

أ- الـــركن المـــادي

تتحقق هذه الجريمة في الحالة التي يكون فيها الشخص قد تمكن من حيازة بيانات إنشاء توقيع إلكتروني والخاصة بالغير والتي لا يكون له الحق في الحصول عليها، أو الإطلاع عليها، أو حفظها أو تخزينها، وإن كانت الحيازة غير المشروعة لهذه البيانات إنما على درجة من الصعوبة إدا ماتمت بواسطة شبكة الأنترنت، كعملية تقنية تحتاج إلى برمجة معقدة، فإنها قد تاخد شكلا آخر أكثر سهولة يتمثل في تتبع التوقيع الإلكتروني لشخص ما بما يستدعي الأمر هنا إحداث إختراق تام من خلال معرفة الخادم المشترك فيه هذا أو داك للشخص، ثم القيام بعد ذلك بالبحث فيه عن الهوية IP الخاصة بدلك الشخص، ثم يقوم بإستنساخ التوقيع الإلكتروني الخاص به[1].

وفي الفروض السابقة، فإن الجاني يقوم بمشاركة صاحب البيانات في الحيازة دون الحرمان منها، وتلك نقطة قد أثارت الكثير من الجدل فيما إدا كان العدوان يدخل في طائلة جرائم الأموال، سيما وان الحيازة في جريمة السرقة أثارت الكثير من الجدل حتى في افضل الفروض حين يقوم الفاعل قد إستولى على المعلومات ثم قام بإلغاء المحل الأصلي، إد يبقى الجدل قائم حول المال محل الحيازة، وفيما إداكان يتميز بالأصالة أم نسخ؟

إن المشرع الجزائري وإن كان له السبق في محاربة الجريمة المعلوماتية، إلا أنه قد أغفل تجريم العديد من السلوكات كما هو الحال بالنسبة للسرقة، إذ انه لم يعدل المادة 350 التي تنص على أن السرقة هي اختلاس شيء غير مملوك للسارق ، لتبقى مسالة دخول المعلومات بطبيعتها المعنوية في نطاقها كما هي محلا الجدل الواسع الذي قد يصل إلى درجة التناقض في مجال الفقه وخلافا يرقى إلى مستوى التعارض في محيط القضاء، خاصة ما يتعلق بالإختلاس حسبما هو مستقر عليه في الفقه والقضاء ومدى انطباقه على الإختلاس المعلوماتي، كون الأول يعني إنهاء الحيازة للمجني عليه للمال وإدخاله في حيازة الجاني، بعكس الحال في الإختلاس المعلوماتي. رغم أن هناك توجه في الفقه[2] يرى امكانية اعتبار المعلومات محلا للسرقة بسبب ان المشرع ذكر لفظ الشيء دون قيد او شرط في المادة 350، وهو ما يدخل في نطاقه الأشياء المعنوية التي يصدق عليها وصف المال، نظرا لقيمتها الإقتصادية.إلا أننا لا نتفق معه، ذلك أن كلمة الشيء التي استخدمها المشرع الجزائري متبعا في ذلك المشرع الفرنسي والتي دفعت البعض إلى القول بان مدلول هذه الكلمة من الاتساع بحيث يشمل الأشياء المادية وغير المادية وهو ما يجعل المعلومات تدخل في نطاق

---

[1]- **د. عمر بن يونس**، الجرائم الناشئة عن إستخدام الأنترنت، المرجع السابق، ص ص421-428.

[2]- **د. أحسن بوسقيعة**، الوجيز في القانون الجزائي الخاص، الجزء الثاني، الطبعة الخامسة، دار هومة، الجزائر، 2006، ص259 وما بعدها. **آمال قارة**، المرجع السابق، ص28 -29. **فايز محمد راجح غلاب** ، المرجع السابق، ص118.

هذه الكلمة أمر لا يمكن إقراره على الإطلاق, ذلك أن تفسير هذه الكلمة ينبغي ألا يكون بمعزل عن العنصر الثاني في السرقة ألا وهو فعل الاختلاس[1] الذي يقتضي نقل الشيء أو أخذه أو نزعه من مالكه[2] متضمنا تغييرا في الحيازة القانونية لهذا الشيء، ويقود مثل هذا المنطق القانوني إلى أن يكون هذا الشيء بطبيعته ماديا. بل حتى إذا ما تحقق الاختلاس دون نزع الشيء من مالكه لأنه تحت اليد العارضة للجاني, فان القول بذلك لا ينفي عن المحل طبيعته المادية, فاليد العارضة تفترض أن الشيء موجود بين يدي الشخص ويعد ذلك دليلا على ماديته. ومثل هذا الأمر يحتاج إلى تفسير ولا يمكن تفسيره في ضوء أحكام السرقة، وإنما في ضوء **نصوص جديدة** تتلاءم والطبيعة الخاصة لهذه النبضات الإلكترونية.

إلا انه في المقابل، أورد نصا خاصا قيد نطاق حماية المعلومات فيه بمجرد الحيازة غير المشروعة للبيانات السرية التي تشكل التوقيع الإلكتروني للموقع، وبدون الحاجة إلى نشاط آخر، ولعل أشهر تطبيقاتها مايتعلق بحركة المعاملات المالية عبر الأنترنت والمشاكل المتعلقة بالمعطيات الرقمية السرية للبطاقات البنكية والتي سنأتي على دراستها في المبحث الثالث من هذه الدراسة.

وتجدر الإشارة، إلى أن الحيازة هنا لا تقوم الا بسيطرة الحائز على هذه البيانات. ويفترض في الحيازة وجود البيانات لدى الحائز دون تقديمها لغيره. وهي من جرائم السلوك المجرد أو جرائم الخطر، لعدم توقف العقاب عليها على حصول نتيجة إجرامية معينة.

وإدا كانت حيازة البيانات أمر خطير، فإن الأخطر من ذلك كله هو القيام بإستعمال هذه البيانات بشكل غير مشروع، قد يتبادر إلى الدهن للوهلة الأولى أن هذه الحالة تتحقق في حالة ما إدا كان إستعمال بيانات إنشاء التوقيع الإلكتروني غير مستند لتفويض أو توكيل من صاحب التوقيع الإلكتروني او كان قد تجاوز حدود هذا التفويض.

الملاحظ في هذا الخصوص، أنه في البيئة التقليدية ، أن توقيع شخص بإسم ولمصلحة الغير لا يعني أنه يوقع بتوقيع الغير، وإنما هو يوقع عن الغير، أما من يوقع بتوقيع الغير فإنه يعتبر منتحلا ويشكل ذلك **تزويـــرا**. وحتى على إحتمال إعتبار أن هذه الحالة تنطبق على الفرض السابق، أي عدم وجود تفويض من صاحب التوقيع، فإن هذا الفرض سرعان ما نرفضه إذا ما رجعنا إلى نص المادة 07 ،حيث نجدها قاطعة الدلالة في ضرورة سيطرة الموقع وحده دون غيره على وسيلة التوقيع، متى سعينا وراء وصف التوقيع المستخدم على هذا النحو بأنه **موصوف**، وهو ما يعني وجوب أن يحافظ الموقع على المفتاح الشفري الخاص به، وأن يحرص على سريته، الأمر الذي نستنتج منه عدم جواز قيام الشخص بإنابة غيره في التوقيع الإلكتروني بإستخدام مفتاحه الخاص، وهو ما تتطلبه سلامة التعاملات الإلكترونية.

---

[1]– **د.نائلة عادل محمد فريدة قورة**، المرجع السابق، ص158.

[2]– قرار لمحكمة النقض (الغرفة الجزائية) بتاريخ 18 نوفمبر 1837، أطلع عليه لـــدى: **بن شيخ لحسين**، مذكرات في القانون الجزائي الخاص–جرائم ضد الأشخاص، جرائم ضد الأموال،– الطبعة الخامسة، دار هومة، الجزائر، 2006، ص127.

والإستعمال يفترض بداهة الحصول على بيانات انشاء التوقيع الإلكتروني، ويتم ذلك عادة في الإستيلاء على منظومة التوقيع الإلكتروني التي تحتوي على بيانات إنشاء التوقيع الإلكتروني(المفتاح الشتفير الخاص) عن طريق معرفة الرقم السري أو القرصة الإلكترونية أو غيرها، ثم يتم بواسطتها التوقيع إلكترونيا باستخدام بيانات إنشاء التوقيع الإلكتروني دون موافقة صاحبه مما يؤدي إلى إلحاق الضرر به أيا كانت صوره، ومن ثم فإن هذه الجريمةتقع في الغالب **مركبة**[1]، مشكلة بدلك أهم خاصية لجريمة **تزوير التوقيع الإلكتروني**.

فضلا عن فعل الإستعمال، تناول المشرع بالتجريم فعل **الإفشاء**، و يفترض في الإفشاء انتقال هذه البيانات الخاصة بالموقع من حيازة الجاني الى غيره من الأشخاص، حيث انه يقوم بتقديم هده المعلومات الى غيره، ولا يقصرها على نفسه. ونظرا لإمكانية وقوع هذا الفعل من طرف موظفي الجهة المرخص لها بإصدار الشهادات، وذلك بكشف مفاتيح التشفير المودعة لدى جهة التصديق، الزمه المشرع بادراج توقيعه على شهادة التصديق الإلكتروني الموصوفة التي يمنحها. حتى يمكن تحديد مسؤوليته ادا اقتضى الأمر ذلك.

هذا ولم يشترط المشرع تحقق غاية معينة من وراء هدا الإفشاء، إد جاء النص عاما في المحافظة على السرية، تغليبا لمصلحة صاحب الشان في افشاء البيانات المتعلقة بانشاء توقيعه. كما انه لم يشترط في الفاعل ان يكون ملزما بموجب وظيفة معينة او عقد ما بكتمان هده البيانات، وهو ما يستفاد من الصيغة المطلقة للتي جاءت عليها المادة 68، وبالتالي تقع الجريمة من أي شخص مهما كانت صفته سواء كان يعمل في مجال التصديق الإلكتروني او لا علاقة له بدلك،خاصة إدا كان مفتاح التشفير الخاص تم حفظه في قرص صلب للحاسوب الشخصي حيث يسهل التقاطه عبر الشبكة، ويتحقق في هذا الفرض التعدد المادي للجرائم، جريمة الإختراق المنصوص عليها في المادة 394 مكرر وجريمة حيازة توقيع الكتروني. وقد عبر عن ذلك المشرع في مطلع المادة "**...كل من يقوم...**".

ولما كان الموظف في مركز سهل يسهل له إرتكاب الجريمة بحكم وظيفته، وهو الأمر الذي يقود بحكم المنطق العقلي والقانوني إلى تشديد العقوبة في هذه الحالة. وهو ما جانبه المشرع الجزائري.

والمتامل في الإتجاه التشريعي المعتنق من قبل المشرع الجزائري يلحظ جنوحا تشريعيا بإتجاه التشدد في حماية التوقيع الإلكتروني الموصوف، ويبدو ذلك واضحا من خلال هذه المادة، حيث تجرم أفعال تنصب على بيانات انشاء التوقيع الإلكتروني الموصوف، وبمفهوم المخالفة فإن التوقيع الإلكتروني البسيط يبقى خارج نطاق الحمـــاية.

ويقصد ببيانات إنشاء هذا التوقيع وفق التعريف الوارد في الفقرة 3 من المادة 2 من قانون التوقيع الإلكتروني "بيانات فريدة، مثل الرموز أو مفاتيح التشفير الخاصة، التي يستعملها الموقع لإنشاء التوقيع الإلكتروني. والملاحظ أن هذا التعريف يرتبط فقط بالعناصر الأساسية لإنشاء التوقيع التي يجب أن تظل سرية لضمان سلامة عملية التوقيع[2].

---

[1]- إذ تتكون من جريمتي الإستيلاء على منظومة التوقيع وإستعمالها: **عبد الإله محمد النوايسة**، مدى توفير حماية جزائية للتوقيع الإلكتروني ومعطياته في القانون الأردني، المجلة الأردنية في القانون والعلوم السياسية، المجلد 2، العدد 2، ربيع الثاني 1431، نيسان، 2010، ص125.

[2]- وعلى ذلك فإن بيانات إنشـــاء التوقيع تعني على الأخص مفاتيح تشفير خاصة سواء كانت منظومة هدا المفتاح مدونة على قاعدة بيانات الحاسب الآلي ام تم الإحتفاظ بها على دعامة خارجية مثاله البطاقة الدكية.

بالإضافة إلى ما تقدم، لم يعتبر المشرع أي منظومة يتم بواسطتها التوقيع إلكترونيا باستخدام بيانات الإنشاء منظومة يصمم بها التوقيع الإلكتروني الموصوف، بل إشترطت ضوابط –كما مر معنا– حددتهما الفقرة 1 و2 من المادة 11، و من الوسائل التي تحقق تلك الشروط نجد بطاقة الداكرة أو البطاقة الذكية، فهده البطاقة توفر بعض الموثوقية ذلك أنه لا يتم إستخدامها إلا بمفتاح واحد صحيح، ورمز سري[1].

وجرائم التعامل غير المشروع في بيانات انشاء التوقيع جرية شكلية اذ لم يتطلب المشرع لقيامها حدوث نتيجة مادية، والمشرع لا يقرر هدا النوع من الحماية في مرحلة مبكرة الا للمصالح بالغة الأهمية وهو ما رآه بالنسبة للمصالح المتعلقة ببيانات التوقيع الإلكتروني.

والأفعال السابقة هي على قدم المساواة في تحقيق النشاط الجرمي المكون للركن المادي لجريمة التعامل غير المشروع في بيانات إنشاء التوقيع الإلكتروني، وهو مايستفاد بوضوح من لفظ "أو" الوارد في المادة اعلاه، وهو ما يعني انه يكفي لتحقق النشاط الإجرامي قيام الجاني باحدى هاته الأفعال.

ب–الركـــن المعـــنوي

جريمة التعامل في بيانات التوقيع الإلكتروني جريمة مقصودة، يتخد الركن المعنوي فيها صورة القصد الجرمي بعنصريه العلم والإرادة. وعلم الجاني لا بد ان يحيط بكافة العناصر الداخلة في تكوين الجريمة، ومن قبيل ذلك ضرورة علم المتعامل انه يقوم بالتعامل في بيانات انشاء توقيع الكتروني موصوف خاصة بالغير، وان هذا السلوك يحمل تهديدا للمصلحة المحمية.

ولا يكفي أن يكون المتعامل عالما بما يفعل لقيام الجريمة، بل يجب أن تكون إرادته متجة الى تحقيق و إتيان أحد المظاهر السوكية التي نص عليها المشرع ومن هي الحيازة والإستعمال والإفشاء رغم علمه بصفتها غير المشروعة.

ولما كانت هده الجريمة شكلية، فان الإرادة فيها لا تنصب الا على النشاط فحسب ولا تتعداه الى النتيجة.

ت–العقوبـــــة

اخضع المشرع المتعامل في هده البيانات لعقوبة الحبس من 3 أشهر إلى 3 سنوات و بغرامة من مليون دينار إلى خمسة ملايين دينار او باجدى هاتين العقوبتين.والملاحظ أن المشرع الجزائري عاقب على هذه الجريمة في قانون التوقيع الإلكتروني، وفي قانون عصرنة العدالة رقم 15–03، حيث نجد نص مماثل وهو نص المادة 17 التي عاقبت **كل شخص يستعمل بطريقة غير قانونية العناصر الشخصية المتصلة بإنشاء توقيع الكتروني يتعلق بتوقيع شخص أخر**" إلا أن ما يميز هذا النص انه يسري فقط على التوقيع الإلكتروني المرتبط ببيانات الوثائق والمحررات القضائية التي تسلمها مصالح وزارة العدل والمؤسسات التابعة لها

[1]**Alain Bensoussan et Charles Copin**, le livre blanc de la signature electronique ; le groupe de travail du Club CSA; *ANALYSES et SYNTHESES; 1999, p42.

والجهات القضائية. ونظرا لحساسية هذا القطاع فقد شدد عقوبه الحبس حيث جعل عقوبتها الحبس من سنة إلى خمس سنوات في حين خفض الغرامة من 100000 دج إلى 500000، وذلك على خلاف النص العام.

رابعا- الحصول بغير حق على التوقيع أو الوسيط الإلكتروني الذي يحويه

أ-الركـــن المـــادي

نص المشرع المصري على هذه الصورة بموجب المادة 23 –ه على مايلي"**يعاقب...كل من توصل باية وسيلة إلى الحصول بغير حق على توقيع أو وسيط أو محرر الكتروني**، بينما إكتفى المشرع الجزائري بالعقاب بموجب المادة 68 على كل من يحوز بيانات إنشاء توقيع إلكتروني خاصة بالغير. كما جرم بموجب نص عام جريمة الدخول غير المصرح به الى النظام كجريمة شكلية بموجب المادة 394 مكرر التي إستطاعت أن تسد العديد من الثغرات في القانون، ادان المشرع وان نحى جانبا العديد من الأفعال التي فات عليه تجريمها بموجب نصوص صريحة، فلا يفلت المجرم من العقاب بل يعاقب استقلالا عن هده الجريمة داتها.

ويتضح من نص المادة السابقة، أن الركن المادي لهده الجريمة يتم بسلوك إجرامي يرتكبه الجاني يتخذ صورة "**التوصل**"، وهو مدلول يفيد السعي من جانب الشخص الى الحصول على شيء معين، ولو تأملنا في البناء المادي لهذه المادة لوجدنا أن المشرع لم يحدد طبيعة الوسيلة المستخدمة في الحصول على التوقيع أو الوسيط الإلكتروني بل وسع من نطاق تطبيقها لتشمل بالتجريم كل الوسائل التي يمكن إستخدامها في إرتكاب الجريمة مهما كانت طبيعتها، بشرط أن يكون الحصول بغير حق.ومن ثم يستوي أن تكون هذه الوسيلة مشروعة أو غير مشروعة. سواء تم ذلك عن طريق معرفة الرقم السري للدخول للمعلومات التي تحويها منظومة التوقيع[1]، أو تم بواسطة شبكة الأنترنت عن طريق القرصنة الإلكترونية أو التجسس الإلكتروني، وهذا السلوك يشكل في ذاته جريمة معاقب عليها وهي **جريمة الدخول غير المشروع إلى النظام**. وبذلك تقع جريمة الدخول غير المصرح به وجريمة الحصول على التوقيع. كما قد يتم ذلك من خلال فض مفاتيح التشفير، وذلك من خلال الحصول على البرامج الخاصة بتشفير التوقيع الإلكتروني، سواء إستطاع الجاني فض الشفرة بنفسه أو بواسطة مختص.

ولما كان التوقيع الإلكتروني يتعرض للإعتداء، فان تشفير البيانات بوصفها طريقة من طرق حماية هده البيانات فنيا قد تكون عرضة للإعتداء بذات الطريقة[2]. ولهذا السبب إهتمت القوانين بمعالجة مسألة حماية البيانات المشفرة، حيث نجد المشرع التونسي يعاقب صراحة بموجب المادة 48 على كل من يستعمل بصفة غير مشروعة عناصر تشفير شخصية متعلقة بامضاء غيره، إلى جانب ذلك نجد المشرع الجزائري يعاقب ضمن المادة 68 على كل من يفشي او يستعمل بيانات انشاء توقيع إلكتروني موصوف خاصة بالغير،

[1]- خاصة إذا كان صاحب الجهاز قد ضغط على تقنية تذكر كلمة الســر فيه".

[2]–**د. عبد الفتاح بيومي حجازي**، الحماية الجنائية لنظام التجارة الإلكترونية، المرجع السابق، ص311.

وبيانات الإنشاء حسب الفقرة 3 من المادة 2 هي بيانات فريدة، من بينها مفاتيح التشفير الخاصة وعلى ذلك فنص المادة يشملها، إلا أن القانون المصري جاء خاليا من نص صريح على تجريم فض مفاتيح التشفير، ولربما يرجع السبب في ذلك إلى كون جريمة التوصل بأي وسيلة إلى الحصول بغير حق على توقيع يتم في الغالب بفض مفاتيح التشفير.

بيد أنه ليس في كل الحالات التي يتم فيها فض مفاتيح التشفير الحصول على التوقيع الإلكتروني، وهو ما دفع البعض[1] إلى القول بضرورة التدخل لتجريم فض مفاتيح الشتفير بنص خاص، إلا أن هناك من يرى[2]– وبحق–أن تجريم كشف مفاتيح التشفير ينطوي على قدر من نقصان الحماية الجزائية لبيانات التعاملات الإلكترونية، لأن التشفير ليس هو الوسيلة الوحيدة لحماية سرية وخصوصية البيانات، فهناك نظم حماية كثيرة. وعلى ذلك فالأصوب ان يكون تدخل المشرع بنص خاص يجرم به التعدي على نظم الحماية التقنية، أو إعتباره ظرفا مشددا، وهو الإتجاه الدي نراه أولى بالإتباع، ذلك أن إستعمالها يعد قرينة على أهمية المعلومات التي تتضمنها النظم، وان كانت النظم ليست في موضع يمكنها التمييز بين الفروض المختلفة للشرعية فان المشرع يميزها بتشديد العقوبة.

اما عن محل هده الجريمة، فهو التوقيع او الوسيط الكتروني، ويقصد بهدا الأخير أداة أو أدوات أو أنظمة إنشـــاء التوقيع الإلكتروني.

فضلا عن ذلك، عاقب المشرع بموجب المادة السابقة على فعل إختـــراق الوســـيط أو إعتراضه أو تعطيله عن أداء وظيفته، والذي يتمثل في نظام معلوماتي أو قاعدة بيانات تتعلق بالتوقيع الإلكتروني ذاته. ويشير فعل الإختراق إلى أي**تفاعل ناجح مع النظام** الذي يحوي التوقيع الإلكتروني على نحو غير مشروع، هدا وقد استخدم المشرع المصري مصطلحات تسمح بتجريم إستعمال أي وسيلة تقنية تسمح بإختراق النظام على نحو غير مشروع.

ويبدو مما سبق وجود تقارب بين هذه الجريمة وجريمة الدخول غير المشروع الى نظام المعالجة الآلية التي عاقب عليها المشرع الفرنسي بموجب المادة 323–1 عقوبات، والمشرع الجزائري بموجب المادة 394مكرر عقوبات، لكن ما يميزها أن نص المادتين السابقتين جاء عاما يشمل جميع نظم المعالجة الآلية،أما النص المصري فيقتصر على نظم إنشـــاء التوقيع الإلكتروني فقط.

أما الفعل الثاني الذي عاقب عليه المشرع المصري فهو فعل الإعتراض، والإعتراض –كما مر معنا– يشير إلى الإلتقاط غير المشروع للمعلومات اثناء إنتقالها، ولما كان هذا الأخير إنتهاكا لإتصال معلوماتي بين النظم المختلفة أثنـــاء عملها، فقد فضلت بعض التشريعات تجريمه ضمن جريمة الدخول غير المشروع، كما هو حال المشرع الفرنسي والجزائري. وإن كان نصيهما جـــاء عاما.

---

[1]– **ايمن رمضان محمد احمد**، المرجع السابق، ص150.

[2]– **د. عبد الفتاح بيومي حجازي**، الحماية الجنائية لنظام التجارة الإلكترونية، مرجع سابق، ص285.

إلى جانب فعل الإختراق والإعتراض، عاقب المشرع المصري على فعل التعطيل، ويقصد بالتعطيل جعل النظام غير قادر على الإستعمال السليم، وذلك بأن يعطي نتائج غير التي تلك كان من الواجب الحصول عليها[1].

والملاحظ أن المشرع لم يبين الحكم فيما لو ترتب على فعل التعطيل توقيف مصلحة ذات منفعة عامة، ففي هذه الحالة تصبح الواقعة جناية عملا بنص المادة 361 عقوبات[2]، ويتطلب الركن المـــادي في هذه الحـــالة تحقق نتيجة محددة وهي تعطيل أعمال مصلحة ذات منفعة عامة.

ب-الـــركن المـــعنوي

كما لاحظنا من خلال دراستنا لنص المادة 23-ه من القانون المصري،أنهده الجريمة مقصودة، و يتطلب القصد العام فيها ان يعلم الجاني انه يقوم باحدى الأفعال التي أوردها النص القانوني، كان يعلم انه يقوم بالإختراق أو الإعتراض على الوسيط الذي يحوي التوقيع الإلكتروني،وأن يعلم أن نشاطه غير مشروع، وأن تتجه إرادته الى إرتكاب هده الأفعال. وكون هذه الجريمة من جرائم الخطر فلا تتعدى إلى النتيجة الجرمية.

ت- العقوبـــــة

عاقب المشرع المصري على هذه الجريمة بموجب المادة 32 بالحبس وبغرامة لا تقل عن عشرة الاف جنيه و لا تجاوز مائة الف جنيه او باحدى هاتين العقوبتين. وضاعف المشرع العقوبة في حالة العود.

الفرع الثاني

الإعتداء على حجية التوقـــيع الإلكتروني

الأصل أن التوقيع يرتبط إرتباطا وثيقا برضاء صاحبه وإقراره بمضمون التصرف القانوني الذي تضمنه المستند بتوقيعه في النهاية، وقد أثار الخلط بين الحماية المقررة للمستند وبين الحماية المقررة للإرادة بعض الصعوبة، ويرجع ذلك إلى صعوبة الجزم بصحة التوقيع الإلكتروني، ومدى الوثوق برضاء صاحبه

---

[1]-**ايمن رمضان محمد احمد**، المرجع السابق، ص161.

[2]-تنص المادة 361 من قانون العقوبات المصري" كل من خرب أو أتلف عمدا أموالا ثانية أو منقولة لا يمتلكها أو جعلها غير صالحة للاستعمال أو عطلها بأية طريقة يعاقب بالحبس مدة لا تزيد على ستة أشهر وبغرامة لا تجاوز ثلاثمائة جنيه أو بإحدى هاتين العقوبتين.

فإذا ترتب على الفعل ضرر مالي قيمته خمسون جنيها أو أكثر كانت العقوبة الحبس مدة لا تجاوز سنتين وغرامة لا تجاوز خمسمائة جنيه أو بإحدى هاتين العقوبتين.

وتكون العقوبة السجن مدة لا تزيد على خمس سنين وغرامة لا تقل عن مائة جنيه ولا تجاوز ألف جنيه إذا نشأ عن الفعل تعطيل أو توقيف أعمال مصلحة ذات منفعة عامة أو إذا ترتب عليه جعل حياة الناس أو صحتهم أو أمنهم فى خطر.

بالتصرف الذي وقع عليه[1]، فإذا شاب إرادة المـــوقع عيب ما بان قام بوضع التوقيع على مستند، بينما إنصب هذا التوقيع على مستند آخر يحوي مضمون مختلف **فهل يشكل هدا الفعل اعتداء على المستند داته، ام ان هناك صورا أخرى من الحماية تختلف عن الحماية المقررة للمستند بصفة عامة؟**[2] ايد المشرع المصري هده الوجهة، وعاقب بمقتضى المادة 23–ب التي **نصت كل من أتلف أو عيب توقيعا أو وسيطا أو محررا الكترونيا او زور شيئا من دلك بطريق الإصطناع أو التعديل او التحوير او باي طريق اخر" كما نصت الفقرة ج من نفس المادة على كل من يستعمل توقيعا أو وسيطا أومحررا الكترونيا معيبا أومزورا مع علمه بذلك".**

أما المشرع الجزائري فقد إكتفى بالنص العام، المتعلق بالتلاعب بالمعلومات كجريمة مستقلة واعاقة أو تحريف تشغيل النظام كظرف مشدد، وبما أن التوقيع الإلكتروني هو عبارة عن بيان الكتروني موجودة على وسيط الكتروني، فان الحماية الجزائية المقررة للنظام ومعطياته تنطبق عليه.

أولا–الـــركن المـــادي

ويتحقق الركن المادي في هذه الجريمة إما بإتلاف أو تعييب، أو تزوير التوقيع الإلكتروني، إستعمال توقيـــع الإلكتروني معيب أو مزور.

أ–إتلاف أو تعييب التوقيع الإلكتروني:

يتحقق الركن المادي في هذه الجريمة بإتلاف أوتعييب التوقيع الإلكتروني، وفعل الإتلاف يتحقق بإفقاد البرنامج المعلوماتي الخاص بالتوقيع الإلكتروني كليا قدرته على العملبأي وسيلة كانت، ومن قبيل ذلك نشر فيروس معلوماتي أو سكب كوب من الماء على الوسيط المحفوظ فيه.

أما التعييب فهو الإفقاد الجزئي لهذا البرنامج الخاص بالتوقيع الإلكتروني، بذات الوسائل السابقة كأن يصدر مشوها أو غير واضـــح[3].

ب–تزوير التوقيع الإلكتروني:

ويتحقق حسب المادة 23–د بتغيير الحقيقة في التوقيع الإلكتروني بطريق الإصطناعوالتعديل أو التحوير على نحو يحقق الإضرار بالغير. والملاحظ أن الطرق التي يتم بها التزوير بالنسبة للتوقيع الإلكتروني جاءت على سبيل التمثيل، ونستدل على ذلك من عبارة "**أو بأي طريق آخر**_الواردة في نص المادة السابقة.

---

[1]–**د. عبد الفتاح بيومي حجازي**، التوقيع الإلترويني في النظم القانونية المقارنة، المرجع السابق، ص357.

[2] – **د. هدى حامد قشقوش**، الحماية الجنائية للتوقيع الإلكتروني –دراسة مدمة إلى المؤتمر الديعقدته كلية الشريعة و القانون بجامعة الإمارات العربية المتحدة في موضوع القانون والأنترنت، 1–1 مايو ، 2000، ص 581. ، **د. أيمن رمضان محمد أحمد**، المرجع السابق، ص99.

[3]- **د. محمد عبيد الكعبي**، المرجع السابق، ص664.**د.عبد الفتاح بيومي حجازي**، النظام القانوني للتوقيع الإلكتروني، المرجع السابق، ص542.

وعلى الرغم من خلو القانون الجزائري من نص صريح على تجريم تزوير التوقيع الإلكتروني، إلا أنه يمكنتدارك ذلك من خلال المادة 68 منه التي عاقبت كل من يقوم بحيازة أو باستعمال بيانات إنشاء توقيع إلكتروني موصوف خاصة بالغير. فالجاني هنا يتصرف على أساس أنه صاحب التوقيع الإلكتروني، ويقوم باستعماله في التصرفات المختلفة التي يتحملها المتعامل الشرعي من خلال إنتحال شخصيته التي يمثلها التوقيع الإلكتروني.

ومن أشهر الوسائل التي يمكن الإعتماد عليها في تزوير التوقيع الإلكتروني إستخدام برامج حاسوبية و أنظمة معلوماتية خاصة بذلك، يتم تصميمها على غرار البرامج والأنظمة المشروعة. أو محاولة البعض كسر الشفرة والوصـــول إلى الأرقام الخاصـــة بالتوقيع الإلكتروني، والقيام بنسخها، وإعادة إستخدامها بعد ذلك[1].

ت-استعمال توقيع الإلكتروني معيب أو مزور:

وهذه الجريمة منفصلة عن جريمة التزوير، ويقوم الركن المادي فيها على فعل الإستعمال، ويقصد باستعمال توقيع الكتروني معيب أو مزور إبرازه والإحتجاج به فيما زور من أجله على إعتبار أنه صحيح[2].على أن ينصب هذا الإستعمال على توقيع الكتروني معيب أو مزور دون التالف، على إعتبار أن الإتلاف قد أنهـــى قيمته، أما الـــمعيب فيؤدي لتعطيل وظيفته ولكن بطريقة منقوصة، ولكنه يرتب آثار قانونية ولا يجوز إستعماله لأن المشرع يمنع ذلك[3].

ثانيا- الركـــن المـــعنوي

نظرا لكون الجرائم السابقة جرائم عمدية، فيتحقق ركنها المعنوي في صورة القصد الجنائي العام في صورة الإتلاف والتعييب والإستعمال، فضلا عن القصد الخاص في جريمة التزوير.

إذ يجب أن يعلم الجاني بأن فعل الإتلاف أو التعييب أو الإستعمال محظور ومعاقب عليه قانونا، وأن تتجه إرادته الى الفعل المجرم ويقبل النتائج المترتبة عليه. وإلى جانب القصد العام، يتطلب القصد الخاص في جريمة التزوير وهو نية إستعمال التوقيع الإلكتروني فيما زور من أجله[4].

ثالثا_العقوبـــــة

أما ما يخص العقوبة، فقد رصد المشرع للأفعال السابقة نفس العقوبة بموجب المادة 23 وهي الحبس والغرامة التي لا تقل عن عشرة آلاف جنيه ولاتجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين ، كما تزداد العقوبة بمقدار المثل في حديها الأدنى والأقصى في حالة العود.ومن تم فإن التكييف القانوني لهذه الواقعة هو

---

[1]- **د. خالد ممدوح ابراهيم**، التوقيع الإلكتروني، المرجع السابق، ص 279.

[2]– **د. سليمان احمد فضل**، المرجـــع السابق، ص164.

[3]–**د. محمد عبيد الكعبي**، المرجـــع السابق، ص666.

[4]–**د. عبد الفتاح بيومي حجازي**، النظام القانوني للتوقيع الإلكتروني، المرجع السابق، ص544. **د. محمـــد عبيد الكعبي**، المرجع السابق، ص666.

التزوير في توقيع عرفي، أما مايخص التوقيع الإلكتروني الرسمي فإن تزويره يشكل جناية، وهو ما يستوجب التشديد في العقوبة، وهو ما أدركه المشرعالمصريمن خلال صدر المادة 23 حين نص"...**مع عدم الإخلال بأي عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون آخر**. وما خلت منه نصوص قانون التوقيع الإلكتروني الجزائري.

نخلص مما سبق إلى إختلاف خطة التشريعات المقارنة في طريقة النص على حماية التوقيع الإلكتروني، حيث ذهب المشرع الجزائري إلى وضع نصوص خاصة ضمن قانون العقوبات كفيلة بزجر مختلف الإعتداءات المنصبة على النظم المعلوماتية، دون ان تضع ضوابط تتعلق بهذه النظم او بطبيعة معلوماتها، وهو ما يسمح بتطبيقها على نظم التوقيع الإلكتروني، كما خصص في المقابل تشريع خاص بالتوقيع الإلكتروني جرم من خلاله مختلف الإعتداءات المنصبه عليه، إلا أنه **ضيق** من نطاقها حين قصرها على التوقيع الإلكتروني **الموصوف** القائم على إجراءات التوثيق. وهي خطوة موفقة في نظرنا نحو كفالة الحماية المناسبة له خاصة من التزوير المعلوماتي، وما خلقه من مشاكل حول التفرقة بين التوقيع المزور والأصلي في مجال المعلوماتية. اما المشرع المصري فلم يضع نصوص تنظم الجريمة المعلوماتية، كما انه لم يدخل تعديلات على التشريعات القائمة، إلا انه افرد تشريع خاص للتوقيع الإلكتروني جرم من خلاله مختلف الإعتداءات التي تمسه.

إلا انه ما يعيب نهجهما، هو أن جرائم الإعتداء على التوقيع الإلكتروني ذات وصف جنحوي، وبالتالي فالعقاب على **الشروع** فيها لابد ان يكون بنص، إلا أن نصوص قانون التوقيع الإلكتروني قد جاءت خالية من النص على الشروع. ولدلك نهيب كلا المشرعين التدخل لتجريم الشروع في الجرائم التي يتصور فيها الشروع.

هذا وقد أقر المشرع الجزائري مبدأ المسؤولية الجزائية للشخص المعنوي في نطاق الجرائم محل الدراسة بموجب المادة 75، حيث اقر عقوبة الغرامة ، جاعلا منها ذات حد واحد، حيث اوجب الأخد بالحد الأقصى لهده العقوبة وهو خمس مرات فيما يتعلق بالجرائم محل الدراسة. كما نص المشرع المصري من جهته صراحة في المادة 24 على مسؤولية الشخص المعنوي عن الجرائم التي ترتكب بالمخالفة لأحكام هذا القانون.

في الأخير يمكن القول أن حماية التوقيع الإلكتروني لم تصبح مسالة خيار للمشرع، خاصة بعد أن تم إستحداث بطاقات دفع متممة للتعاملات الإلكترونية المبرمة عبر بعد بما في ذلك شراء المستلزمات اليومية، من هنا يبرز دور التوقيع الإلكروني، إذ لا بد من توافر شكل معين من أشكال التوقيع لإتمام عملية الدفع، ويسمى إستخدام الرمز السري للدفع بالبطاقة بالتوقيع الإلكتروني.

المبحـــث الثالث

الحماية الجزائيـــة لبـــطاقة الإئتمان

لقد أتاحت تقنية المعلومات وسائل متقدمة جدا في مجال الخدمات والعمل المصرفي، كأنظمة الدفع الإلكتروني بأنواعها، وإدارة الحسابات عند بعد، لذلك ظهرت مفاهيم جديدة تنسجم مع الطبيعة القانونية لتقنية المعلومات كالسفتجة الإلكترونية والشيك الإلكتروني، وبطاقات الدفع البلاستيكية لتبدأ مرحلة جديدة ينتهي معها مفهوم النقود الورقية.معلنه بدء عهد الصيرفة الإلكترونية[1]. وبنوك المستقبل.

ويشير مصطلح بطاقات الدفع البلاستيكية إلى البطاقات التي تتم معالجتها إلكترونيا لإستخدامها في أغراض متعددة من خلال المعلومات المخزنة عليها والدخول بها على الآلات المعدة لذلك بغية تحقيق أغراض معينة[2]، ومن أهم أنواع هذه البطاقات[3]:**بطاقات الإئتمان.**

تعد بطاقات الإئتمان[4] أهم وسيلة وفاء في التعاملات الإلكترونية جعلها تأخذ مكانتها بين وسائل الدفع الحديثة. فقد ربطت الأنترنت المصارف بنقاط البيع الإلكترونية، وأجهزة سحب النقود أينما وجدت، وزاد من فاعليتها تطوير بروتوكولات التعاملات الإلكترونية الأمنيةsecure electronic transaction SET[5] والذي وضع معايير موحدة للأمان عند إستخدام بطاقات الإئتمان، وذلك بتشفير أرقامها والإعتماد على التوقيع الإلكتروني في مسائل مختلفة وغير ذلك.

---

[1]-للمزيد أكثرعن الخدمات المصرفية الإلكترونية أنظر: **عرابة رابح**، دور تكنولوجيا الخدمات المصرفية الإلكترونية في عصرنة الجهاز المصرفي الجزائري، الأكاديمية للدراسات الإجتماعية والإنسانية، العدد 8، 2012، ص15.

[2] -**سحنون محمود**، النظام المصرفي والبطاقات البلاستيكية، مؤتمر عمليات البنوك بين النظرية والتطبيق، كلية القانون بالتعاون مع كلية الإقتصاد والعلوم الإدارية وعلوم التسيير، جامعة اليرموك، الأردن، 2002، ص 1.

[3] –**د. محمود الكيلاني**، التشريعات التجارية والمعاملات الإلكترونية، الطبعة الأولى، دار وائل للنشر، 2004، ص510.

[4] – إختلفت التسميات التي أطلقت على هذة الوسيلة، مثل بطاقة الإعتماد، بطاقة الدفع البلاستيكي، بطاقة الدفع الإلكتروني، إلا أن أكثرها شيوعـــا بطاقة الإئتمان.**د.محمد رأفت عثمان**، مؤتمر الأعمال المصرفية والإلكترونية، الجزء الثاني، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ماي 2003، ص616.

وقد جـــرى العرف المصرفي على تداول مصطلح النقود البلاستيكية أو الإلكترونية كمرادف لمصطلح بطاقة الإئتمان، إلىأن البعض يرى– وبحق– أنه تسمية غير صحيحة، وذلك لأسباب عديدة ترجع في مجلها للخواص التي تتميز بها هذه البطاقة، فهي من جهة من حيث القيمة المخزنة فيها متلاشية، عكس النقود بسبب فترة صلاحيتها المحددة بسنة مما يتطلب الأمر بتجديدها أو إيقافها أو الغاءها، فضلا عن ذلك انها إسمية إذ لا يمكن لأي كان أن يستخدمها، كما أنها لا تتمتع بالقبول العام من جميع الناس، فإذا كان يقبلها ملايين التجار إلا أنه توجد في البلد الواحد عدة متاجر لا تقبل البيع بها لأنها لم تتعاقد مع المصدر على قبولها والبيع بموجبها، كما أنها ثلاثية الأطراف، والمعاملات بها لا تنتهي بمجرد إطلاع التاجر عليها، بل لابد أن تستكمل المعاملة بحصول التاجرعلى حقه نقدا من البنك. **د. محمد عبد الحليم عمر**، بطاقات الإئتمان ماهيتها والعلاقات الناشئة عن إستخدامها بين الشريعة والقانون، مؤتمر الأعمال المصرفية والإلكترونية بين الشريعة والقانون، الجزء الثاني، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ماي 2003، ، ص669.

[5] –هونظام وضع لضمان أمن المعاملات المالية على الأنترنت، وأيد في البداية عن طريق ماستر كارد فيزا ومايكروفست ونتسكب وغيرها، يعطي للمستخدم شهادة رقمية ويتم التحقق من المعاملة بإستخدام مزيج من الشهادات الرقمية، والتوقيع الرقمي بين المشتري والتاجر والبنك بطريقة تضمن الخصوصية والسرية .

http://searchfinancialsecurity.techtarget.com/definition/Secure-Electronic-Transaction

والأصل أن البطاقة تستخدم بواسطة حاملها الشرعي وكونها صحيحة وفي الغرض المخصص لها، وفي حدود سقفها[1]، إلا أنه ظهرت مع تطور دورها في الحياة الإقتصادية وإنتشار إستخدامها من قبل المتعاملين بها، إستخدامات اخرجتها من دائرة المشروعية، فكان لابد من التفات المشرعين سواء على المستوى الدولي أو الإقليمي إلى تنظيم أحكامها وتجريم الإستعمال الخاطيء أو الإحتيالي لها. والتي يطلق عليها **جرائم الدائنية أو الجرائم البلاستيكية**[2]، والتي يمكن ردها إلى طائفتين أساسيتن : أفعال تقع من الحامل نفسه وأخرى تقع من الغير.

ويمكن القول أن فرنسا هي الدولة الأولى على مستوى العالم التي قامت بسن تشريع جزائي خاص في هذا المجال أطلقت عليه قانون أمن الشيكات وبطاقات الوفاء رقم 91-1382[3] ، ثم جاء القانون رقم 2001-1062 [4]والمتعلق بالأمن اليومي والمعدل للقانون النقدي والمالي، وذلك على إثر تزايد الجرائم المتعلقة بإستخدام البطاقات البنكية خاصة في إطار إستخدامها عبر شبكات الأنترنت والوفاء عن بعد، على نحو يهدد الثقة في التجارة الإلكترونية، ليقوم في خطوة تشريعية أخرى وتماشيا مع التوجيه الأروبي رقم 2007-64 [5]المتعلق بخدمة الدفع في السوق الداخلية، بتعديل التقنين النقدي والمالي بموجب الأمر رقم 2009-866[6] المتعلق بالشروط التي تحكم تقديم خدمة الدفع وانشاء مؤسسات الدفع، ليتم تكملته بالمرسوم التنفيدي رقم

---

[1]- **أمجد حمدان الجهني**، جرائم بطاقة الدفع الإلكتروني عبر شبكة الأنترنت، مؤتمرالمعاملات الإلكترونية(التجارة الإلكترونية-الحكومة الإلكترونية)، مركز الإمارات للدراسات والبحوث الإنستراتيجة، 19-20 مايو، 2009، ص2.

[2] -أي أن العالم يتحول من الجرائم التي يستخدم فيها الورق كوسيط وأداة للجريمة إلى الجرائم البلاستيكية: د. **رياض فتح الله بصلة**، جرائم الإحتيال بالبطاقات الإئتمانية وأساليب مكافحتها، جامعة نايف العربية للعلـــوم الأمنيـــة، الرياض،2002، ص72.

[3]-**Loi n° 91-1382 du 30 décembre 1991 relative à la sécurité des chèques et des cartes de paiement** JORF n°1 du 1 janvier 1992 .

[4]-**LOI n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne** JORF n°266 du 16 novembre 2001 .

[5]-Cette Directive repose essentiellement sur trois éléments : • Le **droit de fournir des services de paiement au public** : L'objectif est d'harmoniser les conditions d'accès au marché applicables aux prestataires de services de paiement autres que les établissements de crédit46. • **Les exigences de transparence et d'information** : La Directive impose des obligations d'information à l'ensemble des prestataires de services de paiement, que ces derniers proposent des instruments de paiement SEPA ou des instruments de paiement « traditionnels47 » . • **Les droits et obligations des utilisateurs et des prestataires de services** : La Directive vise enfin à clarifier les principaux droits et obligations des utilisateurs et des prestataires de services de paiement en harmonisant les règles nationales48, ce qui devrait contribuer à un renforcement de la sécurité juridique.

Directive 2007/64/CE du Parlement européen et du Conseil du 13 novembre 2007 concernant les services de paiement dans le marché intérieur modifiant les directives 97/7/CE, 2002/65/CE, 2005/60/CE ainsi que 2006/48/CE et abrogeant la directive 97/5/CE

Cette Directive repose essentiellement sur trois éléments : • Le **droit de fournir des services de paiement au public** : L'objectif est d'harmoniser les conditions d'accès au marché applicables aux prestataires de services de paiement autres que les établissements de crédit46. • **Les exigences de transparence et d'information** : La Directive impose des obligations d'information à l'ensemble des prestataires de services de paiement, que ces derniers proposent des instruments de paiement SEPA ou des instruments de paiement « traditionnels47 » . • **Les droits et obligations des utilisateurs et des prestataires de services** : La Directive vise enfin à clarifier les principaux droits et obligations des utilisateurs et des prestataires de services de paiement en harmonisant les règles nationales48, ce qui devrait contribuer à un renforcement de la sécurité juridique.

[6]-**Ordonnance n° 2009-866 du 15 juillet 2009 relative aux conditions régissant la fourniture de services de paiement et portant création des établissements de paiement**

2009–934 [1]، في خطوة الهدف منها كفالة المزيد من الأمان القانوني لمستخدم أدوات الدفع. حيث نضم المشرع الجرائم المتصلة بإستخدام بطاقة الإئتمان من خلال الفصل 3 من الكتاب الأول من التقنين النقدي و المالي تحت عنوان الجرائم المتعلقة بالشيكات وأدوات النقد غير المادي من خلال المادة س163–3 وما بعدها.

كما نجد الإتفاقية العربية قد ذهبت لتجريم الإستخدام غير المشروع لأدوات الدفع الإكترونية، وذلك بمقتضى المادة 18، وان كانت الجزائر من أولى الدول التي ضمت جهودها إلى المجتمع العربي، بمصادقتها على هده الإتفاقية، إلى أنها لم تنتهي إلى وضع اداة وطنية لمواجهة الإستخدام غير المشروع لبطاقة الإئتمان. وهو نفس النهج الذي إتبعته العديد من التشريعات كما هو حال المشرع المصري، إلا أن هذا القصور يجب الا يقف حائلا دون البحث في النصوص القائمة على الأقل، لبيان **مدى إحاطتها بهذا التوع المستحدث من الأنشطة الإجرامية. ام أنه من الضروري إدخال نصوص قانونية جزائية خاصة لتكملة النقص في القواعد السابقة؟وإن كان كذلك، فما هي الأحكام التي يجب أن تتضمنها تلك النصوص القانونية الجزائية المستحدثة؟**

وعلى هدي ما تقدم، فان دراسة الحماية الجزائية لبطاقة الإئتمان تقتضي منا التعريف بهذه البطاقة و أنواعها وطبيعتها، ومن ثم نعرض لأوجه الحماية الجزائية من خلال المطالب الثلاثة التاليـــة:

المطلب الأول: نطاق الحماية الجزائية(بطاقة الإئتمان)

المطلب الثاني: : المسؤولية الجزائية عن الإستخدام غير المشروع لبطاقة الإئتمان من قبل حاملها

المطلب الثالث: : المسؤولية الجزائية عن الإستخدام غير المشروع لبطاقة الإئتمان من قبل الغير

المطلب الأول

نطاق الحماية الجزائية(بطاقة الإئتمان)

كي نصل إلى غاية البحث حول المسؤولية الجزائية للإستخدام غير المشروع لبطاقة الإئتمان، فلا مناص من الإلمام ببعض المباديء والاصول المعرفية العامة عن البطاقة محل الدراسة، في خطة الهدف منها تحديد ماهيتها ومن تم تحيديد نطاق الحماية الجزائية، بغية الوقوف على مفهوم تلك البطاقات مع توضيح اللبس الذي يكتنف تعريفها مع كثرة الأنواع والنمادج المختلفة للبطاقات بصفة عامة(الفرع الأول)، فضلا عن الوقوف على طبيعتها(الفرع الثاني).

[1]-Décret n°2009-934 du 29 juillet 2009 pris pour l'application de l'ordonnance n°2009-866 du 15 juillet 2009 relative aux conditions régissant la fourniture de services de paiement et portant création des établissements de paiement, J.O. du 31 juillet 2009, p. 12744.

الفــرع الأول

مفهــوم بطاقــة الإئتمان

يكتنف مفهوم بطاقة الإئتمان بعض الغموض في التداول، نتيجة للتماثل في البناء المادي الكبير بين أنواع البطاقات المختلفة، إلا أنها تختلف فيما بينها في نوعية المعاملة التي تقوم بها، لذلك سنحاول إزالة هذا الغموض من خلال التطرق لأنواعها، وتمييزها عن غيرها من البطاقات، على أن يسبق ذلك كله تحديد مدلولها.

أولا- تعريف بطاقة الإئتمان وتمييزها عن غيرهــا

أ-تعريف بطاقة الإئتمان

بطاقة الإئتمان إختراع أمريكي ظهرت فكرتها في بداية القرن العشرين[1]، لتنتشر بسرعة كبيرة بسبب مرونتها وسهولتها في إتمام الصفقات، وإعتبارها مفتاح التعاملات الإلكترونية ووسيلة التبادل بين المتعاملين فيها من خلال مواقع التعاملات الإلكترونية[2].

---

[1]- وبالرجوع إلى تاريخ نشأة بطاقة الإئتمان وتطورها، نلاحظ أن الفضل في إستخدام هذه الأداة يعود إلى شركات البترول الأمريكية، التي إستخدمتها في مطلع العقد الثاني من القرن العشرين في عام 1950 ، إستعمل الأمريكيون بطاقة diners clubفي المجال التجاري، كما تم إستخدامها كوسيلة دفع هامة في الأعمال المصرفية، بدأت صناعة البطاقة عموما أول الأمر في صورة بطاقة تجارية ثم بطاقات سفر وسياحة ثم بطاقة إئتمانية، وكانت العلاقة بين بطاقات المحلات التجارية وزبائنها علاقة ثنائية، أدت هــذه البطاقة إلى زيادة حجم المبيعات، ثم تطورت أنظمة الدفع الإلكترونية وأصبحت واسعة الإستعمـــال في جميع المجالات لأداء الخدمات بمختلف أنواعها. **عرابة رابح**، المرجع السابق، ص16.

[2]– وعلى مستوى بلادنا العربية، فقد بدأت تجربة المصارف في مصر في بطاقات الائتمان متأخرة، فقد بدأ بنك مصر بإصدار بطاقة (فيزا بنك مصر) عام 1990 ثم إشتــرك أيضاً في عضوية بطاقة ماستر كارد بإصدار بطاقة ماستر كارد بنك مصر، بفئات ثلاث مرتبة تنازلياً حسب الحد الأقصى للبطاقة إلى (جولد كارد، بيزنس كارد، استار كارد). كما قام البنك الأهلي المصري بإصدار (بطاقة ضمان الشيك) ثم بطاقة فيزا البنك الأهلي المصري، وبطاقة ماستر كارد البنك الأهلي المصري، وفي أواخر عام 1996 بدأ بنك القاهرة في إصدار أول بطاقة ائتمان: **د.علي عدنان الفيل**،المسؤولية الجزائية عن إساءة إستخدام بطاقة الإئتمان الإلكترونية –دراسة مقارنة– ، مقال متاح على الموقع الإلكتروني التالي:
http://almuhamahresalah.blogspot.com/2015/10/blog-post_67.html.4 ، ص

أما في الجزائر، فإن وسائل الدفع المستعملة في النظام المصرفي الجزائري تتميز بأنها تقليدية في أغلبها ولا تتناسب مع الواقع العالمي الجديد، و لكن تبعا لحرص الجزائر على مواكبة الأحداث والتطورات التكنولوجية في العمل المصرفي خاصة في مجال الصناعة المصرفية، وسعيها نحو الصيرفة الإلكترونية شرعت في تقديم وتبني بعض وسائل الدفع والسحب الحديثة، من خلال إصـــدار **بطاقة السحب لبريد الجزائر**[2] التي تمكن حاملها من إجراء عمليات السحب من الشباك الآلي ، **بطاقة الدفع البنكية التابعة لبريد الجزائر** وهي بطاقة خاصة بالسحب والدفع تسمح بتسديد قيمة مشتريات المتعامل مباشرة من المتجر الذي قبل التعامل معها، فضلا عن البطاقات المصرفية للسحب والدفع للمصارف التالية: بنك الفلاحة والتنمية الريفية، بنك الجزائر الخارجي، القرض الشعبي الجزائري، الصندوق الوطنـــي للتوفير والإحتياط، بنك البركة الجزائري.

البطاقات العالمية: كفيزا وماستر كارد وهي متاحة من خلال البنوك الجزائرية التالية: القرض الشعبي الجزائري ، بنك التنمية المحلية، بنك الجزائر الخارجي.

://www.poste.dz/services/particular/monetique

- فمثلا القرض الشعبي الجزائري يمنح على المستوى الوطني بطاقة cpa cashوهي على 4 أنواع: البطاقة البلاستيكية العادية البطاقة الكلاسيكية النظامية الدهبية العادية والبطاقة البيبنكية المشتركة، ويعد حاملي البطاقة الأخيرة اكبر مقارنة بحاملي البطاقات الأخرى، نظرا لإستخدامها من جهة السحب من أي جهاز للصراف الألي ببنك منخرط ضمن الشبكة النقدية ما بين البنوك، وأيضـــا الدفع لدى التجار المتعاقدين مع بنك cpa وذلك لتسديد

لم تولي أغلب التشريعات إهتمامها بتعريف بطاقات الدفع الإلكتروني عامة، وبطاقات الإئتمان خاصة، على خلاف ذلك قام المشرع الفرنسي بإحداث البطاقة البنكية بصفة عامة بمقتضى القانون رقم 91-1382 والخاص بتأمين الشيكات وبطاقات الوفاء، فضلا عن القانون 2001-1062 والمتعلق بالأمن اليومي والمعدل للقانون النقدي والمالي، حيث قام بتعريفها بموجب المادة 132-1[1] على أنـــه" تعتبر بطاقة الدفع كل بطاقة صادرة عن إحدى مؤسسات الإئتمان أو إحدى الجهات المنصوص عليها في المادة 518-1 وتسمح لحاملها بسحب أو تحويل النقود.

تعتبر بطاقة سحب كل بطاقة صادرة عن الهئيات السابقة، وتسمح لحاملها بسحب الأموال فقط"، ليقوم بعد ذلك بإدخال أحكام التوجيه الأروبي2007-64 ضمن المنظومة التشريعية بموجب الأمر رقم 2009-866 المتعلق بالشروط التي تحكم تقديم خدمة الدفع وإنشاء مؤسسات الدفع[2]، ثم المرسوم التنفيدي رقم 2009-934 ، ليعدل المادة 132-1 ويضيف المادة 133-4[3] إلى التقنين النقدي والمالي التي عرفت وسيلة الدفع على أنها "كل جهاز شخصي ومجموعة من الإجراءات المتفق عليها بين مستخدم خدمة الدفع ومزود خدمة الدفع تمكن مستخدم الخدمة من إعطاء الأمر بالدفع". والملاحظ أن المشرع الفرنسي تبنى تعريف واسع يشمل في نطاقه جميع أدوات الدفع من بينها بطاقة الإئتمان.

كما قام المشرع الجزائري وبموجب القانون 05-02 المؤرخ بـــ 06 فيفري 2005 بإضافة الباب الرابع إلى الكتاب الرابع من القانون التجاري والمعنون في "بعض وسائل وطرق الدفع" ، ليضمن في الفصل الثالث منه بطاقات السحب والدفع وذلك في المادة 543 مكرر 23، وقد جاء مضمون هذه المادة مطابقا تماما لنص المادة 132-1 من التقنين النقدي والمالي الفرنسي. وكما هو ملاحظ أن المشرع تطرق إلى بطاقة الدفع

قيمة المشتريات. أما البطاقات على المستوى الدولي فهناك بطاقة فيزا وماستر كارد، إلا أن هذه الأخيرة تم استخدامها حديثا في وكالة cpa، وتستخدم cpa visa على نوعين cpa visa gold[2] البطاقة الدهبيةو cpa visa classique البطاقة العادية أو الكلاسيكية. **مصطفى دالع** ، واقع التجارة الإلكترونية في الجزائر ، مقالة نشرت بموقع:www.ialamtic.com

تجدر الإشارة إلى أن نجاح نظام الدفع الإلكتروني مرتبط بالإستعمال المزودج لبطاقات الدفع والسحب من طرف زبائن البنوك، الأمر الذي مازال مطروحا على مستوى المنظومة المصرفية الجزائرية، حيث نجد بطاقات السحب معروضة على زبائن البنوك، وانعدام الطرف الآخر في العلاقة- بطاقات الدفع واجهزة الدفع في المحلات التجارية. انظر: **بحبح عبد القادر**، إشكالية التحكم في وسائل الدفع البنكية وأثرها على الخدمات المصرفية – حالة الجزائر 1962-2010، مجلة الباحث، عدد 9، 2011، ص26.

[1]-**Article L132-1 du Code monétaire et financier** dispose que "Constitue une carte de paiement toute carte émise par un établissement de crédit ou par une institution ou un service mentionné à l'article L. 518-1 et permettant à son titulaire de retirer ou de transférer des fonds.

Constitue une carte de retrait toute carte émise par un établissement, une institution ou un service mentionné au premier alinéa et permettant, à son titulaire, exclusivement de retirer des fonds."

[2]- معظم الأحكام التي جاء بها هذا الأمر تم إدخالها ضمن التقنين النقدي والمالي، سواء بتعديل النصوص القائمة أو بإضافة نصوص جديدة، وقد جـــاء هذا الأمر بجملة مباديء لإدراجها ضمن النظام القانوني لأدوات الدفع منها:

خدمة الدفع**Services de paiement**، أمر الدفع و الإلغاء**Ordres de paiement et revocation**مدة تنفيد الأمر بالدفع **Délai d'exécution des ordres de paiement. Date de valeur**، امن الدفع**Sécurité des paiements**، عملية الدفع غير المصرح بها **Opérations de paiement non autorisées**، سوء تنفيد عمليات الدفع**Opérations de paiement mal exécutée**، إسترداد الدفع

Remboursement d'un paiement ordonné par le bénéficiaire ou par le payeur qui a donné l'ordre par l'intermédiaire du bénéficiaire,voir notamment **Christian Gavalda † Jean Stoufflet**; INSTRUMENTS DE PAIEMENT ET DE CRÉDIT; Effets de commerce, carte de paiement, transfert de fonds; 7e ÉDITION; LexisNexis SA; paris; **2009**;p 1 et s

[3]-Article L133-4 du Code monétaire et financier ;Créé par Ordonnance n°2009-866 du 15 juillet 2009 - art. 1

والسحب دون باقي البطاقات الأخرى، لكن ذلك لا يعني عدم إدخال بطاقة الإئتمان ضمن المفهوم السابق، ذلك أن البطاقة ذاتها ووفقا لإتفاق المبرم بين العميل والجهة المصدرة لها قد تمارس وظيفة الإئتمان والوفاء والسحب معا، وأمام عدم وجود تعريف دقيق وواضح لها، أخــذ الفقه على عاتقه هذا التحديد.

فمن وجهة النظر الفقهية، فإن لبطاقة الإئتمان تعريفات عديدة منها بأنها **بطاقة خاصة يصدرها المصرف لعميله كي تمكنه من الحصول على السلع والخدمات من محلات و أماكن معينة عند تقديمه هذه البطاقة، ويقوم بائع السلع أو الخدمات بتقديم الفاتورة الموقعة من العميل إلى المصرف مصدر الإئتمان، فيسدد قيمتها له، ويقدم المصرف للعميل كشفا شهريا بإجمالي القيمة لتسديدها أو بخصمها من حسابه الجاري لطرفه**"[1]. أو انها "**البطاقة التي تسمح للعميل بشراء بضائع أو الحصول على خدمات من منافد البيع أو الخدمات، شريطة أن يتم الدفع على فترات، حيث يحق للعميل دفع جزء من المبلغ أخر الشهر بينما يقسط الباقي على شهور تالية بنسبة فائدة تتراوح بين 17–19 وفق نصوص العقد بين العميل و المصرف.**[2]

وهناك من عرفها "**بطاقة من ورق أو بلاستيك أو مادة أخرى يصعب العبث في بياناتها أو تزويرها، تصدؤها جهة –بنك أو شركة غستثمار–يدكر فيها إسم العميل الصادرة لع وعنوانه و رقم حسابه لدى الجهة التي أصدرتها، وعندما يحصل هذا العميل على سلعة أو خدمة فبدلا من أن يدفع الصمن فورا فإنه يقدم بطاقة الإعتماد إلى البائع الذي يدونها بياناها في الفاتورة، التي يوقعها العميل، ثم يرسل البائع الفاتورة إلى مصدر البطاقة حيث يسددها له، ثم تقوم الجهة مصدرة البطاقة بإرسال الفاتورة إلى العميل أخر كل شهر أو مدة متفق عليها طالبة سدادها**"[3].

أما مجمع الفقه الإسلامي الدولي بقراره رقم 65–1–7 لسنة 1412 هجري قام بتعريفها على أنها **مستند يعطيه مصدره، لشخص طبيعي أو إعتباري بناء على عقد بينهما يمكنه من شراء السلع أو الخدمات ممن يعتمد المستند، دون دفع الثمن حالا، لتضمنه التزام المصدر بالدفع، ومنها ما يمكن من سحب النقود من المصارف**[4].

بعد إستعراضنا للتعريفات السابقة، نستخلص جملة من العناصر نوردها بالتحليل كمايلي:

–جل التعريفات إستخدمت مصطلح بطاقة ولفظ بلاستيك، وهي تعبر بذلك عن الجانب الشكلي الذي يتمثل في صناعة البطاقة من مواد بلاستيكية.

– جوهر البطاقة هو أنها تعطي لحاملها **إئتمان** فعلي وتسهيلات إئتمانية، ويتم ذلك بأن يقوم المصدر بدفع قيمة مشتريات الحامل من التجار المتعاقدين مع المصدر العضو في إصدار البطاقة مسبقا بقبول البيع وتأدية

---

[1]- انظر:د.**سعد محمد سعد**، البطاقات البلاستيكية كوسيلة وفاء بالإلتزام، بحث مقدم في مؤتمر تشريعات عمليات البنوك بين النظرية والتطبيق، جامعة اليرموك، 2002، ص4. **د. محمد رأفت عثمان**، ماهية بطاقات الإئتمان وأنواعها وطبيعتها القانونية وتمييزها عن غيرها، بحث مقدم لمؤتمر الأعمـــال المصرفية الإلكترونية بين الشريعة والقانون، الجزء الثاني، كلية الشريعة والقانون، جامعة الإمارات العربية، 2003، ص618.

[2]–**د. رياض فتح الله بصلة**، جرائم بطاقات الإئتمان، الطبعة الأولى، دار الشروق، 1995، ص14.

[3]– د. **عصام حنفي محمود موسى**، الطبيعة القانونية لبطاقات الإئتمان، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، الجزء الثاني، كلية الشريعة والقانون، جامعة الإمارات العربية، 2003، ص873.

[4]–**د. الصديق محمد الأمين الضرير**، بطاقات الإئتمان، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، الجزء الثاني، كلية الشريعة والقانون، جامعة الإمارات العربية، 2003، ص673، **د. محمد عبد الحليم عمر**، المرجع السابق، ص664.

الخدمات بموجبها، ودفع مسحوباته النقدية من البنوك ثم رجوع المصدر على حامل البطاقة فيما بعد لإستيفاء هذه المدفوعات مع الفوائد إلى أجل متفق عليه ، فإن فقدت هذه الخاصية تكون **بطاقة وفاء** فقط.

-مصدر البطاقة قد يكون البنك أو منشآت التمويل الدولية أو كما يسميها البعض المنظمات البنكية أو المؤسسات المالية مثل مؤسسة أمريكان اكسبرس. منظمة فيزا، منظمة الماستر كارد، حيث تعتمد هذه الشركات الحصص الكبرى في أسواق بطاقات الائتمان في العالم، حيث تعتبر American Express Company أكبر مصدر للبطاقات الأئتمانية في الولايات المتحدة, بنسبة تقارب 24% من عمليات البطاقات الأئتمانية.[1] ومعنى هذا أن الجهة التي إبتكرت هذا النظام هي صاحبة الحق في إصدار البطاقات وفق شروط خاصة، أو إنابة غيرها بإصدار مثل هذه البطاقات، ومن ثم فان المصارف التي أنيبت في إصدار هذه البطاقة من صاحب الحق الأصلي يطلق عليها **البنك الوسيط.**

-بعض التعريفات أوردت كلمة الشخص طبيعي أو إعتباري، ونرى أنه لا حاجة لذلك لأن كلمة شخص تشملها معا عند الإطلاق، ولأنه في العادة تمنح للأشخاص الطبيعيين، وأنه كما يتم إصدار البطاقة بموجب عقد بين المصدر حامل البطاقة فإنه يتم توقيع عقد أو إتفاقية بين البنك والتاجر، وفي مجموع العقدين تظهر مشارطات من شأنها تنظيم العلاقة بين حامل البطاقة والتاجر[2]، ومن ثم يحسن النص عليها في التعريف إضافة لرجوع المصدر على الحامل لإستيفاء حقه[3].

- تعتبر هذه البطاقة وعاء لمعلومات معينة ذات أثر قانوني مثل المركز المالي لصاحب البطاقة، كما تعتبر مستند من الناحية القانونية يعطيه مصدره - بنك أو مؤسسة مالية أو مصرف حكومي- لشخص بناء على عقد أو إتفاقية بينهما.

لقد أصبحت لبطاقات الإئتمان في المجتمعات الحديثة شأنا مهما ومن الأساسيات، فهي تحقق فوائد كثيرة لأطرافها سواء الحامل أومصدرها أو التاجر[4]، وإن كانت كذلك فلهذه البطاقة ميزة التنوع فلا تأتي على شكل واحد بل لها العديد من الصور وهو ما سنتناوله فيمايلي.

---

[1]- American Express to slash 7000 jobs". Bloomberg. Sydney Morning Herald. October 31, 2008.disponible en lingne á l'adresse suivante: http://www.smh.com.au/business/american-express-to-slash-7000-jobs-20081030-5eu9

[2]-**د. علي محمد الحسين موسى،** البطاقات المصرفية تعريفها أنواعها وطبيعتها، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الخامس، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ماي 2003، ص1994.

[3]-**د. محمد عبد الحليم عمر،** المرجع السابق،، ص662.

[4]- فبالنسبة **لحاملها** تحقق له فوائدة عدة، فهو لا يحتاج إلى حمل نقود كثيرة معه، مما يجنبه تعرضه للسرقة وغيرها. كما تمكنه من شراء ما يبدو له شراؤه في ظروف مفاجئة لم يستعد لها، وتمكنه من الحصول على إئتمان بطريقة سهلة وميسرة، كما تزوده بتسهيلات نقدية في أي دولة كان ضمن حدود ممنوحة له عند طلبه. أمـــا بالنسبة **لمصدرها،** تسهم في تقليص نفقاته بحيث يتم عملها وإستعاملها بوسائل تكنولوجية حديثة، كما تعتبر بالنسبة له من العمليات المربحة نظير ما تتقاضاه من عمولات وفوائد وإيرادات، مثل الرسوم المحصلة من حملة البطاقات والعمولة المستقطعة من التجار، والفوائد على المبالغ غير المحصلة من من حملة البطاقات، وفروق سعر الصرف في حالة السداد بعملة أجنبية. فضلا عن توطيد الثقة بين البنوك وعملائها المعروفين لديها الذين لهم علاقات مصرفية شبة دائمة. أمـــا بالنسبة **للتاجر،** فهي تجنبه قيام عملائه بإصدار شيكات ليس لها رصيد، كما أنها تخفف عليه مخاطر الإحتفاظ بمبالغ نقدية كبيرة في متجره، فيأمن من السرقة أو السطو المسلح. **د. نزيه محمد الصادق المهدي،** نحو نظرية عامة لنظام بطاقات الإئتمان من الوجهة القانونية، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الثاني، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ماي 2003، ص 755.

ب-تمييز بطاقة الإئتمان عن غيرها من البطاقات

أفرز التعامل الإلكتروني عامة والتعامل المالي خاصة العديد من البطاقات التي تبدو مشابهة لبطاقة الإئتمان، إلا أنها تختلف عنها إنطلاقا من الوظيفة التي تؤديها كل بطاقة.

1-بطاقة الإئتمان وبطاقة الوفاء

تخول بطاقة الوفاء لحاملها بدفع قيمة السلع والخدمات التي يحصل عليها من بعض المحلات التجارية المتعاقدة مع الجهة المصدرة لها، وذلك بتحويل قيمة البضائع والخدمات من حساب حامل البطاقة إلى حساب التاجر البائع بصورتين أحدهما مباشرة ON LINE والأخرى غير مباشرة OFF LINEحيث تقوم الجهة المصدرة بسداد الإيصلات بعد وصولها إليها، ويطلق عليها في هذه الحالة إسم **بطاقة الوفاء المؤجل**, وهاتان الطريقتان تستخدمان في بطاقة الإئتمان أيضا[1].

ومن خلال التعريف السابق، يتضح أن بطاقة الوفاء ليست بطاقة إئتمانية لقيام الجهة المصدرة بتسوية الدين بين حامل البطاقة والتاجر إن وجد رصيد دائن لحامل البطاقة دون تقديم تسهيلات إئتمانية، أما في بطاقة الإئتمان فإن الجهة المصدرة تتعهد بتقديم تسهيلات إئتمانية للحامل والتاجر معا[2].

2-بطاقة الإئتمان وبطاقة ضمان الشيكات: تعرف هذه البطاقة أنها بطاقة بموجبها يتعهد البنك لعميله حامل البطاقة بضمان سداد الشيكات المسحوبة من قبله على هذا البنك وفقا لشروط البطاقة.

رأينا أن بطاقة الإئتمان تضمن وفاء قيمة السلع والخدمات التي حصل عليها حامل البطاقة من التاجر، وتقوم الجهة المصدرة بسداد المبالغ المطالب بها من الحامل لاحقا، بينما بطاقة ضمان الشيكات تضمن الوفاء بقيمة الشيك المسحوب من الحامل والبنك المسحوب عليه من حقه رفض الشيك في حالتي تجاوز الحد الأقصى للرصيد وعدم وجود رصيد غير كاف مما يجعل أركان جريمة إصدار شيك دون رصيد متوافرة[3].

3-بطاقة الإئتمان وبطاقـــة الصراف الآلي

بطاقة الصراف الآلي لا تقدم للعميل سوى سحب المبالغ المودعة لدى البنك، ولا يقوم الجهاز بصرف أي مبلغ في حال عدم وجود رصيد للعميل، لذلك يرى البعض[4] أنها ليست بطاقة إئتمانية لعدم وجود تسهيل إئتماني للعميل عادة.

---

[1]- **د. ثناء أحمد محمد المغربي**، الوجهة القانونية لبطاقات الإئتمان، مؤتمرالأعمال المصرفية الإلكترونية بين الشريعة والقانون، الجزء الثالث، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ماي 2003 ، 248.

[2]- المرجع السابق، 949، **كميت طالب البغدلدي**، الإستخدام غير المشروع لبطاقة الإئتمان، المسؤولية الجزائية والمدنية، دار الثقافة للنشر والتوزيع، عمان، 2009، ص75.

[3]- د. **ثناء أحمد محمد المغربي**، المرجع السابق، ص947.

حيث أن بطاقة ضمان الشيكات تعطي للعميل إمكانية السحب الأسبوعي أو الشهري لمبلغ محدد بواسطة شيك، وذلك من كل البنوك التي تنضم لهذا النظام، و يضمن البنك مصدر هذه البطاقات الوفاء بقيمة الشيكات التي يصدرها العميل حامل البطاقة، لذا تعد نوعا من أنواع الضمان الصادر في ورقة مستقلة، ويتعين أن يضع العميل رقم البطاقة على ظهر الشيك حتى يستطيع المستفيد الإفادة من هذا الضمان. **د. أبو الوفا محمد أبو الوفاء إبراهيم**، المسؤولية الجنائية عن الإستخدام غير المشروع لبطاقة الإئتمان، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الخامس، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ماي 2003، ، ص2051.

[4]- **د. ثناء احمد محمد المغربي**، المرجع السابق، ص 949.

ولكن قد تعتبر بطاقة الصراف الآلي أحد أنواع بطاقات الإئتمان التي ترعاها المنظمات العالمية و المؤسسات المالية[1] إذا كان من ضمن خدماتها دفع قيمة المشتريات والخدمات للتجار بالإضافة إلى السحب بواسطتها من الآلات، حيث يتوفر ضمان البنك بالوفاء بقيمة المشتريات إلى التاجر إذا كانت ضمن الحدود المتفق عليها بين العميل والبنك عند إصداره هذه البطاقة، حيث أن هذا النوع من البطاقات يمثل آلة لتوفير الخدمة الذاتية السريعة وبنوعية أفضل.

وتتجه البنوك العالمية نحو دمج بطاقة الإئتمان والتحويل الإلكتروني والصراف الألي في بطاقة واحدة، حيث تحمل البطاقة شعار البنك جنبا إلى جنب مع شعار المنظمات العالمية، مثل فيزا كارت وماستر كارد و امريكان إكسبرس كارد، كما يمكن لحاملي البطاقات العالمية من إستخدام بطاقاتهم داخل البلاد على أجهزة التحويل الإلكتروني[2].

ثانيا- أنواع بطاقات الإئتمـــان

تتعدد أنواع البطاقات بحسب الزوايا التي ينظر إليها، سواء من حيث مزاياها أو الجهة المصدرة لها أو من حيث نظم تكوينها. إلا أننا سنتناول التقسيم المبني على طبيعة العلاقة وكيفية التعامل بها، كون التقسيمات الأخرى تندرج فيها ولا تؤثر علي ماهيتها.

أ-بطاقة الخصم الشهري أو الدفع المؤجل[3]:

وهي بطاقة تمكن حاملها من إستخدامها في المحلات التجارية للشراء، أو تلقي الخدمات في مكاتب الطيران أو الفنادق...الخ، وإصدارها لا يتطلب من حاملها الدفع المسبق للبنك المصدر في صورة حساب جاري، وإنما يطالب البنك المصدر حامل البطاقة بقيمة مشترياته ومسحوباته في نهاية كل شهر على أن يسددها في مدة تالية تتراوح بين 25-40 يوما، واذا تأخر عن السداد يحمل بفائدة. ومن أشهر هذه البطاقات: بطاقة الفيزا، الماستر كارد الأمريكان إكسبرس.

ب-بطاقة الإئتمان القرضية أو السداد على فترات لاحقة[1]:

---

[1]- **كميت طالب البغدادي**، المرجع السابق، ص74.

[2]-**د. ابو الوفا محمد أبو الوفاء**، المرجع السابق، ص2051.

[3]-د **مبارك جزاء الحربي**، بطاقات الإئتمان، مؤتمر الاعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الخامس، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ماي 2003، ص2159. د. **محمد عبد الحليم عمر**، المرجع السابق، ص665.**ممدوح البحر وعدنان احمد العزاوي**، بطاقات الائتمان والاثار القانونية المترتبة بموجبها، مؤتمر الاعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الثالث، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة،ماي 2003، ص 1000.**د. محمد رأفت عثمان**، المرجع السابق، ص622.

وأهم ما تمتاز به هذه البطاقات: أنه يمكن إستخدامها محليا ودوليا ، يدفع للعميل من أجلها رسوم إشتراك ورسوم تجديد، فوائد الإقتراض والتاخير. كما يمكن استخدامها كبطاقة الصرف الالي للسحب، قد لا يلزم لإصدارها وجود حساب للعميل كما في حالة اصدار بطاقة امريكان اكسبرس و داينرز كلوب، وقد تشترط بعض جهات الإصدار والبنوك وجود حساب دائن لدى البنك المصدر للبطاقة كي يستوفي منه قيمة استخدام البطاقة.

تتميز هذه البطاقة عن سابقتها بأن التسديد فيها يكون على شكل دفعات، قد تكون منتظمة وقدتكون غير منتضمة، بحيث يكون دائما لدى العميل قدرة على إستخدام البطاقة في حدود إئتمانية متفق عليها مادام هو منتظما في سداد الفوائد المستحقة شهريا، ولها نفس ميزات بطاقة الخصم الشهري من حيث الإستخدامات الأخرى. وتعتمد هذه البطاقة جملة من العناصر منهاأنه لا يلزم لإصدارها وجود حساب للعميل، ويقوم البنك المصدر بإقراض العميل مبلغا له حد أعلى يسمى الخط الإئتماني، والتسديد يكون بالتقسيط على شكل دفعات، وليس محددا شهرا، كما يلزم حاملها بأربع دفعات رسم الإشتراك ورسوم التسجيل وفوائد الإقراض وفوائد التأخير. كما تعتمد على فرض الفوائد المترتبة على التأخير، والتي تحسب يوميا على المبالغ المعلقة. وأنها تمثل اداة وفاء وإئتمان لأنها تؤدي إلى إنشاء دين متجدد في ذمة حامل البطاقة هو قيمة مشترياته الشهرية أو مسحوباته النقدية.

ت–بطاقة الصراف الألي (أي تي ام) أو بطاقة الخصم الفوري[2]:

يتم إصدارها بأن يقوم حامل البطاقة بفتح حساب جاري لدى البنك المصدر للبطاقة يودع فيه مبلغا معينا يعادل الحد الأقصى المسموح له بالشراء من حساب العميل الجاري، بعد إرسال فواتير الشراء أو أداء الخدمة من التجار للبنك، كما يتم أيضا خصم قيمة المسحوبات النقدية بالبطاقة من آلات السحب أو من البنوك، وفي نهاية كل شهر يرسل البنك كشف حساب الى حامل البطاقة مطالبا إياه بايداع مبلغ مماثل في الحساب الجاري حتى يعود الرصيد المطلوب الإحتفاظ به لدى البنك الى كامل المبلغ. وفي هذا النوع من البطاقات لا يتمكن العميل من إستخدام البطاقة في كل مرة إلا بعد خصم مبلغ الإستخدام من رصيد حسابه.

من خلال ما تقدم ذكره من تفصيلات عن بطاقة الإئتمان، نلاحظ أنها تنفرد ببعض الخصائص التي تميزها عن غيرها من وسائل الوفاء الأخرى لما تقوم عليه من كفاءة إئتمانية، كما تقدم بعض المزايا أهمها، أنها تعتبر بطاقة وفاء وإئتمان في آن واحد، فبطاقة وفاء، لأن حاملها يستطيع الوفاء بإلتزاماته بتقديمها دون الحاجة لحمل النقود، كما أنها أداة إئتمان حيث يقدم مصدرها –بنك أو المؤسسة المالية– عادة تسهيلات وآجال للوفاء بقيمة مسحوباتهم. وبطاقة الإئتمان تقوم على علاقة ثلاثية الأطراف، مصدر البطاقة الحامل التاجر، وكل طرف من هذه الأطراف تترتب له حقوق وعليه إلتزامات، ويرتبط مع الآخرين كل على حدى بعقود مستقلة[3].

---

[1]–**د. محمد رأفت عثمان**، المرجع السابق، ص 623.**د. مبارك جزاء الحربي**، المرجع السابق،ص 2160.

[2]- **د. محمد رأفت عثمان**، المرجع السابق، ص623. **د. محمد عبد الحليم عمر**، المرجع السابق، ص665.

[3]– كما أنها تتميز بخصاص أخرى منها: كونهاتستخدم على المستوى المحلي والدولي، تعتبر إحدى وسائل الحد من الطلب على العملات الأجنبية، إذ أنها وسيلة دولية تستخدم بجميع العملات ويتم مطالبة العميل بالعملة الوطنية مما يقلل الطلب على العملات الأجنبية لأغراض إستهلاكية وإحداث نوع من التوازن بسوق الصرف الأجنبي، هي بطاقة مملوكة للبنك، وتبقى كذلك في جميع الأوقات، فالعقد القائم بين البنك ومصدر البطاقة موضوع لمدة محددة و مجدد ضمنيا إلا إذا أفصـــح مصدر البطاقة أو الحامل عن رغبته في عدم التجديد، فإذا كانت هذه الرغبة صادرة من البنك مصدر البطاقة فإن الحامل يجب عليه أن يعيدها إلى البنك بناء على هذا الطلب، كما يجوز للحامل في أي وقت أن يفسخ هذه الإتفاقية فيما يختص باستعماله البطاقة وذلك بتسليم البطاقة إلى البنك، كما يجوز للبنك إلغاء البطاقة في أي وقت دون إشعـــار مسبق، كما يجوز له أن يرفض إعادة إصدارها أو تجديدها أوإستبدالها كما يحتفظ البنك بحقه في تعديل شروط عمل البطاقة مع إخطار الحامل بدلك، وهذا الأخير له الحق في الموافقة أو الرفض وتسليم البطاقة، كما أنه في علاقة

الفــرع الثانـــي

طبيـــعة بطاقـــة الإئتمـــان

للجرائم المتعلقة ببطاقة الإئتمان خصوصية تستوجب منهجية تعريفية تحليلية تكاملية في دراستنا لها، كي نقف في النهاية على كيفية جريان الإعتداءات عليها، بناء عليه سنتطرق في هذا العنصر للطبيعة التكوينية والقانونية للبطاقة ذاتها.

أولا- الطبيعة التكوينية لبطاقة الإئتمان[1]

لما نتحدث عن بطاقة الإئتمان، فإننا نتحدث عن 3 عناصر كل منها يمثل ضلعا متساوي الأضلاع، الأول هو البطاقة، الثاني هو المعلومات، والثالث هو النظام. حيث تصنع البطاقة من البلاستيك، وتأخذ شكل مستطيل ذا أطراف شبة دائرية يتراوح عرضها _5-5,5 وطولها 8-8,5 وسمكها 0,8 ، و يتم تغليف جسم البطاقة بمواد كيمياوية أخرى تشكل غطاء البطاقة تمهيدا لصياغة وتثبيت البيانات والمعلومات والأشكال عليه، حيث يتم تصنيع البطاقة من مادة كلوريد الفينيل المتعدد وغير المرن.

وبغرض التعامل مع الآلة كونها لا تقرأ إلا سيلا من النبضات ثنائية الشفرة، تحتوي البطاقة على **وسائل تخزين معلومات**، وتضم بذلك **المكونات المقروءة بصريا** من مطبوعات الحبر الممغنط والخطوط المشفرة ومطبوعات الحروف والعلامات المقروءة ضوئيا، فضلا عن **المكونات المقروءة الكترونيا**، ونقصد بذلك الشريط الممغنط والرقيقة المجهرية، التي توجد في البطـــاقة.

يسجل على الشريط الممغنط **البيانات الخاصة** بالعميل والتي يحتاجها الحاسوب للتعرف عليه، مثل رقم البطاقة وسقف البطاقة والتواريخ والرموز الأخرى الخاصة بالتعاملات الإلكترونية، والبيانات المسجلة على الشريط عبارة عن تغييرات مغناطيسية يتم قراءتها بطرق خاصة.

فضلا عما سبق، تتكون البطاقة من عناصر ذات فاعية تأمينية أو ثبوتية خاصة "**شريط التوقيع**، وهويوجد بظهر البطاقة، حيث يقوم العميل بالتوقيع عليه عند إستلامه للبطاقة، والتوقيع هنا هو وسيلة للتحقق من هوية حامل البطاقة عن طريق مضاهات التوقيع على البطاقة بتوقيع حاملها على إيصال أو فاتورة التعامل عند اللزوم، وهو شريط ينشأ من الورق أو مادة مكافئة، يأخذ شكل طبقة رقيقة من مواد متماسكة على هيئة شريط مترسب أسفل الشريط الممغنط. ولكونها تقترب لتصبح بطاقات هوية فإنها تحمل صورة العميل،

البنك مصدر البطاقة بالتاجر يكون الإتفاق بينهما عادة لمدة سنة قابلة للتجديد الضمني ولكن يحتفظ كل منهما بحقه في فسخ العقد في أي وقت بدون إخطار سابق أو إبداء الأسباب طالما أرسل خطاب بهذا الطلب.**د. ثناء احمد محمد المغربي**، المرجع السابق،ص950، **د.عصام حنفي محمود موسى**،الطبيعة القانونية لبطاقات الإئتمان، مؤتمر الأعمال المصرفية الإلكترونية، المجلد الثاني، كلية الشريعة والقانون، جامعةالإمارات العربية المتحدة، ماي ، 2003، ص885.

[1] -أنظر بخصوص الطبيعة التكوينية للبطاقة : **د.رياض فتح الله بصلة**، جرائم بطاقة الإئتمان، المرجع اليسابق، ص37 ومابعدها،**د.محمد نور الدين سيد**، المسؤولية الجنائية عن الإستعمال غير المشروع لبطاقات الوفاء، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، ص30، **براهمي حنان**، المرجع السابق، ص263.**كميت طالب البغدادي**، المرجع السابق، ص65.

وإضافة لذلك يسلم العميل رقم التعريف الشخصي يتكون عادة من 4 خانات ويرمز له ب PIN ليستخدمه عند السحب أو الشراء من نقاط البيع الإلكترونية، وهو صورة مبسطة من صور **التوقيع الإلكتروني.**

وتجدر الإشارة إلى البطاقة على النحو السابق بيانه، يمكن تقسم نظمها إلى نظم عديدة، اكثرها شهرة البطاقة الرقائقة وهي تلك البطاقة التي تحتوي على شريحة داكرة كشريحة السليكون مطمورة في الجسم اللدائني للبطاقة، وتقوم البطاقة بتسجيل كمية النقود في الحساب المصرفي للشخص، وهي مبرمجة كي تضيف أو تطرح من حسابه، وهي على 3 أنواع: **بطاقة ذاكرة، بطاقة ذكيةبطاقة حادة الذكاء**[1].

كما أنها لا تمنحها البنوك إلا بعد التأكد من ملائمة العميل أو الحصول منه على ضمانات عينية أو شخصية كافية، ويتم إستعمالها بعد تقديم المتعامل طلبا للحصول على البطاقة من البنك وملئه للمعلومات الضرورية سواء أكان هذا الشخص متعاملا مع البنك فقط أم لديه رصيد أو حساب جاري، وبعد تقصي البنك عن سمعة المتعامل الإئتمانية يمنحه البطاقة وبمجرد الحصول عليها يستطيع إستعاملها في شراء السلع والخدمات في المحلات التجارية المتفق عليها، وهناك طريقتان لاستعاملها[2]، الأولى**يدوية** اذ لا تتضمن وجود قناة إتصال بين التاجر والبنك أو شركة الدفع سوى جهاز الهاتف للتاكد من كفاية الرصيد، والثانية **الكترونية** ويتم عن طريق جهاز التحويل عند نقط البيع، وبمجرد طرق الرقم السري يتبادل هذا الجهاز المعلومات المشفرة الكترونيا على البطاقة مع البيانات المخزنة سلفا على جهاز الحاسوب لدى البنك أو شركة الدفع ليخصم المبلغ فورا من حسابه.

ثانيا– الطبيعة القانونية لبطاقة الإئتمان

لقد إختلف الرأي حول الطبيعة القانونية لبطاقة الإئتمان، ولعل من دواعي هذا الخلاف القصور القانوني الملحوظ بشأن تنظيمها، سنحاول عرض موجز لأهم الطروحات التي قيلت بهذا الصدد.

ذهب البعض إلى القول أن نظامها القانوني يقترب من **حوالة حق**[3]، فمصدر البطاقة –المحال له– الحق في مطالبة حامل البطاقة –المحيل عليه–بسداد المبالغ التي قام بالوفاء بها للتاجر –المحيل–مقابل دفع عمولة.

إلى أن هذا يتعارض مع نص المادة 1690 من القانون المدني الفرنسي المقابلة للمادة 241 من القانون المدني الجزائري والمادة 305 مدني مصري، إذ تكون الحوالة نافدة قبل المدين أو قبل الغير إلا إذا قبلها المدين أو أعلن عنها، على أن نفادها قبل الغير بقبول المدين يستلزم أن يكون هذا القبول ثابت التاريخ وهو الأمر الغير متوافر في بطاقات الوفاء.

---

[1]- **بطاقة الذاكرة:** لا تتضمن سوى وسيلة ذاكرة لتخزين البيانات كما هو الحال في بعض بطاقات الهاتف. **البطاقة الذكية:** تتضمن معالج بيانات ووسيلة ذاكرة لتخزين المعلومات على رقيقة معباة في بنية بطاقة الإئتمان. **بطاقة حادة الذكاء:** تتضمن معالجا صغيرا للبيانات وذاكرة وشريط ممغنط وشاشات عرض ومفاتيح إدخال بيانات والتي تتيح بمجملها عملية تخزين المعلومات الشخصية والبيانات المالية لحاملها، وتعتمد على خوارزمية برامجية هي خوارزمية المفتاح العام التي تسمح بإنشاء مباشر للتوقيعات الرقمية. د. **رياض فتح الله بصلة**، المرجع السابق، ص21.

[2]– **د. محمد صبحي نجم**، المسؤولية الجزائية عن الإستخدام غير المشروع لبطاقة الإئتمان، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الثالث، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ماي 2003، ص 1162.

[3]أنظـــر: **د. احمد محمد المغربي**، المرجع السابق، ص 951.

بينما يتجه رأي آخر إلى القول أنها تشبه في نظامها القانوني لـــ: **فكرة الوكالة**، إذ تنص المادة 571 من القانون المدني الجزائري وتقابلها المادة 699 من القانون المدني المصري أن الوكالة عقد بمقتضاه يفوض شخص شخص آخر للقيام بعمل شيء لحساب الموكل وبإسمه. وبالرجوع لبطاقة الإئتمان يقوم حامل البطاقة بتوكيل البنك في دفع ثمن السلع والخدمات التي حصل عليها خصما من حسابه لديه[1]. إلا أن هذا الراي وجهت له عدة انتقادات منها[2]: أن التزام البنك هو إلتزام شخصي ومباشر، بمقتضى العقد المبرم بينه وبين التاجر بالوفاء له بدين حامل البطاقة، وهذا الإلتزام مستقل، ومجرد عن علاقة التاجر والحامل، وهذا مالا نجده في عقد الوكالة، حيث لا يكون للتاجر إلا أن يطالب حامل البطاقة وليس له الرجوع على الوكيل كون أثر العقد ينصرف إلى الموكل.

بينما يتجه رأي آخر إلى القول بأن بطاقة الائتمان الإلكترونية هي **نقود إلكترونية** تشبه العملات الأخرى كالنقود الورقية والمعدنية المعترف بها في التداول قانوناً وتعاملاً[3] ، إلا أن هذا الرأي منتقد لأنه يتجاهل الصفة الذاتية للنقود باعتبارها أداة للوفاء وكونها تحظى بالقبول الإلزامي بين الأفراد وهي قابلة أيضاً لإعادة الاستعمال من عدة أشخاص. وهذا مالا يتلاءم وبطاقة الائتمان. فهي غير متداولة لشخصية إستخدامها ولايمكن تحويلها أو نقل ملكيتها للغير، كما يوجد نوع من التباين في قيمتها نظرا لإختلاف التسهيل الإئتماني الذي يمنح لحاملها كلا حسب مقدرتـــه.

ويذهب البعض أن بطاقة الإئتمان هي **أوراق تجارية**[4] تضاف إلى سند السحب وسند الأمر والشيك، على إعتبار أن بعض التشريعات التجارية العربية وعلى رأسها قانون التجارة المصري في مادته 378 لم يذكر الأوراق التجارية على سبيل الحصر، وقد تبنى المشرع الجزائري الإتجاه الأخير، حيث خص بطاقات السحب والدفع بفصل خاص من القانون التجاري وهو الفصل الثالث من الباب الرابع من الكتاب الرابع الخاص **بالسندات التجارية**، تحت عنوان في بطاقات السحب والدفع، ولعل في طريقة خصه بنصوص خاصة وحدها ضمن الأوراق التجارية الكلاسيكية، هو مسلك يتفق والإعتراف بانفرادها بوضع قانوني لانظير له، ولا يمكن ادراجها تحت أي ورقة تجارية، وإن كانت من بين أنواعها[5].

---

[1]–**د. عمر سالم**، الحماية الجنائية لبطاقات الوفاء، الطبعة الأولى، دار النهضة العربية، القاهرة، 1995، ص ص17–19.

[2]–**نداء كاظم المولى**، الطبيعة القانونية لنظام البطاقة المصرفية، مقال منشـــور على المـــوقع التـــالي:

www.arablawinfo.com

[3]-Tronche, La monaie electrinique, Revue de La association nationale en Droit, No. 42, 1982, p. 3;

مشار اليه لدى: **علي عدنان الفيل**، المسؤولية الجزائية عن إساءة إستخدام بطاقة الإئتمان الإلكترونية –دراسة مقارنة– ، مقال متاح على الموقع الإلكتروني التالي:

http://almuhamahresalah.blogspot.com/2015/10/blog-post_67.html

[4]-**ممدوح خليل البحر، عدنان احمد ولي العزاوي**، بطاقات الإئتمان والأثار القانونية المترتبة بموجبها، دراسة قانونية مقارنة، مؤتمر الأعمال المصرفية الإلكترونية، الجزء الثالث، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ماي 2003، ص1002.

[5]– فمن خصائص الأوراق التجارية قابليتها للتداول بالتظهير أو بالمناولة والتسليم اليدوي، في حين أن بطاقات الإئتمان والبطاقات المصرفية إجمالا لا يمكن التنازل عنها. كما أن بطاقات الإئتمان لا تتضمن بيانات إلزامية محددة كما هو الحال في الأوراق التجارية. وبالتالي علينا أن نتعامل مع هذه البطاقات كمستجد من الأعمال التجارية المصرفية ونتحـــرر من القوالب القانونية التي إعتدنا عليها على صعيد القانون التجاري والمدني معا، وأن نفسح

ومجمل القول، نرى أن محاولة إدخال بطاقة الإئتمان تحت القوالب التشريعية التقليدية يعتبر عقبة أمام التطور الذي تقوم عليه التعاملات الإلكترونية. فتعددية الصيغ السابقة تعكس بيقين حيرة الفقه في التعامل مع هذا المتغير ومحاولة طرح جملة من التكييفات، إنما يرد إلى تعذر تكييفها وفق صيغ العقود المعروفة، إلا أنه ينبغي أن نشير إلى أن هذه الوسيلة حديثة، فالأيسر والأصوب الإنتظار حتى يستقر النظام القانوني لهذه البطاقات لبيان أحكامه الأساسية التي يقوم عليها، حتى يتم وضع تشريع ثابت خاص بها وبطبيعتها القانونية الخاصة، و يشمل جميع التطورات التي تمس هذه البطاقة مستقبلا.

المطلب الثاني

المسؤولية الجزائية عن الإستخدام غير المشروع لبطاقة الإئتمان من قبل حاملها

لا يمكن ضبط مفهوم الإستخدام غير المشروع لبطاقة الإئتمان إلا من خلال بيان نقيضه، وهو الإستخدام المشروع للبطاقة، ويكون كذلك –كما مر معنا–حين يتم بواسطة الحامل الشرعي والبطاقة صحيحة، وفي الغرض المخصص لها، وفي حدود سقفها، وبالتالي فإن أي إستخدام للبطاقة من قبل حاملها لا تتوافر فيه الشروط السابقة يخرج به من دائرة المشروعية ويضعه في دائرة اللامشروعية. ونميز في هذا لإطار بين حالتين:الإستخدام غير المشروع للبطاقة خلال فترة صلاحيتها(الفرع الأول) والإستخدام غير المشروعللبطاقة بعد إنتهـــاء صلاحيتها(الفرع الثاني)

الفرع الأول

الإستخدام غير المشروع للبطاقة من قبل حاملها خلال فترة صلاحيتها

رغم كون أن البطاقة صحيحة وأن مستعملها هو الحامل الشرعي لها إلا أنه قد يساء إستخدامها من قبله، ويتخذ ذلك صورتين: الأولى وهو الحصول على السلع والخدمات مع عدم وجود رصيد كافي، والثانية هي السحب من الجهاز مع عدم وجود رصيد كاف.

أولا– تقديم البطاقة للتاجر لشراء سلعة مع عدم وجود رصيد كاف

يتحقق هذا الفرض حالة ما إذا قدم حامل البطاقة بطاقته إلى التاجر لشراء سلعة منه أو للحصول على خدمة دون دفع قيمتها نقدا، معتمدا على بطاقة الإئتمان التي يحملها وإكتشف التاجر أو الجهة المصدرة بعد ذلك بعدم وجود رصيد كاف لحامل البطاقة لتغطية قيمة هذه العملية، وهو مايثير مسألة التكييف القانوني

المجال لتقبل نظام جديد سيجد له مستقرا إلى جانب النظم المصرفية المعروفة.**احمد زيادات وابرهيم العموش**، الوجيز في التشريعات التجارة الأردنية، الطبعة الأولى، دار وائل للنشر، عمان، 1996،، ص293.

السليم في هده الحالة؟ في غياب نصوص خاصة صريحة في هذا الشأن، إنقسم الفقه إلى إتجاهين، البعض يرى مساءلتـــه جزائيا، والبعض الأخر يرى عكس ذلك كمايلي:

الإتجاه الأول: مساءلة حامل البطاقة جزائيا

حاول هـــذا الإتجاه تطويع نصوص قانون العقوبات وتفسيرها باسلوب يؤدي الى إخضاع هذا النشاط لأحكامه، وذلكبرد هذه الظاهرة إلى إحدى النظم القانونية القائمة وخاصة جريمة الإحتيال.

حيث يرى أنصار هذا الرأي[1] أن حامل البطاقة الذي تقدم بها إلى التاجر وإستخدمها للحصول على السلعة أو الخدمة منه، وتجاوز بهذا الإستخدام المبلغ المتفق عليه مع مصدر البطاقة، أنه إرتكب جريمة الإحتيال، وأن الـــركن المادي متحقق بإعتبار أن تقديم الحامل للبطاقة إلى التاجر يمثل طريقا إحتياليا يغطي الإدعاء بوجود سقف يغطي مشترياته، وتقديم البطاقة يمثل الوقائع الخارحية أو الأفعال المادية التي تعزز الإدعاء والتي من شأنها توليد الإعتقاد بأن حامل البطاقة لم يتعد السقف المحدد له بالعقد، وبالتالي يكون التاجر قد سلم البضاعة إلى الحامل معتقدا بصحة إدعاء الحامل مما يحقق عنصر الغش والخداع، والركن المعنوي متوافر لأن الحامل سيء النية يعلم ويدرك بأنه يتجاوز الحدود الإئتمانية لبطاقته عند إستخدامها لشراء البضاعة. وأنه كان على علم وقت الشراء أنه لن يقوم بتغطية نفقاته سواء في نهاية الشهر أو بعد ذلك[2].

بالرجوع الى نص المادة 372 من قانون العقوبات الجزائري، والتي تقابلها المادة 313 –1 عقوبات فرنسي[3] والمادة 336 عقوبات مصري، نجدها تنص ***: كل من توصل او تلقى اموال او منقولات او سندات او تصرفات او اوراق مالية او وعود او مخالصات او ابراء من التزامات أو الى الحصول على اي منها اوشرع في ذلك.***

–وكان ذلك بالإحتيال لسلب كل ثروة الغير او بعضها او الشروع فيه

– اما باستعمال اسماء او صفات كادبة او سلطة حالية او اعتماد مالي خيالي او باحداث الأمل في الفوز باي شيء او في وقوع حادث او اية واقعة اخرى وهمية او الخشية من وقوع شيء منها.

وباستقراءنا لهده المادة، نجد أن طرق الإحتيال محددة على **سبيل الحصر**، وعلى ذلك فإن مجرد تقديم الحامل للبطاقة لا يعد إستعمالا لطرق احتيالية لا سيما وأن التاجر يعلم بالمبلغ الذي يلتزم المصدر بالوفاء به مما يعدم أساس قيام جريمة الإحتيال[4]. قد يكون في هذا الفرض انه قد كذب على التاجر أو المصدر، لكن هذا الكذب لم يدعم بظاهر مادية يؤدي الى وقوع التاجر أو المصدر في غلط دفعه الى تسليم البضاعة أو النقود،

---

[1]-د. **ابو الوفا محمد ابو الوفا ابراهيم**، مرجع سابق، ص2074. د. **محمود احمد طه**، المرجع السابق، ص1133.

[2]–**د. نائلة عادل فريد قورة**، المرجع السابق، ص527.

[3]-**Article 313-1 du CPf**Modifié par Ordonnance n°2000-916 du 19 septembre 2000 - art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002 **dispose que :** L'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manoeuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge.

L'escroquerie est punie de cinq ans d'emprisonnement et de 375 000 euros d'amende.

[4]- **د. ابو الوفا محمد أبو الوفا**، المرجع السابق، ص2075.

بسبب أنه صاحب حق في إستخدام بطاقته الشخصية الصحيحة وبالطريقة الصحيحة. أما إذا تم ذلك بناء على وقوع عطل فني أو قصور في التعليمات المخزنة الموجودة في ذاكرة جهاز نقطة البيع، فلا يمثل ذلك خداعا أو غشا من حامل البطاقة مما ينفي وجود طرق إحتيالية[1].

الإتجاه الثاني: عدم مساءلة حامل البطاقة جزائيا

يرى هذا الإتجاه[2] أن تجاوز حامل البطاقة السقف الإئتماني الممنوح له من مصدر البطاقة وكان هذا الأخير ضامنا له في الحدود المتفق عليها أمام التاجر، فإن على التاجر القيام بالتأكد من صلاحية البطاقة وسقفها الإئتماني إذا كانت البطاقة من النوع الذي يكتب عليها مثل تلك البيانات، واذا لم يكتب عليها فعلى التاجر الإتصال بمركز التفويض للتاكد من وجود ائتمان لهذا الحامل، ولا يقبل منه الإدعاء بأنه قدم السلعة نتيجة خداعه من الحامل، كما أنه لم يستول على السلعة دون رضائه أو علمه، فهذا الأخير وان كان سيء النية، فقانون العقوبات لا يعاقب على النوايا،وعلى ذلك وتحاشيا للدفوعات المستقبلية يمكن للمصرف مصدر البطاقة أن يبادر إلى إلغاء البطاقة ورفض تجديد عقد إصدارها في المستقبل[3].

لكن ماذا لو أن التاجر حاول الإتصال مع الجهة المصدرة لمعرفة الغطاء المسموح به للحامل بالرغم من محاولاته الإتصال كأن تكون شبكة الإتصال مع البنك غير فعالة؟ يرى جانب من الفقه[4] أنه لا مسؤولية على الحامل في هذه الحالة كون أن الجهة المصدرة ملزمة بالوفاء للتاجر بقيمة المشتريات لديه والرجوع لا حقا على الحامل بما يجاوز الغطاء على أساس **المسؤولية العقدية.**

ونرى من جهتنا أن هذه الحالة لا تخرج عن كونها إخلال بالتزام تعاقدي الذي يربط حامل البطاقة مع مصدرها الوارد عادة في عقد إصدار البطاقة. ولاتحتاج في المقابل إلى تدخل المشرع بنص خاص لتجريم هذا الفعل، كون أن التاجر يعلم سلفا بالمبلغ المسموح التعامل في نطاقه مع حامل البطاقة، وبالتالي هو غير محتاج لحماية جزائية، وكون أن البطاقة غير قابلة للتداول على خلاف الشيكات، فإن الغير غير محتاج هو الآخر للحماية الجزائية.

ثانيا- السحب من الجهاز مع عدم وجود رصيد كاف

ينص العقد المبرم بين المصدر وحامل البطاقة عادة على أن يلتزم الحامل عند كل عملية سحب بالتأكد من كفاية رصيده، وفي المقابل يتم برمجة أجهزة السحب الآلي للنقود بتعليمات محددة سلفا للإمتناع عن الرضوخ لأمر السحب في هذه الحالة، ومن ثم يعد قيام حامل البطاقة مستغلا إعتماد الجهاز على نظام off

---

[1]- **د. علي عبد القادر القهوجي**، الجديد في أعمال المصارف بين الوجهتين القانونية والإقتصادية، أعمال المؤتمر العلمي السنوي لكلية الحقوق بجامعة بيروت العربية، الجزء الثالث، الجرائم المتعلقة باعمال المصارف، منشورات الحلبي الحقوقية، بيروت لبنان، مشار اليه لدى: **كميت طالب البغدادي**، المرجع السابق،151.

[2]- **د. احمد محمد المغربي**، المرجع السابق، ص976.

[3]- **د. ابو الوفا محمد أبو الوفاء**، المرجع السابق، ص2073، **كميت طالب البغدادي**، المرجع السابق، ص156.

[4]- **د. ثناء احمد المغربي**، المرجع السابق، ص976.

line[1] بسحب نقود تتعدى الرصيد المسموح به إخلالا بإلتزاماته تجاه مصدر البطاقة، لكن وفي غياب نصوص تجريمية صريحة، هل يندرج هذا التصرف تحت النصوص التجريمية العادية؟

في ضوء موقف الفقه والقضاء يمكننا التمييز بين اتجاهين في هذا الصدد:

الإتجاه الأول ويتفق أصحابه كون هذا الواقعة تخضع لنصوص قانون العقوبات، إلا أنهم إختلفوا حول التكييف الصحيح لها، فهناك من يرى معاقبته عن جريمة السرقة، وهناك من يرى مساءلته عن جريمة الإحتيال، وهناك من يرى مساءلته عن جريمة خيانة الأمانة[2].

يرتكز القائلين على كون تصرف العميل يشكل جريمة سرقة على عدة حجج منها[3] ما قضت به محكمة النقض الفرنسية من أن المدين الذي أعطى حافظة نقوده إلى الدائن لكي يأخذ ما يستحقه يرتكب جريمة السرقة، ولا يختلف الأمر بالنسبة لصاحب البطاقة الذي يزيد في سحبه للنقود–في رأي المحكمة– عما له بالفعل لدى البنك عن موقف هذا الدائن[4].

أما وكون تصرف العميل يشكل جريمة خيانة أمانة في إعتبار البعض الآخر، بسبب أن حامل البطاقة قد تسلمها من مصردها على سبيل الأمانة، وقام بإستعمالها بطريقة تعسفية متوصلاً بذلك إلى الاستيلاء على مال للبنك[5].

بينما اتجه البعض الآخر من الفقه إلى ما ذهبت اليه بعض أحكام القضاء الفرنسي[6] إلى إعتبار أن الواقعة تشكل جريمة نصب، استنادا الى ان العميل قد إدعى صفة غير صحيحة وهي أن له رصيدا دائنا في البنك.

الإتجاه الثاني: يرى جانب كبير من الفقه[7] وهو –ما نؤيده–عدم إنطباق النصوص التجريمية في قانون العقوبات على هذه الواقعة، ومن ثم لا ينطوي قيام حامل البطاقة الإئتمانية بسحب النقود أكثـــر من الرصيد المسموح به جريمة سواء سرقة أو نصب أو خيانة أمانة، ولا يتعدى أكثر من كونه إخلالا بأحد الإلتزامات التعاقدية التي قد تمنح مصدر البطاقة الحق في إتخاد إجراءات إدارية كسحب البطاقة أو ترتب مساءلته مدنيا إذا توافرت شروطها.

---

[1]-**د. نائلة عادل فريد قورة**، المرجع السابق، ص533.

[2]– حول هذا الإتجاه انظر: **كميت طالب البغدادي**، المرجع السابق، ص160 وما بعدها.

[3]– انظر في بقية الحجج:د. **عبد الفتاح بيومي حجازي**، جرائم الكمبيوتر والأنترت في القانون العربي النموذجي، المرجع السابق، ص433.

[4]-crim,21 avr 1964,bull crim n 121, jcp,1965,11,13973,rev,sc,crim,1965,p424

كما أصدرت بعض المحاكم الفرنسية أحكاما بوقوع جريمة السرقة في هذا الفرض استنادا الى توافر الإختلاس وعدم تـــوافر رضـــا البنـــك بالســـحب، مثـــل:.CA LYON 20 AVR,1982, D 1982, p538, **bouzat et pinatel**, crimes et delits contre les biens, rev sc,crim,1982,p91 مشارإليه لدى **نائلة عادل فريد قورة**، المرجع السابق، ص175.

[5]-**Michel Masse**. L'utilisation abusive de distributeur automatique de billets, Expertises des systemes dinformation, Nov. 1981, p. 6.

[6]- انظر: **د. محمود عبد الله حسين علي**، سرقة المعلومات المخزنة في الحاسب الآلي، الطبعة الثانية، دار النهضة العربية، القاهرة، 2002، ص229.

[7]–**د. محمود أحمد طه**، المرجع السابق، ص1132، د. **نائلةعادل فريد قورة**، المرجع السابق، ص534، **كميت طالـــب البغـــدادي**، المرجـــع الســـابق، ص170. **د. عبد الفتاح بيومي حجازي**، جرائم الكمبيوتر والانترنت، المرجـــع السابق، ص433.

ذلك أن حكم محكمة النقض الفرنسية بشان الدائن والمدين، يتعلق بواقعة سرقة بعد التسليم، عكس السحب في هذه الحالة يتم بهدف الحصول على التسليم، كما أن التسليم الصادر من جهاز الصراف الآلي هو تسليم إختياري يعبر حتما عن رضا البنك الذي يتمثل في إرادة القائمين على برمجة وتخزين المعلومات في ذاكرة الجهاز، فهؤلاء قد أعطوا الجهاز التعليمات محددة سلفا والتي ليس من بينها منع إعطاء العميل النقود إذا تحول رصيد العميل من رصيد دائن للبنك إلى مدين له، ومؤدى ذلك أن البنك لم يفصح بداية عن إرادته في رفض تسليم النقود، بما يتعين معه القول بقيام عنصر الرضى لدى البنك عن فعل الأخذ، فضلا عن الطبيعة الإلكترونية لأجهزة الصراف الألي التي هي وسيط فقط في عملية التسليم، تستجيب لكل طلب مطابق للنظام المحدد سلفا من جانب المصرف. وهو ما **ينفي وصف السرقة،**

كما لا يمكن تكييفه على أساس **النصب** فالحامل لم يلجأ إلى احدى الطرق الإحتيالية المحددة في القانون. كما لا يمكن تكييفها على أساس أنـــها **خيانة أمانة،** ذلك أنه يجب التفرقة بين تسليم العميل للبطاقة على سبيل الأمانة والتزامه بردها للبنك متى طلب منه ذلك، وبين إستخدامها إستخداما غير مشروع.

وقد أيد القضاء الفرنسي في العديد من أحكامه هذا الإتجاه[1]، أهمها ما إنتهت إليه محكمة النقض الفرنسية في أحد أحكامها المهمة، فدهبت للقول ***إن قيام حامل البطاقة بسحب مبلغ من النقود من أحد أجهزة التوزيع الألي، متجاوزا رصيده الدائن في الحساب، ينظر إليه على أنه مخالفة لشروط التعاقد بين البنك والعميل و لا يدخل تحت أي نص من نصوص قانون العقوبات[2].***

ومن جهتنا نرى أنه وإن كانت هذه الصورة مجرد فرضية بعيدة عن التطبيق بسبب نجاح التقنيات العلمية في المجال الإلكتروني في برمجة الأجهزة الآلية لتوزيع النقود، حيث تقوم في هذه الحالة برفض البطاقة، و إستبعاد تجريمها وفق الصيغ التقليدية، لا يعني رفض لكل حماية لها، بل يمكن حمايتها تحت مظلة نصوص جزائية أخرى، ومن ذلك نص المادة 323-3 عقوبات فرنسي و394مكرر 1 عقوبات جزائري،فهذه المواد تجرم كل من أدخل بطريق الغش معطيات في نظام المعالجة الألية .."، سواء كانت صحيحة أو لا، وهو ما يسمح بتطبيقها في الحالة التي يسيء فيها حامل البطاقة نفسه إستخدام بطاقته ورقمها السري عن طريق سحب ما يجاوز الرصيد، حيث ينطوي على ما قام به على إدخال غير مصرح به لمعلومات صحيحة.

وإن كان هذا موقف كل من المشرع الفرنسي ونظيره الجزائري، فإن بعض التشريعات لم تحسم الخلاف بعد حول مدى مسؤولية الحامل في هذه الحالة، كما هو حال المشرع المصري.

---

[1]- C P d 'engers, 2 decembre 1980,revue judiciaire de l 'ouest; 1981 – 2 p115
C P de lyon; 9 juillet 1981,Gaz, Pal , 1981 ,2, Note Sousi roubi blanche;
Crim. 24 oct. 1983, D. 1984.465, note Lucas de Leyssac

[2] LE PREVENU AVAIT UTILISE, EN SE CONFORMANT AUX REGLES TECHNIQUES D'EMPLOI DE L'APPAREIL, LA CARTE DONT IL ETAIT TITULAIRE ;… QU'EN EFFET LES FAITS REPROCHES A X... S'ANALYSENT EN L'INOBSERVATION D'UNE OBLIGATION CONTRACTUELLE ET N'ENTRENT DANS LES PREVISIONS D'AUCUN TEXTE REPRESSIF; cass crim 24 novembre 1983, **N° de pourvoi: 82-90672** ;disponible enlingne á l'adresse suivante:https://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000007061606

الفرع الثاني

الإستخدام غير المشروع للبطاقة من قبل حاملها بعد إنتهاء مدة صلاحيتها أو الغائها

لا تعد بطاقة الائتمان صالحة للاستخدام ولا يمكن تقديمها للتاجر في ثلاث حالات[1]، أولها إذا تم إلغائها من قبل البنك مصدر البطاقة، وثانيها إذا انتهت مدة صلاحيتها المبينة في العقد المبرم بين حامل البطاقة والبنك مصدر البطاقة، وثالثها إذا أخبر حامل البطاقة عن فقدانها أو سرقتها أو ضياعها.

لكن قد يحدث أن يقوم الحامل بإستخدامها سواء في السحب أو في الوفاء، أو أن يمتنع عن ردها للبنك، فهل يمكن تطبيق الأوصاف التقليدية على سلوك الفـــاعل في هذه الحالـــة؟

أولا- إمتناع حامل البطاقة رد بطاقته الملغاة أو المنتهية الصلاحية

يتجه رأي في الفقه[2] إلى أنه في حالة إنتهاء صلاحية البطاقة، ورفض صاحبها إرجاعها للبنك ينطبق عليه وصف خيانة الأمانة. فإلى أي مدى يمكن القبول بهذا التكييف؟

تنص المادة 376 عقوبات جزائري "***كل من إختلس أو بدد بسوء نية أوراقا تجارية أو نقودا.....لم تكن قد سلمت إليه إلا على سبيل الإجازة أو الوديعة أو الوكالة أو الرهن أو عارية الإستعمال أو لأداء عمل بأجر أو بغير أجر بشرط ردها أو تقديمها أو لإستعمالها أو لإستخدامها في عمل معين وذلك إضرارا بمالكيها أو واضعي اليد عليها أو حائزيها..."***

من خلال إستقراء هذا النص نجد أن هذا السلوك يقع تحت طائلة هذا النص، على إعتبار أن المشرع إعتبر بطاقات الدفع والسحب **أوراقا تجارية**جديدةإضافة إلى الأوراق التجارية الكلاسيكية وهي السفتجة والشيك والسند لأمر حسب الفصل 3 من الباب 4 من الكتاب 4 من القانون التجاري. وهو ما تطلبته المادة 376 من قانون العقوبات الجزائري، وباعتبارها تمثل حق حاملها في استخدام مبلغ معين في تنفيد مشترياته فتدخل في معنى المال المادي المنقول الذي ترد عليه جريمة خيانة أمانة وفق ما تشترطه المادة 314-1 عقوبات فرنسي والمادة 341 عقوبات مصري. على أن يسلم للجاني بناء على إرادة صحيحة ناقلا للحيازة الناقصة بموجب عقد من عقود الأمانة، وهي حسب المادة 376 هي" ***الإجازة او الوديعة او الوكالة او الرهن او عارية الإستعمال او لأداء عمل باجر او بغير*** .."،. إلا أن الجاني يقوم بتغيير نوع حيازته سواء بالإختلاس أو بالتبديد[3] إضرارا بمالكها أو واضعي اليد عليها أو حائزيهـــا.

ولما كان العقد المبرم بين مصدر البطاقة وحاملها يتضمن عادة شرطا بالتزام الحامل برد البطاقة عند إنتهاء صلاحيتها أو عند فسخ العقد، بما يعني أن التسليم هنا المصحوب بهذا العقد كان على سبيل الوديعة أو

---

[1]-**د. علي عدنان الفيل**، المرجع السابق، ص19.

[2] – د. **محمود أحمد طه**، المرجع السابق، ص1134.

[3]-**د. محمود نجيب حسني**، شرح قانون العقوبات القسم الخاص، المرجع السابق، ص1202.

الإستعمال وليس على سبيل التملك، فتنتقل الحيازة بذلك إلى الحامل بعنصرها المادي فقط_حيازة ناقصة– في حين يبقى العنصر المعنوي فيها محفوظا لمالك البطاقة وهو البنك. إذن فعلاقة البنك بالعميل حامل البطاقة علاقة تعاقدية قائمة على عقد عارية الإستعمال[1] وهو أحد عقود الأمانة حسب ما ورد في المادة 376 عقوبات جزائري والمادة 341 عقوبات مصري، وفي المادة 314–1 عقوبات فرنسي[2]، ذلك أن هذه الأخيرة وإن كانت لم تحدد نوع معين من العقود إلا أنه تقع الجريمة في كل حالة يسلم فيها المال ويقع على الجاني إلتزام برد المال[3] الذي يتم النص عليه في العقد أيا كان نوعـــه.

ومن ثم فإذا إمتنع عن ردها–حتى ولو لم يستعملها بعد ذلك– مع علمه بأنه يحتفظ ببطاقة منتهية الصلاحية أو ملغاة وأنه يجب عليه ردها، يعد إختلاسا وهو أحد صور النشاط الإجرامي لجريمة خيانة الأمانة، ومن باب أولى لو إستعملها، فإن إستعماله لهذه البطاقة رغم إلغائها فإنه يكشف بذلك عن تغيير نيته في نقل حيازته للشيء من حيازة ناقصة إلى حيازة كاملة[4].

هذا وقد إتجه القضاء الفرنسي إلى إنطباق وصف خيانة الأمانة على هذه الحالة، فقد قضت محكمة cretel الإبتدائية 15 جانفي 1985 على أنه *يعد مرتكبا جريمة خيانة الأمانة حامل البطاقة الذي على الرغم من مطالبة البنك المتكررة برد البطاقة و المبررة بالإستعمال التعسفي لها قد إستمر في إستعمالها* [5]

ثانيا– إستخدام الحامل لبطاقته الملغاة أو منتهية الصلاحية

يتحقق هذا الفرض حالة ما إذا كانت البطاقة لا تحمل تاريخ إنتهائها، أو لم تقم الجهة المصدرة بإخبـــار التاجر بإلغاء البطاقة أو إنتهائها، ومع ذلك قام الحامل بإستخدامها لإتمام مشترياته لدى التـــاجر مـــع تـــوافر القصد الجنائي لديه من علم وإرادة، مستغلا الفترة الزمنية الواقعة بين قيام البنك بمحو البرمجـــة الخاصـــة بالموزعات أو أجهزة السحب الآلي بحيث لا تقبل البطاقة، وإحاطة التاجر بهذا الإلغاء،وإذا كان الإتفاق حول ضرورة مؤاخذة الحامل جزائياً حماية للثقة في البطاقة وللمعاملات التي تستخدم فيها ، فإن الخلاف قد ثـــار حول **التكيـــيف القانوني** لفعله أي الجريمة التي يسأل عنها.

---

[1]– **د. محمود طه**، المرجع السابق، ص1135.

[2]-**Article 314-1 du CPF** Modifié par Ordonnance n°2000-916 du 19 septembre 2000 - art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002 .dispose que "L'abus de confiance est le fait par une personne de détourner, au préjudice d'autrui, des fonds, des valeurs ou un bien quelconque qui lui ont été remis et qu'elle a acceptés à charge de les rendre, de les représenter ou d'en faire un usage déterminé".

[3]- **Cour de Cassation Chambre criminelle**14 novembre 2000**N° de pourvoi : 99-84522**Publication : Bulletin criminel 2000 N° 338 p. 1003 Droit pénal, avril 2001, n° 4 p. 4, note S. JACOPIN. Le Dalloz, 2001-05-03, n° 18 p. 1423, note **B. de LAMY**. Revue trimestrielle de Droit civil, octobre décembre 2001, n° 4 p. 912 916, note Thierry REVET. Décision attaquée : Cour d'appel d'Aix-en-Provence, 1999-04-29

[4]–د. **محمود نجيب حسني**، شرح قانون العقوبات القسم الخاص،المرجع السابق، ص1204.

[5]-on peut considérer que l'abus de confiance est consommé lorsque le client effectue encore des retraits après injonction de restitution de la carte par la banque pour utilisation contraire aux dispositions contractuelles initialement prévues TGI Créteil 15 janv. 1985, D. 1985, Inf. rap. 344, obs. Vasseur et Rev. sc. crim. 1986.379, obs. Bouzat

كنا قد حسمنا مسؤولية حامل البطاقة في مواجهة المصدر، كونه يكون مرتكب جريمة **خيانة أمانة** كما سبق وأوضحنا في الفرض السابق، ويتمثل الضرر المترتب عن إستعمال البطاقة المنتهية الصلاحية أو الملغاة في قيام الجهة المصدرة بسداد قيمة الفواتير المرسلة إليها من التاجر المستخدمة فيها البطاقة، وذلك إذا ما أغفلت توجيه إخطار للتاجر بالبطاقات المنتهية الصلاحية أو الملغاة، فضلا عن الضرر الذي يعود على المصدر من إهتزاز ثقة الجمهور في مثل هذه البطاقات[1]. هذا من جهة.

ومن جهة أخرى، يكون حامل البطاقة قد إرتكب **جريمة الإحتيال** في مواجهة التاجر،وهو المنحى الذي سارت عليه بعض الإجتهادات القضائية الفرنسية[2]، وأيده الغالبية من الفقه[3]، فقيام الحامل بتقديم بطاقة الائتمان الملغاة يهدف إلى الإقناع بوجود إئتمان وهمي والحصول من التاجر على البضائع والمشتريات، مما يشكل إستيلاء على ثروة الغير.لأن التاجر لم يسلم للحامل هذه المشتريات لولا الكذب، فتقديم هذه البطاقة الملغاة وعدم وقوع خطأ من جانب التاجر الذي قبلها بعد تأكده من صلاحيتها وذلك من خلال الوسائل الموضوعة تحت تصرفه، يعد إستخدامالصفة غير صحيحة، لأنه بإلغاء البطاقة تزول كل صفة عن الشخص باستخدامها، مما يؤدي إلى القول بقيام جريمة الاحتيال بإستعمال صفة غير صحيـــحة.

ومن ثم يمكن تطبيق ما نصت عليه المادة 372 عقوبات جزائري والمادة 313 –1 عقوبات فرنسي والمادة 336 عقوبات مصري على هذه الحالة.

أكثر من ذلك، فإن النص الفرنسي لم يقصر العقاب على الحامل الذي يحصل على المنقولات المادية، وإنما عاقب صراحة فيما إذا حصل على خدمات[4] "à fournir un service" وهو الأمر الذي خلت منه المواد السابقة في القانون الجزائري والمصري.

ويتخذ الركن المعنوي في هذه الجريمة صورة القصد العام وهو علم الحامل وقت إرتكاب الفعل بأنه يستعمل طرق إحتيالية من أجل الإستيلاء على مال منقول للغير، وكما أن نيته قد إنصرفت فعلا لتملك المشتريات التي إستخدم البطاقة في شراءها من التاجر. والتي تمثل القصد الخاص[5].

ذلك كان عن إستخدام البطاقة في الوفاء، أما إستخدامها في السحب ونظرا للإستحالة المادية لعملية سحب النقود بإستخدام البطاقة الملغاة، نظرا للبرمجة التي يقوم عليها البنك لأجهزة الصراف الآلي، حيث تقوم إما بإبتلاع البطاقة أو على الأقل رفضها، نتيجة عمليات الفحص داخل الموزع، فلن نتطرق لدراستها، وإن كان يمكن مواجتهتها من خلال نص عام، والمتمثل في تجريم الدخول غير المشروع الى نظام المعالجة

---

[1]–د. **ثناء احمد المغربي**، المرجع السابق، ص970.وسواء كان الضر مادي أو معنوي، محقق أو إحتمالي:
Cas. crim. 3 janvier 1979 :http://www.lexinter.net/JF/abus_de_confiance.htmdisponible

[2]- قضت محكمة جنح باريس في 16 أكتوبر 1974 باعتبار صاحب بطاقة الائتمان منتهية الصلاحية أو الملغاة مرتكباً لجريمة الاحتيال إذا قام باستخدامها في الوفاء بثمن ما اشتراه ؛
Trib Corr, paris, 16 octobre 1974, banque n 338, p342 obs Martin (l-m)

[3]– **د.علي عدنان الفيل**، المرجع السابق، ص21. د. **ثناء احمد المغربي**، المرجع السابق، ص974. د. **محمد نور الدين سيد**، المرجع السابق، ص169.

[4]– انظر بهذا الشأن د. **عبد الفتاح بيومي حجازي**، جرائم الكمبيوتر في القانون العربي النموذجي، المرجع السابق، ص488.

[5]– **د. ثناء احمد المغربي**، المرجع السابق، ص974.

الآلية، على نحو ما ذهب المشرع الجزائري في المادة 394 مكرر والمشرع الفرنسي في المادة 323-1، ذلك أن الحامل قد جرد من صفته كحامل ومستخدم شرعي للبطاقة، فاذا ما إستخدمها في سحب النقود من أجهزة الصراف الآلي فإنه يدخل إلى نظام معلوماتي غير مصرح له بالدخول إليه. كما يمكن مساءلته على أساس جريمة إدخال معطيات إلى نظام المعالجة الآليـــة.

المطلب الثالث

المسؤولية الجزائية عن الإستخدام غير المشروع لبطاقة الإئتمان من قبل الغير

يقصد بالغير في هذا المطلب الأشخاص دون أطراف التعامل بالبطاقة، ويشكل وقوع البطاقة في أيديهم تهديدا لأطرافها، ويمكن حصر الإستعمالات غير القانونية من قبلهم في حالتين: أن تكون بطاقـــة الائتمـــان المستعملة صحيحة(الفرع الأوول) أو أن تكون غير صحيحة بمعنى آخر مزورة(الفرع الثاني)

الفـــرع الأول

سرقة بطاقة الإئتمـــان

تتكون البطاقة من جسم مادي ورقم سري يتم من خلاله التعامل بها، فيتم الإستيلاء على الدعامة المادية مع الرقم السري، وأحيانا ما يقتصر التعامل بالرقم السري فقد دون حاجة لإستخدام هذا الجسم المادي للبطاقة كما في حالة التعامل من خلال شبكة المعلومات الدولية، فيقتصر الأمر حينئد على الإستيلاء على المعلومات السرية عن طريق إنشاء مواقع وهمية على شبكة الإنترنت أو عن طريق التجسس وغيرها من الأساليب التي تتطور يوما بعد يوم[1]. وقد تطرقت الإتفاقية العربيةبمقتضى المادة 18 تحت عنوان "**الإستخدام غيرالمشروع لأدوات الدفع الإلكتروني**" على أنه تلتزم كل دول طرف بتجريم " ***كل من إستولى على بيانات أي أداة من أدوات الدفع وإستعملها أو قدمها للغير أو سهل للغير الحصول عليها"***

كل من إستخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول بدون وجه حق إلى أرقام أو بيانات أي أداة من أدوات الدفع".

أما التشريعات الجزائية المقارنة، فقد جاءت خالية من أي نص يشير إلى ذلك، فماهي النظرة القانونية في المعاملة الجزائية لكل حالة من تلك الحالات؟

أولا- الإستيلاء على البطاقة أو الكارت الإلكتروني(الدعامة المادية)

[1]-**د. حسين بن سعيد بن سيف الغافري**، لجرائم الواقعة على التجارة الإلكترونية، مقال متاح على الموقع الإلكتروني التـــالي:
http://www.mohamoon.com/montada/Default.aspx?Action=Display&ID=106198&Type=3

يتفق الفقه[1] على أن القيام بالإستيلاء على البطاقة يخضع لنشاط الإختلاس وبالتالي لتجريم السرقة، وذلك أمر بديهي لتحقق مفهوم الشيء المادي فيها، وبالتالي فإنه يمكن إختلاسه ويتحقق بهذا الفعل إخراج الشيء من حيازة المجني عليه، وإدخاله في حيازة الجاني بصرف النظر عن إستخدام البطاقة في السحب، فالسرقة شيء والاستفادة من الشيء المسروق شيء آخر[2].

وعلى ذلك يعاقب من سرق بطاقة إئتمان عن جريمة السرقة حسب المادة 311-1 من قانون العقوبات الفرنسي، والمادة 350 من قانون العقوبات الجزائري، والمادة 311 عقوبات مصري.

وتجدر الإشارة الى أن المشرع الفرنسي وبمقتضى أحكام التقنين النقدي والمالي، أوجب على الحامل في حالة إكتشافه إختفاء بطاقته أو فقدها أو أي إستعمال غير مصرح به لها أو لبياناتها، أن يقوم بإخطار المؤسسة البنكية حالا بالهاتف مباشرة أو عن طريق خدمة مابين البنوك، والقيام **بالمعارضة**[3] حتى يقوم البنك بمنع استعمالها، قبل أن يؤكد ذلك عن طريق رسالة موصى عليها مع إشعار العلم بالوصول. حيث يتم الإستناد على تاريخ الإرسال في حالة نشوب نزاع مع البنك[4].

وفي حالة ما إذا تمت عملية الدفع غير المصرح بها، قبل إعلام مزود الخدمة وفق ما نصت عليه المادة س133-17، يتحملها الدافع في حدود سقف 150 يورو حسب المادة س133-19[5] من التقين النقدي والمالي بدل من 400 يورو وفق المادة س123-3 الملغاة بموجب الأمر رقم 2009- 866.[6] بإستثناء حالة عدم إستخدام أداة الأمن الشخصي(الرمز السري (code confidentiel) أو رقم الأمان code de sécurité، فلا يكون هناك مشاركة في الخسارة الناتجة عن عملية الدفع غير المصرح بها[7].

وفي حالات نادرة، فإن مسؤولية الحامل تقوم حتى بعد عملية المعارضة بتحمله عبء سداد عملية الوفاء أو السحب، إذا كان تصرفه خاطئي أو تم بإهمال منه كما لو سجل الرقم السري في ورق لاصق بالبطاقة، وفي كل الأحوال يقع عبء إثبات هذا الإهمال على البنك[8].

---

[1]-انظر :**د. ايمن عبد الله فكري**، المرجع السابق، ص552.د. **علي عدنان الفيل**، المرجع السابق، ص29. **طالب البغدادي**، المرجع السابق، ص207.

[2]-**د. أحمد فتحي سرور**، الوسيط في قانون العقوبات -القسم الخاص-، دار النهضة العربية، القاهرة، 1992، ص842.

[3]-**Article L133-17**du code **monétaire et financier dispose que** dispose que I. # Lorsqu'il a connaissance de la perte, du vol, du détournement ou de toute utilisation non autorisée de son instrument de paiement ou des données qui lui sont liées, l'utilisateur de services de paiement en informe sans tarder, aux fins de blocage de l'instrument, son prestataire ou l'entité désignée par celui-ci.
II. # Lorsque le paiement est effectué par une carte de paiement émise par un établissement de crédit, une institution ou un service mentionné à l'article L. 518-1 et permettant à son titulaire de retirer ou de transférer des fonds, il peut être fait opposition au paiement en cas de procédure de redressement ou de liquidationVoir aussi **Frédéric LEPLAT**; LA REFORME DES CARTES BANCAIRES PAR LA LOI DU 15 NOVEMBRE 2001**;**Revue générale du droit , 2012, numéro 840. **p3.**

[4]-والتزام الحامل بالمعارضة في حالة السرقة أو الفقد محل نص في جميع العقود.

[5]-**Article L133-19**du code **monétaire et financier dispose que:** I. # En cas d'opération de paiement non autorisée consécutive à la perte ou au vol de l'instrument de paiement, le payeur supporte, avant l'information prévue à l'article L. 133-17, les pertes liées à l'utilisation de cet instrument, dans la limite d'un plafond de 150 euros.

[6]- voir notamment: **Jules Yossa**. Fraude à la carte bancaire : la victime est-elle remboursée ? En savoir plus sur http://www.village-justice.com/articles/Fraude-carte-bancaire-victime-est,17425.html#uXpf5xiCbqcGhoXi.99

[7]-**Christian Gavalda †Jean Stoufflet**,INSTRUMENTS DE PAIEMENT ET DE CRÉDIT; 7e ÉDITION; LexisNexis SAParis;2009.p5

[8]- Pour un exemple de négligence du client reconnue par les tribunaux, voir l'arrêt n° 14-29906 rendu par la chambre commerciale de la Cour de Cassation le 31 mai 2016..
https://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000032638638

أما في حالة السرقة الصورية، وفيها يقوم الحامل الشرعي للبطاقة باستعمالها بعد الإعتراض الكاذب عن سرقتها للبنك وتقديم شكواه للشرطة؟ ففي هذه الحالة يكاد يجمع الفقه[1]، على أن إستخدام البطاقة في هذه الحالة من الحامل يعتبر تحايلا منه، بخداع البنك وسلب بعض ماله سواء بالوفاء للتجار أو دفع مبلغ مساو للمبلغ المسحوب، وهذا التحايل أو الخداع تقوم به الطرق الإحتيالية في صورة تقديم أوراق أو مستندات تؤيد أكاذيب هذا الحامل-الإعلان الكاذب- ، وهو ما يسمح بتطبيق النص المتعلق بجريمة النصب. وعلى نفس النهج سارت محكمة النقض الفرنسية.[2]

ثانيا- إختلاس المعلومات السرية للبطاقة وإستخدامها

على عكس الحالة السابقة، وعلى الرغم مما يتوافر فيها من خطورة، فإنه في هذه الحالة والتي يقوم فيها الجاني بالحصول على المعلومات السرية للبطاقة وإستخدامها في الدفع لحسابه أو لحساب آخرين، خاصة بعد ما أمتد نشاط هذه البطاقات إلى شبكة الإنترنت الذي وإن شكّل عملية متسارعة لكونه يعد إحدى الطرق السهلة لشراء كل شيء تقريبا، إلا أن هذا الفضاء المفتوح يجعل من بيانات هذه البطاقة وأرقامها عرضة للإصطياد والإلتقاط من قبل العديد من القراصنة لإستخدامها في مشترياتهم أو السحب من الرصيد عن طريق شبكة المعلومات وايداعها في حسابهم.وهو ما وقع مع زبائن البنك الكندي، في قضية المتهم (ف.محمد) الدي أرسل برامج فيروسية ضمن أنظمة الدفع الإلكتروني مهمتها تسجيل المعطيات الرقمية أثناء إستعمال البطاقة ليتم إستعمالها لتحويل الأموال أو إقتناء مشتريات عن طريق الأنترنت.

وإن كان قد أجمع الفقه على ضرورة مؤاخدة الفاعل جنائيا، إلا أنهم إختلفواحول نوع الجريمة التي يساءل عنها. خاصة وأن النشاط هنا مركب يتمثل في حيازة المعلومات وإستخدامـــها.

أ-الحيازة غيرالمشروعة للمعلومات الســرية المتعلقة بإستخدام البطاقة

إنقسم الفقه بصدد هذه المسالة إلى إتجاهان: الإتجاه الأول[3]: فيرى بأن عدم مادية المعلومة يحول دون وقوع الإختلاس عليها، كما أن مفهوم الإختلاس لا يتحقق في إختلاس المعلومة لأنها تخرج من حيازة المجني عليه بل تظل في حيازته حتى بعد إستيلاء الجاني عليها.

وهذا الإتجاه يتماشى على ما إستقرت عليه العديد من التشريعات الجزائية بخصوص جريمة السرقة، فلم يقم المشرع الجزائري بالتعديل في محل جريمة السرقة بالمادة 350 ، لتبقى مسالة دخول المعلومات في نطاقها كما هي محلا للخلاف الفقهي. وكذلك هو الشان في التشريع المصري.

---

[1] - **د. نائلة عادل فريد قورة**، المرجع السابق، ص552. د. **محمد عبد الحليم عمر**، المرجع السابق، ص682.**د. محمد نور الدين سيد**، المرجع السابـــق، ص207.

[2]- cas crime 16 juin 1982 disep, 1987, n 18,p9,note le clech (PH):

[3] انظر في هذا الراي، د. **أيمن عبد الله فكري**، المرجع السابق، ص553.

Frédéric LEPLAT,op, cit; p 4**.**

وفي هذا الإطار يرى البعض من الفقه الفرنسي [1] أن عبارة du vol,…ou des données qui lui sont liées الواردة في المادة 133-17 من التقنين النقدي والمالي التي تتعلق بالإعتراض في حالات معينة ، فإن سرقة هذه البيانات(رقم، تاريخ الصلاحية...) لايشكل سبب مباشر للإعتراض، ويمكن في هذه الحالة تسبيب الإعتراض بخطر التهديد من الإحتيال. ففي القانون الجزائي فإن الأشياء غير الملموسة،مثل البيانات ليست عرضة للسرقة.على الرغم من أن اختلاس الكتابة المحققة لهذه البيانات يمكن ان تشكل سرقة.

أما الإتجاه الثاني[2]: يرى بأن مجرد حيازة المعلومات في تلك الحالة وبدون الحاجة إلى نشاط آخر مكون لنشاط الإختلاس.

وقد غلب المشرع الجزائري من جهته هذا الإتجاه، حينما نص في المادة 68 من قانون التوقيع الإلكتروني على انه "**كل من من يقوم بحيازة...بيانات إنشاء التوقيع الإلكتروني موصوف خاصة بالغير**" ، وبيانات الإنشاء كما سبق ورأينا تمثل التوقيع الإلكتروني الذي يستخدمه الموقع، والذي هو بيانات إلكترونية تخزن عبر وسيط الكتروني، وعلى رأسها البطاقة الذكية، أما المشرع الفرنسي فقد جرم بمقتضى المادة 323-3 عقوبات فعل حيازة او نقل أو إستخراج أو إعادة إنتاج بغش المعلومات، بموجب التعديل الدي أدخله على قانون العقوبات بالقانون رقم 2014-1353.

كما قام المشرع الفدرالي الأمريكي من جهته إيمانا منه بخطورة **حالات إختلاس هذه الأرقام عبر الأنترنت فقد عدها جريمة** وفق **A. 1.7** 18 U.S. Code § 1030، فقد حدث في عام 1996 أن تم إختراق حاسوب محمول يحتوي 314000 رقم لبطاقات إئتمان تخص أحد المكاتب التابعة لمؤسسة visa card int في كاليفورنيا وفي عام 1997 قام carlossadalgo بإستخدام حاسوب في جامعة سان فرانسيسكو وإختلس اسماء مالكي وأرقام log-onsعدد 100000 بطاقة إئتمان وكذلك بيانات أخرى من خلال إختراقه لمجموعة مزودي خدمات أنترنت ispsوقام بوضعها على أسطوانة مضغوطة cd ثم قام بتشفيرها وعرضها للبيع بمبلغ 250000دولار.وحوكم وعوقب بالسجن ثلاثين شهرا[3].

ب-إستخدام المعلومات السرية للبطاقة

لا يكتفي من يقوم بالإطلاع على البيان السري والذي يتعامل به صاحب الرصيد بمجرد الحيازة، بل يقوم بإستخدامه في إجراء سحب غير مشروع، ما يترتب عليه نقص في الذمة المالية للمجني عليه، الأمر الذي يترتب عليه إضرار بالمعاملات الإلكترونية[4].

---

[1]-**A. Lucas, J. Devèze, J. Frayssinet**, Droit de l'informatique et de l'Internet, PUF, Thémis, Droit privé, 2001, n° 989 sur l'exclusion de la qualification de vol; Rappr. Crim. 12 déc. 1990, Bull. crim. n° 430, D. 1991.346, note Mirabail ; GP. 1992.1.111 ; Rev. sc. crim. 1992.84, obs. Bouzat à propos de l'utilisation d'un minitel sans autorisation. **Frédéric LEPLAT**,op,cit,p 4.

[2] -**د. هدى حامد قشقوش**، الحماية الجنائية للتجارة الإلكترونية، المرجع السابق، ص ص62-63.

[3] -USA, JUN 23 1 23 PM '97, CRIMINAL NO. CR97 00197 VRW https://cryptome.org/jya/smak.htm

[4] -**د. ايمن عبد الله فكري**، المرجع السابق، ص553.

هذا وقد إختلف الفقه حول التكييف القانوني لهذا النشاط الإجرامي، فمنهم من ذهب إلى أن هذا النشاط يشكل جريمة سرقة، ومنهم من رأى فيه جريمة نصب، وهناك من إعتبره تزوير وإستعمال محرر مزور.

يذهب الفقه والقضاء الفرنسي إلى أن المتهم يسأل عن **جريمة نصب**،[1]بسبب أن الجاني يقوم بإستخدام إسم كاذب أو صفة غير صحيحة بأنه هو صاحب هذا الإئتمان الذي يتعامل من خلاله.

وهناك من يكيفها على أساس **جريمة السرقة**[2]، فإذا لجأ الجاني الى سرقة المعلومات بوصفها مال معنوي قابل للسرقة ثم إستخدمها في السحب عن طريق شبكة الأنترنت وإيداعها في حسابه من خلال معاملة إلكترونية معينة، يشكل هذا الفعل جريمة سرقة لأنه خلصت له حيازة النقود المسروقة رغم عدم قبضها و تسليمها إياه، وذلك لأن هذا الأمر يعد أثرا من آثار الجريمة، وهو الأمر الذي يميز ما بين السرقة المعلوماتية والسرقة التقليدية. فالسرقة المعلوماتية ذات طبيعة مركبة وتحل على أساس قواعد الإرتباط المادي بين الجرائم المرتكبة لغرض واحد.

وهناك من يذهب إلى تكييفها على أساس **جريمة التزوير**[3]، لأن الجاني عندما يقوم بإستعمال المعلومات السرية الخاصة بصاحب الرصيد فهي تمثل التوقيع الإلكتروني الذي يستخدمه صاحب الرصيد ويكون في إستيلاء الجاني عليه وإستخدامه في السحب من الرصيد إستخدام لتوقيع صاحب الرصيد.

وقد غلبت بعض التشريعات التكييف الأخير، كماهو حال المشرع الجزائري بالمادة 68 والتي تنص "***...حيازة أو إفشاء أو إستعمال بيانات إنشاء توقيع الكتروني موصوف خاصة بالغير***"، وإلى جانب المشرع الجزائري نجد المشرع المصري هو الآخر نهج نفس النهج حين نص في المادة 23 من قانون التوقيع الإلكتروني" ***إستعمل توقيعا أو وسيطا أو محررا الكترونيا معيبا أو مزورا مع علمه بذلك***".

من وجهة نظرنا، نرى بأن هذه الواقعة–وإنطلاقا من تحليل أفعـــال الجاني–يمكن أن تخضع لأكثر من وصف قانوني،ويعاقب الجاني بوصف الجريمة الأشد إعمالا لنص المادة 32 من قانون العقوبات الجزائري. ذلك أن سلوك الفاعل يمكن أن يشكل **جريمة إحتيال** حسب المادة 372 عقوبات جزائري والمادة 3131–1 عقوبات فرنسي،نظرا لإستخدامه الطرق الإحتيالية(الإسم الكاذب وهو إسم صاحب البطاقة الحقيقي و الصفة الكادبة)، وهو أحد الصور الإحتيالية لجريمة الإحتيال لإقناع المجني عليه بوجود إئتمان، فنكون أمام تعدد مادي للجرائم، ذلك أن هناك نصوص تعاقب على الدخول غير المشروع (المادة 394 عقوبات جزائري– 323– عقوبات فرنسي) أوعلى مجرد حيازة المعلومات(المادة 68 قانون التوقيع الإلكتروني)، ونظرا لأن الإستيلاء على متعلقات الهوية تم بغرض إستعمالها فنكون بصدد إرتباط **غير قابل للتجزئة**.

كما تشكل هذه الواقعة **تزوير حسب المادة 441–1 عقوبات فرنسي والمادة 68 من قانون التوقيع الإلكتروني الجزائري، والمادة 23 من قانون التوقيع الإلكتروني المصري**، لأن الجاني حينما يقوم بالإستيلاء

---

[1]– **د. محمود طه**، المرجع السابق، ص1153. **د. ثناء المغربي**، المرجع السابق، ص980.

Frédéric LEPLAT,op,cit, p 4

crim, 19 mai 1987:gaz pal,1988,1,somm 5 note doucet; .bordeaux,25 mars 1987,D,1987,424,note pradel, code penal,dalloz, 106 edition,2009,p818

[2]–**د. عبد الفتاح بيومي حجازي**، النظام القانوني لحماية التجارة الإلكترونية، المرجع السابق، ص201.

[3]– **عمر سالم**، المرجع السابق، ص ص41–42.

على الرقم السري والذي يمثل التوقيع الإلكتروني، فقد توصل الى الوسيلة التي تعبر عن هوية المستخدم الشرعي، وبالتالي التصرف على أساس أنه صاحب تلك الهوية، وإجراء التصرفات المختلفة التي يتحمل تبعتها المستخدم الشرعي من خلال إنتحال شخصيته التي يمثلها التوقيع الإلكتروني، وينسب الجاني لنفسه هذا التوقيع على غير الحقيقة[1]. كما تشكل في الوقت ذاته جريمة **سرقة**. كما تشكل جريمة **التعامل في معلومات متحصلة من جريمة** حسب الفقرة 2 من المادة 394 مكرر 2 عقوبات جزائري.

ولم يتبنى القضاء الجزائري– قبل تدخل المشرع بنص خاص في قانون التوقيع الإلكتروني– هذا التفسير، حيث قضى قسم جنح عنابة بتوافر جنحة تصميم وإدخال عن طريق الغش لمعطيات للمعالجة الآلية في منظومة معلوماتية والمتاجرة فيها أدت إلى تعديل معطيات تلك المنظومة في حق المتهم (ف.محمد) الذي إستعمل أرقام حسابية وأرقام سرية لبطاقات دفع الكترونية في تحويل الأموال واقتناء اجهزة الكترونية عبر الأنرنت، والتي تم الحصول عليها عن طريق تصميم موقع شبيه بالموقع الرسمي للبنك الكندي.

الفرع الثـــاني

تزوير بطاقـــة الإئتمـــان

قد تقع بطاقة الإئتمان في يد الغير، فيقوم بتغيير حقيقتها كليا أو جزئيا لإستخدامها فيما بعد للإستيلاءعلى الأموال.والتزوير الواقع على البطاقة قد يتخذ صورة تزوير كلي _التقليد_، أوالبيانات فقط كالرقم السري أو التوقيع. وعلى العموم فإن المحور الأساسي الذي يرتكز عليه هذا النشاط هو المكونات المقروءة إلكترونيا التي تغدي جسم البطاقة وتفعيلها وطرحـــها للتداول.

ولقد أناطت التشريعات الجزاية – كما مر معنا سابقا– قواعد التجريم في جريمة التزوير في المحررات بأنه يجب أن يكون تغيير الحقيقة منصب على محرر، ومن ثم يطرح التساؤل من جديد حول مسألة مدى إنطباق نصوص التجريم الخاصة بالتزوير على تحريف الحقيقة الواقعة على **البيانات** المخزنة بطريقة غير مرئية على البطاقة.

كنا قد ناقشنا هذه المسألة عندما تناولنا تزوير المستند الإلكتروني، وقد توصلنا من خلال إستقراءنا لنصوص بعض التشريعات، كما هو حال المشرع الجزائري، أنه حتى نخضع التلاعب فيها لجرائم التزوير لا بد أن يكون هناك ارتباط بين اتخاد اجراءات التصديق والإعتراف لهده البيانات بالحجية خصوصا في حالة التعامل بالرقم السري للبطاقة فقط عبر الأنترنت، ومن تم يشملها النص الخاص بتزوير المحررات العرفية أو التجارية أو المصرفية.

وإن كان ذلك كذلك، فإن النص التقليدي للتزوير لا يكفل الحماية الكاملة من التغيير الواقع على الشريط المغناطيسي أو الشريحة الرقائقية، ونلمس ذلك من خلال عدم إنسجامه مع طبيعة البطاقة بتجاوزه التعداد الجصري لصور ومظاهر السلوك، وعدم تركيزه على إحداث التغيير في الحقيقة بصورة مفتعلة توقع الضرر

[1]– د. **حسن طاهر داود**، جرائم نظم المعلومات، اكاديمية نايف العربية للعلوم الأمنية، الرياض، 2000، ص84–89.

أو تهدد به دون أن تعير بالا لطريقة أو مظهر تغيير الحقيقة. فالأصوب أن يلتفت المشرع الجزائي وأن ينص على هذه الصورة الحديثة للتزوير. وهو مافعلته بعض التشريعات مثل التشـــريع الفرنسي.

فحماية للبطاقة ذاتها وللذمم المالية لأصحابها، فقد قام المشرع الفرنسي بإضفاء طابع جزائي خاص على كل من زيف أو زور هذه البطاقات بإعتبارها صورة من صور وسائل الأداء الحديثة في الدفع. حيث تناول الحماية الجزائية للبطاقة الإئتمانية من التزوير في المواد س163-3 وما بعدها من التقنين النقدي والمالي، صيانة منه لأسس ومبادي النظام العقابي، لكن هل نصوصه تماشت لتشمل تجريم إستعمال البطاقات المزورة؟ هذا ما سنعالجـــه من خلال النقاط التاليـــة.

أولا- تزوير أو تقليد بطاقة الإئتمان

نصت المادة س 163-3 يعاقب ***... كل من قلد أو زور شيك أو اداة من الأدوات المنصوص عليها في المادة س 133-4***"

بإستقراءنا لنص المادة س163 والمادة س133-4 ، وإستنادا على القواعد العامة في التزوير عموما، يتضح لنا أن بنيان هذه الجريمة يقوم على ركنين، ركن مادي ويتم بسلوك إجرامي يرتكبه الجاني قد يتخذ صورة التزوير أو التقليد، وينصب هذا السلوك على محل معين هو أدوات الدفع، ولكي تتم الجريمة بشكل كامل لابدمن توافر القصد الجرمي الذي يمثل صورة الركن المعنوي لهده الجريمة.

أ-الركـــن المـــادي

إنطلاقا من نص المادة السابقة، يتضح أن **النشاط الإجرامي** في هذه الجريمة يتمثل في صورة التقليد أو التزوير.

ويقصد بالتقليد صناعة شيء على غرار شيء سابق[1]، وفي مجال تزوير بطاقة الإئتمان يعني صناعة بطاقة على غرار بطاقة أخرى سابقة. وهو ما يسميه خبراء الكشف عن التزوير بطريقة **التزوير الكلي**، حيث يتم تقليد الرسوم الخاصة الموجودة على جسم البطاقة ثم تغليفها ولصق الهولوجرام والشريط الممغنط وشريط التوقيع ثم إستيحاء الطباعة النافرة عن طريق إنشائها بالمعلومات التي يتحصل عليها هؤلاء المزورين[2].

والواقع أن **التقليد** ما هو إلا طريقة يمكن أن يقع بها التزوير، فكان يمكن أن يكتفي المشرع بنص التزوير فقط، وقد فسر البعض[3] منهج المشرع هذا برغبته بالفصل بين التزوير الذي يقع على البطاقة ذاتها كمحرر، والتزوير الذي يأخذ صورة الإصطناع.

---

[1]-**د. محمود نجيب حسني**، شرح قانون العقوبات، القسم الخاص، المرجع السابق، ص238.

[2]-**د. علي عدنان الفيل**، المرجع السابق، ص35. **معادي اسعد محمد صوالحة**، بطاقات الإئتمان النظام القانوني وآليات الحماية الجنائية والأمنية، دار الأفاق المغربية للنشر والتوزيع، الرباط، 2008، ص330.**د. رياض فتح الله بصلة**، جرائم الإحتيال بالبطاقات الإئتمانية، المرجع السابق، ص95.

[3]-**د. محمد عبيد الكعبي**، المرجع السابق، ص686.

أمـــا التزوير فلم يحدده المشرع بطريقة معينة مما يعني أن أي تغيير في البطاقة وبأية طريقة يتحقق به فعل التزوير[1]، وهو بهذا لم يحد عن النهج الذي إتبعه في قانون العقوبات فيما يتعلق بالمادة 441-1، وطرق التزوير متعددة يتم اللجوء إليها من طرف العصابات المتخصصة في ذلك، أهمها النسخ عن طريـــق كشـــط معلومات الشريط الممغنط وهو ما يطلق عليه skimming Devise [2] والتزوير بالصقل[3].

أما عن محل الجريمة، فقد حدده المشرع الفرنسي بالإحالة إلى نص الماة 133-4من الفصل 3 من الكتاب 1 تحت عنوان: ***القواعد المطبقة على ادوات الدفع الأخرى، والتي تنص على أنه:***

"يقصد **بجهاز الأمن الشخصي** على أنه كل وسيلة فنية مملوكة لمستخدم خدمة الدفع، تستخدم في اداة الـــدفع، وتوضع تحت عنايته وتتعلق بالتوثيق.

تعني **اداة التعريف الفريدة**، على أنها مزيج من الحروف و الأرقام والرموز المحددة لمستخدم خدمة الدفع.

اداة الدفع هي كل جهاز شخصي ومجموعة من الإجراءات المتفق عليها بين مستخدم خدمة الـــدفع **ومـــزود خدمة الدفع**[4] تمكن مستخدم الخدمة من إعطاء الأمر بالدفع .

من خلال ما سبق يتبين ان المشرع جمع كل **ادوات الدفع** في تعريف واحد، مما يجعل من مدلول وسيلة الدفع شاملا الحوالة المصرفية والخصم المباشر وتبادل البيانات الإلكترونية، والدفع بالبطاقات ســـواء كـــان وطني أو عابر للحدود داخل منطقة الدفع بالأورو SEPA[5] وغيرها[6] من الآليات التي تسمح بتنفيد عمليـــات

---

[1]– انظر:د. **ايمن عبد الله فكري**، المرجع السابق، ص413.

[2]- ويقصد بها سرقة البيانات المكونة للشريحة الممغنطة لبطاقة الإئتمان، حيث يقوم المحتالين بوضع أجهزة الكترونية خاصة على نقاط الدفع واجهزة الصراف الآلي ، بل حتى على الأنترنت لإلتقاط البيانات الموجودة على الشريحة الممغنطة ، لمعرفة هوية الحامل ، رقم البطاقة وتاريخ الصلاحية بهدف تقليد أو تزوير البطاقة .والرمز السري يمكن معرفته من خلال كاميرات مصغرة تصويرية.

Marc-Antoine Bindler, Le top 4 des fraudes à la carte bancaire; disponible en lingne á l'adresse suivante: http://www.europe1.fr/france/le-top-4-des-fraudes-a-la-carte-bancaire-1374767

أنظر كذلك الموقع التـــالي:

http://fr.euronews.com/2015/06/05/fraude-a-la-carte-bancaire-en-quoi-consiste-la-technique-du-skimming

[3]-يتطلب هذا النوع من التزوير وجود قاريء الكترومغناطيسي يشبه جهاز التسجيل يقوم بقراءة البيانات من على الشريط الممغنط وتخزين بياناته داخل ذاكرته ثم تفريغه بعد ذلك في بطاقة أخرى فارغة: **معادي اسعد محمد صوالحة**، المرجع السابق، ص277.

[4]- Un prestataire de services de paiement (PSP) est une entreprise agréée pour offrir des services de paiement. Il s'agit soit : Î des établissements de crédit (dont les banques) traditionnellement engagés dans ces activités puisque la loi leur conférait jusqu'à présent l'exclusivité de la mise à disposition et gestion des moyens de paiement ; Î des « établissements de paiement » nouvellement créés , qui ne sont pas des établissements de crédit, mais peuvent désormais également offrir des services de paiement. Sous cette catégorie, on peut trouver par exemple des opérateurs technologiques (téléphonie, internet) ou encore des entreprises proposant des services d'envois d'argent liquide (par exemple aux migrants vers leur pays d'origine).

Les nouvelles règles de fonctionnement des Services de Paiement; L e s M i n i - G u i d e s B a n c a i r e s; la Fédération Bancaire Française" Paris 2009 p.5

[5]-l'**espace unique de paiement en euros**est un espace de paiement en euro unifié mis en place par les banques membres du Conseil européen des paiements(l'**EPC**, *European Payments Council*) en réponse à la demande de la Commission européenne. https://fr.wikipedia.org/wiki/Espace_unique_de_paiement_en_euros

[6] - **Jean Devèze**, Instruments de paiement et de credit, disponible en lingne á l'adresse suivante*:*http://197.14.51.10:81/pmb/COURS%20ET%20TUTORIAL/DROIT/Droit%20Prive/Instruments%20de%20paiement%20et%20de%20credit.pdfqrticle ; ***Pierre Emmanuel OMBOLO MENOGA*INSTRUMENT DE CREDIT ET DE PAIEMENT**; disponible en lingne á l'adresse suivante*:*http://lumiairedudroit.centerblog.net/36-instruments-de-credit-et-de-paiement: **Eric A. Caprioli**Vade-mecum juridique de la dématérialisation des documents juridiques - Fédération des Tiers de Confiance; 7ÈME ÉDITION;p 20.

الدفع. بما تشمله من عناصر يثمرها المزور في عملية التزوير كالشريط الممغنط وشريط التوقيع، صـــورة الحامل.

فضلا عن ذلك فـــإنه لو تاملنا في نص المادة السابقة، نلاحظ أن المشرع قد وسع من نطاق تطبيقها لتشمل بالتجريم أدوات التعريف الفريدة للبطاقة(رقم البطاقة، تاريخ انتهاء الصلاحية..) وأجهزة الأمان الشخصي(الرمز السريCode confidentiel) ، ذلك أنه وللإستفادة من خدمة الدفع عادة ما تقدم مؤسسة الدفع للمستخدم في مرحلة أولى كلمة تعريفية، وبعد نجاح الإستفادة من خدمة الدفع تطلب المؤسسة من الزبون عبر موقعها الإلكتروني تحديد توقيعه الإلكتروني، الذي سيحتفظ به بطبيعة الحال سريا، بهدف التأمين التام للعملية.

ولا يمكن أن يكتمل الركن المادي لجريمة التزوير دون تحقق عنصر **الضرر** سواء كان مادي أو معنوي، فردي أو اجتماعي، حال أو إحتمالي[1].

ب-الركـــن المعنـــوي

يتخذ الركن المعنوي في هذه الجريمة صورة القصد الجنائي العام، بعنصريه العلم ولإرادة، كما يشترط المشرع قصدا خاصا ويتجسد في نية الجاني إستعمال البطاقة في الحال أو المآل فيما أعدت لها، وقد وضحت محكمة النقض الفرنسية للقصد الجنائي في قرار لها بقولها" ***القصد الجنائي للفاعل يظهر مهما كانت بواعثه من وعيه بتزييف الحقيقة في محرر من شانه اقامة الدليل على حق او واقعة تترتب عليها نتائج قانونية***"[2]

ت-العقوبـــــة

يعاقب المشرع على الجريمة بعقوبة الحبس 7 سنوات و بغرامة 750000 يورو.

ثانيا- إستعمال أو محاولة إستعمال بطاقة مقلدة أو مزورة

نص المشرع على هذه الجريمة بموجب الفقرة 2 من المادة س163 -3 كمايلي: ***كل من إستعمال أو حاول إستعمال شيك أو أداة أخرى منصوص عليها في المادة س133-4 .***

أ-الركـــن المـــادي

[1]-إستقر الإجتهاد القضائي للمحكمة العليا انه لا يوجد تزوير معاقب عليه إلا إذا سببت الوثيقة المقلدة أو المزيفة ضررا حالا أو محتملا للغير" قرار المحكمة العليا ، تاريخ 21-12-1999، قضية رقم 227350 ، مشار اليه لدى: **نجيمي جمال**، المرجع السابق، ص523.

[2]- «l'intention coupable de l'agent résulte, quel que soit son mobile, de sa conscience de l'altération de la vérité dans un document susceptible d'établir la preuve d'un droit ou d'un fait ayant des conséquences juridiques,» cass crime; chambr criminel , 3 ,mai 1995 **N° de pourvoi: 94-83785 :p 6**disponible en lingne á l'adresse suivante*:* https://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000007559501

يتحقق الركن المادي لهذه الجريمة بنشاط يرتكبه الجاني يتخذ صورة الإستعمال أو محاولة الإستعمال- الشروع-، ويقصد بالإستعمال كما عرفه الفقه بأنه تقديم أو إبراز المحرر والإحتجاج به على أنه صحيح، وفي نطاق بطاقة الإئتمان فإن هذا السلوك يتحقق بإبراز الجاني البطاقة والإحتجاج بها على أنها سليمة وتقديمها لشخص ما للتعامل بها على أنها صحيحة[1] وتكون كذلك عندما يستخدمها للوفاء لدى أحد التجار، أو عند إستخدامها في السحب من الآلة، وما يؤكد الحالة الأخيرة أن المشرع جرم كذلك محاولة الإستعمال – **الشروع**- وعاقب عليه بنفس العقوبة[2].

و ينصب هذا السلوك على محل محدد وهي البطاقة المزورة أو المقلدة، ومن تم يخرج من نطاق التجريم وفق هذا النص البطاقات الصحيحة، وإن كان يمكن أن يتابع الجاني وفق نموذج قانوني آخر -**كالنصب أو السرقة**- إذا توافرت أركـــانها.

ب-الركـــن المعنـــوي

يتخذ الركن المعنوي في هذه الجريمة صورة القصد الجنائي العام، بأن يعلم الجاني بأن البطاقة مزورة أو مقلدة وتتجه إرادته إلى إبرازها والإحتجاج بها على أنها بطاقة صحيحة، ومن ثم ينتفي القصد إذا ثبت أن مستعملها لا يعلم بتزويرها.

ت-العقوبـــــة

يعاقب المشرع على الجريمة بعقوبة الحبس 7 سنوات و بغرامة 750000 يورو.

ثالثا-قبـــول التعامـــل ببطاقة مقلدة أومزورة

نص المشرع على هذه الجريمة بموجب المادتس163-3 "***كل من قبل الدفع عن طريق شيك أو أي أداة أخرى منصوص عليها في المادة س133-4 مقلدة أو مزورة وهو يعلم بذلك.***

أ-الركـــن المـــادي

يتمثل الركن المادي في هذه الجريمة في نشاط إجرامي يقوم به الجاني يتخذ صورة قبول الشخص بالوفاء عن طريق بطاقة إئتمان على الرغم من علمه بتقليدها أو تزويرها، سواء كان تاجر أو غيـــره، وقـــد ثـــار التساؤل حول جدوى هذا النص والذي رأى فيه بعضهم أن القواعد العامة كانت تكفي لمواجهـــة مثـــل هـــذا

[1]-**د. محمود محمود مصطفى**،شرح قانون العقوبات، القسم الخاص، الطبعة الثامنة، مطلعة جامعة القاهرة، 1984، ص 177.

[2]-**د. ايمن عبد الله فكري**، المرجع السابق، ص414.**د. محمد عبيد الكعبي**، المرجع السابق، ص692.

النشاط، في حين رأى البعض الآخر أن القواعد العامة في الإشتراك في الجرائم لا تكفي، وأن هـذا الـنص يمتد ليشمل كل من قبل التعامل بالبطاقة المزورة حتى ولو كان صاحبها أو البنك المسحوب عليه[1].
أمـا المحل الذي ينصب عليه هذا السلوك فهو البطاقة المقلدة والمزورة وفق الشـرح السـابق بيانه.

ب-الركـن المعنـوي

يتخذ الركن المعنوي لهذه الجريمة صورة القصد الجنائي العام بعنصريه العلـم والإرادة.

ت-العقوبـة

يعاقب المشرع على الجريمة بعقوبة الحبس 7 سنوات و بغرامة 750000 يورو.

رابعا- التعامل في معلومات أو أدوات صالحة لإرتكاب جريمة تزوير أو تقليد بطاقة الإئتمان

نصت المادة س163-4[2] من التقنين النقدي والمالي***"يعاقب ...كل من قام بصناعة أو الحصولأو حيازة او توفير او الوضع تحت التصرف تجهيزات ادوات برامج معلوماتية او معطيات مصممة او معدة لإرتكاب الجرائم المنصوص عليها في الفقرة 1 من المادة س163-3 "***

وقد جاء في سبب تجريم هذا النشاط، كون أن العديد من الأفعال قد تكون مجرمة في نطاق نصوص سابقة، مثل النصوص المتعلقة بالنصب، أو الدخول غير المشروع إلى نظام المعالجة الآلية، لكن هناك من السلوكات التي لا يمكن أن تندرج تحت أي وصف، فهذه المادة تشمل تجريم الأفعال الجديدة في مجال تزوير وتقليد أدوات الدفع[3].

وهذا أمر طبيعي كون فرنسا قد صادقت على إتفاقية بودابست، حيث نصت عليها هذه الأخيرة في المادة 7 تحت عنوان إساءة إستخدام الأجهزة، كما تطرقت بدورهاالإتفاقية العربية في المادة 18 فقرة 1 الى هذا النشاط حين نصت ***"كل من زور او اصطنع او وضع أي اجهزة او مواد تساعد على تزوير او تقليد أي اداة من ادوات الدفع الإلكترونية باي وسيلة كانت.***

أما المشرع الجزائري فإكتفى بالنص العام في قانون العقوبات وهو النص 394 مكرر 2 بفقرتها الأولى المتعلق بالتعامل في معلومات صالحة لإرتكاب جريمة من جرائم الإعتداء على نظم المعالجة الآلية، وهو ما يشمل في نطاقه جريمة التلاعب بالمعلومات المخزنة في نظام المعالجة الآلية.

---

[1]-**د. محمد عبيد الكعبي**، المرجع السابق، ص694.

[2]- **Article L163-4** du Code monétaire et financier Modifié par Ordonnance n°2009-866 du 15 juillet 2009 - art. 2dispose que "Est puni de sept ans d'emprisonnement et de 750 000 euros d'amende le fait, pour toute personne, de fabriquer, d'acquérir, de détenir, de céder, d'offrir ou de mettre à disposition des équipements, instruments, programmes informatiques ou toutes données conçus ou spécialement adaptés pour commettre les infractionsprévues au 1° de l'article L. 163-3"

[3]- https://www.senat.fr/rap/l00-329/l00-32921.html

أ- الركـــن المـــادي:

تناول المشرع الفرنسي بالتجريم مجموعة من الأفعال إستشعر بخطورتها فإعتبر أن من شأن تركها دون عقاب مضاعفة كم جرائم التزوير في البطاقات الإئتمانية، وتشمل هده الأفعال كافة العمليات السابقة على تزوير أو تقليد البطاقة، وهو الأمر الذي تم الدعوة إلى تجريمه وإفراد عقوبة له من طرف اتفاقية بودابست والإتفاقية العربية.

وهذه الأفعال هي على قدم المساواة في تحقيق النشاط الإجرامي المكون للركن المادي للجريمة، وهو ما يستفاد من لفظ" أو" الواردة في المادة الســـابقة.

1-التصنيـــع: وهو أول عماية في سلسلة التعامل، وتتمثل في عملية صناعة *تجهيزات ادوات، برامج معلوماتية او معطيات* مصممة خصيصا للتزوير أو التقليد، وهذا العمل يقوم به عادة المتخصصين في هذا المجال، كصناعة آلة طابعة خاصة، أو أجهزة آلية أو كيميائية التي تسمح بمحو شريط التوقيع، أو صناعة جهاز إلكتروني صغير يمكنه التقاط المعلومات والبيانات السرية للبطاقة الائتمانية الإلكترونية خلال بضعة ثواني ومن ثم اصطناع بطاقات مزورة بالرقم السري المسروق نفسه.

2-الحيـــازة أو الحصـــول: ويشير هذا المصطلح إلى سيطرة الحائز الإرادية على التجهيزات أو المعلومات على نحو يستيطع معها الحائز ان يتصرف فيها بالإستعمال أو الإنتفاع وغيره، كما أشار المشرع إلى فعل الحصول، ومن قبيل ذلك تقليد بطاقة إئتمانية من خلال الحصول على الرقم السري لها.

3-توفير أو الوضع تحت التصرف: ويشير هذا المصطلح إلى عرض المعلومات وإتاحتها على الخط en ligne، ليتم إستخدامها بواسطة الغير، كان يتم توفير على شبكة الأنترنت برنامج لخلق رقم بطاقة الإئتمان على موقع carding [1].

أما عن محل هذه الجريمة، فلو تأملنا قليلا في البناء المادي للمادة س163-4 لوجدنا أن المشرع قد وسع من نطاق تطبيقها لتشمل بالتجريم كل الوسائل التي يمكن إستخدامها في التزوير أو التقليد مهما كانت طبيعتها، سواء كانت ذات طبيعة مادية " **التجهيزات أو الأدوات** أو دات طبيعة معنوية كما هو حال **البيانات و البرامج المعلوماتية**، إلا أنه حد من هذا التوسع عندما تطلب أن تكون هذه الوسائل **مصممة خصيصا** لإرتكاب جريمة التزوير والتقليد.

ب-الركـــن المعـــنوي:

جريمة التعامل في وسائل معدة خصيصا لإرتكاب جريمةتزوير أو تقليد بطاقة الإئتمان جريمة مقصودة، يتخد الركن المعنوي فيها صورة القصد الجنائي العام بعنصريه العلم والإرادة، دون القصد الخاص، فصفة الوسائل المعدة خصيصا لإرتكاب الجريمة تجعل من القصد العام كافيا لقيامها.

[1]- https://www.senat.fr/rap/l00-329/l00-32921.html

فلابد أن يحيط الجاني علما بكافة العناصر الداخلة في تشكيل الجرية، وأن هذا السلوك يشكل تهديدا للمصلحة المحمية، وأن يعلم بعدم مشروعية هذه الوسائل كونها ترتكب بها الجريمة، وأن تكون إرادته متجهة إلى تحقيق أحد المظاهر السلوكية التي نص عليها المشرع، ومن قبيل ذلك التوفير أو التصنيع رغم علمه بصفتها غير المشروعة.

ت-العقوبـــــة:

يعاقب المشرع على الجريمة بعقوبة الحبس 7 سنوات و بغرامة 750000 يورو، وهي نفس العقوبة التي عاقب بها على الجرائم السابقة، كما عمد المشرع إلى تقرير العقاب على الشروع في جريمة التقليد والتزوير وجريمة التعامل في وسائل مصممة لإرتكاب الجريمة الأخيرة بالعقوبة المقررة للجريمة نفسها بموجب المادة س163-4-1.

وتغلظ العقوبة لتصبح من عشرة سنوات حبس ومليون يورو في حالة إرتكاب الجرائم السابقة من قبل جماعة منظمة(مادة س163-4-2[1]).

كما أضاف المشرع إلى العقوبة الأصلية عقوبة تكميلية وجوبية بموجب المادة س163-5[2] هي مصادرة المواد والآلات والمعدات والأدوات والبرامج المعلوماتية وكل البيانات التي إستخدمت أو أعدت للإستخدام في صناعة تلك الأدوات، إلا إدا كان ذلك بدون علم المالك.

من خلال ما سبق شرحه عن الجرائم المتعلقة ببطاقة الإئتمان، يتضح أن التشريعات الجزائية و إن لم تكفل حماية خاصة لبطاقات الإئتمان من الإستخدام غير المشروع لها، فإنه أمكن إخضاع أغلب هذه الإستخدامات للقواعد العامة في قانون العقوبات كما سبق وأن رأينا بالعقاب عليها على حسب الوصف الجرمي التي تتصف به تلك الأفعال، في حين أن البعض الآخر لا يخضع لأي نموذج تجـــريمي تقليدي وإن كان يمكن مواجتهتها من خلال نصوص المساس بنظم المعالجة الآلية بالنسبة للتشريعات التي جرمت هذا النموذج المستحدث كما هو حال التشريع الجزائري.

أما الوضع في التشريع الفرنسي، فقد إنفرد في إتـــجاهه التشريعي على النحو السابق بيانه، إلا أن حمايته إقتصرت على تجريم تزوير البطاقة وإستعمالها أو قبولها مع العلم بتزويرها، فضلا عن التعامل في الوسائل المصممـــة لإرتكاب جريمة تزوير البطاقة.

إلا أنه في المقابل، فإن المشرع الفرنسي زاد في حرصه لدرجة أوقعته فيما يعرف بالتعدد المعنوي، ذلك أنه وبالرغم من أن نص المادة 441-1 يشمل بالتجريم التزوير في البطاقة أيا كانت طرقه، إلا أنه أضـــاف الفقـــرة الأولـــى مـــن نـــص المـــادة س163-3 مـــن التقنـــين النقـــدي والمـــالي.

[1]-Article L163-4-2 du CMF Créé par LOI n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (1) - art. 3

[2]-Article L163-5 du Code monétaire et financier Modifié par Ordonnance n°2009-866 du 15 juillet 2009 - art. 2

البـــاب الثـــاني

الجوانب الإجرائية للحماية الجزائـــية للتعاملات الإلكترونية

إن الإجراءات الجزائية لجرائم التعاملات الإلكترونية هي الوجه العملي لإتحاد شقي التجريم والعقاب في القاعدة الجزائية، فهي المحرك الفعال لقانون العقوبات، إذ تنقل نص التجريم من حالة الركود إلى حالة الحركة، فعلى فرض أن المشرع إستطاع أن يحيط بالقاعدة الموضوعية لجرائم التعاملات الإلكترونية، فإن نجاحه يظل مرتهنا بمدى فاعلية التنظيم الإجرائي الذي يضمن تحقيق الهدف من العقـــاب. ومعنى ذلك أنه إذا لم يوجد قاعدة إجرائية فإن القاعدة الموضوعية تبقى قاعدة نظرية لا تجدا سبيلا إلى التطبيق.

وقد ترتب على ثورة تكنولوجيا الإعلام والإتصال ظهور بعض الصعوبات الخاصة بتطبيق قانون الإجراءات الجزائية على الكثير من الجرائم الماسة بالتعاملات الإلكترونية، ويرجع السبب في ذلك إلى أن هذه القواعد الإجرائية قد وضعت لتطبق وفقا لمعايير مادية معينة، ولم تكن مخصصة لهذه الظواهر الإجرامية المستحدثة.

وإن كانت بعض التشريعات لم تصدر قانونا لمكافحة الجرائم الواقعة على التعاملات الإلكترونية من الناحية الإجرائية، كما هو حال التشريع المصري، فإن البعض الآخر منها عملت إلى إستحداث قواعد إجرائية جديدة وتعديل القائم منها لتواكب التغيرات والتطورات المطردة في مجال الجرائم الواقعة على التعاملات الإلكترونية، كما هو حال التشريع الجزائري والفرنسي، مع الإشارة إلى أن هذه القواعد ليست حكرا على الجرائم محل الدراسة دون غيرها من الجرائم الواقعة في العالم الرقمي، فما ينطبق على المساس بالتعاملات الإلكترونية في مجال الجوانب الإجرائية ينطبق على مختلف الجرائم المتصلة بتكنولوجيات الإعلام والإتصـــال.

وتتمثل الإصلاحات الإجرائية الحديثة إلى دمج كافة الإبتكارات والتطبيقات الناتجة عن تقنية المعلومات في مجال الإجراءات الجزائية، حتى تستجيب لإحتياجات الأجهزة المكلفة بالتحقيق والمحاكمة في هذا المجال.

غير أن الأمر لا يتوقف عند هذا الحد، إذ أنه من الضروري تتبع الدعوى الجزائية في تلك الجرائم وصولا لإنزال العقاب على الجاني، وهو ما يتطلب تحديد المحكمة الجزائية المختصة بنظر فعل الإعتداء، وسلطتها في قبـــول الدليل الإلكتروني في هذه الجـــرائم.

وعلـــى ضوء ما تقدم سوف نقسم دراســـة هذا الـــباب إلى فصلين على النحو التـــالي:

الفصل الأول: قواعد التحقيق في الجرائم الواقعة على التعاملات الإلكترونية

الفصل الثاني: قواعد الإثبات الجزائي والإختصاص القضائي في الجرائم الواقعة على التعاملات الإلكترونية

الفصـــل الأول

قواعد التحقيق في الجرائم الواقعة على التعاملات الإلكترونية

نظرا للطابع الخاص لطبيعة ووسائل جرائم التعاملات الإلكترونية، فإن تطبيق القواعد الإجرائية التقليدية على مثل هذه الجرائم يثير مشاكل عديدة تعرقل عمل أجهزة العدالةفي مواجهتها ومكافحتها لها، وتعرقل سير الدعوى العمومية في جميع مراحلها.

وتعد مرحلة جمع الإستدلالات في الجرائم محل الدراسة، بل وفي جميع الجرائم الواقعة في العالم الرقمي حجر الزاوية الذي سيتم على أساسه بناء الدعوى برمتها، فما يتم جمعه من معلومات وأدلة معنوية في هذه المرحلة التي تعقب إرتكاب الجريمة مباشرة، قد لا يبقى متاحا بعد مرور وقت قصير على إرتكابها، والسبب في ذلك يعود إلى الطبيعة التقنية لهذه الجرائم.

ويعد ضباط الشرطة القضائية هم أصحاب الإختصاص العام في مكافحة الجرائم كأصل عام، فهم **خط الدفاع الأول** ضد الجريمة، ولهم في ذلك جملة من الإختصاصات منها ما تباشر في الظروف العادية ومنها ما تباشر في الظروف الإستثنائية، والجرائم محل الدراسة لا تخرج عن هذا الأصل، وإن كان في المقابل لا يتوجب إعادة النظر في كيفية قيام هذه الجهة بوظائفها في إطار الجرائم الواقعة على التعاملات الإلكترونية في الظروف العادية أو الإستثنائية فحسب، بل وجب السماح باتخاذ في شأنها إجراءات متميزة تتماشى وخصوصية هذه الجرائم.

لكن المشكل أن الوصول إلى الدليل خاصة إذا كان مخزن في الخادم أو الملقم[1] يجب أن يسبقه أحيانا تدابير تقنية وإجراءات أولية تستهدف في غالب الأحيان الحفاظ عليه من التلف أو المحو أو التلاعب أو التبخر، كالتحفظ على المعطيات المخزنة بما في ذلك المعطيات المتعلقة بحركة السير ومحتوياتها – كالمستندات الإلكترونية–، أوإنتاج معطيات معلوماتية، وهو ما إستلزم في المقابل إتباع **نظام الزام مقدمي الخدمات** بالتعاون مع رجال الضبط القضائي، بتسليم أو كشف ما تحت أيديهم من معلومات والتي يطلب منهم حفظها لمدة معينة، أو التحفظ عليها من أجل الإجابة عن طلب أو أمر، وقد يتعداها لتسجيل وجمع في الوقت الفعلي للمعطيات المتعلقة بمحتوى إتصالات معينة.

وبناء على ذلك سوف نتناول بالدراسة الإختصاصات المعتادة والمتميزة لضباط الشرطة القضائية ومدى تعاون مقدمي الخدمات مع هؤلاء، وحرصا لعدم التكرار لن نتطرق لمرحلة التحقيق الإبتدائي كون أن أهم الأعمال التحقيقية سنتناولها بالدراسة ضمن الإختصاصات المعتادة لهم المندرجة ضمنها سلطاتهم الإستثنائية، فضلا على أن معظم الجرائم الواقعة على التعاملات الإلكترونية جنحية الوصف، ومن تم فإن التحقيق الإبتدائي ليس إلزاميا فيها، على أن يكون ذلك من خلال المبـــاحث الثلاثة التالـــية:

المبحث الأول: الاختصاصات المعتادة لضباط الشرطة القضائية في مكافحة الجرائم الواقعة على التعاملات الإلكترونية

[1]- الخادم أو الملقم هو حاسوب ضخم مهمته تحقيق حركة الإتصال بالمواقع والصفحات والإنتقال المباشر للمواقع التي تمت إستضافتها على هيئة رقمية فيه، وللخادم وظائف عديدة أخرى بالإضافة إلى الوظائف السابقة، وهي تخزين البريد الإلكتروني للمستخدمين وتأمينه للمستخدم عند الإستدعاء من قبله، وتأمين ربط المستخدمين بغرف المحادثة وغيرها من الوظائف، أنظر: **د. عمر بن يونس**، الدليل الرقمي، الطبعة الأولى، دون دار النشر، 2007، ص17.

المبحث الثاني: الإختصاصات المتميزة لضباط الشرطة القضائية في مكافحة الجرائم الواقعة على التعاملات الإلكترونية

المبحث الثالث:تعاون مقدمي الخدمات مع رجال الضبط القضائي

المبحث الأول

الاختصاصات المعتادة لضباط الشرطة القضائية في مكافحة الجرائم الواقعة على التعاملات الإلكترونية

بمجرد وصول نبأ وقوع جريمة ما لضباط الشرطة القضائية، سواء تم العلم بها شخصيا أو عن طريق شكوى مقدمة من المتضرر منها، أو عن طريق الإبلاغ عنها أو بأية طريقة أخرى[1]، ينعقد لهذه الأخيرة جملة من الإختصاصات بحسب السلطة المخولة لهم قانونا، وبحسب ما إذا كان إختصاصهم إختصاص **عادي** يمارس في ظل الأحوال التي يمارس فيها عضو الضبط القضائي إختصاصه نتيجة تلقيه نبأ وقوع الجريمة بأي طريق ما عدا التلبس، **أو إستثنائي** يباشره في غير هذه الظروف.

فأما تلك التي تباشر في الظروف العادية هي : تلقي الشكاوى والبلاغات، الإنتقال لمكان الجريمة ومعاينته وإثبات الحالة وتحرير المحاضر وسماع أقوال المشتبه فيه...وكل ما من شأنه الكشف عن الجريمة ومرتكبيها وتعقبهم لتقديمهم للسلطة القضائية المختصة.

وأما في الظروف الإستثنائية، فهي تباشر إختصاصات هي أصلا من صلاحيات سلطة التحقيق، وقد حدد المشرع الحالات التي يجوز فيها للضابط القيام بهذه الصلاحيات على وجه الحصر:

- حالة التلبس[2].
- البحث التمهيدي[3].
- الإنابة القضائية[4].

ومن الصلاحيات الإستثنائية التي أجازها القانون هي: القبض، التفتيش، ضبط الأشياء الناتجة عن التفتيش، التوقيف للنظر.

ويقصد بالتلبس "حالة واقعية يعبر عنها مجموعة من المظاهر الخارجية التي تدل بذاتها على أن جريمة تقع أو بالكاد قد وقعت، وقوامها إنعدام الزمن أو تقاربه بين وقوع الجريمة وإكتشافها"[5] ، وهو3 أنواع: تلبس

---

[1]- كتقدم الجاني بنفسه بالإبلاغ عن جريمته. لمزيد من التفاصيل أنظر: **د.معجب بن معدي الحويقل**، المرشد للتحقيق والبحث الجنائي، الطبعة الأولى، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2003، ص44.

[2]– المادة 41–62 من قانون الإجراءات الجزائية.

[3]–المواد 63 إلى 65 من قانون الإجراءات الجزائية.

[4]–المواد من 138 إلى 142 من قانون الإجراءات الجزائية.

[5]–**د. إبراهيم حامد طنطاوي**، التلبس بالجريمة وأثره على الحرية الشخصية، الطبعة الأولى، المكتبة القانونية، 1995، ص11.

حقيقي أو فعلي وهو الذي يتحقق بإدراك الجريمة أثناء إرتكابها أو عقب إرتكابها ببرهة يسيرة[1]. وتلبس إعتباري أو حكمي وهو الذي يكون حال مشاهدة آثار الجريمة نفسها.[2] وحالة الجريمة المتسمة بصفة التلبس وهي الجريمة المكتشفة في مسكن والتبليغ عنها في الحـــال وضبطها على الـــفور.

وعلة التوسع في الإختصاصات في هذه الحالات هي أن أدلة الجريمة تكون واضحة وناطقة بحد ذاتها، فيتعين فحصها وضبطها على الفور، لأنه يخشى إذا تراخت الإجراءات أن تضعف هذه الأدلة، أو أن تمتد إليها يد التشويه، إضافة إلى أن وضوح الأدلة هنا لا يحتمل التعسف أو الخطأ[3].

وإذا كان ضبط الجاني ملتبسا بجريمة من جرائم الإعتداء على التعاملات الإلكترونية أمرا صعبا من الناحية النظرية، إلا أنه من الناحية العملية يمكن تصور ذلك، ومن ذلك ضبط الجاني متلبسا حال إستخدامه جهاز الحاسوب الخاص به في إقتحام موقع إلكتروني خاص بأحد البنوك[4]، أو إرتكابه للجريمة في مكان عام كاندية الأنترنت التي يجوز للضابط إرتيادها مثله مثل أي شخص عادي، فإذا إطلع على وقوع جريمة فإن ما يقوم به من إجراءات تكون متفقة مع صحيح القانون.

ويمكن أيضا الدخول إلى الموقع الذي يستخدمه مرتكب الجريمة عن طريق تعقب القائم بالإرسال لمعرفة الرقم الذي يتم الإرسال منه، ثم مباغتة الشخص في مكانه وهو يقوم بالفعل محل الجريمة.

كما أنه كثيرا من التشريعات أصبحت تعاقب على مجرد حيازة صور فاضحة، وبالتالي فإن ضابط الشرطة القضائية إذا إكتشف وجود مثل تلك الصور في كمبيوتر المتهم، فيعد ذلك تطبيقا لقيام حالة التلبس إذا ما كان رجل الضبط قد رأى هذه الصور بنفسه، وقد أصبح قانون العقوبات الجزائري يعاقب على هذا النوع من الحيازة في المادة 333 مكرر عقوبات[5]، كما نص عليها المشرع المصري في المادة 178 عقوبات[6].

---

[1]– تنص المادة 41 من قانون الإجراءات الجزائية الجزائري "توصف الجناية أو الجنحة بأنها في حالة تلبس إذا كانت مرتكبة في الحال أو عقب إرتكابها"، وتقابلها المادة 53 في فقرتها الأولى من قانون الإجراءات الجزائية لفرنسي، والمادة 30 الفقرة 1 من قانون الإجراءات المصري.

[2]– تنص الفقرة 2 من المادة 41 من قانون الإجراءات الجزائية الجزائري "كما تعتبر الجناية أو الجنحة متلبسا بها إذا كان الشخص المشتبه في إرتكابه إياها في وقت قريب جدا من وقت وقوع الجريمة قد تبعه العامة بالصياح أو وجدت في حيازته أشياء أو وجدت آثار أو دلائل تدعو إلى إفتراض مساهمته في الجناية أو الجنحة"، وتقابلها الفقرة الثانية من المادة 53 من قانون الإجراءات الجزائية الفرنسي، والفقرة 2 من المادة 30 من قانون الإجراءات الجزائية المصري.

[3]– **د. محمود نجيب حسني**، شرح قانون الإجراءات الجزائية، دار النهضة العربية، القاهرة، 1988، ص533.

[4]– **أيمن رمضان محمد أحمد**، المرجع السابق، ص330.

[5]–تنص المادة 333 مكرر" يعاقب بالحبس من شهرين إلى سنتين وبغرامة من 500 إلى 2.000 دج كل من صنع أو حاز أو إستورد أو سعى في إستيراد من أجل التجارة أو وزع أو أجر أو لصق أو أقام معرضا أو عرض أو شرع في العرض للجمهور أو باع أو شرع في البيع أو وزع أو شرع في توزيع كل مطبوع أو محررا أو رسم أو إعلان أو صور أو لوحات زيتـــية أو صور فوتوغرافية أو أصل الصورة أو قالبها أو أنتج أي شيء مخل بالحياء"، وتقابل المادة 283 من قانون العقوبات الفرنسي القديم، التي تم إلغائها بموجب المادة 372 من القانون رقم 92–1336 المؤرخ في 16 ديسمبر 1992.

Article 283 du CPF Créé par Loi 57-309 1957-03-15 art. 1 JORF 16 mars 1957. Modifié par Ordonnance n° 58-1298 du 23 décembre 1958 modifiant notamment certains articles du code pénal. Modifié par Loi n°77-1468 du 30 décembre 1977 - art. 16 (V) JORF 31 décembre 1977 en vigueur le 1er janvier 1978. Abrogé par Loi n°92-1336 du 16 décembre 1992 - art. 372 (V) JORF 23 décembre 1992 en vigueur le 1er mars 1994

[6]– تنص المادة 178 من قانون العقوبات "يعاقب بالحبس مدة لا تزيد على سنتين وبغرامة لا تقل عن خمسة آلاف جنيه ولا تزيد على عشرة آلاف جنيه أو بإحـــدى هاتين العقوبتين كـــل من صنع أو حاز بقصد الاتجار أو التوزيع أو الإيجار أو اللصق أو العرض مطبوعات أو مخطوطات أو رسومات أو

وإذا كانت القواعد العامة تقضي بأن رجل الضبط القضائي حتى تنفتح له أبواب السلطات الإستثنائية، لزوم كشف حالة التلبس **بالمشروعية**، إلا أن هذا الأمر محل صعوبة في بيئة التعاملات الإلكترونية من ناحية، وتداخل موضوع الحرية الشخصية من ناحية أخرى. حيث تثار في هذا الصدد مشروعية التخفي عبر الأنترنت من قبل ضباط الشرطة القضائية باتخاذ أسماء غير حقيقة وتقمص شخصيات وهمية ثم الولوج إلى الأنترنت والدخول إلى حلقات النقاش وتجاذب أطراف الحديث مع الغير قصد التوصل إلى نتائج محددة قصد التوصل إلى مرتكب الجريمة، أو نتائج غير محددة للبحث عن الجرائم ومرتكبيها[1].

وفي هذا الإطار نظم المشرع الفرنسي **التسرب الرقمي** أو كما أطلق عليه "**التحقيق تحت إسم مستعار**" وذلك بهدف جمع الأدلة في الجرائم والبحث عن الفاعلين فيها، وكذلك فعل المشرع الجزائري وإن إقتصر هذا الأخير على التسرب الكلاسيكي فإنه يمكن القيام به عبر الأنترنت، فإن صادف ضابط الشرطة القضائية أثناء التسرب جريمة متلبس بها إنفتحت له أبواب السلطات الإستثنائية.

أما البحث التمهيدي فقد نظمه المشرع الجزائري في المواد 63,64,65 تحت عنوان التحقيق الإبتدائي، ويخول ضباط الشرطة القضائية طبقا لقواعد البحث التمهيدي سلطات محددة تمكنه من إجراء تفتيش المساكن والتوقيف للنظر المنظمين في المادة 64 و65 إجراءات[2].

أما الإنابـــة، فيقصد بها ذلك الإجراء الذي بواسطته يكلف أحد القضاة قاضيا آخر أو أحد ضباط الشرطة القضائية بالقيام بإجراء تحقيق معين في مضمون الإنابة نظرا لضرورة الظاهرة، لأن مصلحة التحقيق تقتضي الإسراع بإنجازه[3]. ولصحتها يجب أن تكون صادرة من مختص بمباشرة إجراء التحقيق، وأن تكون متعلقة بدعوى تدخل في نطاق الإختصاص المكاني للقاضي المناوب، وفي إجراء يدخل في نطاق إختصاصه النوعي، وأن تصدر للشخص الذي له صفة الضابط، وأن يكون موضوع الإنابة دقيقا فلا يجوز أن تمتد الإنابـــة إلى التحقيق كلـــه.

والجرائم الواقعة على التعاملات الإلكترونية لا تخرج عن هذا الإختصاص المعتاد لضباط الشرطة القضائية، حيث تتبع بشأنها الإجراءات السابقة مع نوع من الخصوصية تتماشى وطبيعتها.

وتجدر الإشارة إلى أن ما يهمنا من تلك الإجراءات في موضوعنا هذا هي: **القبض والمعاينة والتفتيش** نظرا لما تطرحه من إشكالات في ظل الجرائم محل الدراســة.

وعلى ذلك، إرتأينـــا تقسيم هذا المبحث إلى المطالب الثلاثة التالـــية:

المطلب الأول: القبض في جرائم الإعتداء على التعاملات الإلكترونية

المطلب الثاني: المعاينة التقنية لمسرح جرائم الإعتداء على التعاملات الإلكترونية

المطلب الثالث: تفتيش النظم المعلوماتية المستخدمة في إرتكاب جرائم الإعتداء على التعاملات الإلكترونية

إعلانات أو صوراً محفورة أو منقوشة أو رسومات يدوية أو فوتوغرافية أو إشارات رمزية أو غير ذلك من الأشياء أو الصور العامة إذا كانت منافية للآداب العامة".

[1]-. **د.عمر محمد أبو بكر بن يونـــس** ، الجرائم الناشئة عن إستخدام الأنترنت، المرجع السابق، ص851.

[2]- **د. عبد الله أوهايبيه**، شرح قانون الإجراءات الجزائية الجزائري–التحري والتحقيق–، دار هومه للنشر والتوزيع, الجزائر، 2008، ص283.

[3]- المادة 138 من قانون الإجراءات الجزائية الجزائري.

المطلب الأول

القبض في جرائم الإعتداء على التعاملات الإلكترونية

يرتبط مصطلح القبض بمصطلح المطاردة أو التعقب في العالم الإفتراضي، والمطاردة عبر الأنترنت من الموضوعات التي تثار في إطار المطاردة ككل مع تطور حالات الهروب عبره في العالم الإفتراضي، و يعتقد البعض أن الأنترنت وشبكات المعلومات كمجالات فضائية يصعب فيها تطبيق القانون وذلك لغياب نقاط المراقبة على الشبكات، وتقنيات إرسال الرسائل، وعدم ذكر الأسماء أو التحقق من هويتهم، وتشفير التوقيعات،وجعل الكتابة سرية،وهي خصائص يتميز بها الأنترنت تجعل من الصعب تحديد شخصية وملاحقة مرتكب الأفعال المجرَّمة، مما يعقد عمل الشرطة في **القبض** على الفاعل، إلا أن هذا التحليل نسبي بالنسبة للبعض الآخر[1] –ونحن نتفق معه–، الذي يرى بأنه لا يوجد "تجهيل" بالمعنى الصحيح بالنسبة لشبكة المعلومات حيث يترك الفاعل "آثاراً" أثناء تنقله في طرقات شبكة المعلومات تسمح للمحققين من الوصول إليه.

فلتعقب المشتبه به في جرائم التعاملات الإلكترونية، تستخدم بروتوكولات الإتصالات والتطبيقات المعلوماتية، حيث أن الأنشطة التي يجريها مستخدموا شبكة الأنترنت تشكل جانبا بالغ الأهمية في التمكن من القبض على المشتبه فيه، نظرا لإحتواء هذه البروتوكولات على كافة المعلومات المتعلقة بنشاط المستخدم على الأنترنت، ويعتبر نظام IPمن أكثر البروتوكولات المستخدمة في شبكة الأنترنت.

سنحاول من خلال الفروع المتقدمة من هذا المطلب إلقاء الضوء على هذه الآلية في التعقب، تحديد أنواعه، وأشهر الشركات المختصة بعملية التتبع عبر العالم الإفتراضي، على أن نعطي بداية فكرة عامة عن القبض في العالم المادي.

الفرع الأول

التعريف بالقبض بصفة عامـــة

القبض هو عبارة عن حجز الشخص لفترة من الوقت لمنعه من الفرار، تمهيدا لإتخاذ بشأنه من إجراءات بمعرفة الجهة المختصة، وقد تم تعريفه على أنه إمساك المقبوض عليه من جسمه وتقييد حركته وحرمانه من حرية التجول دون أن يتعلق الأمر على قضاء فترة زمنية معينة أي مهما قلت مدته"[2].

---

[1]–أ. د. **صالح أحمد البربري**، دور الشرطة في مكافحة جرائم الأنترنت في إطار الاتفاقية الأوروبية الموقعة في بودابست في 2001/11/23، بحث منشور بموقع الدليل الإلكتروني للقانون العربي على شبكة الأنترنت:
www.arablaw.info.com

[2]– د. **رؤوف عبيد**، مباديء الإجراءات الجزائية في القانون المصري، دار الفكر العربي، القاهرة، 2006، ص329.

والقبض إجراء من إجراءات التحقيق بإعتباره يتضمن مساسا بحرية الأشخاص، ولذلك حرص الدستور على تقرير مبدأ حمايتها وفصل القانون بعد ذلك ضوابط هذه الحماية[1]، فالمادة 32-1 من الدستور الجزائري تنص "الحريات وحقوق الإنسان والمواطن مضمونة" وتنص المادة 34-1 منه" تضمن الدولة عدم انتهاك حرمة الإنسان..." والمادة 47" لا يتابع أحد ولا يوقف أو يحتجز، إلا في الحالات المحددة بالقانون، وطبقا للأشكال التي نص عليها"، كما يؤكد على ذات المعنى الدستور المصري في المادة 40 و41.

أما قانون الإجراءات الجزائية فلم يجز القبض على أحد من قبل عناصر الضبطية القضائية إلا في الحالات التاليـــة:

أولا-تنفيـــذا لأمر قضائي: إعمالا للمادة 109 إجراءات جزائية جزائري وما يليها،حيث تنص هذه المادة "يجوز لقاضي التحقيق حسبما تقتضي الحالة أن يصدر أمرا بإحضار المتهم أو بايداعه السجن أو بالقاء القبض عليه"، كما تنص المادة 119"الأمربالقبض هو ذلك الأمر الذي يصدر إلى القوة العمومية بالبحث عن المتهم وسوقه إلى المؤسسة العقابية المنوه عنها في الأمر حيث يجري تسليمه وحبسه".

وإذا كان المتهم هاربا أو مقيما خارج إقليم الجمهورية فيجوز لقاضي التحقيق بعد إستطلاع رأي وكيل الجمهورية أن يصدر ضده أمرا بالقبض إذا كان الفعل الإجرامي معاقبا عليه بعقوبة جنحة بالحبس أو بعقوبة أشد جسامة ويبلغ أمر القبض وينفذ بالأوضاع المنصوص عليها .."

ثانيا- في حالة التلبس بجناية أوجنحة معاقب عليها بالحبس:ونص على ذلك صراحة المشرع المصري بموجب المادة 34 من قانون الإجراءات الجزائية، والشروط التي تطلبها المشرع لتخويل ضابط الشرطة القضائيةهذا الأمر وهو أن تتوافر إحدى حالات التلبس التي نص عليها القانون، وأن تكون الجريمة موضوع التلبس جناية أو جنحة معاقبا عليها بالحبس لمدة تزيد على ثلاثة أشهر، وأن توجد دلائل كافية على إتهام المقبوض عليه بهذه الجريمة، أما المشرع الجزائري فلم يشر صراحة إلى إختصاص الضابط في القبض على المشتبه فيه، غير أنه وبالرجوع إلى المادة 51 من قانون الإجراءات الجزائية نجدها قد خولت ضابط الشرطة القضائية توقيف المشتبه فيه للنظر مدة لا تزيد عن 48 ساعة إذا رأى أن مقتضيات التحقيق تتطلب ذلك، وعمليا لا يمكن تنفيذ هذا الإجراء إلا بالقبض على الشخص وحجزه.

ثالثا- في إطار التحقيق الأولـــي: بموجب المادة 65 من قانون الإجراءات الجزائية إذا رأى الضابط أنه من المفيد للتحقيق إحتجاز الشخص لمدة لا تزيد عن 48 ساعة، فعمليا لا يتم ذلك إلا بعد القبض على الشخص و إيداعه غرفة الأمن.

رابعا- بموجب إكراه بدنـــي: وذلك إتجاه الشخص الذي صدر ضده حكم كوسيلة للضغط عليه لإجباره على سداد ماعليه من مستحقات للدولة صدر بها حكم بات[2].

---

[1]- **د. محمود نجيب حسني**، شرح قانون الإجراءات الجزائية، المرجع السابق، ص556.

[2]- **أحمد غاي**، ضمانات المشتبه فيه أثناء التحريات الأولية، الطبعة الثانية، دار هومة، الجزائر،2011، ص256.

تلك هي الحالات التي تخول للضابط حق القبض على الأشخاص، والتي تشكل في ذاتها ضمانة للمشتبه فيه فضلا عن الضمانات القانونية الأخرى للحرية الشخصية، والتي تحمي الأفراد من القبض التعسفي، ومن إتخاذ الإجراءات القانونية ضده دون مبرر أو الإستمرار بها، ولعل أهم هذه الضمانات هو إخضاع إجراء القبض **للرقابة القضائـــية**.

هذا فيما يخص الأحكام العامة للقبض، وسنتناول فيما يلي القبض في إطار جرائم التعاملات الإلكترونية، وكيف يتم تعقب المشتبه فيه في بيئة هذه التعاملات ألا وهي الأنترنت؟

الفرع الثاني

تتبع المشتبه فيه وفق عنوان بروتوكول الأنترنتIP

تتيح البنية التحتية للأنترنت إمكانية التعرف على عنوان الحاسوب، وهو ما يعرف في تقنية الأنترنت بمصطلح ip internet protocol الذي يشير إلى رقم يعين الجهاز الذي تم الإتصال منه من خلال الشبكة، ومن ثم هوية الجهاز الذي إستخدم في إرتكاب جريمة من جرائم التعاملات الإلكترونية، لتبدأ عملية إتخاذ الإجراءات الضرورية بغرض القبض على المشتبه به[1].

وهو برتوكول يتكون من عدد 32 بت في شكل رقمي، يأخذ شكل التنقيط العشري Dotted Decimal Form مثل رقم 62.127.30.236، حيث يشير الجزء الأول من اليسار إلى المنطقة الجغرافية، والجزء الثاني لمزود الخدمة، والثالث لمجموعة الحاسبات الآلية المرتبطة، والرابع يحدد جهاز الحاسبات الإلكترونية الذي تم الإتصال منه.

والأساس الكلي الذي تستند عليه فكرة بروتوكول الأنترنت، أن فكرة علاقة بروتوكول الأنترنت بالحاسوب هي كل حاسوب يحمل عنوان بروتوكول منفرد، فهذا البروتوكول كبصمة الأصبع بالنسبة للانسان فليس هناك إمكانية لوجود إزدواج في بصمات أصابع البشر أو حتى تشابه من أي نوع، وذات الأمر ينطبق على الحواسيب أيضا. ومن ثم بدأت تباشير إمكانية تحديد مكان الحاسوب ما دام يمكن معرفة عنوان البروتوكول الخاص به. فالأمر بدا هنا كما لو كان نظام البصمة البشرية معتمد في هذا الإطار. بل ويمكن التقرير بأن نظام عنوان بروتوكول الأنترنتIP address هذا هو البصمة الرقمية والمرادف للبصمة البشرية[2].

ومن ذلك ما حدث في قضية القرصنة التي تعرض لها البنك الكندي caisse populaire des jardins من قبل الهاكرز الجزائري، فمن خلال عنوان الربط IP ADRESS رقم 41209136163 مكنت

---

[1]-**د.عمر محمد أبو بكر بن يونـــس** ، الجرائم الناشئة عن إستخدام الأنترنت، المرجع السابق، ص811.

[2]– **د. عمربن يونس**، الأيكان icann، محاضرة في ندوة تأثير محركات البحث على إدارة الأنترنت (الاسكندرية 31 يوليو – 4 أغسطس 2005)المنظمة العربية للتنمية الإدارية، جامعة الدول العربية، ص6.

الأبحاث على مستوى المتعامل EEPAD أن مستخدم هذا العنوان هو صاحب الخط الهاتفي المسجل باسم أب المتهم (ف.محمد) المتحصل على شهادة ليسانس في الإعلام الآلي.

ونظام عنوان برورتوكول الأنترنت يمكن الحصول عليه عن طريق مزود خدمة الأنترنت، إذ أنه يقوم بالحصول على مجموعة كبيرة من العناوين عن طريق الجهات المسؤولة جغرافيا عن إدارة وتخصيص هذه العناوين، فالجزائر مثلا تملك النطاق العلوي dz حسب ترتيبات المنظمة العالمية المانحة لأسماء النطاقات،ايكان ، فضلا عن إسم النطاق "الجزائر " بالحروف العربية الذي صادقت على ملفه منظمة الأيكان، والمقدم من قبل مركز البحث في الإعلام العلمي والتقني cerist، وجاء ذلك في ضوء النمو المتصاعد والأهمية المتعاظمة للعربية التي حازت هذا الامتياز رفقة عدد من اللغات الحية، كالصينية، اليابانية، الروسية، الهندية.ولا شك أن هذا يحسن إمكانات الدخول إلى الأنترنت في الوطن العربي، وفي عدة مناطق من العالم، كما من شأنه المساهمة في دعم المحتوى الشبكي. هذا ويدير مركز أسماء النطاقات[1] كعضو مرخص من الهيئة العالمية أسماء النطاقات المخصصة للجزائر، حيث يمكن الحصول على إسم النطاق تحت الإمتداد. الجزائر لجميع الجهات المتواجدة بالجزائر أو لها تمثيل مقبول في الجزائر أو حاملي وثيقة تبين حقوق ملكية الإسم.

هناك نوعين رئيسيين لعناوين بروتوكولاتالأنترنت، هما[2]:

– **برتوكولات الأنترنت الديناميكية:** فهي عناوين غير محددة، تتغيير مع كل مرة يتم ربط الجهاز بالشبكة، هذا العنوان يتم تعيينه بواسطة DHCP (Dynamic Host Configuration Protocol).وهو عبارة عن حاسوب يحتوي على قائمة من العناوين الرقمية المتاحة، بحيث يمنح هذا المخدم أحدها للمشترك بشكل ديناميكي.

ويعمد مزود الخدمة لمواجهة التدفقات الإستخدام الطاريء للشبكة من قبل أشخاص لايريد مزود الخدمة تثبيت رقم محدد لعناوينهم، ويمكن الإستدلال على هذا العنوان الديناميكي من خلال وجود كلمة ppp أو كلمة dial أو يحتوي أرقام مثل , Czo.52.e.gوهذه الأرقام عادة جزء من ديناميكية العنوان ويمكن أن يستدل منها على جهة معينة أو منطقة جغرافية محددة.

وهذا العنوان وإن كان يطرح مشاكل فيما يخص تحديد شخص مستخدم العنوان الديناميكي في الوقت المحدد، إلا أن مسارات الولوج يتم الإختفاظ بها لبعض الوقت وعن طريقها يمكن الإستدلال عن شخص المستخدم.

---

[1]-- DZ.NIC est l'organe agréé par l'ICANN pour la gestion du ccTLD .dz relatif à l'Algérie. http://www.nic.dz/

[2]– **د. ممدوح عبد الحميد عبد المطلب،** إستخدام بروتوكول (tcp/ip) في بحث وتحقيق الجرائم على الكمبيوتر, ورقة عمل مقدمة إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية, المنعقد في 26–28 نيسان 2003, بدبي–الإمارات العربية المتحدة، ص17.

Bernard COUSIN, Les protocoles de base d'Internet, disponible en lingne á l'adresse suivantehttp://www.irisa.fr/prive/bcousin/Cours/I1.pdf

Sébastien FONTAINE , Entête IP, disponible en lingne á l'adresse suivante http://www.frameip.com/entete-ip/

– **برتوكولات الأنترنت الثابثة:** وكما يوحي به الإسم، فهو عنوان بروتوكل أنترنت محدد لكل مستخدم، لا يتغير أبدا بمجرد ما يتم تعيينه بالجهاز في الشبكة، وهو يستخدم بشكل رئيسي على صفحات الواب، البريد وخوادم الألعاب الذين يهتمون بإخفاء مواقعها.

ويمكن القول أنه إذا كان المستخدم يقوم بالإتصال عن طريق الخط الهاتفي "مودم" فإن عنوان بروتوكول الأنترنت يتم تحديده ديناميكيا في كل مرة إتصال، بينما إذا إستخدم تقنية adsl فإن عنوان بروتوكول الأنترنت يكون ثابتا لا يتغير وجميع هذه العناوين سواء ديناميكية أو ثابتة يتم تحديددها وفق سلسلة معينة من الأرقام من قبل مزود الخدمة.

وتجدر الإشارة إلى أن عنوان بروتوكول الأنترنت السابق الإشارة إليه، ليس موحدًا على المستوى العالميففي الولايات المتّحدة أو كندا وبعض الدّول الأخرى يمكن للشّخص فيها اقتناء IP خاص به يشير إلى كونه أحد أعضاء الأنترنت، ومن ثمّ يمكن تحديد هذا الشّخص بكل سهولة عند إعتداءه،إلاّ أنّه في دول أخرى مثل أغلب الدّول العربيّة فإنّ مصداقيّة الهويّة عبر الأنترنتIPتتقلّص كثيراً إذا علمنا أنّ كلّ خطّ هويّة على الأنترنت يصادفه عدد من الهويّات الّتي يمكن أن تكون محلّ للتّغاير بين أعضاء الأنترنت المشتركين في مزوّد انترنت واحد[1], وهنا يمكن القول أن مجرّد وجود شخص في الجزائر فإنه يملك فورًا هوية رقمية محددة حقا حال وجوده على الأنترنت, إلاّ أنّه إذا حدث وانقطع الإرسال فإن الشخص إذا عاد من جديد إلى الأنترنت فإن الهويّة السّابقة لن تكون له وإنّما لغيره، إذ من الممكن جداً–بل وهو الأمر المعتاد هنا–أن يتواجد بهويّة IP أخرى.

كما أن هناك عدة تحديات حينما يتم إستخدام عنوان بروتوكول الأنترنت IP لتحديد هوية الحاسوب إنطلاقا من نقطة بدء مسار البرتوكول بغرض إلقاء القبض على المشتبه فيه، كونه يعطي معلومات عن الجهاز وليس الشخص، خاصة إذا تم الإعتداء من قبل حاسوب من مقهى الأنترنت في ظل غياب مسك سجلات حول زمن الإستعمال والإستعلام عن هوية المستخدم، إلا أن التحدي الأصعب يطرح في حالة ما إذا كانت المعلومات المحملة في عناوين IP زائفة، وهذا ممكن حينما تحدث حزمة معلوماتية PACKET بإستخدام مصدر زائف لمصدر عنوان IP، بحيث يظهر أنّ المعلومات جاءت من نظام معالجة محدّد بينما في الحقيقة جاءت من كمبيوتر آخر, ومثال ذلك حينما يقوم برنامج خبيثبإدخال معلومات كاذبة أو غير حقيقيّة عن حقيقة عنوان IP في packetsالإرسال وقبل الولوج في الشبكة المعلوماتيّة. ويحدث ذلك حينما يقوم البرنامج الخبيث بإغراق الشّبكة بالمعلومات أو إرسال العديد من الرّسائل، أو حثّ الماكينة الرّئيسة في مزوّد الخدمة أو الشّبكة على الإسراع أو التّعجيل في العمل. إلاّ أنّه لحسن الحظّ معظم المجرمين لا يعلمون كيف يزيّفون عناوين IPولا يعرفون أيّ من عناوينIP يمكن أن تكون دالّة على شخص المجرم في الجريمة المحدّدة [2].

---

[1]- أنظر: **د.عمر أبو بكر بن يونس**, الجرائم الناشئة عن استخدام الأنترنت, المرجع السابق, ص811. **نبيلة هبة مولاي علي هروال**، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الإستدلالات، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2007، ص98.

[2] **د. ممدوح عبد الجميد عبد المطلب**، إستخدام بروتوكول (*tcp/ip*) في بحث وتحقيق الجرائم على الكمبيوتر، المرجع السابق, ص18.

فضلا عن ذلك، فإن الشبكات الداخلية تعد من الأمور الشائعة في مجال الشركات، حيث يحتاج العاملون في هذه الشركات إلى التواصل وتبادل الملفات فيما بينهم إلكترونيا، ويمكن إستخدام عنوان خارجي واحد لتشغيل عدد من الحواسيب المرتبطة فيما بينها عن طريق شبكة داخلية.

وفي حال إرتكاب جريمة من جرائم التعاملات الإلكترونية، عن طريق أحد الحواسيب الموصولة إلى شبكة داخلية، فإن على ضابط الشرطة القضائية أن يتوصل إلى رقم العنوان الخارجي، ثم يتم تحديد الحاسوب المطلوب عن طريق العنوان الداخلي، ومن ثم يتم معرفة الشخص المقصود[1].

الفرع الثالث

أشهر الشركات المختصة بعملية التتبع عبر الأنترنت

عملت العديدمن الشركات التي تعمل في مجال التكنولوجيا بتقديم نسخ متطورة من التقنيات التي تقوم بتحديد الموقع الجغرافي للمستخدم، ومن أشهر هذه الشركات Quova مقرها كاليفورنيا[2]، الخبيرة في فهم عنوان بروتوكول الأنترنت والرائدة في مجال توفير خدمة ومعطيات التواجد الجغرافي، وقد طورت هذه الشركة خدمة جيوبوينت القائمة على تقنيات معقدة للتنقيب عن المعطيات وإستيرادها من عدة مخازن لكي تحفظها، حيث بامكانها أن تكتشف عنوان مستخدمي المواقع خلال جزئين من المائة وبدرجة تصل إلى 98 بالمئة.[3]

ومن الشركات التي تعمل في نفس المضمار شركة Akamai المختصة في تقديم خدمات الاستضافة وتخزين الملفات، وهي شركة تقدم خدمة لزبنائها، بحيث تسمح هذه الخدمة بتتبع المستخدم عبر الأنترنت، وتحديدموقعه الجغرافي، عن طريق رسم خريطة للعنوان الرقمي العائد لهذا المستخدم، ثم يتم جمع هذه المعلومات في قاعدة معطيات على موقع الشركة الإلكتروني، بجيث تصبح متاحة لزبائنها. فإذا إشترك مالك أحد المواقع الإلكترونية في خدمة Edge Shape فإن أيشخص يقوم بالدخول إلى هذا الموقع في أي وقت، يتم جمع معطيات تفصيلية عنه، مثل البلد الذي تم الدخول منه، والموقع الجغرافي في هذا البلد، و إسم مزود الخدمة الذي دخل من خلاله[4]. هذا وقد سجلت akamai حوالي 666 مليون عنوان آي بي منفرد في حوالي 238 دولة بزيادة أكثر من 6% عن الربع الرابع لسنة 2011 و-14 % مقارنة بالعام السابق كما أنه

---

[1]-**د.محمد طارق الخن**، المرجع السابق، ص271.

[2]-https://www.crunchbase.com/organization/quova#/entity

[3]- Quova et 192.com Business Services s'associent pour la lutte contre la fraude du commerce électronique et le respect du jeu en ligne
http://www.prnewswire.fr/news-releases/quova-et-192com-business-services-sassocient-pour-la-lutte-contre-la-fraude-du-commerce-electronique-et-le-respect-du-jeu-en-ligne-153653955.html

[4] - **د.محمد طارق الخن**، المرجع السابق، ص271.

هناك نمو كبير في هذا المجال خاصة بعد إطلاق البروتوكول IPv6 [1]فقد نمت الصين والبرازيل وإيطاليا وروسيا بسنبه 20 % تقريبا[2].

وبعد دراستنا لآلية تعقب المشتبه فيه في العالم الإفتراضي يتبين لنا أن هناك خصوصية لشـــبكة الأنترنـــت، ولعنوان برتوكول الخاص بها، لذلك فإن تتبع الأثر الإفتراضي للجاني ومحاولة تحديد مكانه لإلقاء القـــبض عليه المحكوم عليه بالفشل هو الذي يتم بعيدا عن توفير الأجهزة التقنية والخبرات الفنية لدى ضباط الشرطة القضائية.

فضلا عن ذلك، ولما كانت جرائم التعاملات الإلكترونية يتم إرتكابها عن طريق نقل الإتصالات بواسطة نظام معلوماتي، هذه الإتصالات يمكن أن تحوي محتوى غير مشروع، كان لابد في المقابل من التركيزعلى أهمية دور مؤدي خدمة الأنترنت كهمزة وصل ضرورية بالنسبة لنقل المعلومات عن طريق **إتباع نظام إلزامهم بالتعاون مع السلطات المكلفة بالتحريات القضائية** بما يساعد على تعقب مخالفي القانون على الشبكة، وذلك كمايلـــــــي[3]:

- يجب على جميع مؤدي خدمات الاتصال للجمهور أن يحددوا على مواقعهم هوية ناشر مضمون الرسالة ومعطياته، ومن شأن هذا الإجراء أن يقدم الكثير من الشفافية بالنسبة للخدمات الموضوعة

1- مع تضخم الاهتمام بالشبكة (الإنترنت) الذي بدأ في منتصف التسعينات فإنه يبدو أنه في القرن القادم سيستخدم الإنترنت لقطاع واسع من الناس، وفي ظل هذه الظروف أصبح على ميثاق (بروتوكول(الأي بي)أن يتطور ويصبح أكثر مرونة، وحين ظهرت هذه المشكلة في عام 1995 قامت اللجنة الخاصة لنظام الأنترنت المعروفة إختصارا بـــ منظمةIETF ببدء العمل لإصدار نموذج جديد من IP, بحيث لا يكون بطيئا في البحث عن العنوان ويحل العديد من المشاكل الأخرى ويكون أكثر مرونة، وأطلقت عليه اسم IPv6 وكانت الأهداف الأساسية منه هي:

1. التعامل مع مليارات من النهايات الطرفية.(Terminals)
2. اختصار حجم جداول التسيير.([[[routing] table]]s)
3. تبسيط الميثاق (البروتوكول) للسماح للمسيرات (Routers) بمعالجة الرزم (packets)بشكل أسرع.
4. تقديم حماية أفضل للمعلومات(مصداقية+خصوصية) من [IP] الموجودة حالياً.
5. صرف اهتمام أكبر لنوع الخدمة المقدمة وخاصة لمعلومات الزمن الحقيقي.
6. السماح للنهايات الطرفية بالتنقل دون تغير عنوانها.
7. السماح للميثاق بالتطور في المستقبل.
8. إمكانية تواجد المواثيق (البروتوكولات) القديمة والجديدة معاً لسنوات قادمة. وقد حقق IPv6 هذه الأهداف المطلوبة بشكل جيد فهو يحوي الميزات الجيدة لـــ [IPv4] ومتفادياً لعيوبه السابقة ويضيف الجديد عند الحاجة, وبشكل عام فإن IPv6 ليس متوافقاً مع IPv4 في بعض الخصائص منها خواص الـــ Header لكلا منهما، ولكنه متوافق معه في بروتوكولات الإنترنت الأخرى بما فيها.DNS,BGP,OSFP,IGMP,UDP,TCP

للمزيد من التفاصيل: أنظر الموسوعة الحرة ويكيبيديا على الموقـــع التالـــي:
https://ar.wikipedia.org/wiki/%D8%A2%D9%8A_%D8%A8%D9%8A_%D9%81%D9%8A6
Marc SCHAEFER, Protocole IPv6, 20 janvier 2011 disponible en lingne á l'adresse suivante:
https://wiki.alphanet.ch/foswiki/pub/Ateliers/ProchainsDefisInternet/protocole-ipv6.pdf

2- إيمان الزبيدي، تقرير شركه akamai حول سرعة الإتصال بالأنترنت للربع الأول من سنة 2012، مقال مـــتاح على المـــوقع الإلكتروني التـــالي:
http://www.tech-wd.com/wd/2012/08/10/akamai-q1-2012-state-of-the-internet-report

3- **د. صالح أحمد البربري**، دور الشرطة في مكافحة جرائم الأنترنت في إطار الإتفاقية الأروبية الموقعة في بودابست في 23-11-2001، المرجع السابق، ص07.

تحت تصرف الجمهور، ويساعد على سهولة تحديد هوية الشخص المسؤول جنائياً. ويجب تعميم ذلك بالنسبة لكل مواقع الشبكات، سواء الشخصية أو المحترفة، طالما أنها تقوم بوضع المعلومات تحت تصرف الجمهور.

- يجب على مؤدي الخدمة أن يكون قادراً على تقديم معطيات شخصية عن زبائنه، في إطار التحقيقات التي تتم بواسطة الشرطة أو رجال النيابة عندما يطلب منه ذلك. هذا الأمر يقتضي من مؤدي الخدمة أن يطلب المعطيات الشخصية لكل عميل يطلب الاشتراك عبر شبكته، فعندما يكون رقم او العنوان التقني معروفا كرقم التلفون او عناون موقع الويب، فإن المعلومات المتعلقة بالمشتركين تتم حيازتها من أجل المساعدة في تحديد هوية الشخص المطلوب.
- يجب على مؤدي الخدمة أن يكون قادرا على حفظ المعطيات التي تتعلق بالاتصالات والتي يقوم بتجميعها أتوماتيكياً عند توصيل المستخدم بالشبكة، فهي ذات قيمة معلوماتية كبرى لرجال التحقيق. ويظهر فيها المستخدم، ووقت بداية ونهاية الاتصال، والرقم الكودي للمتصل، والمواقع التي زارها، والمعلومات التي طلبها والمعطيات التي حصل عليها هذه المعلومات وغيرها تعد بمثابة الآثار التي يتركها المستخدم.

ونظرا لكون هذه التدابير تندرج ضمن مساعدات مزودي الخدمة لضباط الشرطة القضائية،فستكون محل دراسة معمقة في المبحث الثالث من هذا الفصل فنحيل إليها حرصا على عدم التكرار.

المطلب الثاني

المعاينة التقنية لمسرح جرائم الإعتداء على التعاملات الإلكترونية

للمعاينة أهميّة كبيرة في كشف غموض الكثير من الجرائم التّقليديّة، فيما عدا البعض منها والتي لا تصلح بطبيعتها أن تكون محلا للمعاينة، كجرائم الرشوة والذم والقدح، وجريمة التّزوير المعنويّة، لكن هل تحظى بنفس الأهمية في نطاق كشف جرائم الإعتداء على التعاملات الإلكترونية؟ هذا ما سنراه من خلال الفرعين التالين، حيث سنخصص الفرع الأول للمعاينة بصفة عامة، أما الفرع الثاني فنتناول فيه كيفية المعاينة التقتية لمسرح الجرائم محل الدراسة.

الفرع الأول

التعريف بالمعاينة بصفة عامـــة

لم يحدد المشرع المقصود بالمعاينة، الأمر الذي دعا الفقه للتصدي لتعريفها، حيث عرفها البعض على أنها"**مشاهدة وإثبات الحالة في مكان الجريمة، أي مشاهدة وإثبات الآثار المادية الذي خلفها إرتكاب الجريمة**"[1],أو أنها "**الإطلاع أو الفحص أو المناظرة المباشرة لمحل المعاينة**"[2]، أو أنها "**رؤية بالعين لمكان أو شخص أو شيء لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة**"[3]، أو هي "**ملاحظة وفحص حسّي مباشر لمكان أو شخص أو شيء له علاقة بالجريمة لإثبات حالته والكشف والتّحفظ على كل ما قد يفيد من الأشياء في كشف الحقيقة**"[4].

وأيًا كان التّعريف الذي قيل بشأنها، فإنّها تقتضي المبادرة بالإنتقال في الحال إلى مسرح أو مكان وقوع الجريمة لمعاينة وضبط ماقد يوجد به من أشخاص أو أشياء من شأنها أن تؤدي إلى المساعدة في جمع الأدلة المترتبة على إرتكاب الجاني لجريمته قبل أن تمتد إليها يد العبث أو قبل زوال معالمها.

ولم تهتم معظم التشريعات الجزائية المعاصرة بتعريف مسرح الجريمة أو وضع معايير ثابتة لتحديد نطاقه المكاني، ليتولى المهمة في ذلك الفقه، وتدور معظم تعريفات رجال الفقه على أن مسرح الجريمة هو المكان الذي وقعت فيه الجريمة كلها أو بعضها بحيث يتخلف فيه آثار إرتكابها، ويرجع عدم الإهتمام بتعريفه إلى إعتبارين[5]:

-**الأول:** أن معظم القوانين الجزائية لاترتب عادة آثار قانونية بالبطلان أو الإنعدام على تجاوز الحدود المكانية لمسرح الجريمة عند إجراء المعاينة تاركة للقائم بالعملية تقدير دائرة نشاطه الإجرائي في المعاينة داخل محيط إختصاصه الوظيفي حسبما يراه وفقا لما تقتضيه مصلحة التحقيق.

-**الثاني:** أنه لا تثور عادة بشأن تحديد المجال الميداني لمسرح الجريمة منازعة أو جدل بين الخصوم في الدعوى الجنائية أو طلب البطلان تأسيسا على تجاوز هذا النطاق المكاني، فالمعاينة تستهدف التعرف على أبعاد الجريمة وأركانها وظروفها وكشف الحقيقة بشأنها، وليست إجراء موجه ضد شخص معين ماسا بحرمة مستودع سره حتى ينشأ له حق الطعن فيه.

---

[1]- **د. محمود نجيب حسني**، شرح قانون الإجراءات الجنائية، المرجع السابق، ص64.

[2]- **د. أحمد شوقي الشلقاني**، مبادئ الإجراءات الإجرائية في التشريع الجزائري، الجزءالثاني، ديوان المطبوعات الجامعية، الجزائر، 1999، ص459.

[3]-**د. عفيفي كامل، فتوح الشادلي**، المرجع السابق، ص333.

[4]- **د. جميل عبد الباقي الصغير**، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت، دار الفكر العربي، القاهرة، 2001، ص26.

[5]- **سامح أحمد بنتاجي موسى**، المرجع السابق، ص234.

ويمكن تعريف مسرح الجريمة بأنه" كل محل أو وحدة من منشأة أو رقعة من الأرض تضم بؤرة الجريمة و مركزها، بحيث تكون ميدانا لأنشطة الجاني أو الجناة من الفاعلين الأصليين عند إرتكاب الأفعال المؤثمة جنائيا، و التي تدخل في عداد الأعمال التنفيذية المكونة للجريمة أو الشروع فيها"[1].

وغنيّ عن البيان، أنّ المعاينة إجراء يمكن لضابط الشرطة القضائية القيام به، سواء كانت الجريمة متلبس بها أم لا، حيث تنص المادة 12 من قانون الإجراءات الجزائية الجزائري" ***...ويناط بالضبط القضائي مهمة البحث و التحري عن الجرائم المقررة في قانون العقوبات وجمع الأدلة عنها والبحث عن مرتكبيها...***" وتقابلها المادة 24–1 من قانون الإجراءات الجزائية المصري[2]، ومن المسلم به أن التحري عن الجرائم يأتي بمعاينة آثارها والتحري عن ملابسات إرتكابها والمحافظة على تلك الآثار ورفعها، وهو ما نصت عليه المادة 42 إجراءات جزائري – وتقابلها المادة 31–1 قانون إجراءات جزائية مصري[3]– في إطار حصر ضباط الشرطة القضائية في حالة التلبس "***...وعليه أن يسهر على المحافظة على الآثار التي يخشى أن تختفي...***".

كما يمكن لقاضي التحقيق القيام بها متى دخلت الدعوى العامة في حوزته على أن يخطر وكيل الجمهورية بذلك، وهو ما نصت عليه المادة 79 إجراءات جزائري والمادة 90 إجراءات مصري[4]، سواء كان ذلك بنفسه أو ندب ضابط الشرطة القضائية للقيام بذلك، ويقتضي ذلك تحرير محضر بها عن طريق كاتب لأنّها من الإجراءات الّتي تقتضي تفرّغ ذهني من المحقّق، كما للمحكمة أيضا وفقا للمباديء العامة التي تجيز لها البحث عن الحقيقة بأي طريق مشروع أن تجري المعاينة إذا ما رأت في ذلك سبيلا إلى كشف الحقيقة[5].

---

[1]– **د. خالد ممدوحإبراهيم**، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2009، ص72 وما بعدها.

[2]– تنص المادة 24–1 من قانون الإجراءات المصري"يجب على مأموري الضبط القضائي أن يقبلوا التبليغات والشكاوي التي ترد إليهم بشأن الجرائم، وأن يبعثوا بها فوراً إلى النيابة العامة، ويجب عليهم وعلى مرءوسيهم أن يحصلوا على جميع الإيضاحات ويجروا المعاينات اللازمة لتسهيل تحقي الوقائع التي تبلغ إليهم، أو التي يعلنون بها بأية كيفية كانت، وعليهم أن يتخذوا جميع الوسائل التحفظية اللازمة للمحافظة على أدلة الجريمة".

[3]–تنص المادة 31إجراءات مصري "يجب على مأمور الضبط القضائي فى حالة التلبس بجناية أو جنحة أن ينتقل فوراً إلى محل الواقعة ويعاين الآثار المادية للجريمة ويحافظ عليها، ويثبت حالة الأشخاص، وكل ما يفيد كشف الحقيقة ويسمع أقوال من كان حاضراُ، أو من يمكن الحصول منه على إيضاحات فى شـــأن الواقعة ومرتكبها".

[4]– تنص المادة 79 من قانون الإجراءات الجزائرية على أنه " يجوز لقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو للقيام بتفتيشها, و يخطر بذلك و كيل الجمهورية الذي له الحق في مراقبته, ويستعين قاضي التحقيق دائما بكاتب التحقيق ويحرز محضر بما يقوم به من إجراءات". كما تنص المادة 90 من قانون الإجراءات المصري" ينتقل قاضي التحقيق إلى أي مكان كلما رأى ذلك ليثبت حالة الأمكنة والأشياء والأشخاص ووجود الجريمة مادياً وكل ما يلزم إثبات حالته."

[5]– **د. فوزية عبد الستار**، شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، 1986، ص527.

الفرع الثاني

كيفية المعاينة التقنية لمسرح جرائم الإعتداء على التعاملات الإلكترونية

يقصد بمعاينة مسرح الجريمة الواقعة على التعامل الإلكتروني، معاينة الآثار التي يتركها مستخدم شبكة الأنترنت، وتشمل الرسائل المرسلة منه أو التي إستقبلها، وكافة الإتصالات التي تمت من خلال الحاسوب وعبر شبكة الأنترنت[1].

والملاحظ أن الآثار المعلوماتية أو الرقمية المستخلصة من أجهزة الحاسوب من الممكن أن تكون ثرية للغاية بما تحويه من معلومات، فصفحات المواقع، البريد الإلكتروني، الفيديو الرقمي، الصوت الرقمي، غرف الدردشة والمحادثة، الملفات المخزنة في الحاسوب الشخصي الصورة المرئية، الدخول للخدمة، والإتصال بالأنترنت والشبكة عن طريق مزود الخدمة، كل هذه الوسائل والأدوات والوسائط يمكن أن تحوي أدلة تفيد كثيرا في كشف الحقيقة بشأن الجريمة محل التحقيق[2].

وإذا كانت المعاينة تتم بالإنتقال إلى محل الواقعة الإجرامية كقاعدة عامة إجرائية مقررة في هذا الشأن، إلا أنه في إطار جرائم الإعتداء على التعاملات الإلكترونية فإن الإنتقال يعد من الموضوعات الجديدة، وذلك كون مسالة الإنتقال هذه تكون في إطار مسرحين مسرح تقليدي[3] وآخر افتراضي[4]، وإذا كانت عمليّة الانتقال إلى المسرح التّقليدي تتم بطريقة ماديّة، فإنّ الأمر يختلف بالنّسبة إلى المسرح الافتراضي، فلا يكون بالضّرورة عبر العالم المادّي وإنمّا عبر العالم الافتراضي، حيث يستطيع عضو الشرطة القضائية أن يقوم بهذه المعاينة وهو جالس في مكتبه من خلال الحاسوب الموضوع في المحكمة، كما يمكنه أن يلجأ إلى بيت الخبرة القضائيّة أو إلى الخبرة الاستشارية أو إلى مقهى الأنترنت، ويمكنه اللّجوء أيضاً إلى مقرّ مزوّد بالأنترنت الذي يعدّ أفضل مكان يمكن من خلاله إجراء المعاينة[5]. ذلك أنه في كل الأحوال يلزم أن يقوم المحقق بالمعاينة من خلال حاسوب أو حاسوب خادم، ومن ثم فإن مشكلة الإنتقال المادي إلى مكان إرتكاب الجريمة لا تشكل عائق أمام عضو الشرطة القضائية، خاصة مع التسهيلات التي قررتها بعض التشريعاتكالمشرع الجزائري، حيث أجاز بموجب المادة 47 إجراءات إجراء المعاينة في كل ساعة من ساعات النهار أو الليل في كل محل سكني أو غير سكني بناء على إذن مسبق من وكيل الجمهورية المختص.

---

[1]- **Henry, J.F**, "Testimony before permanent Subcommittee On Governmental Affairs, The United States Senate, Ninety, Ninth Congress, 1984. available at :http://www.igc.apc.org/nemesis/aclu/nudishallof shame/henry.html

[2]- **د. ممدوح عبد الحميد عبد المطلب**، إستخدام بروتوكول (tcp/ip) في بحث وتحقيق الجرائم على الكمبيوتر، المرجع السابق، ص7.

[3]- ويقع خارج بيئة تقنية المعلومات، و يتكون بشكل رئيسي من المكونات المادية المحسوسة للمكان الذي وقعت فيه الجريمة، وهو أقرب ما يكون إلى مسرح أية جريمة تقليدية، قد يترك فيها الجاني آثار عدة، كالبصمات وبعض متعلقاته الشخصية أو وسائط تخزين رقمية. **د. حسين بن سعيد الغافري**، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الأنترنت، متاح على الموقع الإلكتروني السابق.

[4]- ويقع داخل البيئة التقنية، ويتكون من المعلومات الرقمية التي تتواجد داخل الحاسوب وشبكة الأنترنت في ذاكرة الأقراص الصلبة الموجودة بداخله. **د.حسين بن سعيد الغافري**، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الأنترنت، مقال متاح على الموقع الإلكتروني السابق.

[5]- **د. عمر أبو بكر بن يونس**، الجرائم الناشئة عن إستخدام الأنترنت، المرجع السابق، ص 895.

وانما المشكلة تكون من خلال الإنتقال إلى العالم الإفتراضي، حيث يلزم أن يكون هذا الإنتقال بالسرعة الكافية التي تمنع زوال آثار الجريمة، ولهذا يجب أن يعجل بإجراء المعاينة خشية ضياع الأدلة[1].

وتماشيا مع متطلبات السرعة في معاينة مسرح الجريمة الإفتراضية، أجازت بعض التشريعات لعضو النيابة المعلوماتية أن يرسل رسالة إلى مزود خدمة الأنترنت يلزمه فيها بالتحفظ على السجلات المطلوبة، إلى حين صدور أمر من المحكمة بإتخاذ هذا الإجراء أو غيره، ومن قبيل ذلك القانون الأمريكي (1)18 U.S. Code § 2703[2].

وتتصف المعاينة في جرائم التعاملات الإلكترونية بطابع التنوع من حيث ضرورة توافقها مع نوعية الجريمة المرتكبة، على أنّ هناك طرقًا عامّة تتوافق مع طبيعة الاتّصال بالأنترنت أو الوسيلة الّتي يتمّ بها ذلك الاتّصال، فمثلاً هناك وسيلة تصوير شاشة الحاسوب impression de captures d'écranوالتي قد تكون بواسطة آلة تصوير تقليديّة[3] أو عن طريق إستخدام برمجيّة حاسوب متخصّصة في أخذ صور لما يظهر على الشّاشة، وهذا ما يعرف بـــ: تجميد مخرجات الشّاشة frozen أو أن يكون ذلك عن طريق حفظ الموقع بإستخدام خاصيّة الحفظ save asالمتوافرة في نظام التّشغيل. وتلتقي هذه الحالة من فحص الحاسب بإستخدام خاصية history حيث أن الحاسوب كلما تم الولوج إلى الأنترنت فإنه يقوم باستنساخ نسخة من كل صفحة أو موقع يتم إستدعائه ويقوم بحفظها في ملف خاص يصنعه نظام التشغيل[4].

ولابد من أن تقتصر عملية المعاينة على ضباط الشرطة القضائية ممن تتوافر فيهم الكفاءة العلمية والخبرة التقنية في المجال المعلوماتي ممن تلقو التدريب الكافي للتعامل مع هذه النوعية من الجرائم. كما لهم الإستعانة بالخبراء نظرا للطبيعة غير المادية لمحل الإعتداء والطابع التقني لأسلوب إرتكابها، فنجاح هذه الجهة في تطبيق القانون يتوقف على حسن إختيار الخبير، الذي لا يكفي أن يكون لديه إمكانيات في مجال التخصص فحسب، بل لا بد أن يكون قد مارس تخصصه في الواقع العملي لوقت كاف يسمح بإكتسابه كفاءة عالية.

---

[1]– **أسامة فرج الله محمود الصباغ**، المرجع السابق، ص203.

[2]-**Daniel A.** Morris, Tracking a Computer Hacker, USA Bulletin (May 2001), available at http://www.leetupload.com/database/Misc/Papers/Asta%20la%20Vista/Web%20Papers/tracking_a_computer_hacker.doc

[3]- **د. جميل عبد الباقي الصغير**، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت، المرجع السابق، ص28.

[4]–أنظر: **د. عمر أبو بكر بن يونس**، الجرائم الناشئة عن إستخدام الأنترنت، المرجع السابق، ص 895. **د.حسين بن سعيد بن سيف الغافري**، السياسة الجنائية في مواجهة جرائم الأنترنت، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 2007، ص355

وإن كان ذلك كذلك، فإن البعض من الفقه يرى بأن المعاينة في مجال كشف غموض الإعتداءات المنصبة على التعاملات الإلكترونية وضبط الأشياء الّتي تفيد في إثبات وقوعها ونسبتها إلى مرتكبيها لا تكونبذات الأهمية, وذلك لأسباب التّالية[1]:

1- إنّ الجرائم التي تنال من التعاملات الإلكترونية قلّما يترتّب على إرتكابها آثار ماديّة.

2- إمكانيّة التّلاعب في المعلومات عن بعد، أو محوها عن طريق التّدخل من خلال وحدة طرفيّة[2]، وهو ما يثير الشك في الدليل المستمد من المعاينة، مما يؤدي إلى طرح هذا الدليل جنائيا، كون أن الأحكام الجنائية تقوم على الجزم والقين لا على مجرد الظن والتخمين.

وتجنبًا لذلك قامت بعض الدّول بتقرير جزاءات على كل من يقوم بإجراء أيّ تغيير على حالة الأماكن الّتي وقعت فيها الجريمة قبل الإجراءات الأوّليّة للتّحقيق، ومن قبيل ذلك ما نصّ عليه المشرّع الجزائري في المادة 43 من قانون الإجراءات الجزائية على أنه:" يحظر في مكان إرتكاب جناية على كل شخص لا صفة له، أن يقوم بإجراء أي تغيير على حالة الأماكن التي وقعت فيها الجريمة أو ينزع أي شيء منها قبل الإجراءات الأولية للتحقيق القضائي، وإلا عوقب بغرامة 200 إلى 1000دج.

غير أنه يستثنى من هذا الحظر حالة ما إذا كانت التغيرات أو نزع الأشياء للسلامة والصحة العمومية أو تستلزمها معالجة المجني عليهم.

وإذا كان المقصود من طمس الآثار أو نزع الأشياء هو عرقلة سير العدالة عوقب على هذا الفعل بالحبس من ثلاثة أشهر إلى ثلاثة سنوات وبغرامة من 1000 إلى 10000 دج"، وتقابلها المادة 55من قانون الإجراءات الجزائيّة الفرنسي[3].

والملاحظ أنّ هذه المواد يمكن تطبيقها عند معاينة مكوّنات نظام التعاملات الإلكترونية غير المادية، عكس المكوّنات غير الماديّة من قواعد معطيات أو معلومات مخزنة في ذاكرة النظام أو على أحد وسائط التخزين لأنّها تتطلّب إجراءات خاصة.

---

[1]- أنظر: **د. حسين بن سعيد الغافري**، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الأنترنت، متـــاح على الموقـــع التـــالي:
http://www.minshawi.com/other/ghafry3.pdf

د. عبد الله حسين على محمود، المرجع السابق، ص357، **حسين بن سعيد بن سيف الغافري**، السياسة الجنائية في مواجهة جرائم الأنترنت، المرجع السابق، ص353.

[2]- **نبيلة هبة هروال**، المرجع السابق، ص217.

[3]-**Article 55** du CPF Modifié par Loi n°92-1336 du 16 décembre 1992 - art. 11 JORF 23 décembre 1992 en vigueur le 1er mars 1994 dispose que " Dans les lieux où un crime a été commis, il est interdit, sous peine de l'amende prévue pour les contraventions de la quatrième classe, à toute personne non habilitée, de modifier avant les premières opérations de l'enquête judiciaire l'état des lieux et d'y effectuer des prélèvements quelconques.

Toutefois, exception est faite lorsque ces modifications ou ces prélèvements sont commandés par les exigences de la sécurité ou de la salubrité publique, ou par les soins à donner aux victimes."

3- كثرة المترددين على مسرح الجريمة خلال المدة الزمنية التي غالبا ما تكون طويلة نسبيا، وذلك ما بين إقتراف الجريمة والكشف عنها، الأمر الذي يمنح فرصة لحدوث تغيير أو تلفيق أو عبث بالآثار المادية أو زوال بعضها، وهو مايلقي ظلالا من الشك على الدليل المستقى من المعاينة.

وقد جاءت المادة 16 من إتفاقية بودابست لتتفادى النقذ الذي وجه للمعاينة في الجرائم الواقعة في العالم الإفتراضي بصفة عامة، ومحاولة جعل المعاينة تتمتع بنفس درجة الأهمية كما هو الحال في الجرائم التقليدية، حيث نصت " يجب على كل طرف أن يتخذ الإجراءات التشريعية، وأية إجراءات أخرى يرى أنها ضرورية من أجل السماح لسلطته المختصة أن تأمر أو أن تفرض بطريقة أخرى التحفظ على المعطيات المعلوماتية المخزنة، وبما في ذلك المعطيات المتعلقة بحركة السير المخزنة بواسطة نظام معلوماتي، وبالأخص عندما تكون هناك أسباب تدعو للإعتقاد بأن هذه المعطيات على وجه الخصوص معرضة للفقد أو التعديل".

وكما هو ملاحظ، فإن هذه المادة لم تحدد طريقة التحفظ على المعطيات، حيث تركت الأمر لكل طرف في أن يقيم النمادج الملائمة للتحفظ، وتحديد ما إذا كان في بعض الحالات فإن التحفظ على المعطيات يمكن أن يشمل أيضا تجميدها، وعبارة يتحفظ على المعطيات تعني حفظ معطيات سبق وجودها في شكل مخزن وحمايتها من كل شيء يمكن أن يؤدي إلى إتلافها أو تجريدها من صفتها أو حالتها الراهنة.

وعلى ذات النهج سارت الإتفاقية العربية، حيث ألزمت في مادتها 23 الدول الأطراف بأن تتبنى الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأمر أو الحصول على الحفظ العاجل للمعلومات المخزنة بما في ذلك معلومات تتبع المستخدمين والتي خزنت على تقنية المعلومات وخصوصا إذا كان هناك إعتقاد أن تلك المعلومات عرضة للفقدان أو التعديل.

وإن كان المشرع الجزائري قد نص صراحة في المادة 11 من قانون 09-04 على إلزام مقدمي الخدمة بالحفاظ على معطيات حركة السير المتعلقة بالإتصالات والتي تعد من الأمور الجوهرية للتعرف على مرتكبي الجرائم والذين سيكونون موضوعا التحري والتحقيق، نظرا لما تسمح به هذه التقنية من عمل مقارنات بين ساعة وتاريخ ومصدر ومآل إتصالات المشتبه فيه، وساعة التدخلات غير القانونية في نظم الضحايا، وهوية الضحايا الاخرين، أو بيان روابط مع شركاء آخرين، إلا أنه يؤخد عليه بداية عدم إقامته أهمية لمسألة ضمان أمن المعطيات من خطر التغيير أو التجريد من صفتها الأصلية للفترة الزمنية المطلوبة إلى غاية الكشف عنها، على عكس ما فعلت اتفاقية بودابست والإتفاقية العربية، ويبدو ذلك واضحا من عبارة "**حفظ**" التي استخدمها في المادة (11) من القانون السابق ذكره هذا من جهة.

ومن جهة أخرى، حدد المعطيات محل الحفظ في المعطيات المتعلقة بحركة السير فحسب مثل adresse IP، رقم الهاتف، عنوان البريد الإلكتروني... دون تعميمه لجميع المعطيات المعلوماتية المخزنة بما يشمل المعطيات التي يضعها الإنسان، وفي ذلك فقدان للعديد من عناصر الإثبات الجوهرية، ذلك أن التحفظ على البريد الإلكتروني الموجود وفي طور التخزين مثلا يمكن أن يكشف عن العديد من الجرائم الواقعة على التعاملات الإلكترونية التي تم إرتكابها.

المطلب الثالث

تفتيش النظم المعلوماتية المستخدمة في إرتكاب جرائم الإعتداء على التعاملات الإلكترونية

لإستكمال الإجراءات المتبعة في هذا المبحث سنستهل هذا المطلب بإعطاء فكرة عامة عن التفتيش في البيئة المادية(الفرع الأول) لندخل من ذلك رحال الفروع الأخرى لبيان مدى إمكانية تفتيش الوسائل الإلكترونية بحثا عن الأدلة التي تفيد في كشف الجريمة أو كيفية إرتكابها(الفرع الثاني) ضوابط هذا التفتيش(الفرع الثاني) ثم النتائج المترتبة على هذا التفتيش (الفرع الثالث).

الفرع الأول

التعريف بالتفتيش بصفة عامة

لقد تزايدت أهمية التفتيش في نظم الإجراءات الحديثة، لكونه يعد أقوى الأساليب الجزائية المقررة لمكافحة تصاعد الإجرام وتطوراته الحديثة، وتكمن الفكرة الأساسية للتفتيش في إباحة إنتهاك الحق في الخصوصية طالما أن هناك مبررا في القانون لهذا الإنتهاك، لذا فهو يعد من بين أقصى الصلاحيات التي تمارسها الدولة ضد المواطن، ويعد أحد مظاهر تقييد الحريات الإنسانية التي ساهمت التشريعات الكبرى الأساسية في دعم المحافظة عليها[1]. فدستور الجزائر 1996 نص في المادة 47 على عدم تفتيش المساكن إلا بمقتضى القانون، وفي إطار إحترامه وبناء على أمر مكتوب صادر عن السلطة القضائية المختصة، أما قانون العقوبات فقد تضمن نصوصا تعاقب على خرق حرمة المنزل وعلى إفشاء الأسرار[2].

---

[1]-**د. عمر ابو بكر بن يونس**، الجرائم الناشئة عن إستخدام الأنترنت، المرجع السابق، ص852.

[2]– تعمل معظم النصوص العقابية الخاصة بجريمة خرق حرمة المنزل عند التعامل فيما بينها بالنسبة لعناصر الجريمة وأركانها مع أفعال الدخول المادي أو البقاء، ويقصد بالدخول هنا الولوج إليه بأية طريقة (المادة (295) من قانون الجزائري) أو باستعمال المناوراتmanoeuvres أو التهديدmenaces أو بالإكراهcontrainte(الفقرة الرابعة (4) من المادة (226)من قانون العقوبات الفرنسي) إلى موضع ذو وجود مادي –المنازل والأماكن التي في حكمها_.

هذا وقد تعددت التعريفات الفقهية لفكرة التفتيش[1]، إلا أنها تجمع على أن التفتيش عبارة عن إجراء من إجراءات التحقيق التي تهدف إلى البحث عن الأدلة المادية لجناية أو جنحة تحقق وقوعها في محل خاص يتمتع بحرمة ، وذلك وفقاً للضمانات والقيود القانونيّة المقرّرة[2].

ومن التعريف الذي قدمناه يتضح ان التفتيش يتميز بـــ 3 خصائص[3]:

1- الأصل أنه عمل من أعمال التحقيق القضائي، إلا أنه إستثناء يدخل في صلاحية الضبط القضائي في الأحوال التي عينها القانون، وطبقا للأشكال التي يحددها والإجراءات والأسباب التي يقررها تحت إشراف وإدارة السلطة القضائية.

2- أنه من أعمال جمع الأدلة في تحقيق جنائي، لأنه غايته التي حددها القانون هي البحث عن الأدلة اللازمة للتحقيق وضبطها.

4- أنه مرتبط بالحرمة، لأنه إطلاع على محل له حرمة.

وان كان المحل الذي يتمتع بحرمة خاصة في القانون قد يكون مسكن الشخص، أو جسمه أو رسائله في الجرائم التقليدية. فإن محل التفتيش في جرائم التعاملات الإلكترونية فيرد فضلا عن الشخص الذي يستخدم نظام التخزين أو التراسل، هذه النظم بذاتها، وبذلك فقد إجتمعت المكونات المادية مع المكونات المعنوية وهو مايثير مشكلات حول طبيعتها المعنوية وكذلك طبيعة إجراءات التفتيش التي هي من نفس الطبيعة؟

الفرع الثاني

مدى قابلية مكونات النظم المعلوماتية للتفتيش

إن النظم المعلوماتية لها مكونات مادية وأخرى منطقية، كما أن لها شبكات إتصال بعدية، سنحاول فيما يلي معرفة مدى خضوع هذه المكونات للتفتيش على النحو التالي:

أولا- مدى قابلية تفتيش المكونات المادية للنظم المعلوماتية

لايختلف إثنان في أن البحث في المكونات المادية لنظم الحوسبة أو الإتصال بحثا عن شيء يتصل بجريمة من جرائم التعاملات الإلكترونية وقعت، ومن ثم يفيد في كشف الحقيقة عنها وعن مرتكبها، لايثير مشكلة كون أن هذه المكونات تدخل بطبيعتها في مفهوم الأشياء المادية كلوحة المفاتيح أو شاشة اللمس أو

---

[1]- راجع تعريف التفتيش: **د. أحمد شوقي الشلقاني**،المرجع السابق، ص40.**ود. هلالي عبد الله أحمد**، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة، 2006، ص45 وما بعدها. **د.علي حسن محمد الطوالبة**، التفتيش الجنائي على نظم الحاسوب والأنترنت، دراسة مقارنة، الطبعة الأولى، عالم الكتب الحديث، أربد، 2004، ص11. **د. عبد الله أوهابيبه**، المرجع السابق، ص266.

[2]- **د. سامي حسني الحسيني**، النظرية العامة للتفتيش في القانون المصري والمقارن، دار النهضة العربية، القاهرة، 1972، ص37.

[3]-**د.توفيق محمد الشاوي**، حرمة الحياة الخاصة ونظرية التفتيش، منشاة المعارف بالإسكندرية، 2006، ص27.

نظام الفأرة، وإن كان المدخلات السابقة لا يتصور تفتيشها، ولكن من الممكن إستخدامها لإثبات علاقة المتهم بالحاسوب كعلاقة مادية أي "بصمات".

كما يمكن أن يشمل التفتيش الحيز المادي(الحقيبة التي بها الكمبيوتر أو الهاتف النقال) وما بها من مفكرات وخلافه.

وتبقى المشكلة الرئيسية في صدور إذن التفتيش، هي **وجود جريمة قد وقعت بالفعل** من حيث تطلب وجود نص تشريعي يجرم الفعل، مع مراعاة طبيعة المكان الموجود فيه، وهل هو مكان عام أو مكان خاص، إذ أن لطبيعة المكان وصفته أهمية خاصة في مجال التفتيش[1].

فبالنسبة للأماكن العامة، فقد تكون أماكن عامة بطبيعتها وقد تكون أماكن عامة بالتخصيص، ومن أمثلتها دور الحكومة والحدائق العامة والصحاري والطرق العامة والقطارات والحافلات العامة، وكذلك المصانع والمحلات المفتوحة للجمهور كالمقاهي والمتاجر ومكاتب المحامين وعيادات الأطباء والفنادق والمستشفيات الخاصة وهذه الأماكن وإن إتفقت فيما بينها في أنها ليست مساكن إلا أنها قد تختلف فيما بينها في مدى جواز الدخول إليها، وما إذا كان يجوز لرجل الضبط القضائي الدخول إليها في أي وقت[2]، فإذا وجد شخص وهو يحمل أو يسيطر أو حائز للمكونات المادية للنظم المعلوماتية فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص بنفس الضمانات والقيود المنصوص عليها في هذا المجال.

ويجب على الضابط القائم بالتفتيش في جرائم التعاملات الإلكترونية التأكد من أن الحاسب الإلكتروني ينتفي عنه الخصوصية التي تحول دون القيام بالتفتيش، كما لو كانت المستندات المعلوماتية تتسم بسرية من شأن الإفصاح عنها إلحاق ضررا بالغا بالغير[3].

وإذا كان المستقر عليه، أنه من حق ضابط الشرطة القضائية دخول الأماكن العامة دون الحصول على إذن مسبق وذلك بهدف الإشراف على تنفيد القوانين واللوائح، إلا أنه رغم ذلك فلا يجوز له أن يقوم بفتح الأشياء المغلقة الموجودة في المحال العامة[4].

وفي هذا الصدد قررت محكمة النقض المصرية أن الأصل هو أن لرجال السلطة العامة في دوائر إختصاصهم دخول الأماكن العامة لمراقبة تنفيد القوانين واللوائح، وهو إجراء إداري مقيد بالغرض السالف البيان، ولايجاوزه إلى التعرض إلى حرية الأشخاص وإستكشاف الأشياء المغلقة غير الظاهرة، مالم يدرك الضابط بحسه وقبل التعرض لها كنه مافيها، مما يجعل أمر حيازتها أو إجراءها جريمة تبيح التفتيش، فيكون التفتيش في هذه الحالة قائما على حالة **التلبس**[5].

---

[1]- **د. هلالي عبد الله احمد**، تفتيش نظم الحاسب الآلي، المرجع السابق، ص73.

[2]– **د. عوض محمد عوض**، التفتيش في ضوء محكمة النقض، دراسة نقدية، الإسكندرية، 2006، ص90.

[3]– **د. أيمن عبد الحفيظ**، حدود مشروعية أجهزة الشرطة في مواجهة الجرائم المعلوماتية، مجلة مركز بحوث الشرطة، العدد 25 ، يناير 2004، ص380.

[4]– نقض 1 نوفمبر 1987 ، مجموعة أحكام النقض، س 38، رقم 169، ص917.

[5]– نقض 30812 لسنة 67 ق ج 18 من أبريل سنة 2007.

أما إذا كانت موجودة في **مكان خاص كمسكن المتهم أو احد ملحقاته** كان لها حكمه، فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه وبنفس الضمانات المقررة قانونا في التشريعات المختلفة،وتتوقف حرمة المسكن بمدلوله الواسع على إستمرار خصوصيته، فإذا أزال صاحب المسكن هذه الخصوصية وسمح للجمهور بغير تمييز بالتردد على هذا المكان، فإن قواعد التفتيش لا تحميه، إذ لا يكون في هذه الحالة مستودعا للسر، ولذلك فإن المحال العامة التي يسمح للجمهور بدخولها دون تمييز لا تعد مسكنا.

وفي إطار التقرير بوجود حرمة، نص المشرع الجزائريفي المادة 64 من قانون الإجراءات الجزائية الجزائري على أنه " لا يجوز تفتيش المساكن ومعاينتها وضبط الأشياء المثبتة للتهمة إلا برضا صريح من الشخص الذي ستتخذ لديه هذه الإجراءات، ويجب أن يكون هذا الرضا بتصريح مكتوب بخط يد صاحب الشأن، فإن كان لا يعرف الكتابة فبإمكانه الاستعانة بشخص يختاره بنفسه، ويذكر ذلك في المحضر مع الإشارة صراحة إلى رضاه.

وتطبق فضلا عن ذلك أحكام المواد من 44 إلى 47 من هذا القانون".

وتشير الإحالة السابقة إلى المواد المتعلقة بالإذن والحضور والميقات في التفتيش، وإن كان ذلك كذلك، رجع المشرع الجزائري بموجب الفقرة الأخيرة من هذه المادة ليستثني تطبيق هذه الضمانات على طائفة من الجرائم المذكورة في المادة 47 في فقرتها 3 التي تنص ""وعندما يتعلق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنية أو الجرائم **الماسة بأنظمة المعالجة الآلية للمعطيات** وجرائم تبييض الأموال والإرهاب وكذا الجرائم المتعلقة بالتشريع الخاص بالصرف فإنه يجوز إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل و ذلك بناء **على إذن مسبق من وكيل الجمهورية المختص**".

ولعل هذا الإستثناء له ما يبرره من الناحية العملية، ذلك أن الجرائم المنصبة على النظم المعلوماتية بمختلف تطبيقاتهاهي جرائم قابلة للإختفاء في أقل من ثانية، كما أن الدليل الذي يمكن أن يسفر عنه هذا التفتيش قد يكون الدليل الوحيد الذي يمكن التعويل عليه في الوصول إلى إظهار الحقيقة، ومن تمّ إرتكاز كلّ العمليّة الإثباتية على وجوده، وإهماله من شأنه أن يؤدي إلى فرار المجرمين من العدالة.

ثانيا– مدى قابلية تفتيش المكونات غير المادية للنظم المعلوماتية

لاشك أن أي برنامج يتم تثبيته على الحاسب الآلي المستخدم في النفاد للشبكة يترك آثارا رقمية له حتى بعد إلغائه، ومن خلال هذه الآثار يمكن معرفة ما إذا كانت تلك البرمجية تتعلق بأي مجال، فمثلا في القرصنة الإلكترونية باصطياد المعطيات الرقمية المتبادلة بين الزبائن والبنك، لابد من وجود برامج خاصة تمكن الوصول إلى الأرقام السرية أو توليد الأرقام الخاصة بالطاقة، كما يمكن العثور على العديد من الآثار الرقمية حول صفحات الواب المستعملة في عملية النصب، والرسائل الإلكترونية المستخدمة في تحويل المبالغ المالية.

كما أن برامج التجسس تترك في الجهاز نوع من أنواع السجلات التي تم التجسس عليها من هذا الجهاز، أو تم جمعها من جهاز معين History-Cookies، وغيرها كثير.

وإذا كان الأمر قد إنته بنا إلى صلاحية مكونات النظم المعلوماتية المادية كمحل يرد عليه التفتيش، فإن إمتداد ذلك إلى مكوناته غير المادية بحثا عن الأدلة التي تفيد في كشف الجريمة أو كيفية إرتكابها، هو محل جدل فقهي كبير نظرا لغياب المظهر المادي المحسوس للمعلومات المجردة على دعامتها أو وسيط التخزين:

فذهب رأي إلى القول أن النصوص المتعلقة بالتفتيش في بعض التشريعات تسمح بتفتيش المكونات غير المادية، ذلك أن صياغة هذه النصوص من العموم بما يسمح توسيع تفسير عبارة ضبط " أيّ شيء" لتشمل المكوّنات غير المادية[1].

وعلى عكس أصحاب الإتجاه الأول، يرى أصحاب هذا الإتجاه أن بعض التشريعات حددت الهدف من التفتيش بأنه البحث عن شيء أو أشياء وضبطها، وهذا الشيء يقتصر مفهومه على المال ذي الحيز المادي المحسوس، ولايمتد إلى الكيانات المنطقية التي تستلزم وجود أحكام خاصة بها تكون أكثر ملاءمة لها[2].

وفي مقابل هذين الرأين، يوجد رأي آخر نادى بنفسه عن البحث عما إذا كانت كلمة شيء تشمل المعطيات المعنوية لمكونات الحاسب الآلي أم لا، فذهب إلى أن المعلومات أو البرامج وإن لم يكن لها كيان مادي محسوس، إلا أنها تشغل حيزا ماديا في ذاكرة الحاسوب أو وسائط التخزين، يمكن قياسه بمقياس معين وهو البايت، إذ أن سعة أو حجم الذاكرة الداخلية للحاسوب تقاس بعدد الحروف التي يمكن أن تخزن فيها. فالمعطيات تكون في شكل نبضات إلكترونية ممثلة بالرقمين صفر أو واحد، وهي تشبه التيار الكهربائي الذي إعتبرته الكثير من التشريعات من الأشياء المنقولة، وبالتالي فإن المعلومات يمكن أن تدخل في نطاق الأشياء المادية[3].

وفي تقديرنا، فإن الإتجاه الأول والأخير أي كانت المبررات التي يقوم عليها، لا يمكن القبول به، لنفس الأسباب التي ذكرناها فيما يخص السرقة المعلوماتية وذلك في معرض حديثنا عن التعامل غير المشروع في معطيات إنشاء التوقيع الإلكتروني، فمثلا كلمة الشيء التي إستخدمتها بعض التشريعات الجزائية بشكل مجرد لا يمكن تفسيرها بمعزل عن طبيعة إجراء تفتيشها أوالحصول عليها وضبطها الذي يكون له طبيعة مادية، كما أن المعلومات هي عبارة عن **نبضات إلكترونية تستمد حياتها من الطاقة** ولا يمكن بأي

---

[1]– فالمادة 487 عقوبات كندي تقضي بإمكانية إصدار أمر قضائي لتفتيش وضبط أي شيء... تتوافر بشأنه أسس ومبررات معقولة تدعو للاعتقاد بأن الجريمة قد وقعت أو يشتبه في وقوعها، أو هناك نية لاستخدامه في ارتكاب جريمة، أو أنه سينتج دليلا على وقوع الجريمة، حتى الآن يفسر هذا النص بوضوح تام على أنه يسمح بتفتيش المكونات المعنوية لنظام المعالجة الآلية.مشار إليها لدى: **د. هلالي عبد الله أحمد**، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص201. ومن أمثلة التشريعات العربية التي أوردت كلمة شيء: القانون الجزائري في المواد 41 حتى 44 ،84، القانون المصري في المواد من 30 إلى 36، الأردني 34 –81–86.

[2]– **د. موسى مسعود أرحومة**، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، بحث مقدم إلى المؤتمر المغاربي الأول حول: المعلوماتية والقانون، أكاديمية الدراسات العليا، 28–2009/10/29، طرابلس، ص8.

[3]– **د. علي حسن محمد الطوالبة**، المرجع السابق، ص30.

حال من الأحوال إعتبارها طاقة أو قوة كما هو شأن التيار الكهربائي[1]،وإن كانت التشريعات إعتبرتها من الأشياء المنقولة فهي نصوص شرعت خصيصا لتطال الأنماط التي تنظمها، وهي نصوص خاصة لا يتوسع في القياس عليها، بل لا نبالغ إن قلنا أن **جزءا من النصوص الخاصة يعد إستثناء على أصل والاستثناء لا يتوسع فيه.**

وبعبارة موجزة، يمكن القول أن النصوص الخاصة بالتفتيش بمعناه التقليديتمثل **قيداً على الحرية الفردية،** والقياس على الأشياء المادية محظوراً لمنافاته الشرعية الإجرائية. وهو مايستلزم وضع نص خاص الهدف منه إقامة **سلطة مساوية خاصة بالمعطيات المخزنة[2].**

وجاءت الفقرة الأولى من المادة 19 من إتفاقية بودابست لتقر أحكام خاصة لتفتيش المعطيات المعالجة، حاسمة بذلك الخلاف الفقهي، فنصت على أنه "يجب على كل طرف أن يتبنى الإجراءات التشريعية وأية إجراءات أخرى يرى أنها ضرورية من أجل تخويل سلطاته المختصة سلطة التفتيش أو الولوج...لنظام معلوماتي أو لجزء منه وكذلك **المعطيات المعلوماتية** المخزنة فيه وعلى أرضه، لدعامة تخزين معلوماتية تسمح بتخزين معطيات معلوماتية"[3].

وقد جاء في المذكرة التفسيرية للإتفاقية إلى أن المعطيات المعلوماتية المخزنة لا تعتبر في حد ذاتها كأشياء مادية، وبالتالي لا يمكن الحصول عليها أو ضبطها لأغراض التنقيب والتحري كإجراء جنائي بنفس طريقة الأشياء المادية، لكن يمكن على الأقل ضبط حاملة المعطيات[4].

وكذلك فعلت الإتفاقية العربية، حيث نصت بموجب المادة 26" تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين سلطاتها المختصة من التفتيش....**والمعلومات المخزنة فيها** أو عليها".

وقد تأثر المشرع الفرنسي بإتفاقية بودابست، فقام بتعديل نصوص التفتيش، حيث قام بإضافة عبارة"**المعطيات المعلوماتية**" في المادة 94 من قانون الإجراءات الجزائية، وذلك بموجب المادة42 [5] من القانون رقم 545-2004 المتعلّق بالثّقة في الاقتصاد الرّقمي، لتصبح المادة على النّحو التالي"***يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء أو معطيات معلوماتية يكون كشفها مفيدا لإظهار الحقيقة***"[6].

كما لم يخلو من ذلك المشرع الجزائري، حيث أجاز تفتيش المعطيات المعلوماتية وذلك بموجب المادة 5 من القانون رقم 09-04 لسنة 2009 المتعلّق بالقواعد الخاصّة للوقاية من الجرائم المتصلة بتكنولوجيات

---

[1]– **نهلا عبد القادر المومني**، المرجع السابق، ص111.

[2]-un pouvoir équivalent relatif aux données stockées., **Rapport explicatifde la Convention sur la cybercriminalité; op cit;**p36

[3] - **Article 19** " Perquisition et saisie de données informatiques stockées" du C C B dispose que**:** 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder d'une façon similaire: a à un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées; et b à un support du stockage informatique permettant de stocker des données informatiques sur son territoire.

[4]- Rapport explicatif de la Convention sur la cybercriminalitéBudapest, 23.XI.200,op,cit, p36

[5]- Art 42 du L.C.E.N dispose que:"A l'article 94 du code de procédure pénale, après les mots : « des objets », sont insérés les mots : « ou desdonnées informatiques ».

[6]-Art 94 du C.P.P.F ,dispose que :'les persquisitions sont efféctuées dans tous les lieux ou peuvent se trouver **des objets ou des données** dans tous découverte serait utile á la manifestation de vérité"

الإعلام والاتصال ومكافحتها، حيث أجازت هذه المادّة للسلطات القضائية المختصّة وكذا لضبّاط الشّرطة القضائيّةفي إطار قانون الإجراءات الجزائيّة الدّخول بغرض التّفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها وكذا **المعطيات المعلوماتيّة المخزّنة فيها** وكذا منظومة تخزين معلوماتيّة. وذلك في الحالات المنصوص عليها في المادّة (4) من هذا القانون ، وهذه الحالات هي:

-للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

-توفّر معلومات عن إحتمال إعتداء على منظومة معلوماتيّة على نحو يهدّد النّظام العام أو الدّفاع الوطني أو مؤسّسات الدّولة أو الاقتصاد الوطني، وللوقاية من الجرائم الماسة بأمن الدّولة.

-لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى التفتيش.

- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

وكما هو ملاحظ، فإن الحالة الأولى والثانية، تفترق عن التفتيش الذي الأصل فيه أنه يتخذ للبحث عن أدلة **جريمة وقعت**، ذلك أنهما يدخلان ضمن نطاق متميز لا يختلط فيه بالتفتيش القانوني، بل هو إجراء إحتياطي تمليه ضرورة الأمن، وهو مايصطلح عليه **بالتفتيش الوقائي**.

فضلا عن ذلك، فإن المشرع أدرج منضومة تخزين معلوماتية ضمن محل التفتيش الإلكتروني، ومثالها الأقراص المضغوطة أو البطاقات الذكية والأشرطة الممغنطة وما تحتويه من ملفات، كما لو تضمنت أرقام بطاقات الإئتمان أو أرقام الدخول السرية لمواقع معينة.... وذلك إيمانا من المشرع بأن تطبيق إجراء التفتيش يستلزم غالبا ليس فقط تفتيش النظام، بل أيضا كل منضومة تخزين تكون موجودة بجانب النظام المعلوماتي.

وان كان التفيش عن المعطيات أصبح مشروع قانونا، فإنه معقد عمليا، لكونها تحتوي في طياتها على عمليات إلكترونية غاية في التعقيد، فقد تكون المنظومة محمية بكلمة سر، كما قد تكون المعطيات المطلوبة مشفرة مع وضع عناوين مضللة لها وتخزينها في شكل ملفات غير تقليدية، أو يتم خلطها مع ملاين الملفات، وأمام إستبعاد إجبار الشخص على الإفصاح عن معلومات ذات طبيعة معنوية-ككلمة السر أومفتاح التشفير- من أجل تسهيل النفاذ إلى المنظومة المعلوماتية أو مافي حكمها، إعمالا للقاعدة المعروفة أن المتهم لا يجوز إجباره على الإجابة عن الأسئلة التي من شأنها أن تفضي إلى إدانته[1]، إذ من حقه الاعتصام بالصمت دون أن يُفسَّر ذلك الصمت ضد مصلحته، فإنه يجوز إجبار غير المتهم على تقديم المعلومة التي من شأنها تيسير الدخول إلى المنظومة للبحث عن المعلومة، كإلزام مديري النظام الذين لديهم معرفة جيدة عن النظام المعلوماتي محل البحث بأن يقدموا المساعدة اللازمة وذلك بالنسبة لأفضل طريقة للقيام بعملية التفتيش، وفي هذا الصدد تشير المذكرة التفسيرية لإتفاقية بودابست إلى أن المعلومات التي يمكن إلزام مدير النظام بتقديمها

[1]- حيث نص المشرع الجزائري في المادة 100 إجراءات "...وينبهه بانه حر في عدم الإدلاء باي قرار..."، وهي ترجمة حرفية لنص المادة 114 -1 إجراءات فرنسي قبل تعديلها بالقانون رقم 2015-993 المؤرخ في 17 اوت 2015 المتعلق بتكييف الإجراءات الجزائية وفق قانون الإتحاد الأروبي. **LOI n° 2015-993 du 17 août 2015 portant adaptation de la procédure pénale au droit de l'Union européenne**

كما نص على ذلك ضمنا قانون الإجراءات المصري في المادة 274-1 "لايجوز استجواب المتهم إلا إذا قبل ذلك..."

هي المعلومات الضرورية التي تسمح بتطبيق إجراء التفتيش والضبط أو تطبيق طريقة مشابهة للدخول والحصول على المعطيات، ويشترط فيها أن تكون ضرورية عقلا كأن يتعلق الإتصال في بعض الحالات بكلمة مرور أو إجراء أمني آخر[1].

وقد تأثر المشرع الفرنسي بإتفاقية بودابست، وفرض هذا الإجراء القسري لتسهيل عملية التفتيش، وذلك بموجب الفقرة الأخيرة من المادة 57–1 من قانون الإجراءات الجزائية الفرنسي[2]، كما حرص على مسألة مهمة وهي موضوع التشفير وفك الشفرة، فنصت المادة 230–1 من قانون الإجراءات الجزائية المضافة بموجب المادة 30 من القانون الصادر في 15 نوفمبر 2001 في شأن الأمن اليومي[3] على أنه عندما تكون المعطيات اللازمة لتحقيق جنائي مشفرة فإن لوكيل الجمهورية أو لسطة التحقيق أو لسطة الحكم المختصة بنظر الدعوى أن يعينوا شخصا طبيعيا أو معنويا مؤهلا للقيام بعملية فك التشفير إذا كان ذلك ضروريا[4]".

كما نجد المشرع الجزائري هو بدوره حرص على إرساء نظام "تسخير مديري النظام"، وذلك بموجب الفقرة الأخيرة من المادة 5 من القانون رقم 09–04، ومما لا شك فيه أن إرساء هذا النظام للتعاون يعفي مدير النظام من كل إلتزام تعاقدي أو غير تعاقدي بعدم إفشاء المعطيات.

من خلال ما سبق يمكن القول أن التفتيش يعتبر فن بقدر ماهو علم، وهو ما يستدعي في المقابل تأهيل أعضاء الشرطة القضائية على المستوى اللائق للتطور التقني في مجال تكنولوجيا الإعلام والإتصال. فضلا على إمكانية استشارة الأشخاص الدين لديهم معرفة جيدة عن النظام المعلوماتي محل البحث بتقديمهم المعلومات الضرورية التي تسمح بتطبيق إجراء التفتيش والضبط، كأن يتعلق الإتصال في بعض الحالات بكلمة المرور، أو إجراء أمني آخر، فبدون تأكيد هذا التعاون يمكن أن تبقى السلطات في الأماكن المراد تفتيشها ومنع الوصول إليها عبر النظام المعلوماتي فترة طويلة من الزمن، مما قد يخلق عبئا إقتصاديا بالنسبة للشركات أو لعملائها والمشتركين الذي يجدون أنفسهم في حالة إستحالة للوصول إلى المعطيات أثناء عملية التفتيش، وإن كان الأمر في نظرنا في الحقيقة لازال يحتاج إلى مزيد من التأمل القانوني فيما يخص **المستندات المشفرة** ومدى إعتبارها أوراقا مغلقة ومن تم عدم الإطلاع عليها إلا وفق ضوابط معينة، فتنص

---

[1]- Les informations que l'on peut obliger l'administrateur de système à fournir sont celles qui sont nécessaires pour permettre d'appliquer la mesure de perquisition et de saisie ou de mettre en oeuvre un moyen similaire d'accès et d'obtention de données. Seules toutefois doivent être fournies les informations « raisonnablement » nécessaires. Dans certains cas, il pourra s'agir de communiquer un mot de passe ou une autre mesure de sécurité aux autorités chargées de l'enquête. **Rapport explicatif de la Convention sur la cybercriminalité**. OP.CIT. P39:

[2]- Les officiers de police judiciaire peuvent, par tout moyen, requérir toute personne susceptible :
1° D'avoir connaissance des mesures appliquées pour protéger les données auxquelles il est permis d'accéder dans le cadre de la perquisition ;
2° De leur remettre les informations permettant d'accéder aux données mentionnées au 1°.

[3]-**Loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne**

[4]-**Article 230-1** Créé par Loi n°2001-1062 du 15 novembre 2001 - art. 30 JORF 16 novembre 2001 dispose que " le procureur de la République, la juridiction d'instruction ou la juridiction de jugement saisie de l'affaire peut désigner toute personne physique ou morale qualifiée, en vue d'effectuer les opérations techniques permettant d'obtenir la version en clair de ces informations ainsi que, dans le cas où un moyen de cryptologie a été utilisé, la convention secrète de déchiffrement, si cela apparaît nécessaire."

المادة 84[1] إجراءات جزائري أنه ***لقاضي التحقيق أو ضابط الشرطة القضائية المنوب عنه وحدهما الحق في الإطلاع عليها قبل ضبطها وكذلك إحصاء الأشياء و الأوراق ووضعها في أحراز مختومة، ولايجوز فتح هذه الأحراز و الوثائق إلا بحضور المتهم مصحوبا بمحاميه أو بعد إستدعئهما قانونا***"

خاصة وأن المادة 5 من القانون 09-04 نصت"...يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة في إطار قانون الإجراءات الجزائية..."؟

ثالثا: مدى قابلية تفتيش النظم المتصلة مع بعضها البعض الواقعة في أماكن متفرقة

لا يواجه القائم بالتفتيش مشكلات بخصوص تفتيش شبكة الأنترنت، فهذه الأخيرة شبكة عالمية مفتوحة يجوز الدخول عليها، الإطلاع، وضبط المعطيات المتاحة للجمهور وذلك بدون إذن،[2] ويمكن إعتبارها في هذا الإطار من قبيل أعمال الإستدلال، غير أن ذلك مشروط بعدم التعدي على الحق في الخصوصية، أي بعدم الدخول في الأجزاء الخاصة من الشبكة **(البريد الإلكتروني والمحادثة الفورية).**

كما لا يواجه مشكلة إذا وقعت الجريمة على النظام داخل الدولة، فيجوز بالنسبة لها إصدار الإذن بالتفتيش، إلا أن صدور هذا الإذن وفقا للضوابط القانونية ينفد بالنسبة للنظام الصادر بالنسبة له الإذن بالتفتيش فقط، إلا أنه قد يتصل النظام محل التفتيش بنظام آخر يحوي جريمة موجودة في مكان آخر داخل إقليم الدولة، كما لو تعلق الأمر بمتهم قام بتخزين معلوماته في حواسيب أخرى، بهدف عرقة التحقيقات، فيقوم ضابط الشرطة القضائية بإستخدام برنامج معين والدخول به إبتداء من الجهاز محل التفتيش إلى جهاز ثان، ومن تم فإن صحة هذه الإجراءات تكون محل مناقشة إذا تم ضبط رسائل إلكترونية أو أي معطيات بما فيها المحفوظة بالإدخال في الجهاز الثاني، **فهل يكون هذا الضبط صحيحا؟أم تم الخروج عن حدود الإذن بالتفتيش؟ وتكمن المشكلة في أن الفترة التي يراد حصول إذن بشأنها للنظام الثاني إمكانية قيام الجاني بتدمير أو محو المعطيات أو نقلها أو تعديلها**[3]. والمشكلة تظهر أكثر عندما يكون هذا الجهاز الثاني متواجد في الخارج. ومن تم فالسؤال الذي يطرح نفسه هنا هو: هل يمتّد تفتيش نظام معيّن إلى الأجهزة المرتبطة به الموجودة داخل البلاد أو خارجه؟ لإجابة على هذا السؤال هناك إحتمالين:

الفرض الأول: اتصال نظام المتهم بنظام أو مخدم موجود في مكان آخر داخل الدولة

وجدت بعض التشريعات المقارنة حلا لهذه المشكلة كما في الولايات المتحدة الأمريكية، عندما أجازت أن يمتد إذن التفتيش الصادر لمقر شركة معينة إلى فروعها الكائنة في نفس العقار[4].

---

[1]- حيث نصت المادة 84 على أنه لقاضي التحقيق أو ضابط الشرطة القضائية المنوب عنه وحدهما الحق في الإطلاع عليها قبل ضبطها وكذلك إحصاء الأشياء و الأوراق ووضعها في أحراز مختومة، ولايجوز فتح هذه الأحراز والوثائق إلا بحضور المتهم مصحوبا بمحاميه أو بعد إستدعئهما قانونا .

[2]- **د. شيماء عبد الغني**، المرجع السابق، ص351.

[3]-**Jean-Wilfrid Noël** : Internet et enquête judiciaire,disponible en lingne á l'adresse suivante www.droit-internet.com.

[4]-**Pascal Vergucht**, La répression des délits informatiques dans une perspective internationale; Thèse de doctorat en Droit privé; Montpellier 1; 1996; p368 .

مشار إليه لدى: **ايمن رمضان محمد أحمد**، المرجع السابق، ص299.

كما تسمح إتفاقية بودابست للدّول الأعضاء أن تمدّ نطاق التّفتيش الّذي كان محلّه جهاز كمبيوتر معيّن إلى غيره من الأجهزة المرتبطة به في حالة الاستعجال إذا كان يتواجد به معلومات يتم الدّخول إليها في هذا الجهاز من خلال الجهاز محلّ التّفتيش، فتنصّ الفقرة الثانية 2 من المادة 19 من القسم الرّابع على أنه من حقّ السّلطة القائمة بتفتيش الكمبيوتر المتواجد في دائرة إختصاصها أن تقوم في حالة الاستعجال بمدّ نطاق التّفتيش إلى أيّ جهاز آخر إذا كانت المعلومات المخزّنة يتم الدّخول إليها من الكمبيوتر الأصلي محلّ التفتيش[1].

كما أجازت الإتفاقية العربية التفتيش عن بعدمن خلال الفقرة 2 من المادة 26، إذا كان هناك إعتقاد بأن المعلومات المطلوبة مخزنة في تقنية معلومات أخرى أو جزء منها في إقليمها، وكانت هذه المعلومات قابلة للوصول قانونا أو متوفرة في التقنية الأولى.

كما حسمت بعض التشريعات هذه المسألة، فنجد المشرّع الفرنسيوبمناسبة تعديله قانون الإجراءات الجزائية بموجب القانون رقم 239- 2003 بشأن الأمن الداخلي[2]، حيث أضاف المادة 57-1 من قانون الإجراءات الجزائية بموجب المادة 17-1 منه والمعدلة بالقانون رقم 2016-731[3]،و التي كرست نظام **التفتيش عن بعد**، حيث أجازت لرجال الضبط القضائي الدخول من الجهاز الرّئيسي على المعلومات التي تهم عمليّة البحث و التّحري، فتنص المادّة 57-1 على أنّه " يجوز لضباط الشرطة القضائية أو تحت مسؤولياتهم أعوان الشرطة القضائية، وفي إطار التفتيش المنصوص عليه الدخول عن طريق الأنظمة المعلوماتية المثبتة في الأماكن التي يتم فيها التفتيش على المعطيات التي تهم التحقيق والمخزنة في النظام المذكور أو في أي نظام معلوماتي آخر بما أن هذه المعطيات يتم الدّخول إليها أو تكون متاحة إنطلاقا من النّظام الرّئيسي"[4].إذن فهذا الدخول لا يحصل إلا بخصوص أماكن التفتيش[5].

أما بالنسبة للمشرع الجزائري، فبمناسبة تعديله لقانون الإجراءات الجزائية بموجب القانون رقم 06-22 أجازت المادة 47 لقاضي التحقيق وفي جرائم الإعتداء على نظم المعالجة الآلية أن يقوم بنفسه أو يأمر

---

[1] Art 19 alinéa 2 .du C.C.B, dispose que" Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que, lorsque ses autorités perquisitionnent ou accèdent d'une façon similaire à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe 1.a, et ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou l'accès d'une façon similaire à l'autre système."

[2]**-Loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure**

[3]**-LOI n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale**

[4]- Art 57-1 alinèa 1 du C.P.P.FModifié parLOI n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme ,et **LOI n° 2016-731**dispose que" Les officiers de police judiciaire ou, sous leur responsabilité, les agents de police judiciaire peuvent, au cours d'une perquisition effectuée dans les conditions prévues par le présent code, accéder par un système informatique implanté sur les lieux où se déroule la perquisition à des données intéressant l'enquête en cours et stockées dans ledit système ou dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial."

[5]**Patrick Mennucci** , Rapport d'enquête de la commissiond'enquête sur la surveillance des filières et des individus djihadistes: "Face à la menace djihadiste, la République mobilisée"Assemblée nationale, 2 juin 2015-p106

ضابط الشرطة القضائية بإجراء عملية التفتيش أو الحجز ليلا أو نهار، وفي أي مكان على **إمتداد التراب الوطني.**

أما بالنسبة لتفتيش المعطيات عن بعد، فقد نصت عليها الفقرة 3 من المادة 5 من القانون رقم 09-04، حيث أجازت هذه المادة لمقتضيات التحريات والتحقيقات القضائية، تمديد التفتيش بسرعة إذا كانت المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعلومات يمكن الدخول إليها إنطلاقا من المنظومة الأولى أوجزء منها وذلك **بعد إعلام السلطة القضائية المختصة مسبقا.**

إلا أن الأمر ليس بهذه السهولة دائما، فبالنسبة لتفتيش الحاسوب الخادم قد يكون ذلك صعبا من الناحية الفنية كون أن المعلومات التي يحتفظ بها الحاسب الخادم تكون لفترة محددة حسب كل خادم ونوعية التعليمات في البلد الذي يوجد فيه، ويتطلب الأمر حينئذ الحصول على المعطيات المخزنة في الحاسب الخادم أن تأمر السلطات القضائية مقدم الخدمة بالتحفظ على المعطيات المعلوماتية لحين التفتيش، وهذا ما أكده المشرع الجزائري في المادة 11 من قانون 09-04، وإن كان هذه المادة أنشات إلتزام معين بالنسبة للمعطيات المتعلقة بحركة السير فقط دون المعطيات المخزنة بصفة عامة.

وإذا تم تلافي المشكلة من الناحية القانونية في الدول التي عدلت من تشريعاتها، فإن بعض التشريعات لازالت تعمل بنصوصها التقليدية ، كما هو حال المشرع المصري، وإن رأى البعض[1] أن تطبيق المواد الواردة من 90 إلى 95 من قانون الإجراءات الجزائية على تفتيش النظم المعلوماتية داخل الدولة بمكوناتها المادية ، فإننا نرى أن ذاتية تفتيش أجهزة الكمبيوتر التي تميزه عن القواعد التقليدية تظهر بصورة جلية في حالة تمديد إجراء التفتيش إلى الأجهزة المتصلة بالجهاز الذي صدر إذن تفتيش بخصوصه إذا كان الجهاز ينتمي إلى شخص غير المتهم وخاصة إذا تم هذا التفتيش دون إخطاره أو حضور من ينوب عنه[2] وذلك بإستخدام برامج الدخول.

الفرض الثاني: اتصال ظام المتهم بنظام أو مخدم موجود في مكان آخر خارج الدولة

يظهر أحيانا في أثناء التحقيقات أنه من الضروري تفتيش جهاز حاسوب متواجد في الخارج كما لو تعلق الأمر بشركة أم(رئيسية) وفروعها في الخارج حيث ترتبط أجهزة الشركة ببعضها البعض، أو قد يقوم المجرمون بتخزين معطياتهم في أنظمة تقنية خارج الدولة مستخدمين شبكة الإتصالات بهدف عرقلة عملية جمع الأدلة، ومن ثم فإن إمتداد الإذن بالتفتيش إلى خارج الإقليم الجغرافي للدولة التي صدر من جهتها المختصة الإذن ودخوله في المجال الجغرافي لدولة أخرى هو ما يسمى **بالتفتيش عبر الحدود.**

تسمح بعض التشريعات بتفتيش الأنظمة المتصلة حتى ولو كانت متواجدة خارج إقليم الدولة، حيث أجاز المشرع الفرنسي بموجب الفقرة الثانية 2 من المادة 57-1 من قانون الإجراءات الجزائية المضافة بموجب المادّة 17 الفقرة 2 من قانون الأمن الدّاخلي رقم 239-2003 لضابط الشرطة القضائية أن يقوم بتفتيش الأنظمة المتّصلة حتّى ولو تواجدت خارج الإقليم فنصت :" إذا تبين مسبقا أن هذه المعطيات مخزنة

[1]- **أيمن رمضان محمد أحمد**، المرجع السابق، ص329.

[2]- **د. شيماء عبد الغني**، المرجع السابق، ص301.

في نظام معلوماتي موجود خارج الإقليم الوطني, و أنه يمكن الدخول إليها أو أنها متاحة إنطلاقا من النظام الرئيسي, فإنه يمكن الحصول عليها من طرف ضابط الشرطة القضائية مع مراعاة الشّروط المنصوص عليها في المعاهدات الدّولية[1].

وفي نفس الإتجاه صدرت عن المجلس الأوروبي توصيّات تجيز أن يمتدّ تفتيش الحاسوب إلى الشّبكة المتّصلة بها، ولو كانت تلك الشّبكة تقع خارج إقليم الدّولة، فتنصّ التّوصية رقم 13 لسنة 1995 المتعلّقة بالمشكلات القانونيّة لقانون الإجراءات الجزائيّة المتّصلة بتقنيّة المعلومات على أنّه:" لسلطة التّفتيش عند تنفيذ تفتيش المعلومات وفقاً لضوابط معيّنة أن تقوم بمدّ مجال التّفتيش كمبيوتر معيّن يدخل في دائرة اختصاصها إلى غير ذلك من الأجهزة مادامت مرتبطة بشبكة واحدة وأن تضبط المعطيات المتواجدة فيها, مادام أنّه من الضّروري التّدخل الفوري للقيام بذلك"[2].

وكذلك فعل المشرع الجزائري، وذلك بموجب الفقرة 3 من المادة 5 من القانون المتضمّن القواعد الخاصّة للوقاية من الجرائم المتّصلة بتكنولوجيات الإعلام والاتّصال ومكافحتها لسنة 2009، التي أجازت الحصول على المعطيات المبحوث عنها والمخزنة في الأنظمة المتّصلة الواقعة خارج الإقليم الوطني والّتي يمكن الدّخول إليها إنطلاقا من المنظومة الأولى وذلك بمساعدة السّلطات الأجنبية المختصّة طبقًا للاتّفاقيات الدّولية ذات الصّلة وفقًا لمبدأ المعاملة بالمثل.

وإن كان ذلك هو الوضع في التشريعات السابقة، فإن هذه المسالة لم تحظى بإهتمام تنظيمي من قبل بعض التشريعات، كما هو حال المشرع المصري. وإن كنا نرى أن التفتيش الإلكتروني العابر للحدود وإن كانت تسمح به الطبيعة المتعدية الحدود للأنترنت، فضلا عن متطلبات السرعة في إجراءه بما ينفي إنتظار إذن الدولة التي يتواجد فيها الحاسوب، إلا أنه يتعين أن يوجد أساس قانوني لإمتداد هذا النوع من التفتيش، وهو ما يقتضي أن يتم في إطار المساعدة القضائية من سلطات الدولة التي يقع على إقليمها النظام سواء بإتفاقيات خاصة ثنائية أو دولية ، وهذا ما يؤكد على أهمية التعاون الدولي في مجال مكافحة الجرائم التي تقع في المجال الإلكتروني، وذلك عن طريق **الإنابة القضائية الدولية.**

وتطبيقا لذلك، فقد حدث في ألمانيا أثناء جمع إجراءات التحقيق عن جريمة غش وقعت في معطيات النظام، فقد تبين وجود إتصال بين النظام المتواجد في ألمانيا وبين شبكة إتصالات في سويسرا حيث تم تخزين معطيات المشروعات فيها، وعندما أرادت سلطات التحقيق الأمنية ضبط هذه المعطيات، فلم تتمكن من ذلك إلا عن طريق إلتماس المساعدة الذي تم بالتبادل بين الدولتين[3].

---

[1] Art 57-1 alinèa 2 du C.P.P.Fdispose que: ' S'il est préalablement avéré que ces données, accessibles à partir du système initial ou disponibles pour le système initial, sont stockées dans un autre système informatique situé en dehors du territoire national, elles sont recueillies par l'officier de police judiciaire, sous réserve des conditions d'accès prévues par les engagements internationaux en vigueur

[2]- During the execution of a search, investigating authorities should have the power, subject to appropriate safeguards, to extend the search to other computer systems within their jurisdiction which are connected by means of a network and to seize the data therein, provided that immediate action is required.available at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f6e76

[3]– **د. علي محمود علي حمودة** ، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، بحث مقدم ضمن أعمال المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية، أكاديمية شرطة دبي، في الفترة من 26 إلى 48-4-2003، ص44.

وتفتيش النظام المخزنة فيه المعلومات المطلوبة الذي يقع خارج مكان وجود النظام الأول يعتمد بشكل أساس على مسألتين مهمتين متلازمتين: أولا أن يكون الجهاز موصولا بمغذي الطاقة وفي حالة عمل والقول بغير ذلك يجعل من الدخول إليه والبحث عن المعلومات المطلوبة مستحيلا، ثانيا أن يكون النظام المخزونة فيه المعلومات متصلا بالشبكة[1].

الفرع الثاني

ضوابط تفتيش النظم المعلوماتية

يمكن تقسيم الضوابط العامة للتفتيش إلى ضوابط موضوعية وأخرى شكلية، ولايختلف الأمر في التفتيش الإلكتروني سواء إتخدت المعطيات محل التفتيش الشكل المادي أو الشكل الإلكتروني، وهو ما أكده المشرع الجزائري في المادة 3 من قانون الوقاية "...لمستلزمات التحريات أو التحقيقات القضائية الجارية وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون...القيام بإجراءات التفتيش"، وفيما يلي بيـــان لهذيـــن النـــوعين:

أولا-الضوابط الموضوعية لتفتيش النظم المعلوماتية

أ- سبب تفتيش النظم المعلوماتية

إن سبب التفتيش في الحالات التقليدية بوصفة إجراء من إجراءات التحقيق هو وقوع جريمة، وإتهام شخص أو أشخاص معينين بارتكابها أو المشاركة فيها، وتوافر إمارات قوية أو قرائن على وجود أشياء تفيد في كشف الحقيقة لدى المتهم أو غيره، وهو ما ينطبق على جرائم الإعتداء على التعاملات الإلكترونية على النحو التالـــــــي:

1-وقوع جريمة من جرائم الإعتداء على التعاملات الإلكترونية

حتى يكون التفتيش صحيح لا بد وأن تقع جريمة من جرائم التعاملات الإلكترونية مما يعتبرها القانون جناية أو جنحة، عملا بقاعدة "**لاجريمة ولاعقوبة إلا بنص**"،وقد سبق البيان أن جرائم الإعتداء على التعاملات الإلكترونية هي تلك التي تقع بالمخالفة لنظم التعاملات الإلكترونية المخاطبة الأشخاص الذين يتعاملون مع المعلومة النظامية والمستندات المعلوماتية القانونية، بدءا من إنتاجها إلى إستخدامها، فضلا عن أنظمة مكافحة الجرائم الإلكترونية، إذ هي تسير على نفس الخطى في الحماية من خلال الشق الجزائي، وقد إعتبرتها التشريعات المقارنة من الجنح المعاقب عليها بالحبس، ومن ثم فهي مما يجوز فيها إصدار إذن بالتفتيش.

[1]- د. **سامي جلال فقي حسين**، التفتيش في الجرائم المعلوماتية- دراسة تحليلية- دار الكتب القانونية، 2011، ص234.

ومع أن بعض التشريعات كالتشريع الجزائري تضمن تجريم بعض الإعتداءات التي تنال من التوقيع الإلكتروني من خلال قانون التوقيع والتصديق الإلكترونيين، كما جرم المساس بنظم المعالجة الآلية ضمن قانون العقوبات وعزّز هذه الحماية بموجب القانون رقم 09-04 والذي **وسع نطاق التفتيش** ولو عن بعد إلى كافة الجرائم المتصلة بتكنولوجية الإعلام والإتصال، ومع ذلك بقيت بعض الجرائم التي تمس التعاملات الإلكترونية خارجة عن نطاق التجريم، مثل سرقة المعلومات والتعدي على سلامة نظام التعاملات الإلكترونية كجريمة عمدية والمعالجة غير المشروعة للمعطيات الشخصية رغم الإملاء الدستوري في هذا الإطار، وهو ماقد يدفع البعض إلى محاولة ردها إلى إحدى النظم القانونية القائمة، إلاّ أن هذه الأخيرة **قد تكون من السعة بما يكفي لاستيعاب الظواهر الإجرامية المستحدثة**, وقد **لا تكون كذلك** فتضيق بها أو لا تستوعبها, ولا مناص حينئذ من إيجاد أنظمة قانونية جديدة لها.

أما المشرع المصري فلم يجرم جميع صور العدوان على التعاملات الإلكترونية، بل إقتصر في الحماية على أنواع معينة منها، ومن قبيل ذلك التوقيع الإلكتروني والمستند الإلكتروني من خلال قانون التوقيع الإلكتروني، وهو ما يتطلب المشرع سد هذا الفراغ التشريعي حتى يمكن القول بتحقق سبب التفتيش في حالة القيام به، فضلا عن تعديله قانون الإجراءات الجزائية لتتلائم وتفتيش نظم الحوسبة والإتصال على نحو ما فعل المشرع الجزائري والفرنسي.

2-إتهام شخص أو أشخاص معينين بارتكاب جريمة من جرائم الإعتداء على التعاملات الإلكترونية

إذ ينبغي أن يتوافر في حق المراد تفتيش شخصه أو مسكنه دلائل كافية تدعو للإعتقاد بأنه قد ساهم في إرتكاب جريمة من جرائم التعاملات الإلكترونية سواء بصفته فاعلا أصليا أو شريكا فيها. ويمكن القول أن تعبير الدلائل الكافية يقصد به مجموعة من القرائن أو الإمارات المعينة التي تقوم على المضمون العقلي والمنطقي لملابسات الواقعة، وكذلك على خبرة القائم بالتفتيش التي تؤيد نسبة تلك الجريمة إلى ذلك الشخص بوصفه فاعلا أوشريكا[1].

ومن التطبيقات على الدلائل الكافية، تحميل فيديوهات إباحية خاصة بالأطفال بإستعمال برنامج التحميل والتبادل والنشر edonkey ، ورابط أنترنت يخص الهاتف الثابث المسجل بإسم المدعوة (ب.م) ام المتهم الطبيب النفساني بوهران[2].

3-توافر إمارات قوية أو قرائن على وجود أشياء أو أجهزة أو معدات معلوماتية تفيد في كشف الحقيقة

التفتيش لا يتم إلا إذا توافرت لدى المحقق أسباب كافية على أنه يوجد في المكان أو لدى الشخص المراد تفتيشه أدوات إستعملت في جريمة من جرائم التعاملات الإلكترونية، أو أشياء متحصلة منها أو أية مستندات الكترونية يحتمل أن يكون لها فائدة في إستجلاء الحقيقة لدى المتهم أو غيره.[3]

---

[1]- **د. هلالي عبد الإله**، تفتيش نظم الحاسب الآلي، المرجع السابق، ص115.

[2]-المديرية العامة لأمن الوطني، أمن ولاية وهران، المصلحة الولائية للشرطة القضائية، محضر تفتيش إيجابي، 22 نوفمبر 2016، (حيازة مواد إباحية متعلقة بالقصر)، 2016. أنظـــر في ذلك ايضـــا:

United States v. Cervini, No. 00-6331, 2001 WL 863559 (10th Cir. July 31, 2001)

[3]-**د، حسين بن سعيد الغافري**، السياسة الجنائية في مواجهة جرائم الأنترنت، المرجع السابق ، ص381.

ب-محـــل التفتيش :

المحل الذي يقع عليه التفتيش للحصول على أدلة في جرائم التعاملات الإلكترونية هو النظام المعلوماتي أونظام المعالجة الآلية كنظام منفصل أو مجموعة من الأنظمة المتصلة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين، بما يشمل من مكونات، كالمخدمات والمضيفات والبرمجيات والملحقات التقنية الأخرى، فضلا عن المعطيات المعلوماتية والآثار الرقمية التي تم إحتواها سواء في داخل النظام المعلوماتي أو جزء منه أو على دعامة تخزين مستقلة، فضلا عن الشخص الذي يستخدم النظام موضوع التفتيش.

ولكي يتمّ التّفتيش على هذه المحال، فإنّه ينبغي الإشارة أنّ هذه الأخيرة لا تكون قائمة بذاتها، بل تكون إمّا موضوعة في مكان ما سواء عام أو خاص، أو تكون صحبة مالكها أو حائزها كما هو الشّأن في الحاسوب المحمول أو تلفون متصل بجهاز المودم أو بطاقة ذكية.

ويجب أن يتوفر في هذا المحل شرطان: الأول أن يكون المحل معينا وأن يكون مما يجوز تفتيشه، فبالنسبة للشرط الأول، فإن الإلتزام به صعب عمليا، وذلك لصعوبة التوصل إلى المعلومات أحيانا بسبب تداخل وتشابك الملفات التي تحتوي على هذه المعلومات، فيظطر القائم على التفتيش بإجراء بحث عام للتوصل إلى الدليل وهو ما ينتهك حق الخصوصية للأشخاص بالإطلاع على ملفات لا يشملها إذن التفتيش.

أما بالنسبة للشرط الثاني، فإن المشرع يستثني من التفتيش محلات معينة بسبب تعلقها بمصلحة معينة عامة كانت أو فردية يرى أنها أولى بالرعاية من مصلحة التحقيق التي تتطلب إجراء التفتيش[1]، مثل مقر البعثة الدبلوماسية والمبعوثين الدبلوماسيين، وأعضاء المجالس النيابية، فضلا عن حصانة مكاتب المحامين ومراسلاتهم بينهم وبين موكليهم، حتى لو توافرت شروط التفتيش بإستثناء أن يكون المحامي قد إرتكب الجريمة.

ففي الحالات السابقة، إن كانت تسري الحصانة على هؤلاء الأشخاص وتلك المحلات، فإنها تسري على نظم المعالجة الآلية وملحقاتها التابعة لهم.

وإن كنا قد ناقشنا ما تبقى من مسائل في ما سبق، إلا أنه في الواقع هناك سؤال يتبادر إلى الأذهان في موضوع التفتيش يتعلق**بمـــدى جواز تفتيش الإتصـــالات الإلكترونية؟**

مما لاشك فيه أن الدخول إلى المعطيات المخزنة في نظم المعالجة الآلية والمنظمة بنصوص التفتيش في إطار التحقيق قد لا تكون كافية في ضوء تطورين: الإستخدام المتزايد لبعض وسائط التخزين الخارجية بهدف عدم ترك أي معلومات على الكمبيوتر،وإستخدام الأجهزة من مقاهي الأنترنت[2]، وبناء عليه فإن المشرع الفرنسي وعلاوة على تنظيمه إعتراض المراسلات التي تتم عن طريق الإتصالات الإلكترونية وفقا للمادة 100 إجراءات، سمح بموجب المادة 706-102-1[3] اجراءات وما بعدها تحت عنوان "**إلتقاط**

[1]- د. **سامي جلال فقي حسين**، المرجع السابق، ص130.

[2]- https://www.senat.fr/rap/l09-517/l09-51723.html

[3]- **Article 706-102-1** Modifié par LOI n°2016-731 du 3 juin 2016 - art. 5 Si les nécessités de l'enquête relative à l'une des infractions entrant dans le champ d'application des articles 706-73 et 706-73-1 l'exigent, le juge des libertés et de la

المعطيات المعلوماتية" بوضع ترتيبات تقنية وذلك بغرض إلتقاط في الوقت الفعلي للمعطيات المعلوماتية، ويكون دلك بدون رضا الشخص، بالدخول في كل الأمكنة، في معطياته المعلوماتية، تسجيلها حفظها وتحويلها، سواء كانت ظاهرة على شاشة مستخدم نظام المعالجة الآلية أو مرسلة أو مستقبلة عبر وسائل سمعية بصرية بما في ذلك **المحادثات القصيرة عبر السكايب**[1].

وقد حدد نطاق تطبيق هذا الإجراء في جرائم عديدة نص عليها في المادة 706-73 و706-73-1 إجراءات من بينها السرقة المرتكبة في إطار جماعة منظمة، إتلاف الأموال في إطار جماعة منظمة، تزوير العملات، الإحتيال في إطار جماعة منظمة، الإعتداء على نظم المعالجة الآلية للمعطيات ذات الطابع الشخصي التي تنفذها الدولة والمرتكبة في إطار جماعة منظمة والمنصوص عليها في المادة 323—4-1 من قانون العقوبات.

وفي نفس الإتجاه، أجاز المشرع الجزائري إعتراض المعطيات في مرحلة النقل والتحويل بناء على أمر بذلك أثناء حدوثها، وذلك بتسجيل الإتصالات الإلكترونية التي تمثل أدلة إلكترونية اثناء عملية الإتصال داتها، بموجب المادة 4 من القانون 09-04، كما نصت عليها المادة 21 من اتفاقية بودابست.والمادة 29 من الإتفاقية العربية تحت عنوان "إعتراض معلومات المحتوى".

وللإطلاع على محتوى الرسائل أو الإتصالات وجب التمييز بين ثلاثـــــة فروض[2]:

الفــرض الأول: **إعتراض الإتصالات أثناء تبادلها:** ويتعلق الأمر هنا بمعطيات في طور الإنتقال وليس بمعطيات مسجلة أو مخزنة، ويلزم في هذه الحالة إتباع إجراءات أكثر صرامة وفقا للقوانين (المادة 4 من القانون رقم 09-04).

الفــرض الثاني:**تفتيش الإتصالات المخزنة في الجهاز الخادموذلك بعد وصولها أو وصول الرسالة الإلكترونية:** فبدون شك فإن هذه الإتصالات هي معطيات مخزنة، والدخول إليها في هذه الحالة يلزم توافر شروط التفتيش لفتح الجهاز للإطلاع عليها من قبل ضابط الشرطة القضائية، سواء المتعلقة بالمكان-إذا لم يكن التفتيش عن بعد[3]- أو الشخص.

---

détention peut, à la requête du procureur de la République, autoriser par ordonnance motivée les officiers et agents de police judiciaire requis par le procureur de la République à mettre en place un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles sont stockées dans un système informatique, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données, telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques audiovisuels.

Le procureur de la République peut désigner toute personne physique ou morale habilitée et inscrite sur l'une des listes prévues à l'article 157, en vue d'effectuer les opérations techniques permettant la réalisation du dispositif technique mentionné au premier alinéa du présent article. Le procureur de la République peut également prescrire le recours aux moyens de l'Etat soumis au secret de la défense nationale selon les formes prévues au chapitre Ier du titre IV du livre Ier.

[1]- **Thierry Vallat**, Surveillance informatique: captation des données s'affichant à l'écran en temps réel avec le décret du 18 décembre 2015, disponible en lingne á l'adresse suivante https://translate.google.dz/?hl=fr#fr/ar/bref%20y%20

[2]-**د. شيماء عبد الغني**، المرجع السابق، ص308.

[3]- تقيم أحكام القضاء التماثل بين مراسلات البريد الإلكتروني والمراسلات التي تتم عن طريق البريد العادي، وبناء عليه لا يجوز التداخل للإطلاع على البريد الإلكتروني دون إذن صاحبه، مالم يصدر إذن قضائي بذلك، تطبيقا لذلك قضي بعدم مشروعية الدليل في الولايات المتحدة الأمريكية بالنسبة للمتهم maxiwell الذي كان يحوز صورا فاضحة خاصة بالأطفال إستنادا إلى أن رجال الضبط القضائي لجأوا إلى مزود الخدمات الخاص بهذا المتهم، لكي

وقد كرست التوصية رقم R95-13 الصادرة من المجلس الأروبي هذا المعنى بنصها على أنه يجب إقامة التمييز بين تفتيش المعلومات المخزنة وضبطها وبين إعتراض تلك المعلومات عند إنتقالها[1].

الفــرض الثالث: **الإتصال بشبكة عامة:** أي يسمح لعدد غير محدود من الأفراد بالإتصال بها حتى ولو كان ذلك نظير دفع رسم معين، وفي هذه الحالة لا يلزم الحصول على إذن كون أن الإتصال لا يعد لا من قبيل الإعتراض أو الإلتقاط ولا من قبيل التفتيش بل هو من قبيل التحريات التي يجوز القيام بها من قبل الضابط[2].

وجدير بالملاحظة أنه يتعين التمييز بين الوسائل التقنية التي من شأنها الإطلاع على جهاز المتهم وهو مغلق لا يستخدمه في الإتصال كالوضع بالنسبة لوسيلة key logger system، و بين الحالة التي فيها يتم التنصت على إتصالات المتهم عند قيامه بها كما في حالة إستعمال برنامج يسمى المفترس carnivore، والذي يتيح إلتقاط الرسائل عند تداولها[3]، ففي الحالة الأولى يكفي إصدار إذن بالتفتيش، أما في الحالة الثانية فيتعين الإلتزام بالشروط التي يتطلبها القانون بالنسبة لمراقبة الإتصالات الإلكترونية.

ت-السلطة المختصة بتفتيش النظم المعلوماتية:

جعل المشرع الإجرائي الإختصاص بالتفتيش إجراء تحقيق لقاضي التحقيق في بعض الدول كفرنسا والجزائر، وللنيابة العامة بصفة أصلية ولقاضي التحقيق في حالات خاصة في مصر، ولا يتولى عضو الضبط القضائي التفتيش إلا في حالات معينة لا يتعداها:

1- **حالة التلبس**[4]: تقر الشريعات على إختلاف توجهاتها حالة التلبس وترتب عليها جواز التفتيش بدون سبق الحصول على إذن بذلك، وإن كانت تختلف فيما بينها حول مدى جواز تفتيش المساكن بناء على حالة التلبس، وهو مالا يجيزه المشرع الجزائري وذلك إعمالا للمادة 47 من الدستور، والمشرع المصري إعمالا للمادة 50

يساعدهم على الدخول إلى بريده الإلكتروني والتعرف على ما يحوزه من تلك الصور، ومعرفة من يتعامل معهم في هذه الصور وذلك دون سبق الحصول على إذن قضائي بذلك.

Usc, Maxwell 45 m.j 406(1996): cited by **René PÉPIN**, Le statut juridique du courriel au Canada et aux États-Unis, Lex Electronica, vol. 6, n°2, Hiver / Winter 2001, disponible en lingne á l'adresse suivante http://www.lex-electronica.org/files/sites/103/6-2_pepin.pdf

[1]-The legal distinction between searching computer systems and seizing data stored therein and intercepting data in the course of transmission should be clearly delineated and applied.
Recommendation No. R (95) 13 of the Committee of Ministers to member states concerning problems of criminal procedural law connected with information technology adopted on 11 September 1995,

[2]- قضي بأن الإتصال بشبكة الميناتل (شبكة داخلية خاصة بفرنسا) من جانب رجل الضبط وقراءته للرسائل المتاحة لكل مستخدمي هذه الشبكة لا يشكل تنصتا في مفهوم المادة 100 من قانون الإجراءات الجزائية.

Ne constitue pas, au sens des articles 100 et suivants du Code de procédure pénale, une interception de communications émises par la voie télématique le fait, pour un enquêteur, de se connecter à un tel réseau au moyen d'un terminal mis à la disposition du public par l'opérateur, sans modification préalable de l'installation, aux fins de lire les annonces offertes par tel ou tel service. chambre criminelle Cour de cassation N° de pourvoi: 00-80829 Audience publique du 25 octobre 2000 ; bull;crim, n317

[3]-**د. شيماءعبد الغني**، المرجع السابق، ص258.

[4]-راجع المادة 44 و 45 من قانون الإجراءات الجزائية الجزائري.

من الدستور، على خلاف المشرع الفرنسي الذي أجازه بدون إذن بمقتضى المادة 56 من قانون الإجراءات الجزائية[1] ، أما في القانون الأمريكي فإن حالة التلبس تجيز الضبط ولاتجيز تفتيش المسكن[2].

وتطبيقا لذلك، إذا ضبط الشخص في حالة التلبس أمكن تفتيشه وتفتيش حاسوبه المتواجد بحوزته أو منظومة تخزين معلوماتية كالبطاقة الذكية المخزن فيها المفتاح الشفري الخاص أو قرص مضغوط يحمل برنامج لفك شفرة التوقيع الإلكتروني، وذلك سواء في القانون الجزائري أو القانون الفرنسي، إذ أن حالة التلبس تجيز القبض والقبض يجيز التفتيش[3]. كذلك هو الشان في القانون المصري، وإن كان يقتصر التفتيش وفق أحكامه على الأشياء المادية لعدم وجود معالجة تشريعية فيما يخص تفتيش المنظومة المعلوماتية والمعطيات المخزنة فيها.

أما إذا كان هذا الحاسوب متواجدا في مسكن المتهم، فإنه يلزم في هذه الحالة صدور إذن قضائي للتفتيش وفقا للقانون الجزائري والمصري.

وغالبا ما يصدر الإذن[4] بتفتيش مسكن المتهم أن ينصرف هذا الإذن إلى كل ما يتواجد في المسكن، وتطبيقا لذلك إذا صدر إذن بتفتيش مسكن في اطار الجرائم محل الدراسة فمن حق ضابط الشرطة القضائية أن يقوم بتفتيش أجهزة الكمبيوتر المتواجدة في المسكن، مادام أن ذلك يفيد في كشف الحقيقة عن الجريمة التي صدر الإذن بخصوصها، ولكن عندما يقوم ضابط الشرطة القضائية بتفتيش الكمبيوتر فإن عليه أن يلتزم بالبحث عن الحقيقة في التهمة التي صدر الإذن بشأنها، كما لو كان صادرا للتفتيش عن جريمة حيازة معطيات إنشاء توقيع إلكتروني موصوف خاص بالغير.

وفي هذا الصدد، أجاز المشرع الجزائري للسلطات القضائية المختصة ولضباط الشرطة القضائية الدخول بغرض التفتيش **ولو عن بعد:** إلى منظومة معلوماتية أو جزء منها، وكذا المعطيات المعلوماتية المخزنة فيها، فضلا عن منظومة تخزين معلوماتية بموجب المادة 5 من القانون رقم 09-04 ،فكما هو ملاحظ فإن صيغة النص لا تسمح بتفتيش الحاسوب أو المعطيات أو أي منظومة تخزين معلوماتية تبعا لتفتيش الأشخاص والأماكن فحسب، بل تمتد لتشمل التفتيش عن بعد داخل الإقليم الوطني وخارجه، ويشمل ذلك التفتيش في حالة الجريمة المتلبس بها.

إلا أنه من بين المشاكل المثارة في **الإذن بصـــفة عامـــــة** الصادر في مجال تفتيش النظم المعلوماتية، أنه ثمة صعوبة في إحترام الشرط الخاص بتحديد محل التفتيش فيه، ذلك أن هذه النظم تحوي

---

[1]-**Article 56 du CPF** Modifié par LOI n°2016-731 du 3 juin 2016 - art. 58 dispose que "Si la nature du crime est telle que la preuve en puisse être acquise par la saisie des papiers, documents, données informatiques ou autres objets en la possession des personnes qui paraissent avoir participé au crime ou détenir des pièces, informations ou objets relatifs aux faits incriminés, l'officier de police judiciaire se transporte sans désemparer au domicile de ces derniers pour y procéder à une perquisition dont il dresse procès-verbal."

[2]- د. **شيماء عبد الغني**، المرجع السابق، ص336.

[3]– أنظر المادة 51 والمادة 42 من قانون الإجراءات الجزائية الجزائري، والمادة 34 و36 من قانون الإجراءات الجزائية المصري.

[4]– لقد تدخل المشرع الجزائري بموجب القانون رقم 06-22 وأضاف الفقرة 3 التي تناولت المعطيات الواجب ذكرها في الإذن : وهي بيان وصف الجرم موضوع البحث عن الدليل، وعنوان الأماكن التي ستتم زيارتها وتفتيشها وإجراء الحجز فيها، وذلك تحت طائلة البطلان.

الكثير من الملفات، ومن الممكن أن تكون المعلومات محل التفتيش غير معروفة الموقع داخل الحاسوب المراد تفتيشه، ففي هذه الحالة يمكن للقائم بالتفتيش العثور على هذه المعلومات المخزنة إذا عرف إسم الملف المخزونة فيه المعلومات، إذ يتم إيجادها عن طريق البحث العام عن الملف، حيث يتم إدخال إسم الملف ونوعه ويتم البحث عنه تلقائيا من قبل الحاسوب ولكن هذه الطريقة تكون مستحيلة إذا كان القائم بالتفتيش لا يعرف إسم الملف أو نوعه، وهنا يثار التساؤل التالي: **هل يجوز تفتيش جميع الملفات المخزنة بهدف إيجاد الملفات المطلوبة والمخزونة فيها المعلومات التي يجري البحث عنها؟** فهل يعد هذا خروجا عن حدود الإذن بالتفتيش الأمر الذي يصم الإجراءات بالبطلان؟

يرى البعض من الفقه[1] أنه وإن كانت تقضي القواعد العامة تحديد محل التفتيش تحديدا دقيقا كونه من الإجراءات الماسة بالحرية الشخصية للأشخاص وحرمة المساكن، إلا أن هذه القاعدة لا تنطبق على التفتيش الإلكتروني، ويقيسون عملية البحث عن الملفات المطلوبة داخل النظام على التجوال داخل غرفة المنزل للعثور على الدليل جاري البحث عنه. وقد أيد القضاء الأمريكي التفتيش العام بحثا عن الملفات المطلوبة، في قضية runyan عام 2001 حين قررت الدائرة الإستئنافية الخامسة "*أن الشرطة لا تتجاوز البحث و التفتيش الخاص حال فحص المزيد من الأشياء داخل حاوية مغلقة أكثر مما يفعل المفتش الخاص*"[2].

ونؤيد ما ذهب إليه الفقه والقضاء الأمريكي، فإذا كان لا يعقل أن يصدر إذن التفتيش بعدد الملفات الموجودة داخل الحاسوب كون هذا الأخير ونظرا للسعة التخزينية المتعددة لقرصه الصلب يمكن أن يحوي ضمن ملف واحد العديد من الملفات، وما يعقد المسالة أكثر تحديد مواضع الملفات التي تحتوي على أدلة تفيد في كشف الحقيقة كون أن أسماءها لاتدل بالضرورة على ماتحتويه.

ومن جهة أخرى، ومن المباديء المقررة أن إذن التفتيش يصدر بخصوص جريمة معينة، مثلا جريمة إختراق موقع مما يعني السعي هنا يكون وراء الحصول على ما يفيد في إطار هذه الجريمة، إذا قام رجل الضبط القضائي بتفتيش أشياء لم يحددها الإذن الصادر بالتفتيش، فإن ذلك يجعل التفتيش باطلا، وذلك إستنإذا إلى أن القائم بالتفتيش قد خالف الإذن بالتفتيش، ويسمى القانون الأمريكي تلك الحالة **بالمخالفة الواضحة للإذن**[3].

وعليه نقترح وضع نص قانوني ينص على جواز تفتيش جميع الملفات في حال عدم معرفة اسم الملف أو مكان وجوده. لكن ماذا لو أن الضابط وحين فحصه للملفات فوجد عرضا ملفات تحوي جريمة.

---

[1]- **أسامة أحمد المناعسة وآخرون**، المرجع السابق، ص279.**سامي جلال فقي حسين**، المرجع السابق، ص230.

[2]-USA v. Runyan, 275 f,3d 449, 464-65(5th Cir.2001)

مشار إليه لدى: **د.عمر بن يونس**،الإجراءات الجنائية عبر الأنترنت في القانون الأمريكي، المرشد الفدرالي الأمريكي لتفتيش وضبط الحواسيب وصولا إلى الدليل الإلكتروني في التحقيقات الجنائية،دون دار نشر، 2008، ص61.

وفي نفس الاتجاه قررت الدائرة العاشرة الفدرالية أن الحواسيب والملفات *files* ليست كونتينيرات مغلقة *closed containers* وبالتالي لا تتطلب إذن تفتيش *searchwarran*tخاص.

USA, v, Simpson, 152f.3d 1241 (10th CIR. 1998)

مشار إليه لدى: **د. عمرمحمد بن يونس**،أشهر المبادئ المتعلقة بالأنترنت في القضاء الأمريكي، الطبعة الأولى، دار أكاكوس، 2004، ص953.

[3]– **د. شيماء عبد الغني**، المرجع السابق، ص292.

في هدا الصدد كرس المشرع الجزائري شرعية معاينة الجرائم المكتشفة ولو لم تذكر في الإذن، حيث نصت المادة 44 الفقرة الأخيرة من قانون الإجراءات الجزائية ***"إذا اكتشفت اثناء هذه العمليات جرائم اخرى غير تلك التي ورد ذكرها في اذن القاضي فان ذلك لا يكون سببا لبطلان الإجراءات العارضة ،"***بمعنى أن الجرائم الجديدة لتي تم إكتشافها عرضا والغير معلنة بالإذن يمكن إخطار بها وكيل الجمهورية أو قاضي التحقيق حسب الأحوال ليتخذ ما يراه بشأنها.

نخلص مما سبق أن تنفيد الإذن في المسائل الإلكترونية يخضع لعدة قواعد، بعضها يستمد من القواعد العامة مع تطويعها لكي تتلائم مع تلك المواد، والبعض الآخر يجب أن يراعى فيه ما للتفتيش في البيئة الإلكترونية من ذاتية.

2- الإنـــــــابة: فضابط الشرطة القضائية الذي يكون مفوضا من قبل المحقّق المختصّ بموجب إنابة قضائية يمكن أن يباشر التفتيش في جميع الأماكن، ومنها المساكن التي يمكن العثور فيها على أشياء أو وثائق تفيد التحقيق وإظهار الحقيقة[1]. وقد تتلازم حالة التلبس مع حالة الندب، فلو أن ضابط الشرطة القضائية ندب لتفتيش شخص فوجده عرضا حائز على أشياء تعد حيازتها جريمة قائمة بداتها، ففي هذه الحالة يعتبر صاحبها في حالة تلبس، وتطبيقا لذلك قضى بأن الأمر بالتفتيش لا يمنع البحث وإكتشاف أشياء أخرى أو بضاعة مهربة[2].

ولصحة أمر الندب أو الإنابة القضائية لا بد أن يخضع لعدة قواعد من بينها: أن يكون مكتوبا وموقعا، ولا يوجد ما يمنع من تطبيقها في مجال التفتيش، إلا أن تبليغه في مجال هذه الجرائم تحقيقا للسرعة قد يتم عن طريق الفاكس أو الأنترنت ويتم التفتيش بموجبه إلى أن يتم إرسال النسخة الأصلية[3].

فالإنابة للتفتيش تحتاج للسرعة، وبالمقابل فقد يكون الشخص الذي يتم إنابته في مكان غير المكان الذي يتواجد فيه قاضي التحقيق، وبالتالي يمكن إرسال نسخة من أمر الإنابة بالطريق الإلكتروني، عن طريق البريد الإلكتروني مثلا، وهو ما تضمنته المادة 9 من قانون عصرنة العدالة، حيث أجازت إرسال الوثائق والمحررات القضائية والمستندات بالطريق الإلكتروني.

على أن تضمن الوسائل الإلكترونية المستعملة في إرسال الوثائق بالطريق الإلكترونية: التعرف الموثوق على أطراف التراسل الإلكتروني، سلامة الوثائق المرسلة، أمن وسرية التراسل، حفظ المعطيات بما يسمح بتحديد تاريخ الإرسال والإستلام من طرف المرسل إليه بصفة أكيدة.

ويمكن في هذه الحالة إعتبار أمر الإنابة المرسل بالطريق الإلكتروني بمثابة وثيقة أصلية إذا أعدت وفق الشروط السابقة.

---

[1]- راجع المادة 138 والمادة 81 من قانون الإجراءات الجزائية الجزائري.

[2]- قرار رقم 13 955 بتاريخ 1993/02/12 عن الغرفة الجزائية، أشار له أ. **يوسف دلاندة**، قانون الإجراءات الجزائية، دار هومة، الجزائر، 2001، ص 46.

[3]- **د. علي حسن الطوالبة**، المرجع السابق، ص110.

ثانيا- الضوابط الشكليـــة لتفتيش النظم المعلوماتية

وتتمثل هذه الضمانات فيمايلـــي:

أ- قاعدة الحضـــــــور:

إستقرت غالبية التشريعات على عدم إشتراط صحة تفتيش الأشخاص حضور الشهود، إلا أنها لم تسر على وتيرة واحدة فيما يخص تفتيش المنازل وما في حكمها، ففي حينإشترط كل من المشرع الفرنسي والجزائري حضور شاهدين أثناء إجراء تفتيش مسكن المتهم سواء كان القائم به قاضي التحقيق أو ضابط الشرطة القضائية، وذلك بعد تعذر حضور المتهم وقت ذلك الإجراء وإمتناعه عن تعيين ممثل له أو هروبه[1]، غاير المشرع المصري في الضمانات المقررة وفقا للشخص القائم به، حيث إشترط حضور شاهدين في حالة ما إذا كان التفتيش يباشر بمعرفة أحد مأموري الضبط القضائي، وعلى أن يكون هذان الشاهدين بقدر الإمكان من أقارب المتهم البالغين أو من القاطنين معه بالمنزل أو من الجيران[2]، أما إذا كان القائم بالتفتيش هو قاضي التحقيق أو عضو النيابة العامة، فيصح إتخاذ الإجراء دون حاجة إلى إستدعاء شهود، ويستوي الأمر عند قيام عضو الضبط القضائي بمباشرة التّفتيش بنا على ندبه لذلك من سلطة التّحقيق، فلا يلتزم باستدعاء الشهود لأنّ المندوب يحلّ محل النائب تمامًا.

بالرغم من أن القصد من قاعدة الحضور باعتباره شكل جوهري في منطق القانون والواقع، هو ضمان الإطمئنان إلى سلامة الإجراء وصحة الضبط، يترتب على مخالفتها البطلان، فإن إلتقيد بهذه القاعدة قد يشكل في الحقيقة عائق حقيقي يحول دون ضبط الأدلة التي تفيد في كشف الحقيقة، نظرا للطبيعة الخاصة للدليل المستوحى من الوسط التقني، حيث يسهل التلاعب فيه من قبل المتهم عن بعد سواء تعديلاً أو إتلافاً بسرعة متناهية بهدف طمس معالم الجريمة أو أيّ عنصر إثباتي لشخصيّة.

وإدراكا من المشرع الجزائري لذلك، عاد بموجب الفقرة الأخيرةمن المادة 45إجراءات[3] وإستثنى من تطبيق أحكام المادّة السّابقة -فيما يخصّ حضور الأشخاص المحدّدين في الفقرة الأولى من هذه المادّة_ عدّة جرائم ومن بينها جرائم المساس بنظم المعالجة الآلية للمعلومات، وقد كان ذلك بموجب التعديل الذي ألحقه على قانون الإجراءات الجزائية بموجب القانون رقم 06-22 المعدل والمتمم لقانون الإجراءات الجزائية.

ب-الميقات الزمني لإجراء التفتيش:

---

[1]- أنظر المادة 45 من قانون الإجراءات الجزائية الجزائري، والتي هي ترجمة حرفية للمادة 56 إجراءات فرنسي.

[2]-أنظر المادة 51 من قانون الإجراءات الجزائية المصري.

[3]- تنص الفقرة الأخيرة من المادة 45 من قانون الإجراءات الجزائية على أنه: " لا تطبق هذه الأحكام إذا تعلق الأمر بجرائم المخدرات و الجريمة المنظمة عبر الحدود الوطنية و الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و جرائم تبييض الأموال و الإرهاب و الجرائم المتعلقة بالتشريع الخاص بالصرف, **باستثناء الأحكام المتعلقة بالحفاظ على السر المهني** وكذا جرد الأشياء وحجز المستندات المذكورة أعلاه".

قد يحضر المشرع إجراء تفتيش المساكن في وقت معين، إمعانا في الحرص على تضييق مجال الإعتداء على الحرية الفردية، وكعنصر من عناصر تحقيق الموازنة بين حق المجتمع وحقوق الأفراد. فتنص المادة 47 من الدستور الجزائري تضمن الدولة عدم انتهاك حرمة المسكن فلا تفتيش إلا بمقتضى القانون وفي إطار إحترامه"، كما نص الدستور الفرنسي مند البداية على أن منزل كل مواطن يقطن الإقليم الفرنسي ملجأ حصين، لايجوز دخوله ليلا إلا في حالات الحريق أو الغرق أو الإستغاثة[1]"

وإستقرت تلك القاعدة في القانون الفرنسي، وجاءت الفقرة 1 من المادة 59 من قانون الإجراءات الجزائية[2] فاعتنقت قاعدة عدم جواز تفتيش المنازل ليلا،حيث حدّده من الساعة السادسة صباحًا إلى السّاعة التّاسعة مساءاً, والحكمة من ذلك من هذا القيد أن المواطنين ينبغي عدم إزعاجهم ليلا، فإذا خالف المحقق هذه القاعدة عد مرتكبا لجريمة إنتهاك حرمة المسكن.

ويبدوا أن المشرع الفرنسي لم ينفرد في إتجاهه التشريعي على النحو السابق بيانه، إذ نجد المشرع الجزائري بدوره حظر إجراء التفتيش ليلا، وحدده من الساعة الخامسة صباحاً إلى الساعة الثامنة مساءاً، وذلك من خلال المادة 47 إجراءات جزائية[3].

ومثل هذا الأمر ليس مطلقا في التشريعات، إذ يمتنع المشرع عن حظر إجراء التفتيش ليلا، فيترك للقائم بالتفتيش تحديد الوقت المناسب للقيام به، كما هو شأن المشرع المصري.

القاعدة إذن، في القانون الفرنسي والجزائري، أنه لا يجوز دخول المساكن وتفتيشها أثناء الليل، وإن كان بالإمكان بمحاصرة المنزل وحراسة منافده ومراقبته من الخارج حتى يبزغ النهار تجنبا لهرب المتهم أو تهريب الأشياء المراد ضبطها.

وإن كانت تلك هي القاعدة العامة –وعلى خلاف المشرع الفرنسي– فقد إستثنى منها المشرع الجزائري عدة حالات[4]يصحّ فيها إجراء التّفتيش ليلاً أو نهارًا, ومن هذه الحالات **الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات**، فتنص الفقرة 3 من المادة 47 إجراءات جزائري المضافة بموجب القانون رقم 06–22 المعدل والمتمم للأمر رقم 66–155 والمتضمن قانون الإجراءات الجزائية على أنه "*وعندما يتعلق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنية* ***أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات*** *و جرائم تبييض الأموال و الإرهاب و كذا الجرائم المتعلقة بالتشريع الخاص بالصرف فإنه يجوز إجراء التفتيش و المعاينة و الحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل و ذلك بناء على إذن مسبق من وكيل الجمهورية المختص*".

---

[1]- المادة 67 من دستور 22 فريمير للسنة الثانية، مشار إليه لدى: **د. سامي حسني الحسيني**، المرجع السابق، ص294.

[2]-**Article 59 du CPPF** Modifié par Loi 93-1013 1993-08-24 art. 20 JORF 25 août 1993 en vigueur le 2 septembre 1993 dispose que" Sauf réclamation faite de l'intérieur de la maison ou exceptions prévues par la loi, les perquisitions et les visites domiciliaires ne peuvent être commencées avant 6 heures et après 21 heures.**"**

[3]– تنص المادة 47 إجراءات جزائية جزائري على أنه " *لا يجوز البدء في تفتيش المساكن أو معاينتها قبل الساعة الخامسة صباحا، ولا بعد الساعة الثامنة مساءا، إلا إذا طلب صاحب المنزل أو وجهت نداءات من الداخل أو في الأحوال الاستثنائية المقررة قانونا*".

[4]– وهذه الحالات هي: طلب صاحب المسكن المقيم به، حالة الضرورة، تفتيش الفنادق والمساكن المفروشة، بمناسب جرائم معينة كجرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنية، الدخول للمسكان بغرض تنفيذ العمليات المقررة في المادة 65 مكرر .

إن في إستثناء المشرع الجزائري للجرائم الواقعة على النظم المعلوماتية بمختلف تطبيقاتها من حظر التفتيش ليلا له ما يبرره من الناحية العملية، ذلك أن المعطيات موضوع التفتيش قد تكون عرضة للفقد والطمس الكلي من قبل الفاعل وفي زمن قصير جدا، وبالتالي فإن تأخير إجراء التفتيش قد يؤدي إلى زوال الدليل في حد ذاته، ويدق المشكل أكثر إذا ماكان هذا الدليل هو الوحيد في الدعوى.

فضلا عن ذلك، فإن هذه الضّمانة بدأت تتضاءل أهمّيتها مع ظهور ما يسمى بـــ "التّفتيش عن بعـــد"، أو مـــا يطلق عليها في الفقه الفرنسي مصطلح التّفتيش على المباشر *Perquisition en ligne*[1] والذي يساهم تطبيقه في إختصار زمن الإجراء الذي يستغرق وقتاً طويلاً في العادة وملاءمته مع زمن الشبكات الذي يتم لحظيـــاً، خاصة إذاكانت المعطيات المبحوث عنها مخزنة لدى مؤدي خدمة أجنبي، فاختلاف التوقيت الدولي يمكن أن يؤدي إلى أن الجريمة التي تقع في الجزائر أو تبدأ منها تكون خارج الساعات المسموح بها قانوناً للتفتـــيش، ومن هنا يكون من غير المسموح إتخاذ الإجراءات التي من شأنها وقف هذه الجرائم[2]. إلا أن الأخـــذ بـــذلك يستلزم موافقة سلطات البلد المعني ووفقاً للإجراءات المعقدة للتعاون القضائي.

وتجدر الإشارة، إلى أن التوسع في إختصاص الضابط في الدخول والتفتيش والضبط في أي وقت حسب المادة 47 إجراءات مرهون بشرطين:

-أن يتعلق الأمر باحدى الجرائم الخطيرة، ومنها جرائم الإعتداء على نظم المعالجة الآلية.

-أن يأذن وكيل الجمهورية المختص بذلك، أو أن يصدر قاضي التحقيق أمرا لضباط الشرطة القضائية للقيام بتلك الإجراءات[3].

ذلك كان عن الجرائم الماسة بنظم المعالجة الآلية المنصوص عليها في القسم السابع من قانون العقوبات، أماّ بخصوص بقية الجرائم الماسة بالتعاملات الإلكترونية، فإنّه وعملاً بالأحكام العامة تسري عليها القواعد العامة الخاصة بالجرائم التقليدية التي تحدد الفترة الزمنية لإجراء التفتيش، ولذلك فحبذا لو يتدخل المشرع وينص على الإستثناء الخاص بالتوقيت ليشمل جميع الجرائم التي تقع في الوسط الإلكتروني.

أما الوضع في التشريع الفرنسي، فقد حدده هدا الأخير من خلال إتفاقية بودابست في المادة 19 التي أقرت أن جميع المعطيات يتم تفتيشها خلال الفترة الزمنية المقررة للتفتيش، أي أنه يتم من السادسة صباحا إلى التاسعة ليلا.

ت-محضر التفتيـــش:

1-Nicole Spoerhase-Eisel,:La perquisition en ligne et la surveillance d'Internet sont illicites; disponible en lingne á l'adresse suivante http://merlin.obs.coe.int/iris/2008/4/article15.fr.html

[2]-**صالح أحمد البربري**، المرجع السابق، ص9.

[3]-**د. عبد الله أوهايبه**، المرجع السابق، ص273.

القاعدة أن أعمال التحقيق جميعا ينبغي إثباتها بالكتابة، ويطلق على المحرر الرسمي المثبت لهذه الأعمال إصطلاح المحضر، والمحضر هو المحرر الذي يثبت فيه موظف عمومي شهادة من الأعمال التي تمت في حضوره أو تلك التي باشرها بنفسه، ومن ثم فالمحضر هو الشهادة المكتوبة التي يعلن بمقتضاها القائم بالتفتيش ماشاهده من وقائع، وما إتخده في شأنها من إجراءات وما توصل إليه من نتائج[1].

ولما كان التفتيش عملا من أعمال التحقيق، فينبغي تحرير محضر به، يثبت ما تم من إجراءات بشأنه، وما أسفر عنه من أدلة. وتجب لصحته أن تتوافر فيه الشروط الشكلية العامة في جميع المحاضر، وأهمها وجود المعطيات الجوهرية كإسم محرر المحضر وتوقيعه ومكان تحرير المحضر وزمانه والمعطيات المتعلقة بموضوع المحضر[2].

وفيما يتعلق بمحضر تفتيش النظم المعلوماتية فإنه يلزم بالإضافة إلى الشكليات السابقة ضرورة إحاطة رجل الضبط القضائي المأذون بالتفتيش بتكنولوجيات الإعلام والإتصال، ولما كانت الجرائم التي تقع في محيط الوسائل الإلكترونية تتميز بطبيعة فنية متأثرة في ذلك بالطبيعة الفنية للعمليات الإلكترونية، فإن هذا الأمر يزيد من أهمية الخبراء ومساعدتهم في صياغة مسودة المحضر. فضلا عن المحافظة على الأدلة المتحصلة عليها من كل تلف أو مسح للمعطيات.

من خلال ما سبق، نخلص إلى أن المشرع الجزائري وإدراكا منه لخصوصية الجرائم الواقعة على نظم المعالجة الآلية إستثنى تطبيق بعض ضوابط التفتيش، ليبقي **على شرط الحصول على الإذن وإحترام السر المـــهني.**

الفرع الثالث

النتائج المترتبة على التفتيش الصحيح للنظم المعلوماتية

يهدف التفتيش إلى ضبط الأدلة المادية التي تفيد في كشف الحقيقة، فالضبط هو غاية التفتيش القريبة أي الأثر المباشر الذي يسفر عنه هذا الإجراء، ومن ثم فهو إجراء من إجراءات التحقيق، تنطبق بشأنه ذات القواعد التي تنطبق بشأن التفتيش ذاته، ويؤدي بطلانه إلى بطلان الضبط[3].

والضبط كإجراء من إجراءات التحقيق هو "وضع اليد على الشيء واستبقاؤه تحت تصرف المحقق لمصلحة التحقيق"[4].

ومادام أن الضبط أثرا مباشرا للتفتيش، فينبني على هذا الإرتباط نتيجتان هامـــتان:

---

[1]– **د. سامي حسني الحسيني**، المرجع السابق، ص377، **د. توفيق محمد الشاوي**، المرجع السابق، ص408.

[2]– **د. توفيق محمد الشاوي**، المرجع السابق، ص408.

[3]–**د. سامي حسني الحسيني**، المرجع السابق، ص302.

[4]– **د. توفيق محمد الشاوي**، المرجع السابق، ص41.

الأولـــى: أن الضبط لايجوز أن يقع على شيء إلا بوصفه دليلا من أدلة الجريمة التي يجري التفتيش بشأنها، فالتفتيش هو الشاهد المادي فيما يقع عليه الضبط، ولما كان التفتيش لايصح إلا بصدد البحث عن أدلة جريمة معينة، هي الجريمة الجاري حصول التحقيق بشأنها، فكذلك الضبط، أساسه القانوني هو العلاقة التي تربط بينه وبين الأشياء المتعلقة بالجريمة التي يشملها التحقيق، ومن تم وجب أن تكون ثمة علاقة بين السلوك الإجرامي وبين الدليل الإجرامي.

الثانيـــة: أنه لما كان التفتيش يجري للكشف عن الحقيقة المجردة، سواء تمثلت في إدانة المتهم أو في برائته، فإنه ينبغي ألا يقتصر الضبط على الأشياء التي قد تؤدي إلى إدانة المتهم فحسب، بل لابد أن ينصب أيضا على الأشياء التي تفيد في كشف الحقيقة جميعا وإن أدت إلى تبرئة المتهم[1].

وتجدر الإشارة إلى أن التشريعات الجزائية عادة ما تجمع بين أحكام الضبط والتفتيش في موضع واحد، ولكن ليس معنى ذلك أن الضبط لا يحصل دون تفتيش، إذ يجوز أن تضبط الأشياء التي قدمها المتهمون أو الشهود بإختيارهم، ومن ثم يكون هذا الإجراء منفصلا عن التفتيش في ذاتيته وأحكامه، كما قد يكون نتيجة لمعاينة.

وفي نطـــــاق التفتيش:

- يصح لضابط الشرطة القضائية ضبط الأشياء التي تظهر عرضا أثناء التفتيش وتعد حيازتها جريمة، وهذا النوع من الضبط لا يحتاج إلى نص يقرره، فقيام حالة التلبس يجعل الضابط من واجبه أن يضبط ما كشف عنه التفتيش عرضا [2].
- لا يجوز ضبط غير الأشياء والوثائق النافعة في إظهار الحقيقة أو التي قد يضر إفشاؤها بسير عملية التحقيق، فتنص المادة 84 إجراءات جزائري على وجوب إحصاء الأشياء والوثائق المضبوطة فورا ووضعها في أحراز مختومة، وإدا تعلق الأمر بضبط نقود أو سبائك أو أوراق تجارية ذات قيمة مالية، جاز لقاضيالتحقيق التصريح للكاتب بإيداعها في الخزينة العامة، مالم يكن الإحتفاظ بها من ضرورات التحقيق لإظهار الحقيقة أو المحافظة على حقوق أطراف الدعوى، وإذا تم القيام بفك أو فض أو فتح تلك الأحراز فإن العملية يجب أن تتم بحضور المتهم مصحوبا بمحاميه، أو بعد إستدعائهما قانونا، وكذلك حضور كل من ضبطت لديه تلك الأشياء والأوراق أو المستندات، ويجوز لكل من يعينه الأمر الحصول على نفقته على نسخة أو صورة فوتوغرافية من الوثائق والمستندات المضبوطة، مالم تكن مقتضيات التحقيق تمنع ذلك، كما تنص المادة 55 والمادة 91 إجراءات مصري لمأموري الضبط القضائي أو قاضي التحقيق أن يضبط الأوراق والأسلحة وكل ما يحتمل أن يكون قد أستعمل فى إرتكاب الجريمة أو نتج عن إرتكابها أو ما وقعت عليها الجريمة ، وكل ما يفيد فى كشف الحقيقة.
- لايجوز ضبط المراسلات بين المتهم و الدفاع عنه.

---

[1] – **د. سامي حسني الحسيني**، المرجع السابق، ص304.

[2] – **د. أحمد شوقي الشلقاني**، المرجع السابق، ص243.

- مراعاة أثناء عملية الضبط الضوابط السابق الإشارة إليها المتعلقةبالحضور والميقات الزمني وغيرها، والإستثناءات الواردة عليها فيما إذا تعلق الأمر بجرائم المساس بنظم المعالجة الآلية.

والأصل أن الضبط يرد على الأشياء المادية وليس على الأشياء المعنوية بوجه عام، وهو ما يستخلص صراحة من تتبع الأحكام السابقة. وهو ما لا يحول دون تطبيقها على ضبط المكونات المادية للنظم، مثل وحدات الإدخال بما تشمله من مفردات ووحدة المخرجات وما تشمله من وسائل فضلا عن وحدات التخزين المختلفة.

وإن كان ذلك كذلك، فإن النصوص العامة في الضبط قد إستثنت تطبيق بعض الضمانات– كتلك المتعلقة بالتوقيت الزمني أو قاعدة الحضور أو الإختصاص المحلي كما سنرى – على جرائم المساس بنظم المعالجة الآلية ، وهو ما يدفعنا للقول بأن المشرع الجزائري قرر هذا الإستثناء لخصوصية ضبط الأدلة الإلكترونية، إلا أن هذه الفرضية سرعان ما تتلاشى إذا ما علمنا أن طريقة رفع المعطيات المعنوية تختلف عما هو متبع عند ضبط الأشياء المادية، وهو ما نلمسه من خلال الفقرة 3 من إتفاقية بودابست، حيث أنها إستخدمت "**الحصول بطريقة مشابهة**" على المعطيات المعلوماتية التي تكون موضوع التفتيش للإشارة إلى أساليب أخرى مستحدثة للضبط في البيئة التقنية، إلى جانب مصطلح الضبط للإشارة لضبط دعامات التخزين المعلوماتية.

ومن تم فإن تلك الأحكام تختص فقط بالمكونات المادية للنظم المعلوماتية في التشريع الإجرائي الجزائري، أما المكونات المعنوية فقد أثارت طبيعتها جدلاً فقهيًا حول مدى إمكانية ضبطها وهي مجردة من دعامتها المادية المثبة عليها، كضبط المستندات الإلكترونية المزورة كمعطيات داخل ذاكرة الحاسب الآلي، وضبط عمليات الغش والنصب التي تتم بالنسبة لأنظمة الصراف الآلي طبقا لما هو مسجل من معطيات حقيقية داخل هذه الأنظمة، خصوصاً وأن الضبط–حسب الأصل_ لا يرد إلا على الأشياء المادية.

وإنقسم الفقـــه في ذلك إلـــى إتجـــاهـــين[1]:

الإتجاه الأول: ويرى أنصار هذا الإتجاه أن الضبط لا يمكن أن ينصب على المعطيات، كونها ليس لها مظهر مادي محسوس كالأشياء المادية وبالتالي لا يمكن ضبطها بسبب طبيعتها غير المحسوسة إلا بعد تفريغها في كيان مادي محسوس مثل **طبع** هده البيانات على الورق أو **خزنها** على دعامة مادية مثل الأقراص المغناطسيسية أو **تصوير** المعطيات على الشاشة أو اية واسطة خزن أخرى.

ومن أنصار هذا الإتجاه الفقه الألماني والروماني والياباني.

الإتجاه الثاني:ويرى أنصارهذا الإتجاه ما يمنع من أن يرد الضبط على المعطيات، مستندين في ذلك إلى أن الضبط يشمل كل الأشياء التي تفيد في إظهار الحقيقة، وبالتالي يمكن ضبط الأدلة الإلكترونية المخزونة في الحاسوب والإستفادة منها في كشف الحقيقة.

---

[1]–في هذه الاتجاهات أنظـــر: **د. هلالي عبد الله أحمد**، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص199. **د.عبد الفتاح بيومي حجازي**، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2006 ، ص218 و ما بعدها، وأنظـــر أيضا: **نبيلة هبة مولاي علي هروال**، المرجع السابق، ص265.

ومن أنصار هذا الإتجاه الفقه والتشريع في بلجيكا وكنـــدا.

والمتأمل في الإتجاهين السابقين، يجد أن الإختلاف بينهما ليس إختلاف جوهري، فإن كان الإتجاه الأول يشترط لضبط المعطيات أن يتم تفريغها في وسط مادي معين فهو رأي يتلائم والواقع العملي، كون أن الأدلة الإلكترونية التي يتم الحصول عليها، لا يمكن رؤيتها وضبطها إلا بعد خزنها على وسط مادي كطبعها على الورق أو خزنها على وسيط تخزين أو عرضها على الشاشة، فهي تشبه الحقيبة التي تحفظ فيها الأوراق.

وهي نفس النتيجة التي يمكن إستخلاصها من الرأي الثاني، وإن لم يشترط ذلك، ويبقى أن يتم إستحداث تشريعات تنص صراحة على صلاحية المعطيات في أن تكون محلا للضبط، وهذا ما ما فعله المشرع الجزائري، فإدراكا منه للمشاكل القانونية والعملية التي يثيرها ضبط المعلومات، ولأهميتها، إستحدث المادة 6 من القانون المتضمّن القواعد الخاصّة للوقاية من الجرائم المتّصلة بتكنولوجيات الإعلام والاتّصال ومكافحتهاالتي جاءت تحت عنوان **حجز** المعطيات المعلوماتية، حيث نصت على أنّه "*عندما تكتشف السّلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة, يتم* ***نسخ المعطيات محل البحث و كذا المعطيات اللازمة لفهمها*** *على دعامة تخزين إلكترونية تكون قابلة للحجز, والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية.*

يجب في كل الأحوال على السلطة التي تقوم بالتفتيش و الحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية. غير أنه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل او اعادة تشكيل هذه المعطيات، قصد جعلها قابلة للإستغلال لأغراض التحقيق، شرطك أن لايؤدي ذلك إلى المساس بمحتوى المعطيات.

كما نصت المادة 7 على أنه في حالة ما إذا إستحال إجراء الحجز وفق المادة 6، يتعين على السلطة التي تقوم بالتفتيش إستعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة أو إلى نسخها الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة.

من خلال النصوص السابقـــة نخلص إلى أن ضبط المعطيات يتم كمايلي:

1- يتم حجز الجهاز بأكمله للتغلب على بعض المشاكل الفنية، كون أن بعض الأجهزة تكون محمية بكلمة المرور، فإن لم يكن كذلك فيتم عمل نسخ للمعلومات فحسب، وكذا المعطيات اللازمة لفهمها وذلك على جميع دعائم التخزين، والذي يتناسب مع تسمية الحجز المعلوماتي، الذي هو غير متعارض مع الضبط المادي التقليدي لدعائم التخزين المعلوماتية المستخرجة من نفس مكان التفتيش، أي بدل حجز القطع الصلبة التي تتضمن المواد الممنوعة، فيتم مثلا نسخ المواد التي تحتاج إلى فك شفرتها لكي يتم التعرف على محتوياتها، أو نسخ المعطيات التي يتم وضعها في إطار برمجية تحتوي قنبلة زمنية موقوتة[1].

[1]-**د. فتحي محمد أنور عزت**، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية للمجتمع المعلوماتي، الطبعة الثانية، دار الكتب، 2010، ص636.

وتثور مشكلات عملية تتعلق بضبط المعلومات حيث تحدث أحيانا تغييرات في المعطيات عند أخذ نسخة منها، وهو ما حدا بمحكمة النقض الفرنسية إلى عدم إعتبار أخذ نسخة من المعطيات المسجلة في الكمبيوتر وعدم ضبط الجهاز نفسه بما فيه من ذاكرة تحتوي تلك المعلومات من قبيل الضبط[1]. وهنا يتعين إعمال الحجز عن طريق منع الوصول إلى المعطيات.

2- جعل النسخة الأصلية غير قابلة للوصول اليها، وذلك بأي طريقة إلكترونية تمنع الدخول إلى هذه المعطيات كترميزها أو تقييدها.

3-لابد من إتخاذ إجراءات تكميلية من أجل التحفظ على سلامة المعطيات في الحالة التي تم العثور عليها عليها.

وفي حال ما إذا كانت المعطيات المحجوزة ذات محتوى مجرم، أجاز المشرع للسلطة التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الإطلاع على المعطيات التي يشكل محتواها جريمة، لا سيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك[2].

ومن الجدير بالذكر أن تقرير ضبط المعلومات في التشريع الجزائري كان نتيجة حتمية لتقرير التفتيش الإلكتروني، كون أن الغاية منه هو ضبط كل ما يفيد في كشف الحقيقة، ولا يعقل أن يكون التفتيش الكتروني والضبط مادي.

وإلى جانب المشرع الجزائري نجد المشرع الفرنسي الذي قام بإدخال تعديل على قانون الإجراءات الجزائية الفرنسي لسدّ هذا الفراغ التشريعي، وذلك بموجب قانون الأمن الدّاخلي لسنة 2003 حيث إستحدث الفقرة الثالثة من المادة 57-1 التي تنصّ على أنّ "المعطيات التي يتمّ بلوغها في ظل الشروط المنصوص عليها في المادة السابقة، يتعين نسخها على دعامات، ودعامات التخزين المعلوماتية هذه يتعين تحريزها في أحراز مختومة وفق الشروط المنصوص عليها في هذا القانون" .

يمكن لضابط الشرطة القضائية، بكل الوسائل، أن يطلب أي شخص مناسب يعرف كيفية حماية المعطيات التي تم الوصول إليها وإعادة تشكيلها.[3]

إن تدخل المشرع الفرنسي على النحو السابق مسلك طبيعي باعتبار أنّ فرنسا من الدّول الموقعة على إتّفاقية بودابست، حيث نصت هذه الأخيرة على الضّبط في الفقرة الثالثة من المادّة 19 من القسم الثالث منها على أنّه"

يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى، وذلك لمنح سلطاته المختصة صلاحية ضبط أو تأمين معطيات الكمبيوتر التي يتم الدخول عليها طبقا للفقرتين 1و2 وتشمل هذه الإجراءات صلاحية:

1- ضبط أو تأمين نظام الكمبيوتر أو جزء منه أو وسيط تخزين المعطيات.

2- عمل نسخة من هذه المعطيات والإحتفاظ بها.

---

[1]-**Cour de cassation ;chambre criminelle Audience publique du mardi 13 octobre 1998 N° de pourvoi: 98-82522**

[2]- المادة 8 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها.

[3]Art 57-1 alinèa 3 du C.P.P.F dispose que' Les données auxquelles il aura été permis d'accéder dans les conditions prévues par le présent article peuvent être copiées sur tout support. Les supports de stockage informatique peuvent être saisis et placés sous scellés dans les conditions prévues par le présent code..''

3- المحافظة على تجانس معطيات الكمبيوتر المخزنة ذات الصلة.

4- جعل هذه المعطيات غير قابلة للدخول عليها أو إزالتها على نظام الكمبيوتر الذي يتم الدخول عليه[1].

والمعروف أن بعد تفتيش النظام وأخذ نسخ من المعطيات، يقوم ضابط الشرطة القضائية بتحريز هذه الدعامات المخزن عليها المعطيات وتأمينها فنيا، وذلك وفقا للشروط المنصوص عليها في قانون الإجراءات الجزائية، وهذا ما نصت عليه المادة 57-1 من قانون الإجراءات الجزائية الفرنسي في فقرتها الثالثة، والفقرة 1 من المادة 6 من القانون 09-04 الجزائري[2].

كما دعت إتفاقية بودابست على تفعيل بعض الإجراءات التقنية الأولية التي من شأنها المساعدة على ضبط المعطيات، ومن قبيل ذلك **التحفظ العاجل على المعطيات** المخزنة المنصوص عليه في المادة 16[3] وذلك لمدة 90 يوما للسماح للسلطات المختصة بإتخاد إجراء التفتيش والضبط ، وكذلك فعلت الإتفاقية العربية في المادة 23 و24 منها.

وإن كان قد تأثر المشرع الجزائري بإتفاقية بودابست، ونص على حفظ المعطيات المتعلقة بحركة السير وذلك بمقتضى المادة 11 من القانون رقم 09-04 ، وهو ما يمكن السلطات بتحديد منبع ومصب الإتصال فضلا عن تحديد هوية أي فاعل أو فاعلين للجريمة تمهيدا لقبضه، إلا أنه لم ينص على التحفظ على المعطيات المخزنة بمختلف أنواعها.

كما أن من المشكلات التي يمكن أن تظهر في مجال ضبط المعطيات، حينما تكون هذه الأخيرة مخزنة في نظم معلوماتية تقع خارج الدولة، وهو ما يفرض التعاون الدولي في تنفيذ هذه الإجراءات، وهو ما كرسه المشرع الجزائري صراحة في الفصل السادس من القانون 09-04 تحت عنوان "التعاون والمساعدة القضائية الدولية و الإختصاص القضائي".

---

[1]- Art 19 alinéa 3 du C.C.B . dispose que "Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou à obtenir d'une façon similaire les données informatiques pour lesquelles l'accès a été réalisé en application des paragraphes 1 ou 2. Ces mesures incluent les prérogatives suivantes:
a saisir ou obtenir d'une façon similaire un système informatique ou une partie de celui-ci, ou un support de stockage informatique; b réaliser et conserver une copie de ces données informatiques; c préserver l'intégrité des données informatiques stockées pertinentes; d rendre inaccessibles ou enlever ces données informatiques du système informatique
consulté.

[2]- أنظر المادة: 45 و84 من قانون الإجراءات الجزائية الجزائري، المواد 55، 56، 98 ،199 ،157 اجراءات مصري.

[3]-**Article 16 Conservation rapide de données informatiques stockées** dispose que "1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'imposer d'une autre manière la conservation rapide de données électroniques spécifiées, y compris des données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification. Lorsqu'une Partie fait application du paragraphe 1 ci-dessus, au moyen d'une injonction ordonnant à une personne de conserver des données stockées spécifiées se trouvant en sa possession ou sous son contrôle, cette Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à conserver et à protéger l'intégrité desdites données pendant une durée aussi longue que nécessaire, au maximum de quatre-vingt-dix jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Une Partie peut prévoir qu'une telle injonction soit renouvelée par la suite".

وإن كان الضبط يرد على مكونات الوسائل الإلكترونية المادية والمعنوية على النحو السابق بيانه، فقد يكون محله أيضا المراسلات الإلكترونية التي تتم عبر هذه الوسائل، ولما كانت مراقبة الإنصالات الإلكترونية محل دراسة مفصلة في المبحث الثالث من هذا الفصل فنحيل إليها منعا للتكـــرار.

نخلص مما سبق، أن الطبيعة الخاصة للجرائم الواقعة في العالم الإفتراضي، دفعت المشرع إلى تعزيز صلاحيات ضباط الشرطة القضائية، بإقرار نظام خاص للتفتيش والضبط في نطاقها، ولكنه لم يكتفي بذلك بل إستحدث وسائل حديثة للبحث والتحري، وهو ما سنراه فيمايلـــي.

المبحث الثاني

الإختصاصات المتميزة لضباط الشرطة القضائية في مكافحة الجرائم الواقعة على التعاملات الإلكترونية

إن النمو الدائم للوسائل الإلكترونية فتح آفاقا جديدة للإجرام سواء تعلق الأمر بالجرائم التقليدية أو الإجرام التكنولوجي الجديد وعلى رأسه الجرائم الواقعة على التعاملات الإلكترونية، وفي هذا الصدد لا يكفي تطويرالقواعد الإجرائية التقليدية فحسب لإستخلاص الدليل في نطاقها وإماطة اللثام عنها، بل لا بد على التوازي من تبني قواعد جديدة مناسبة وذلك على إثر تنامي نغمة التفاعل الإنساني مع العالم الإفتراضي بقصد إحداث إتصال بين القاعدة الموضوعية والقاعدة الإجرائية.

وإيمانا بذلك، عمدت التشريعات إلى تعزيز الإجراءات التقليدية بإستحداثها وسائل تحري وتحقيق خاصة تتناسب مع العالم الرقمي محققة بذلك غاياتها **من التعرف على الحقيقة في جرائم لم تتخطى هذا العالم** إلى العالم المادي، وهو ما فعله المشرع الجزائري، حيث نجده قد كرس إختصاصات متميزة لضباط الشرطة القضائية، بعضها منصوص عليها في القانون رقم 04-09 المتضمن القواعد المتعلقة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، وهي المراقبة الإلكترونية وحفظ المعطيات المتعلقة بحركة السير، ومنها مانص عليها في قانون الإجراءات الجزائية، وذلك بموجب التعديل الذي أجراه عليه بالقانون رقم 22-06، حيث تم إستحداث إجراءات جديدة تتعلق بالبحث والتحري والتحقيق حول جرائم الإعتداء على نظم المعالجة الآلية، لم يشهدها القانون الجزائري من قبل وهي إعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور، فضلا عن التسرب، وهي إجراءات لاتخرج عن مفهوم "**المراقبة**"، كما وسع من الإختصاص الإقليمي لضباط الشرطة القضائية كإطـــار إجـــرائي.

وإلى جانب المشرع الجزائري، نجد المشرع الفرنسي هو بدوره قد تناول هذه الإجراءات ضمن قانون الإجراءات الجزائية بمقتضى المواد 706 -81 إلى المادة 706-87، والمادة 100 ، كما تضمن المشرع المصري البعض منها في المادة 95 و206 من قانون الإجراءات الجزائية.

وإذا كان من الطبيعي أن يكون تناول المشرع لهذه القواعد ينطبق على الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، فإننا ونحن بصدد دراسة الجرائم الواقعة على التعاملات الإلكترونية، سوف نتناول مدى إنطباق تلك القواعد الإجرائية عليها وصولا لما إذا كانت تلك القواعد تنطبق على الجرائم محل الدراسة من عدمه.

سنتناول فيمايلي إجراء التسرب وإعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور، على أساس أن المراقبة الإلكترونية والحفظ وإن كانت تدخل في الإختصاص المتميز لضباط الشرطة القضائية إلا أنه لمقدمي الخدمة دور فيها، لدلك ندرجها ضمنمدى تعاون الوسيط في التعامل الإلكتروني مع رجال الضبط القضائي، ومن ثم يبدو ملائما تقسيم هذا المبحث إلى المطالب الثلاثة التالية:

المطلب الأول: التســـرب

المطلب الثاني:إعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور

المطلب الثالث:توسيع الإختصاص الإقليمي لضباط الشرطة القضائية

المطلـــب الأول

التســـرب

يعتبر التسرب عملية ميدانية بالغة الخطورة، تستخدم لمراقبة الأشخاص المشتبه في إرتكابهم الجريمة، على أساس أن القائم به هو فاعل معهم أو شريك أو متهم بالجريمة[1]. يمارسه رجل الضبط القضائي في إطار قانون العقوبات وقانون الإجراءات الجزائية، وفي هذا الإطار نظم المشرع الجزائري عملية التسرب بصفة عامة ضمن ثمانية مواد، ليكرسه كـــواقع قانوني.

كما نص المشرع الفرنسي على التسرب من المادة 706 –81 إلى المادة 706–87 إجراءات جزائية، والأصل في فرنسا أن التسرب محدد في إطار مكافحة جريمة الإتجار بالمخدرات، ومع تطور الجريمة المنظمة والإرهاب والجريمة الإلكترونية جاء القانون 2004–204 المتعلق بتكييف العدالة مع تطورات الجريمة[2]، ليؤطر بصرامة التسرب الكلاسيكي الذي يسمح بالدخول في تواصل مع الأشخاص المشتبه بهم، كما كرس التحقيق تحت إسم مستعار، حيث أن هذه التقنية من التسرب تستخدم للبحث عن دليل الجريمة،في الشبكات الرقمية خاصة عبر شبكة الأنترنت يصطلح عليه **بالتسرب الرقمي**[3].

[1] -**Myriam Quéméne**, Nouvelles techniques d'enquêtes numériquesdisponible en lingne á l'adresse suivantehttp://www.adij.fr/wp-content/uploads/2015/01/Nouvelles-techniques-d%E2%80%99enqu%C3%AAtes-num%C3%A9riques-MQ.pdf; p6

[2]-**Loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité .**

[3]-voir **Myriam Quéméne**, Nouvelles techniques d'enquêtes numériques,disponible en ligne á l'adresse précédente.

ولما كان مفهوم التسرب لايخرج عن كونه مراقبة، فهو يحمل في طياته نوعا من التدخل في الحريات الشخصية للأشخاص، وذلك من خلال رصد ومتابعة تصرفاتهم وأحوالهم، ولذا يجب أن يتم إجرائه في إطار المشروعية سواء كان كلاسيـــكي(الفرع الأول) أو رقمـــــي(الفرع الثاني).

الفرع الأول

التسرب الكلاسيكي

سنحاول من خلال هذا الفرع الإحاطة بفمهوم التسرب، وكذا بيان الشروط والإجراءات التي وضعها المشرع الجزائي لمباشرته.

أولا- مفهوم التسرب

التسرب لغة مشتق من الفعل تسرب تسربا، أي دخل وإنتقل خفية وهي الولوج والدخول بطريقة أو بأخرى إلى مكان أو جماعة وجعلهم يعتقدون بأنه ليس غريبا عنهم وإشعارهم بأنه واحد منهم، وهو ما يمكنه من معرفة إنشغالاتهم وتوجهاتهم[1].

أما قانونا، فقد عرف المشرع الجزائري هذه العملية في المادة 65 مكرر12 على أنها: قيام ضابط الشرطة أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية **بمراقبة** الأشخاص المشتبه في إرتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك أو خاف. وهذا التعريف منقول حرفيا من الفقرة الثانية من نص المادة 706-81 من قانون الإجراءات الجزائية الفرنسي المعدلة بموجب القانون رقم 2015-993 المتعلق بتكييف الإجراءات الجزائية وفق قانون الإتحاد الأروبي[2].

فمن خلال هذه المادة نجد أن المشرع قد أجاز لوكيل الجمهورية أو لقاضي التحقيق، بعد إخطار وكيل الجمهورية، عن طريق ضابط أو عون الشرطة القضائية القيام بعملية التوغل والإختراق داخل جماعة إجرامية ومراقبتهم وذلك بإيهامهم أنه فاعل أصلي أو شريك أو مخفيا لمحصلات الجريمة، حتى يحظى بثقتهم ليكشف ملابسات الجريمة والتعرف على هوية مرتكبيها.

ويلجأ إلى هذا الإجراء عادة عندما تقتضي عملية التحري أو التحقيق في إحدى الجرائم الخطيرة، وقد عددها المشرع الجزائري في المادة 65 مكرر من قانون العقوبات وهي: جرائم المخدرات، الجريمة المنظمة عبرالحدود الوطنية، **الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات** ، جرائم تبييض الأموال والإرهاب،

---

[1]-**سهيل حسيب سماحة**، معجمي الحي، الطبعة الأولى، مكتبة سمير ،1984، ص130.

[2]- Article 706-81 du C PP Modifié par LOI n° 2015-993 du 17 août 2015 portant adaptation de la procédure pénale au droit de l'Union européenne dispose que" L'infiltration consiste, pour un officier ou un agent de police judiciaire spécialement habilité dans des conditions fixées par décret et agissant sous la responsabilité d'un officier de police judiciaire chargé de coordonner l'opération, à surveiller des personnes suspectées de commettre un crime ou un délit en se faisant passer, auprès de ces personnes, comme un de leurs coauteurs, complices ou receleurs"

والجرائم المتعلقة بالتشريع الخاص بالصرف. وهو ما يسمح بإمتداده إلى الجرائم الواقعة على نظم التعاملات الإلكترونية.

كما ذكرها المشرع الفرنسي في المادة 706-73 والمادة 706-73-1 من قانون الإجراءات الجزائية، ومن بينها جرائم الإعتداء على نظم المعالجة الآلية للمعلومات ذات الطابع الشخصي التي تنفذها الدولة، المرتكبة في إطار جماعة منظمة والمنصوص عليها في المادة 323—4-1 من قانون العقوبات.

والملاحظ أن هذا الإجراء ليس هو بالأصل، بل هو عملية إستثنائية تقتضيها عدم فعالية الأساليب العادية وحتى غير العادية في إظهار الحقيقة بجمع الأدلة، بتعزيز الإشتباه أو تأكيد الإتهام، وهو ما عبر عنه المشرع الجزائري في مطلع المادة 65 مكرر 11 "عندما **تقتضي ضرورات التحري أو التحقيق ...**"، كذلك فعل المشرع الفرنسي في المادة 706-81 *Lorsque les nécessités de l'enquête ou de l'instruction*

لكن في الجرائم الواقعة في العالم الإفتراضي فهو عملية معقدة نوعا ما حتى يتم القبض على المجرمين وتفكيك الشبكات التي تتم عبر القنوات الرقمية[1]، عبر عنوان بروتوكول الأنترنت IP.

و إن كان كل من المشرع الجزائري والفرنسي قد أطرا التسرب الكلاسيكي، إلا أن هذا لا يمنع من تكييف هذه الحيلة الإجرائية مع الرقمية، وبالتالي يمكن إنابة بعض رجال الضبطية القضائية لعملية التسرب الرقمي[2].

ويمكن تجسيد عملية التسرب الرقمي في قيام ضابط أو عون الشرطة القضائية بالولوج بواسطة نظامه على شبكة الأنترنت، بطريقة مخفية مستخدما إسما مستعار أو صفة وهمية في منتديات النقاش أو على مواقع الأنترنت[3]، فيتناول الأحاديث العادية مع الغير، دون أن يدفعه إلى إرتكاب الجريمة، فيظهر وكأنه يسعى لإضاعة الوقت والهروب من الملل، إلى أن تنكشف حقيقة الجريمة ومرتكبيها، كأن يدور الحديث حول طريقة الحصول على أرقام بطاقات الإئتمان بصورة إحتيالية، أو كيفية إختراق المواقع، أو زرع الفيروسات...ألخ، ويمكن للمتسرب أن يقوم بطرح الأسئلة على الغير حتى يتمكن من الحصول على أكبر قدر ممكن من المعلومات[4].

ثانيا- شروط عملية التسرب

[1] - **Anmonka Jeanine-Armelle Tano-Bian**, **Anmonka Jeanine-Armelle Tano-Bian**, La r´epression de la cybercriminalit´e dans les Etats de l'Union europ´eenne et de l'Afrique de l'Ouest, LA REPRESSION DE LA CYBERCRIMINALITE DANS LES ETATS DE L'UNION EUROPEENNE ET DE L'AFRIQUE DE L'OUEST, Thèse pour le Doctorat en Droit Public, Paris, 2015 , p304.

[2]- **Anne MOREAUX;** Infiltration et enquête sous pseudonyme: le numérique comme arme judiciaire,disponible en ligne á l'adresse suivante: http://www.affiches-parisiennes.com/infiltration-et-enquete-sous-pseudonyme-le-numerique-comme-arme-judiciaire-6073.html#ixzz42iWuMgmJ

[3]-**Myriam Quéméner**, Concilier la lutte contre la cybercriminalité et l'éthique de liberté rev Sécurité et stratégie *1 ;* Club des Directeurs de Sécurité des Entreprises 2011 ; p 62

[4]- **د.عمر محمد أبو بكر بن يونس** ، الجرائم الناشئة عن إستخدام الأنترنت، المرجع السابق، ص ص 838- 839.

نظرا لخطورة عملية التسرب وطبيعتها، فقد ضبطها كل من المشرع الجزائري والفرنسي بشروط شكلية وأخرى موضوعية يجب مراعاتها تماشيا ومبدأ الشرعية الإجرائية من جهة، وحسن سير العملية من جهة أخرى. معتبرا أن القيام بعملية التسرب أمرا إستثنائيا، محددا بحالات معينة مذكورة فيه على سبيل الحصر.

أ- الشروط الشكليـــة:

وضع القانون عدة ضمانات حقيقية تحمي الأفراد من تعسف سلطات التحري والتحقيق، تتلخص فيما يلـــي:

1-تحرير تقرير مسبق من طرف ضابط الشرطة القضائية: قبل البدء في تنفيد عملية التسرب، يحرر ضابط الشرطة القضائية المكلف بتنسيق العملية تقريرا يتضمن العناصر الضرورية لمعاينة الجرائم، غير تلك التي قد تعرض للخطر أمن الضابط أو العون المتسرب وكل ما يمكن تسخيره للعملية(المادة 65 مكرر 13) وذلك لإطلاع السلطة المختصة بمنح الإذن بشكل تام عن ظروف القضيّة ومتطلّباتها.

وعناصر الجريمة المقصود تحديدها[1]، تتجلى في ذكر جميع المعلومات المتعلقة بالجريمة والعناصر المكونة لها وهي: ذكر هوية الأشخاص المشتبه فيهم، الوسائل المستعملة في إرتكاب الجريمة، وكل المعلومات المتعلقة بالجماعة المقصودة بعملية التسرب. فضلا عن ذكر السبب من طلب الإذن بإجراء هذه العملية.

2-الإذن بمباشرة العملية: يجوز لوكيل الجمهورية أو لقاضي التحقيق، بعد إخطار وكيل الجمهورية عند إقتضاء ضرورة التحري أو التحقيق، أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب.

وحتى يكون هذا الإذن قانونيا، يجب أن يكون حسب الشروط المبينة في المادة 65 مكرر 15 من قانون الإجراءات الجزائية الجزائري، وهو أن يكون مسببا، ومع أن إدراج المشرع لعبارة "مسببا" تكفي للدلالة على أنه مكتوب، فقد أضاف المشرع "مكتوبا"، مستخدما حرف الواو الذي يفيد المغايرة.

ويبدو أن المشرع الجزائري لم ينفرد في إتجاهه التشريعي، إذ نجد المشرع الفرنسي هو بدور نص على أن يكون الإذن مكتوبا وبصفة خاصة مسببا، وذلك بموجب الفقرة الأولى من المادة 706-83[2] إجراءات.

ولا يكفي في التسبيب أن يذكر أن التسرب يتعلق بالحالات المنصوص عليها قانونا، بل يجب أن يحدد الأسباب التي من أجلها أريد جمع معلومات عن الجريمة ومرتكبيها، بأن يكون هو الإجراء الأنسب الذي بواسطته يمكن كشف الحقيقة وضبط الجناة، بعد فشل الإجراءات العادية في ذلك.

كما يجب أن يذكر في الإذن الجريمة التي تبرر اللجوء إلى هذا الإجراء، وهي إحدى الجرائم المستحدثة أو الخاصة أو الخطيرة كما يسميها البعض، ومن بينها جرائم المساس بنظم المعالجة الآلية للمعطيات، والمدة التي تستغرقها العملية وهي أن لا تتجاوز أربعة أشهر،ويمكن أن تجدد حسب مقتضيات التحري أو التحقيق،

[1]- **محمد حزيط**، مذكرات في قانون الإجراءات الجزائية الجزائري، الطبعة الثالثة، دار هومة، الجزائر، 2008، ص73.

[2]- A peine de nullité, l'autorisation donnée en application de l'article 706-81 est délivrée par écrit et doit être spécialement motivée.

ضمن نفس الشروط الشكلية والزمنية، وفي نفس الوقت أجاز القانون للقاضي الذي رخّص بإجرائها أن يأمر في أيّ وقت بوقفها قبل انقضاء المدّة المحدّدة.

فضلا عما سبق، إشترط المشرع في الإذن أن يذكر فيه الهوية الكاملة للضابط الذي تتم العملية تحت مسؤوليته من إسم ولقب، الصفة، الرتبة، المصلحة التابع لها[1].

والملاحظ، أن المشرع الجزائري على غرار المشرع الفرنسي، قد رتب البطلان فقط في حالة عدم مراعاة الكتابة والتسبيب في الإذن حسب الفقرة 1 من المادة 65 مكرر 15، والفقرة 1 من المادة 706-83 إجراءات فرنسي.

3-الجهات المختصة بإصدار الإذن بالتسرب: حتى وإن كان المتسرب هو عون الشرطة القضائية، إلا أنه وضمانا لمشروعية الدليل المستمد منه، إشترط المشرع ضرورة الحصول على إذن بذلك من وكيل الجمهورية وأن تباشر العملية تحت رقابته وإشرافه حتى نهايتها. كما يمكنه الأمر بوقفها قبل إنتهاء المدة المرخص لها، وهذه بمثابة أداة رقابة لوكيل الجمهورية أثناء سير عملية التسرب.

كما يمكن الحصول على هذا الإذن من قاضي التحقيق، بعد إخطار وكيل الجمهورية، ليتم تنفيده بمعرفة ضابط الشرطة القضائية في إطار إنابة قضائية، ويمكنه الأمر بوقفها في أي وقت قبل إنقضاء المدة المحددة له في الإذن. وهذا طبعا بعد أن يقوم ضابط الشرطة القضائية المكلف بتنسيق العملية، بتحرير تقرير مكتوب كما سبق وأشرنا، مرفوقا بطلب منح الإدن لمباشرة العملية.

ب- الشروط الموضوعيـــة:

يمكن إجمال الضوابط أو الشروط الموضوعية في ضابطين إثنين:

1-فائدة التسرب في إظهار الحقيقة: نص المشرع الجزائري في مطلع المادة 65 مكرر11 على أنه عندما تقتضي ضرورة التحري والتحقيق يجوز الإذن بالتسرب، وكذلك فعل المشرع الفرنسي في المادة 706-81، وتقدير الضرورة المبررة للتسرب من حيث قيامها وزوالها متروك للمحقق، وتقديره في هذا الشان خاضع لرقابة القضاء،ومن ذلك أن يبين أن وسائل البحث العادية في كشف الحقيقة وضبط الجناة قد فشلت، أو أن الإستمرار فيها ونجاحها في تحقيق الغرض منها قد أضحى بعيد الإحتمال، أو أن المتهمين من الدهاء والحرص بحيث تعجز الوسائل الأخرى عن إماطة اللثام عن الجريمة وجمع أدلتها.

2-**الجرائم الجائز فيها التسرب:** يمس إجراء التسرب بحريات الإفراد، لذا فإن المشرع ومن خلال سعيه إلى إقامة التوازن بين ما تتطلبه المصلحة العامة في كشف الحقيقة وضبط الجناة، والحريات الفردية، أحاطه بضمانات عدة من بينها أنه لم يجزه إلا إذا كانت الجريمة جناية أو جنحة منصوص عليها في المادة 65 مكرر ومن بينها الجرائم الماسة بانظمة المعالجة الآلية للمعطيات، وتطبيقاته في ذلك موسعة في التعاملات

[1]- الفقرة 2 من المادة 65 مكرر 15، والفقرة 2 من المادة 706-83 اجراءات فرنسي.

الإلكترونية، كالمواقع الإلكترونية أو منظومات التوقيع الإلكتروني، والمستندات المعلوماتية الممثلة في المعطيات المعالجة داخل النظام وغيرها كثير.

وكذلك هو الأمر في التشريع الفرنسي، حيث أنه حددها في الجرائم المنصوص عليها في المادة 706-73 والمادة 706-73-1 إجراءات، ومن هذه الجرائم: الإتجار بالمخدرات، السرقة المرتكبة في إطار جماعة منظمة، إتلاف الأموال في إطار جماعة منظمة، تزوير العملات، الأفعال الإرهابية، تبيض الأموال، الإحتيال في إطار جماعة منظمة، **الإعتداء على نظم المعالجة الآلية للمعطيات ذات الطابع الشخصي التي تنفذها الدولة...**

ثالثا- الحماية المقررة للقائم بعملية التسرب

أ-السريـــة:

يرتبط نجاح عملية التسرب، وأمن وسلامة القائم بها على عنصر مهم ألا وهو **السرية**، وعليه سمح قانون الإجراءات الجزائية إستعمال هوية مستعارة يتم إستخدامها في التسرب[1]، وذلك باستعماله أوراق أو وثائق هوية ذات معلومات خاطئة. كما منع كشف هويته الحقيقية عند أخذه الهوية المستعارة في أية مرحلة من مراحل الإجراءات، ولقد رتب المشرع على مخالفة هذا المنع عقوبات جزائية تتمثل في الحبس والغرامة، وقد وسع المشرع هذه الحماية لعائلة المتسرب، في حالة تسبب هذا الكشف عن تعرض أحدهم لأعمال العنف أو ضرب أو جرح. فتكون العقوبة الحبس من خمس إلى 10 سنوات والغرامة من 200000 دج إلى 500000 دج حسب الفقرة 3 من المادة 65مكرر16 ، و7 سنوات سجن و100000 يورو غرامة حسب الفقرة 3 من المادة 706-84.

أما إذا تسبب هذا الكشف عن الوفاة، فتكون العقوبة الحبس من 10 سنوات إلى عشرين سنة وغرامة 500000 دج إلى 100000 دج حسب الفقرة الأخيرة من المادة65 مكرر 16، والحبس من 10 سنوات و غرامة 150000 يورو حسب الفقرة الأخيرة من المادة 706-84 .

وتماشيا مع مقتضات السرية، أجاز المشرع الجزائري وعلى غرار المشرع الفرنسي في المادة 706-82[2] أن يرتكب المتسرب عند الضرورة الأفعال المذكورة في المادة 65 مكرر 14، دون أن تشكل تحريضا على إرتكاب جرائم، وهو أن يقوم بـــــ:

- إقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتوجات أو وثائق أو معلومات متحصل عليها من إرتكاب الجرائم أو مستعملة في إرتكابها.

---

[1]-الفقرة 2 من المادة 65 مكرر 12 إجراءات جزائري. تقابلها الفقرة الأولى من المادة 706-84 من قانون الإجراءات الفرنسي.

[2]- Les officiers ou agents de police judiciaire autorisés à procéder à une opération d'infiltration peuvent, sur l'ensemble du territoire national, sans être pénalement responsables de ces actes : 1° Acquérir, détenir, transporter, livrer ou délivrer des substances, biens, produits, documents ou informations tirés de la commission des infractions ou servant à la commission de ces infractions

2° Utiliser ou mettre à disposition des personnes se livrant à ces infractions des moyens de caractère juridique ou financier ainsi que des moyens de transport, de dépôt, d'hébergement, de conservation et de télécommunication.

– إستعمال أو وضع تحت تصرف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل أو التخزين أو الإيواء أو الحفظ أو الإتصال.

فضلا عن ذلك، أقر المشرع عدم إيداع رخصة الإذن بالعملية في ملف الإجراءات، حسب الفقرة الأخيرة من المادة 65 مكرر 15 إجراءات جزائري، والفقرة الأخيرة من المادة 706–83 إجراءات فرنسي[1].

ب–توقيف العملية في ظروف تضمن أمن المتسرب:

الأصل أن المدة المطلوبة لعملية التسرب حسبالفقرة الثالثة من المادة 65مكرر 15إجراءات جزائري والفقرة الثالثة من المادة 706–83 إجراءات فرنسي، هي ألا تتجاوز أربعة أشهر،ويمكن أن تجدد حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية،وفي نفس الوقت أجاز القانون للقاضي الذي رخّص بإجرائها أن يأمر في أيّ وقت بوقفها قبل إنقضاء المدّة المحدّدة.

فإذا ما تقرر وقف العملية، أو إنقضاء أجلها دون تجديد من القاضي الذي رخص باجرائها، يمكن للعون المتسرب مواصلة نشاطاته المنصوص عليها في المادة 65مكرر 14 إجراءات جزاري والمادة 706–82 إجراءات فرنسي، للوقت الضروري الكافي لتوقيف عمليات المراقبة في ظروف تضمن أمنه دون أن يكون مسؤولا جزائيا، على أن يتجاوز ذلك مدة 4 أشهر[2].

ت–عدم جواز سماع الشخص المتسرب كشاهد:

من باب الحماية غير المباشرة للعون المتسرب القائم بالعملية، ورغم كونه الشاهد الحقيقي في المسالة، أقر المشرع جواز سماع ضابط الشرطة القضائية الذي جرت عملية التسرب تحت مسؤوليته وبالتنسيق معه، دون سواه بوصفه شاهدا عن العملية. وهو ما نص عليه المشرع الجزائري في المادة 65 مكرر18 ، والمشرع الفرنسي في الفقرة الأولى من المادة 706–86[3].

رابعا– الأثار المترتبة على عملية التسرب[4]

يقوم ضابط الشرطة القضائية بإعتباره المسؤول عن عملية التسرب، بتحرير تقارير عن العمليات التي يقوم بها المتسرب ويحيلها إلى القاضي الذي أذن بها–وكيل الجمهورية أو قاضي التحقيق حسب الحال–على أساس أنه المنسق بين هذا الأخير والمتسرب.

---

[1]- L'autorisation est versée au dossier de la procédure après achèvement de l'opération d'infiltration

[2]- المادة 65 مكرر 17 إجراءات جزائري، المادة 706–85 إجراءات فرنسي.

[3]- L'officier de police judiciaire sous la responsabilité duquel se déroule l'opération d'infiltration peut seul être entendu en qualité de témoin sur l'opération.

[4]-**فوزي عمارة**، إعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور والتسرب كإجراء تحقيق قضائي في المواد الجزائية، مجلة العلوم الإنسانية، عدد33، جامعة منتوري، قسنطينة، جوان 2010، ص250–251.

تعتبر المعلومات التي تحصل عليها المتسرب إستدلالا لا يرقى لوحده إلى دليل ما لم يرفق بدلائل أو عناصر ثبوتية أخرى، وذلك تطبيقا للقواعد العامة للإثبات.

وسبق وأن رأينا، أن الجرائم التي أجاز فيها المشرع التسرب حددها على سبيل الحصر، ومن بينها جرائم الإعتداء على نظم المعالجة الآلية بصفة عامة، إلا أنه أثناء تنفيذ الإذن يحدث أن يصادف المتسرب جرائم أخرى غير تلك التي تم تحديدها في الإذن بالتسرب.

بالرجوع إلى النصوص المنظمة للتسرب لم يوضح المشرع موقفه من الجرائم التي يتم إكتشافها عرضا أثناء أداء المتسرب لمهامه، على عكس ما فعل في إعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور، وذلك بموجب المادة 65 مكرر 6 " إذا اكتشفت جرائم أخرى غير تلك التي ورد ذكرها في إذن القاضي، فإن ذلك لا يكون سببا لبطلان الإجراءات العارضة".

الفرع الثاني

التسرب الرقـــــمي

يعتبر التسرب الرقمي إجراء تقني معمول به في إطار حماية الشبكات المعلوماتية بصفة عامة، ومن أجل خدمة الأنترنت[1]، وعلى الرغم من تكريس المشرع الفرنسي التسرب الكلاسيكي الذي يسمح بسريان نصه على التسرب الذي يتم في شبكة الأنترنت، إلا أنه زاد في حرصه في تقوية مكافحة بعض الجرائم المرتكبة بطريق الإتصالات الإلكترونية، ليكرس بموجب المادة 706-87-1 إجراءات جزائية المضافة بموجب المادة 19 من القانون رقم 2014-1353 الخاص بتعزيز الأحكام المتعلقة بالإرهاب[2]، المعدلة بموجب المادة 11 من القانون 2015-993 المتعلق بتكييف قانون الإجراءات الجزائية الفرنسي مع قانون الإتحاد الأروبي، التسرب في العالم الرقمي، أطلق عليه **التحقيق تحت إسم مستعار**.

حيث أجاز بموجبها وفي الجرائم المحددة في المواد 706-73-1 ,706-73,706-72 ، متى إرتكبت بوسائل الإتصالات الإلكترونية -وذلك بهدف جمع الأدلة والبحث عن الفاعلين فيها - لضابط الشرطة القضائية أو لعون ضابط الشرطة القضائية وفي إطار التحقيقات أو إنابة قضائية إذا تم تكليفهم في خدمة خاصة بموجب قرار من وزير الداخلية، وخولوا خصيصا لتنفيذ هذه التقنية.

إن تقنية التحقيق تحت إسم مستعار يمكن النظر إليها على أساس أنها **تكييف رقمي للتسرب**، تحت هوية مستعارة، حيث يمكن للمحققين جمع الأدلة على شبكة الأنترنت من خلال منتديات النقاش أو رسائل البريد الإلكتروني وحفظها في سجلات.

---

[1]- **Anmonka Jeanine-Armelle Tano-Bian**, op,cit, p 299.

[2]-**LOI n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme** , JORF n°0263 du 14 novembre 2014 page 19162

تجدر الإشارة إلى أن هذا النظام، قد سبق تطبيقه من قبل ضباط الشرطة القضائية للجمارك، حيث أن المادة 28-1 من قانون الإجراءات الجزائية تنص صراحة على تخويل بعض موظفي الجمارك بواسطة قرار من وزارة العدل بوظائف الشرطة القضائية.

والملاحظ أن تنفيذ هذا الإجراء غير خاضع لأي ضمانات والمنصوص عليها في المادة 706-87-1 من قانون الإجراءات الجزائية، حيث يمكن للجمارك إستخدام هذه التقنية في التحقيق دون الحصول مسبقا على إذن من القاضي بهدف التثبت من الجرائم الجمركية[1].

والشروط التي حددها المشرع الفرنسي في المادة 706-87-1 إجراءات هـــــي:

أولا- الأشخاص المكلفين بتنفيد تقنية التسرب الرقمي

فقط ضباط الشرطة القضائية والأعوان المكلفين بخدمة خاصة، حيث أنهم يخضعون لتكوين خاص، بعد أخذ الإذن من وكيل الجمهورية بالمجلس القضائي الذي يباشرون ضمنه وظائفهم المعتادة[2].

والخدمات المعنية عديدة، وقد حددها القرار رقم 21 اكتوبر 2015[3] المتعلق بالتفويض في الخدمات الخاصة للضباط الشرطة القضائية أو أعوانهم قصد إجراء التحقيقات تحت إسم مستعار، في 8 خدمات، والتي تعنينا هي الخدمات والوحدات التابعة الإدارة المركزية للشرطة القضائية والتي تتفرع عنها الإدارة الفرعية لمكافحة الجرائم الإلكترونية[4].

ثانيا- الجرائم الجائز فيها التسرب الرقمي

إن إمكانية التحقيقات بواسطة إسم مستعار من أجل التسرب في الشبكات والحصول على المعلومات عن الجرائم والأشخاص المشتبه فيهم، كانت محصورة في جرائم معينة، كالخاصة بالأحداث، مكافحة الجرائم المنصوص عليها في قانون الصحة العمومي والإرهاب، لكن بعد قانون 17 اوت 2015 المتعلق بتكييف قانون الإجراءات الفرنسي مع قانون الإتحاد الأروبي، وسع من نطاق التحقيقات تحت إسم مستعار إلى حد كبير متجاوزا بدلك **ما شمله التسرب الكلاسيكي**، وذلك في جرائم كثيرة خاصة المعلوماتية منها.

حيث حددها المشرع في الجرائم التي **ترتكب بواسطة وسائل الإتصلات الإلكترونية** والمنصوص عليها في:

---

[1]-**M**. **Michel MERCIER,**Rapport n° 491 (2015-2016) de fait au nom de la commission des lois, déposé le 23 mars 2016; p.161

[2]- Article 2 Arrêté du 21 octobre 2015 relatif à l'habilitation au sein de services spécialisés d'officiers ou agents de police judiciaire pouvant procéder aux enquêtes sous pseudonyme

[3]-**Arrêté du 21 octobre 2015,publié au Journal officiel du 29 octobre 2015, relatif à l'habilitation au sein de services spécialisés d'officiers ou agents de police judiciaire pouvant procéder aux enquêtes sous pseudonyme.**

[4]-- **GUILLAUME CHAMPEAU** L'enquête policière sous pseudonyme sur Internet se généralise disponible en ligne á l'adresse suivante http://www.numerama.com/politique/128642-lenquete-policiere-sous-pseudonyme-sur-internet-se-generalise.html

أ- **المادة 706-72 إجراءات:** وتشمل الجرائم الماسة بنظم المعالجة الآلية والمنصوص عليها في المادة 323-1 إلى 323-4-1 وجريمة تدمير أو إتلاف أو تحويل أي وثيقة، معدات، أدوات، تركيبات، أجهزة أدوات تقنية، أو نظام للمعالجة الآلية والمنصوص عليها في المادة 411-9 عقوبات.

ب- **المادة 706-73 و706-73-1إجراءات:** منها الإتجار بالمخدرات، السرقة المرتكبة في إطار جماعة منظمة، إتلاف الأموال في إطار جماعة منظمة، تزوير العملات، الأفعال الإرهابية، تبيض الأموال، الإحتيال في إطار جماعة منظمة، الإعتداء على نظم المعالجة الآلية للمعطيات ذات الطابع الشخصي التي تنفذها الدولة المرتكبة في إطار جماعة منظمة والمنصوص عليها في المادة 323—4-1 من قانون العقوبات.

ثالثا- الســـرية

حتى يحقق التحقيق تحت إسم مستعار الأهداف المنشودة منه، لابد أن يتم بكل سرية، ولذلك أجاز المشرع للمحقق أن يخفي هويته الحقيقية بإستعمال شخصية مغايرة.

وعلى غرار التسرب الكلاسيكي، أجاز المشرع الفرنسي وتماشيا مع مقتضيات السرية أن يرتكب الضباط أحد الأفعال التي نصت عليها المادة 706-87-1 إجراءات دون أن يكونو مسؤولون جزائيا وهي:

-المشاركة تحت إسم مستعار في تبادلات إلكترونية.

-الإتصال عن طريق وسائل الإتصالات الإلكترونية مع الأشخاص المحتمل كونهم مرتكبي الجرائم.

- إستخراج، إقتناء، الإحتفاظ بواسطة وسائل، عناصر الأدلة والمعطيات عن الأشخاص المحتمل كونهم جناة.

-إستخراج، أو نقل ردا على طلب صريح، إقتناء أو الإحتفاظ بمحتوى غير مشروع في إطار الشروط المنصوص عليها بواسطة مرسوم.

وإن كان يجوز ممارسة أحد الأفعال السابقة لكشف الجريمة وضبطها، فإنه لايجوز لهم التحريض على إرتكابها ولا التدخل في خلقها، ويكون العمل غير مشروع كلما كان فيه مساهمة في خلق الجريمة أو توجيه إرادة المتهم نحوها أي التحريض على إرتكابها. وعدم المشروعية يترتب عليه أثر هام من حيث الإجراءات التي يقومون بها، فإنها تعتبر إجراءات غير مشروعة وباطلة ويجب إستبعاد كل ما ينتج عنها من أدلة. وهو ما أشار اليه المشرع الفرنسي صراحة في الفقرة الأخيرة من المادة 706-87-1 إجراءات " ولا يجوز تحت طائلة البطلان، أن تشكل هذه الأفعال تحريضا على إرتكاب جرائم"[1].

[1]-A peine de nullité, ces actes ne peuvent constituer une incitation à commettre ces infractions.

المطلب الثاني

إعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور

سرية الإتصالات وما يتصل بها تعد تطبيقا خاصا للمبدأ العام"**حرمة الحياة الخاصة**" حيث يتفرع عنه حرمة المسكن، والمراسلات البريدية والبرقية، والمحادثات التي تتم بوسائل الإتصال المختلفة، والمحادثات الخاصة المباشرة، وحق الإنسان على صورته... وقد أكد على ذلك الإعلان العالمي لحقوق الإنسان[1]، والإتفاقيات الدولية لحقوق الإنسان كالإتفاقية الأوروبية لحقوق الإنسان ECHRالتي حرصت على التأكيد على حماية حق الإنسان في الخصوصية وسرية مراسلاته ومحادثاته، وأوجبت على الدول المختلفة ضرورة توفير الحماية له. فضلا عن ذلك نجد الدساتير في كثير من الدول تحيط هذا الحق بالحماية، حيث نص دستور الجزائر في المادة 46 على أن" سرّيّة المراسلات والاتّصالات الخاصّة بكلّ أشكالها مضمونة. ولايجوز بأي شكل المساس بهذه الحقوق دون أمر معلل من السلطة القضائية. ويعاقب القانون على إنتهاك هذا الحكم. كما نص دستور مصر في المادة 57 على "للحياة الخاصة حرمة، وهي مصونة لا تمس، وللمراسلات البريدية والبرقية والإلكترونية والمحادثات الهاتفية وغيرها من وسائل الإتصال حرمة، وسريتها مكفولة ولاتجوز مصادرتها أو الإطلاع عليها أو رقابتها إلا بأمر قضائي مسبب ولمدة محددة، وفي الأحوال التي يبينها القانون".

ولما كان المبدأ القانوني يقضي بأن الدستور هو القانون الأعلى في الدولة، وتبعا لذلك يجب أن تكون بقية القوانين الأخرى مطابقة لأحكامه نصا وروحا تحت طائلة عدم دستوريتها، جاءت القوانين الإجرائية مستجيبة للإملاءات الدستورية، مؤكدة حرمة وسرية الإتصالات والمراسلات وبينت الضمانات بصورة واضحة ومستحدثة في حالة جوازها، وهوما نصت عليه المادة 65 مكرر 5 من قانون الإجراءات الجزائية الجزائري، حيث أجازت لوكيل الجمهورية في بعض الجرائم ومن بينها **جرائم المساس بنظم المعالجة الالية** أن يأذن بإعتراض المراسلات وتسجيل الأصوات والتقاط الصور. وهي تسميات وإن تعددت إلا أنه يمكن إختزالها في مصطلح واحد "**المراقبة**"[2].

وكذلك فعل المشرع الفرنسي بموجب المادة 100 إجراءات المعدلة بموجب القانون رقم 2016-731 المتعلق بتقوية مكافحة الجرائم المنظمة والإرهاب وتحسين فعالية وضمان الإجراءات الجزائية[3]، فضلا عن المشرع المصري وذلك في المادة 95[1] و206[2]، هذا من جهة.

---

[1]Article 12 du Déclaration universelle des droits de l'homme Le 10 décembre 1948Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.

[2]– **فوزي عمارة**، المرجع السابق، ص236، د. **شيماء عبد الغني**، المرجع السابق، ص305.

[3]Art 100 du CPPF Modifié par- LOI n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale dipose que "En matière

ومن جهة أخرى، عاقبت التشريعات العقابية على إعتراض الإتصالات السلكية واللاسلكية دون إذن بذلك، باعتبار أن ذلك يتضمن إنتهاكا لحرمة الحياة الخاصة.

إذن ليس من شك في أن المراقبة تتضمن إنتهاكا لحجاب السرية الذي يحرص القانون على حمايته من الإعتداء عليه بأي وجه من الوجوه، ولاشك أن الحماية التي يكفلها القانون من هذه المراقبة لا يقتصر نطاقها على الصور المختلفة لها، بل أن منطق القول يحتم إمتداد هذه الحماية إلى **المراقبة التي تتم بالوسائل الإلكترونية** من باب أولى على أساس أن الغاية من وراء هذه الحماية هي حماية الحياة الخاصة للإنسان بحماية مستودع أسراره الشخصية، وهذه الأسرار تكون أكثر إنتهاكا إذا ما إستخدمت هذه الوسائل في الوصول إليها، ومن ثم فإنها تكون في حاجة إلى حماية أكثر.

وإن كان ذلك كذلك، فإن تلك الحماية لا ينبغي لها أن تكون مطلقة، فالحق المطلق غير متصور في نظام الجماعة، وانما الحق الإجتماعي، وهذا يتقيد دائما ويتحدد إطاره في ضوء المصالح العامة. وهذا ما سنراه من خلال الفرعين التاليين.

الفرع الأول

حظر إعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور بدون إذن مسبق

على هدي الحماية الدستورية إتجهت التشريعات العقابية إلى معاقبة كل من يعتدي على **سرية** الإتصالات والمراسلات الخاصة للإفراد في غير الحالات المقررة قانونا، بإعتبار أن ذلك يتضمن إنتهاكا

---

criminelle et en matière correctionnelle, si la peine encourue est égale ou supérieure à deux ans d'emprisonnement, le juge d'instruction peut, lorsque les nécessités de l'information l'exigent, prescrire l'interception, l'enregistrement et la transcription de correspondances émises par la voie des communications électroniques. Ces opérations sont effectuées sous son autorité et son contrôle.

La décision d'interception est écrite. Elle n'a pas de caractère juridictionnel et n'est susceptible d'aucun recours".

[1]– تنص المادة 95 إجراءات مصري ""لقاضي التحقيق أن يأمر بضبط جميع الخطابات والرسائل والجرائد والمطبوعات والطرود لدي مكاتب البريد وجميع البرقيات لدي مكاتب البرق وأن يأمر بمراقبة المحادثات السلكية واللاسلكية أو إجراء تسجيلات لأحاديث جرت فى مكان خاص متى كان لذلك فائدة فى ظهور الحقيقة فى جناية أو جنحة معاقب عليها بالحبس لمدة تزيد على ثلاثة أشهر.

وفى جميع الأحوال يجب أن يكون الضبط أو الاطلاع أو المراقبة أو التسجيل بناء على أمر مسبب ولمدة لا تزيد على ثلاثين يوماً قابلة للتجديد لمدة أو مدد أخرى مماثلة."

[2]– تنص المادة 206 إجراءات مصري" لا يجوز للنيابة العامة تفتيش غير المتهم أو منزل غير منزله إلا إذا أتضح من إمارات قوية أنه حاز لأشياء تتعلق بالجريمة.

ويجوز لها أن تضبط لدي مكاتب البريد جميع الخطابات والرسائل والجرائد والمطبوعات والطرود ولدي مكاتب البرق جميع البرقيات ، وأن تراقب المحادثان السلكية واللاسلكية ، وأن تقوم بتسجيلات لمحادثات جرت فى مكان خاص ، متى كان لذلك فائدة فى جنحة معاقب عليها بالحبس لمدة تزيد على ثلاث أشهر.

ويشترط لاتخاذ أي إجراء من الإجراءات السابقة الحصول مقدماً على أمر مسبب بذلك من القاضي الجزئي بعد إطلاعه على الأوراق.

وفى جميع الأحوال يجب أن يكون الأمر بالضبط أو الإطلاع أو المراقبة لمدة لا تزيد على ثلاثين يوما ويجوز للقاضي الجزئي أن يجدد هذا الأمر مدة أو مدداً أخرى مماثلة . وللنيابة العامة أن تطلع على الخطابات والرسائل والأوراق الأخرى والتسجيلات المضبوطة ، على أن يتم هذا كلما أمكن ذلك بحضور المتهم والحائز لها أو المرسلة إليه وتدون ملاحظاتهم عليها . ولها حسب ما يظهر من الفحص أن تأمر بضم تلك الأوراق إلى ملف الدعوى أو بردها إلى من كان حائزا لها أو من كانت مرسلة إليه.

لحرمة الحياة الخاصة، حيث عاقب المشرع الجزائري بموجب المادة 303 عقوبات كل من يفض أو يتلف رسائل أو مراسلات موجهة للغير، كما عاقب بموجب المادة 303 مكرر كل من إلتقط أو سجل أو نقل مكالمات أو أحاديث خاصة أو صورة لشخص، بأي تقنية كانت، وهي نفس الجريمة التي عاقب عليها المشرع الفرنسي في المادة 226-1 والمصري بموجب المادة 309 مكرر عقوبات.

ومن مطالعة النصين السابقين، يمكن القول أنه إذا كان نص المادة الأولى يوفر الحماية للمراسلات بمعناها الضيق بما يعني الخطابات ونستدل على ذلك من عبارة "فض" ذلك أن مادية هذا السوك تقف بالنص موقف العاجز عن مد النطاق التجريم بالنص إلى حد شمول النموذج المستحدث، فإن نص المادة الثانية وإن كانت أحكامها تنطبق على الأحاديث التي تتم عن طريق الإتصالات السلكية واللاسلكية، فإنه ومع التطور الهائل في وسائل الإتصالات فقد أصبح الإعتماد على التكنولوجيا المتطورة في مجال الأنترنت والإتصالات يعطي الفرصة للتسجيل والتصنت ونقل الأحاديث أو تسجيلها من أماكن بعيدة ويتم هذا عن طريق الإتصال بشبكة الأنترنت.

غير أن هناك من قال[1] بأن النص السابق يخص المحادثات الشفوية التي تجري في مكان خاص، كما يخص المحادثات الشفوية التي تتم عن طريق التلفون، وبالتالي فهو ينحصر دون المحادثات التي تتم عن طريق الكمبيوتر والتي تتخد شكل البريد الإلكتروني أو شكل المحادثة الفورية، كما أن شبكة الأنترنت لا تعتبر مكانا خاصا حتى بالنسبة للمحادثات الفورية بنظام التشات.

غير أننا لا نؤيد هذا الرأي على إطلاقه، ذلك أنه وإن كان القول بعدم إنطباق النص السابق على المحادثات التي تتخد شكل البريد الإلكتروني كونه رسالة تتضمن حديثا كتابيا عكس الحديث الشفوي-إن كان هذا الأمر يحتاج لمزيد من التأمل القانوني[2]- فإننا نرى أن إدراج كل من المشرع الفرنسي والجزائري عبارة أحاديث ومكالمات معبرا عنها بصفة خاصة أو سرية، بعدما كان المشرع الفرنسي يشترط في المادة 368 أن تكون في **مكان خاص** المقابلة للمادة 309 مكرر عقوبات مصري، يسمح بتطبيق مقتضيات المادتين(303 مكرر جزائري-226-1 فرنسي) على المحادثة الصوتية التي تتم عن طريق أدوات الإتصال الصوتي الرقمي الخاصة بين المتعاملين[3](Voice Over IPو تختصر (VoIP)، وهي أدواتتُمكّن مستخدميها من

---

[1]-**عائشة بن قارة مصطفى**، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة للنشر، 2010، ص106، د. **شيماء عبد الغني**، المرجع السابق، ص244.

[2]- جيت يتجه البعض من الفقه إلى إعتبار الرسائل تتضمن حديثا كتابيا والمحادثات التلفونية تتضمن حديثا شفويا، ولا يوجد فارق بين الإثنين، فالعبرة بالجوهر وليس بالشكل، وقد نهجت نفس النهج بعض الأحكام في فرنسا، حيث ذهبت محكمة إستئناف بيزانسون إلى أن المحادثات التلفونية ماهي إلا رسائل منقولة بطريق الراديو الكهربائي، وتأخذ هذه المحادثات حكم المراسلات، وهو ما يسري على المراســلات الإلكترونــية.

CA Besançon, 5 janvier 1978, JCP, 1980, II, 19449, note D. Bécourt

أنظر: د.**محمد ابو العلا عقيدة**، مراقبة المحادثات التلفونية، دراسة مقارنة، الطبعة الثانية، دار النهضة العربية، 2008، ص68. **د. ياسر الأمير فاروق**، المرجع السابق، ص178.

[3]- أدوات الإتصال الخاص هي تلك التي يتم نقل المحادثات الشخصية بين طرفين تتعلق بامورشخصية، وان كان فيما مضى وسيلة الهاتف وتقتصر على المحادثات الصوتية وكان القانون يفرض حماية خاصة لها من الإنتهاك، فإن العصــر الحديث فقد تعددت وسائل الإتصال الخاصة وتطورت إمكانياتها فمنها مثلا البريد الإلكتروني وغرف الدردشة عبر الأنترنت والتي يتم فيها نقل الكتابة والصوت والصور من خلالها. د. **أيمن عبد الله فكري**، المرجع السابق، ص634.

التحدث مع آخرين حول العالم كما لو كانوا يحادثونهم هاتفيا، لكن دون تكلفة إن كانت من حاسوب إلى حاسوب، أو بتكلفة قليلة إن كانت من حاسوب إلى هاتف تقليدي، وهذا يجعلها مفيدة جدا، ومن أشهر برمجيات خدمات المحادثة الصوتية تتضمن (Skype و Jitsiو و Yahoo Voice و MSN Messenger.[1]

فضلا عن ذلك، فإن كل من المشرع الجزائري والفرنسي لم يولي كل منهما أهمية لإداة المراقبة، حيت نصا **باية تقنية كانت**، وهو ما يسمح بإستعياب التقنيات الحاضرة والمستقبلية التي يفرزها التقدم العلمي والتي يمكن إستخدامها في إلتقاط المكالمات بمختلف أشكالها ومنها التي تجري عبر الأنترنت، وكذلك فعل المشرع المصري بإستخدامه عبارة جهاز من الأجهزة ضمن المادة 309 مكرر.

وإن كنا نميل إلى إستيعاب النصوص السابقة الإتصالات الإلكترونية أي التي تتم عن طريق الوسائل الإلكترونية بالإضافة إلى الإتصالات السلكية واللاسلكية، إلا أن التردد حول تجريمها يجعل من الأفضل تدخل المشرع لتجريمها صراحة رفعا لكل لبس أو شك حول تجريمها تطبيقا **لمبدأ الشرعية** على نحو مافعلت بعض التشريعات كما هو حال المشرع الأمريكي، فالقانون الجنائي الفدرالي الأمريكي title 18 part 1 chapitre 119, Sec2510عاقب كل من إعترض أو حاول إعتراض أو ساعد غيره على أن يعترض أو يحاول إعتراض أي إتصال سلكي أو شفوي أو **إلكتروني**.[2] بل أن القانون الأمريكي يعاقب كل من أفشى أو حاول أن يفشي محتوى إتصال هاتفي أو إلكتروني إذا كان الفاعل عالما أو كان هناك من الأسباب ما يدعو إلى الإعتقاد أن المعلومات تم الحصول عليها من خلال ذلك الإعتراض المخالف للقانون[3]. كما ذهب القانون الأمريكي إلى أبعد من ذلك عندما عني بوضع تنظيم للمحادثات الإلكترونية، غير مكتف في ذلك بالقواعد العامة في المحادثات التلفونية، فقد ميز بين الإتصالات الإلكترونية والمحادثات الشفوية رغم أنهما محل للحماية ضد التنصت بقوله في المادة title 18 part 1 chapitre 119, Sec2511أن الإتصالات الشفوية تعني اي إتصال شفوي يصدر عن شخص يتوافر لديه توقع–يستند إلى تبرير مقبول– أن مثل ذلك الإتصال ليس محلا للإعتراض او التنصت، ولكن هذا المصطلح لا يشمل الإتصالات الإلكترونية[4].

أما عن الوضع في فرنسا، فقد قرر المشرع حماية جنائية لسرية المراسلات والبريد الإلكتروني في المادة 226–15 من قانون العقوبات[5]، فجرم إنتهاك المراسلات الخاصة حيث نصت على أنه "كل من قام

---

[1]– https://securityinabox.org/ar/guide/secure-communication-/

[2]- Interception and disclosure of wire, oral, or electronic communications prohibited,

(1)Except as otherwise specifically provided in this chapter any person who—

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

[3]-(c)intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

[4]-(2)"oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication;

[5]-**Article 226-15** Modifié par Ordonnance n°2000-916 du 19 septembre 2000 - art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002 dispose que " Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45000 euros d'amende.

بسوء نية بفتح أو حذف أو تأخير أو تحوير المراسلات المرسلة إلى الغير سواء وصلت لمكان الوصول أم لا، أو إطلع بطريقة غير مشروعة على مضمونها، يعاقب بالسجن لمدة سنة وبغرامة 45000 ألف يورو، كما يعاقب بنفس العقوبات كل فعل إرتكب بسوء نية بقصد إعتراض أو تحويل أو إستخدام أو نشر الإتصالات الخاصة، المرسلة أو المستقبلة بوسيلة إتصالات أو بواسطة إعداد أجهزة مهمتها إرتكاب هذه الأفعال"[1].

والبريد الإلكتروني هو مماثل للمراسلة الخاصة المحمية بموجب المادة السابقة[2] كون ركن العلانية لا يتوافر في نظامه، فقد قضي أن المراسلة الخاصة هي تلك التي توجه إلى شخص محدد أو أكثر طبيعيا كان أو معنويا، وعمليا فإن هذا التعريف ينطبق علاوة على البريد الإلكتروني على الرسائل الفورية ورسائل الوسائط المتعددة (sms, mms) ، قوائم المناقشة إذا كان تحديد المستلمين ممكن بطريقة آمنة ودقيقة[3].

وكذلك يمكن للمراسلات التي تتم عن طريق الأنترنت ومنها المراسلات المتعلقة بالتعاملات الإلكترونية أن يتم حمايتها عن طريق نص المادة 432 –9 عقوبات فرنسي[4]، حيث عاقبت هذه المادة بالحبس ثلاث سنوات وبغرامة 45000 يورو كل شخص عام أو مكلف بخدمة عامة إذا قام عند مباشرته لعمله أو بمنسابته بالأمر أو التسهيل أو القيام في غير الحالات المقررة قانونا، بإختلاس أو إزالة أو فتح المراسلات وكشف محتوياتها، ويعاقب بنفس العقوبة الشخص الدي يقوم بتشغيل الشبكات العامة للإتصالات الإلكترونية أو مزود خدمة الإتصالات إذا قام عند مباشرته لعمله بالأمر أو إرتكاب أو التسهيل –باستثناء الحالات المنصوص عليها في القانون– بإعتراض أو إختلاس مراسلات تتم أو تنقل أو تصل بطريق الإتصالات وكذلك بإستعمال أو بفض محتواها.

Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions."

[1]- dont la fabrication l'importation, la détention, l'exposition, l'offre, la location ou la vente, voire la publicité sont désormais punies, nouvel article L226-3 CP, introduit par l'Ordonnance n°2011-1012 du 24 août 2011; Modifié par LOI n°2016-731 du 3 juin 2016 - art. 5

[2]-Voir: **Murielle-Isabelle Cahen,** PROTECTION DES ECHANGES, article *disponible* en ligne á l'adresse suivante http://www.murielle-cahen.com/publications/page2310.asp

[3]--« il y a correspondance privée lorsque le message est exclusivement destiné à une ou plusieurs personnes, physiques ou morales, déterminées et individualisées. »] Jugement du Tribunal d'instance de Puteaux du 28 septembre 1999.

[4]-**Article 432-9** Modifié par Loi n°2004-669 du 9 juillet 2004 - art. 121 JORF 10 juillet 2004 **dispose que "** Le fait, par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public, agissant dans l'exercice ou à l'occasion de l'exercice de ses fonctions ou de sa mission, d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, le détournement, la suppression ou l'ouverture de correspondances ou la révélation du contenu de ces correspondances, est puni de trois ans d'emprisonnement et de 45 000 euros d'amende.

Est puni des mêmes peines le fait, par une personne visée à l'alinéa précédent ou un agent d'un exploitant de réseaux ouverts au public de communications électroniques ou d'un fournisseur de services de télécommunications, agissant dans l'exercice de ses fonctions, d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, l'interception ou le détournement des correspondances émises, transmises ou reçues par la voie des télécommunications, l'utilisation ou la divulgation de leur contenu."

كما يمكن إعتبار هذا العدوان عدوانا على **نظام المعالجة الآلية** بحسب ما هو مقرر من أحكام في المادة 323-1 عقوبات فرنسي والمادة 394 مكرر عقوبات جزائري، حيث يتطلب الأمر هنا حدوث إختراق ثم القيام بعد ذلك بالعدوان على الصفحة المحاطة بسرية ما.

ومن أمثلة الإعتراض غير المشروع للإتصالات الإلكترونية، إقتحام البريد الصوتي للمتعامل الإلكتروني، تثبيت برنامج التجسس على الهاتف المحمول، القرصنة بواسطة هوائيات المحمول.

الفرع الثاني

مشروعية إعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور

ذكرنا سلفا أن الأصل في المراقبة هو الحظر، لأنه إجراء خطير يهدد حقوق وحريات الأفراد، إلا أن توقيع العقاب على مخالفة هذا الحظر يبرز إلى الوجود مشكلة دقيقة، فذلك العقاب ينبغي له أن يكون عادلا، وهو لن يكون كذلك إلا إذا أتيح للمجتمع إكتشاف المجرم وإثبات جرمه، إلا أن هذا الإكتشاف وذاك الإثبات لا يجوز لأيهما أن يكون طاغيا، فتتعارض بذلك مصلحتان المصلحة العامة للمجتمع التي تقتضي العقاب الشامل لكل الجرائم، ويحققها تسهيل وسائل التوصل إلى الأدلة خاصة في الجرائم الخطيرة كالجرائم الماسة بالتعاملات الإلكترونية، ومصلحة المتهم في أن تتخذ ضده إجراءات غير جائرة تحترم إنسانيته وحقه في السرية، وهنا يأتي دور قانون الإجراءات الجزائية.

فلمحاولة إقامة التوازن المذكور يقتضي ضرورة تنظيم هذه المراقبة بنصوص واضحة تشمل جميع الضمانات التي تمنع تعسف السلطات المختصة في إستخدام هذا السلاح الخطير الذي يهدد حريات الأفراد.

أولا- الضوابط الموضوعية لتبرير المشروعية

أ-الجرائم التي يجوز فيها المراقبة:

لقد إختلفت التشريعات في إعتمادها معيار تحديد الجريمة التي تجيز المراقبة، حيث إعتمد المشرع الفرنسي معيار جسامة العقوبة المقرة للجريمة، حيث حددها في المادة 100 من قانون الإجراءات الجزائية بالجنايات والجنح المعاقب عليها بالحبس لمدة لا تقل عن سنتين حبس، وهو نفس المعيار الذي إتبعه المشرع المصري حيث حددها في المادة 95 و206 بالجنايات والجنح المعاقب عليها بالحبس لمدة لا تقل عن ثلاثة أشهر، ويعلل هذا المعيار أن المشرع يستشف خطورة الجريمة من جسامة العقوبة المقررة لها، فتكون العقوبة بمثابة الإرادة المعبرة عن التجريم[1].

وقد سبق وأن رأينا في درساتنا للحماية الجزائية الموضوعية للتعاملات الإلكترونية في مختلف جوانبها، أنه وفي نطاق منهج تقرير وإختيار الجزاء الجزائي، تبين لنا أن كل من المشرع الفرنسي والمصري قد إتبعا

[1]- **د. أحمد فتحي سرور**، الوسيط في قانون العقوبات، القسم العام، دار النهضة العربية، 1989، ص169.

نظام جزائي صارم من حيث العقوبات، ومن بين ما لجأ إليه هو تقرير العقوبات السالبة الحرية بما يزيد عن سنتين وثلاث سنوات حبس، وهو ما يجيز المراقبة في تلك الجرائم.

ذلك هو الوضع في كل من التشريع المصري والفرنسي، ذلك أن المشرع الجزائري إكتفى بإجازة المراقبة أن تكون الجريمة ذات طبيعة معينة حددها المشرع بصرف النظر عن مقدار العقوبة المقررة لها، ومن بين هذه الجرائم المساس بنظم المعالجة الآلية للمعطيات. ورغم كون ما تتميز به هذه الجرائم من خطورة وخاصية مميزة تبرر الإستعانة بهذا الإجراء، إلا أن هذا التحديد يقصي العديد من الجرائم الواقعة على التعاملات الإلكترونية من نطاق تطبيق هذه المراقبة كونه يتم إتخاده فقط بصدد الجرائم التي تقع على النظام فقط **كالدخول إليه بطريقة غير مشروعة أو التلاعب في معطياته.**

وعلى العموم، فإن تبرير اللجوء إلى هذا الإجراء لا يكفي أن تكون الجريمة محل المراقبة على درجة معينة من الخطورة، وإنما يلزم فوق ذلك أن تكون هذه الجريمة قد وقعت فعلا، فلا يصح إتخاذ هذا الإجراء كوسيلة لضبط جريمة مستقبلية أو محتملة، وهو شرط مسلم به في الغالبية العظمى من التشريعات.

ب–فائدة المراقبة في إظهار الحقيقة:

الناظر في التشريعات التي أجازت اللجوء إلى رقابة شخص أو مكان أو حديث أو مراسلة بصورة لا يحس معها الغير بمباشرتها، يلحظ أنها تقيد مباشرة الرقابة بكونها تفيد في ظهور الحقيقة، على النحو الذي يمكن أن نقرر معه أن "ضابط فائدة المراقبة في ظهور الحقيقة يعتبر السند الشرعي المبرر للمراقبة. والتي تتعلق باظهار الحقيقة في كشف غموض الجريمة وضبط الجناة[1]، وهو ما تطلبه المشرع الفرنسي صراحة في المادة 100 إجراءات جزائية[2]، وكذلك فعل المشرع الجزائري إذ قرن مباشرة المراقبة بان تقتضيها ضرورت التحري في الجريمة المتلبس بها أو التحقيق الإبتدائي في جرائم بعينها ومنها المساس بنظم المعالجة الآلية للمعطيات. كما ردد المشرع المصري هو بدوره هذا الشرط في المادة 206 إجراءات، إذ قرن مباشرة المراقبة بأن يكون لها فائدة في ظهور الحقيقة.

وهذا يقتضي بطبيعة الحال توافر دلائل كافية على أن من شأن المراقبة كشف غموض الجريمة وستساعد على ضبط الجناة. ويترك هذا التقدير للسلطة المختصة بإصدارالإذن، ويخضع هذا التقدير لرقابة محكمة الموضوع[3].

ت– محل المراقبة:

يتخد المـــحل الذي ينصب عليه إجراء المراقبة 3 أنـــواع:

---

[1]– **د. محمد أبـــو العلا عقيدة**، المرجع السابق، ص192.

[2]-Art 100 du CPP dispose que " le juge d'instruction peut, **lorsque les nécessités de l'information l'exigent**, prescrire l'interception

[3]-**د. ياسر الأمير فاروق**، المرجع السابق، ص451. **د.محمدأبو العلا عقيدة**، المرجع السابق، ص192.

النوع الأول:**هو المراسلات التي تتم عن طريق وسائل الإتصال السلكية واللاسلكية:**وإذا كانت شبكات الحاسب الآلي تستخدم خطوط التلفون وتستعين في ذلك بجهاز معدل الموجات والذي يستطيع تحويل الإشارات الرقمية المستخدمة بواسطة الحاسب الآلي إلى موجات تناظرية تنقل خلال خطوط التلفون، وبذلك فإنه يتبين وجود علاقة بين المراسلات التي تتم بالطرق التقليدية وتلك التي تتم بالوسائل الإلكترونية[1]، ولذلك فإن الأحكام الخاصة بالمراسلات تنطبق ولاشك على تلك التي تتم عبر الإتصالات الإلكترونية ومن بينها **رسائل البريد الإلكتروني.**

وإن كانت من وجهة النظر المادية فإن شبكة الأنترنت تتم عن طريق الاتصالات اللاسلكية، فقد أجازت التشريعات **صراحة** إعتراض الرسائل الإلكترونية، فالمشرع الفرنسي أجاز بموجب المادة 100 إجراءات إعتراض المراسلات التي تتم عن طريق الإتصالات الإلكترونية، وكذلك فعل المشرع الجزائري في المادة 4 من القانون رقم 09-04 تحت عنوان مراقبة الإتصالات الإلكترونية.

أما النوع الثاني من المحل هو **الأحاديث الخاصة أو السرية:** والمقصود بذلك تسجيل أحاديث المتهم وشركائه عن واقعة معينة من الوقائع المنصوص عليها في المادة 65 مكرر 5 إجراءات جزائري خلسةومن بينها المساس بنظم التعاملات الإلكترونية، أو الوقائع المعاقب عليها بعقوبة لا تقل عن 3 أشهر وفق المادة 95 و206 إجراءات مصري، ويأخذ حكم الحديث الخاص والسري ذلك الحديث الذي يجري في مكان خاص أو في مكان عام، وكان شخصيا وتضمن أدق الأسرار[2]، وإن كانت النصوص السابقة لم تواجه بشكل صريح تسجيل المحادثات الإلكترونية، فإن المشرع الفرنسي وعلاوة على نص المادة 100 إجراءات[3]، أجاز بموجب المادة 706-102-1[4] وما بعدها تحت عنوان "**إلتقاط المعطيات المعلوماتية**" بوضع ترتيبات تقنية(تثبيت عن

---

[1]- **د. هلالي عبد الله**، تفتيش نظم الحاسب الآلي، مرجع سابق، ص221. **سامح أحمد بلتاجي موسى**، الجوانب الإجرائية للحماية الجنائية لشبكة الأنترنت، رسالة دكتوراه، كلية الحقوق، جامعة الإسكندرية، 2010، ص131.

[2]- **فوزي عمارة**، المرجع السابق، ص237.

[3]-الملاحظ أنه في فرنسا يوجد أكثر من نص قانوني ينظم الوضع القانوني للمراقبة الإلكترونية كعمل اجرائي، فعلاوة على نص المادة 100 إجراءات، نجد المادة 706-95 وذلك في التحري في الجريمة المتلبس بها أو التحقيق الإبتدائي في الجرائم المنصوص عليها في المادة 706-73 و706-73-1 حيث أجازت إعتراض وتسجيل ونسخ المراسلات التي تتم عن طريق الإتصالات الإلكترونية على النحو المنصوص عليه في المادة 100 في فقرتها الثانية، 100-1، 100-3 لمدة أقصاها شهر واحد قابلة للتجديد مرة واحدة في نفس الظروف من حيث الشكل والمدة، وتتم العمليات المأذون بها تحت المراقبة المباشرة **لقاضي الحريات والحبس بالمحكمة العاليا** الذي أذن بها بناء على طلب النيابة العامة. ومن تم فإن إعتراض الإتصالات يخضع لنظام مزدوج ، فمن جهة نظام القانون العام بموجب القانون الصادر في 10 دويلية 1991 (100 إجراءات وما بعدها)، ومن جهة أخرى نظام خاص بالجرائم المنظمة (المادة 706-95 إجراءات)، هذا وقد تم إنشاء معالجة آلية للمعطيات الشخصية المشار إليها بإسم "نظام إرسال عمليات الإعتراض القضائي" (STIJ) لتوفير منبر وطني للإعتراض القضائي ومعطيات الإتصال بموجب المرسوم 30 جويلية 2007.
https://cours.unjf.fr/file.php/138/Cours/02_item/texteI1.htm#37

أكثر من ذلك نجد المادة 34-1 من قانون البريد والإتصالات الإلكترونية التي أجازت الدخول إلى قاعدة المعطيات ، فضلا عن المادة 706-102-1 من قانون الإجراءات الجزائية التي أجازت إعتراض المعطيات المعلوماتية .

[4]- **Article 706-102-1 DU CPPF** Modifié par LOI n°2016-731 du 3 juin 2016 - art. 5dispose que Si les nécessités de l'enquête relative à l'une des infractions entrant dans le champ d'application des articles 706-73 et 706-73-1 l'exigent, le juge des libertés et de la détention peut, à la requête du procureur de la République, autoriser par ordonnance motivée les officiers et agents de police judiciaire requis par le procureur de la République à mettre en place un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles sont stockées dans un système informatique, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données, telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques audiovisuels.

بعد برامج كحصان طراودة) بدون رضاء الشخص وذلك بغرض إلتقاط في الوقت الفعلي للمعطيات المرسلة أو المستقبلة عبر وسائل سمعية بصرية بما في ذلك **المحادثات القصيرة عبر السكايب**[1]، إلا أنها حصرتها في الجرائم المنصوص عليها في المادة 706–73 و706–73–1، منها السرقة المرتكبة في إطار جماعة منظمة، إتلاف الأموال في إطار جماعة منظمة، تزوير العملات، تبيض الأموال، الإحتيال في إطار جماعة منظمة، الإعتداء على نظم المعالجة الآلية للمعطيات ذات الطابع الشخصي التي تنفذها الدولة المرتكبة في إطار جماعة منظمة، والمنصوص عليها في المادة 323—4–1 من قانون العقوبات، وذلك بموجب أمر مسبب من قاضي التحقيق بعد أخذ رأي وكيل الجمهورية.

في حين أن النوع الثالث هو **إلتقاط الصور**: هذا المحل إنفرد به المشرع الجزائري، إذ لا نجد له ذكرا في نص المادة 100 فرنسي أو نص المادة 95 و206 إجراءت مصري، فالمشرعين وإن ساوو من حيث التجريم والعقاب بين ما يسمى بالمسارقة السمعية والمسارقة البصرية، فرقا بينهما من الوجهة الإجرائية.

وبمطالعة الفقرة الأخيرة من نص المادة 65 مكرر 5 إجراءات جزائري، يمكن القول أن صيغتها العامة تسمح بإستيعابها إلتقاط الصور الشخصية التي أخدت في أماكن خاصة، والمخزنة على أجهزة الحاسب الشخصية، أو الموجودة في الملفات الشخصية بالبريد الإلكتروني للأشخاص.

د–السلطة المختصة بإجراء المراقبة: يعد إجراء المراقبة من أشد الإجراءات خطورة، سواء نظرنا إليه في ذاته، أو من حيث ما قد يسفر عنه من نتائج، فهذا الإجراء يهدر حرمة الأحاديث الشفوية أو المكتوبة– الرسائل–، سواء تمت بوسائل الإتصال السلكية أو اللاسلكية أو الإلكترونية. ومن ثم فهو إجراء خطير في ذاته، وهذا الإجراء فضلا عن ذلك قد ينتج عنه دليل وهذا وجه آخر من وجه الخطورة. لذلك إتجهت التشريعات إلى وضع إجراء المراقبة في يد السلطة القضائية، وهو ما يعد تطبيقا لمبدأ "الضمان القضائي في الإجراءات الجزائية[2]". حيث أجاز المشرع الفرنسي المراقبة بناء على أمر مسبب من **قاضي التحقيق**[3]، وبالتالي لا يجوز لوكيل الجمهورية أو ضابط الشرطة القضائية إتخاذ المراقبة في أي ظرف من الظروف إلا بعد الحصول على إذن من قاضي التحقيق، وبذلك وضع المشرع نهاية الخلاف الفقهي المثار حول إمكانية المراقبة بواسطة ضباط الشرطة القضائية في حالة التلبس بالجريمة[4].

Le procureur de la République peut désigner toute personne physique ou morale habilitée et inscrite sur l'une des listes prévues à l'article 157, en vue d'effectuer les opérations techniques permettant la réalisation du dispositif technique mentionné au premier alinéa du présent article. Le procureur de la République peut également prescrire le recours aux moyens de l'Etat soumis au secret de la défense nationale selon les formes prévues au chapitre Ier du titre IV du livre Ier.

[1]- **Thierry Vallat**, Surveillance informatique: captation des données s'affichant à l'écran en temps réel avec le décret du 18 décembre 2015, disponible en ligne á l'adresse suivante https://translate.google.dz/?hl=fr#fr/ar/bref%20y%20compris%20les%20conversations%20via%20Skype.%0AThierry%20Vallat%2C%20Surveillance%20informatique%3A%20captation%20des%20donn%C3%A9es%20s'affichant%20%C3%A0%20l'%C3%A9cran%20en%20temps%20r%C3%A9el%20avec%20le%20d%C3%A9cret%20du%2018%20d%C3%A9cembre%202015%0A.

[2]- **د. ياسر الأمير فاروق**، المرجع السابق، ص295.

[3]-.... le juge d'instruction peut, lorsque les nécessités

[4]- أنظر: **د. محمد ابو العلا عقيدة**، المرجع السابق، ص107 وما بعدها.

وكذلك فعل المشرع المصري، فإعمالا لحكم المادة 45 من الدستور التي حظرت المراقبة إلا بأمر قضائي مسبب، جاءت المادة 95 لتجيز لقاضي التحقيق أن يراقب الأحاديث الخاصة، وإشترطت المادة 206 في حالة تولت النيابة العامة التحقيق بنفسها ورأت ضرورة للمراقبة أن تستأذن القاضي الجزئي.

وإن كان الأمر كذلك في كل من التشريع الفرنسي والمصري، فإن المشرع الجزائري قد نهج نهجا مختلفا، ذلك أنه وإن كان قد أناط مهمة إصدار الإذن للقيام بعملية المراقبة لقاضي التحقيق وتحت رقابته المباشرة في حالة فتح تحقيق قضائي حسب الفقرة الأخيرة من المادة 65 مكرر5، أجاز لوكيل الجمهورية المختص أن يـــأذن بها لضابط الشرطة القضائية.

وإن كان الندب للمراقبة لم يثر خلافا في القانون الفرنسي والجزائري من حيث جواز تكليف ضابط الشرطة القضائية بالقيام بالمراقبة، فالمادة 100-3 [1]إجراءات فرنسي صريحة في ذلك، كذلك المادة 65 مكرر5 الفقرة الأخيرة والمادة 65 مكرر 8 إجراءات جزائري، مع خص قاضي التحقيق الإشراف على المراقبة المباشرة لهذه العملية.فإن الخلاف في القانون المصري قائم حول جواز الندب، فبينما ذهب قلة من الفقهاء إلى حضره، فإن غالبية الفقهاء أقروا صحته، وهذا ما أخذت به محكمة النقض[2].

ثانيا- الضوابط الشكلية لتبرير المشروعية

أ-معطيات الإذن بالمراقبة:

تتعدد معطيات الإذن بالمراقبة وتتفاوت فيما بينها في الأهمية، فبعضها وجوبي و بعضها جوازي، ومن المعطيات الواجبة ما نص عليها القانون صراحة، حيث نصت المادة 100-1 إجراءات فرنسي على ضرورة شمول قرار قاضي التحقيق كل العناصر التي تسمح بالتعرف على الإتصالات المطلوب إعتراضها، الجريمة التي تبرر اللجوء إلى الإعتراض ومدتها. ويجب فضلا عن ذلك كتابة محضر بما أسفرت عنه المراقبة يذكر فيه تاريخ وساعة بداية هذه العملية والإنتهاء منها وهو ما شارت إليه المادة 100-4 إجراءات[3].

وكذلك فعل المشرع الجزائري بموجب المادة 65 مكرر7 إجراءات جزائري حيث نصت على ضرورة أن يتطلب الإذن كل العناصر التي تسمح بالتعرف على الإتصالات المطلوب إلتقاطها والأماكن المقصودة سكينة أو غيرها والجريمة التي تبرر اللجوء إلى هذه التدابير ومدتها. كما نصت الفقرة الأخيرة من المادة 65 مكرر 9 على جواز تحرير محضر من طرف ضابط الشرطة القضائية المأذون له أو المناب من

---

[1]-Article 100-3 du CPPFModifié par LOI n°2016-731 du 3 juin 2016 - art. 57 dispose que "Le juge d'instruction **ou** l'officier de police judiciaire commis par lui"

[2]-وإستندت محكمة النقض في ذلك على نص المادة 200 من قانون الإجراءات الجزائية التي تجيز لكل من عضو النيابة العامة في حالة إجراء التحقيق بنفسه أن يكلف أي من مأموري الضبط القضائي ببعض الأعمال التي من خصائصه فهذا النص عام مطلق، ويسري على كافة إجراءات التحقيق : نقض 12-2-1962 محموعة احكام النقض س13 رقم 37 ص 135، نقض27-2-1978 س29 رقم 34 ص193، مشار إليه: **د.ياسر الأمير فاروق،** المرجع السابق، ص376.

[3]-Art 100-4 du CPF dispose Que " Ce procès-verbal mentionne la date et l'heure auxquelles l'opération a commencé et celles auxquelles elle s'est terminée."

طرف قاضي التحقيق عن كل عملية مراقبة، على أن يذكر به تاريخ وساعة بداية العملية والإنتهاء منها. ويوضع هذا المحضر بين أوراق ملف الدعوى أمام القاضي المكلف به.

ولما كان محضر المراقبة وسيلة لإثبات المراقبة التي تمت، فإن عدم وجوده لا يؤدي الى بطلان إجراء المراقبة ذاته، ونستدل على ذلك بعبارة "**يجوز ...**، الواردة في المادة 65 مكرر 9" إجراءات جزائري، ومن ثم يكفي في ذلك أن تقتنع المحكمة من الأدلة المقدمة إليها في الدعوى بأن المراقبة قد أجريت وأنها قد أسفرت عما قيل أنه تحصل منها[1].

أما المشرع المصري فلم ينص على المعطيات التي يجب أن يشملها أمر المراقبة، ومن ثم وجب الرجوع للقواعد العامة التي تحكم إجراءات التحقيق.

لكن السؤال الدي يتبادر إلى الأذهان هنـــا هو: ماذا لو أنه أثناء المراقبة تم إكتشاف جرائم أخرى غير مذكورة في الإذن ؟ أجاب عن ذلك المشرع الجزائري في الفقرة الثانية من المادة 65 مكرر 6" بقوله **إذا إكتشفت جرائم أخرى غير تلك التي ورد ذكرها في إذن القاضي،فإن ذلك لا يكون سببا لبطلان الإجراءات العارضة**".

ب-تسبيب الإذن القضائي الصادر بالمراقبة:

وتبدو أهمية هذا التسبيب في كونه الوسيلة الفعالة في تقييد السلطة القضائية التي أدنت به، وتمكين محكمة الموضوع من بسط رقابتها على الأسباب التي إستندت عليها في إصدارها الإذن.

والأسباب التي يبنى عليها الإذن يجب أن تكون جدية وكافية لحمله، ولايشترط لصحة التسبيب أن تذكر الأسباب تفصيلا على نحو ما يتبع في صياغة الأحكام، بل يكفي الإشارة بإيجاز إلى الدلائل والقرائن التي تصوغ إصدار الإذن، كأن يذكر المحقق أن هناك تحريات جدية وكافية تحمل على الإعتقاد بأن محادثات أو مراسلات المتهم تمس الجريمة المقترفة، وأنه مما يفيد في كشف الحقيقة مراقبتها وإلتقاطها[2].

وهو ما تطلبه المشرع الفرنسي ضمنا في نص المادة 100 إجراءات، بأن يوضح فيه أن المراقبة إستدعتها ضرورة التحقيق، بمعنى أن تحديد الجناة وضبطهم أضحى مستحيلا، أو على الأقل صعبا بوسائل التنقيب والتحري المعتادة.

ولم يذهب المشرع الجزائري بعيدا عما قرره المشرع الفرنسي بشأن المراقبة، حيث إستلزم أن يكون الإذن مسببا وهو ما يستفاد ضمنا من المادة 65 مكرر 5 إجراءات، عملا بحكم المادة 46 من الدستور. وكذلك فعل المشرع المصري بموجب المادة 95 و 206 إجراءات عملا بحكم المادة 45 من الدستور.

ت-تحديد مدة المراقبـــة:

[1]- **د. ياسر الأمير فاروق**، المرجع السابق، ص580.

[2]-انظر: **د.محمد ابو العلا عقيدة**، المرجع السابق، ص186. **د. ياسر الأمير فاروق**، المرجع السابق، ص581.

حرصت معظم التشريعات المعاصرة على تحديد مدة معينة للمراقبة منعا من التعسف وإساءة إستعمال السلطة، غير أنها لم تسر على وتيرة واحدة في شأن هذه المدة، فمنها من أطال زمن المدة، كما هو حال المشرع الفرنسي الذي سار على نهجه المشرع الجزائري، حيث حددها بـــ 4 أشهر قابلة للتجديد ضمن نفس الشروط الشكلية والزمنية، إلا أن المشرع الفرنسي إشترط أن لا تتجاوز المدة كاملة للمراقبة سنة، حسب المادة 100-2 إجراءات، وإذا ما تعلقت الأمر بالجرائم المنصوص عليها 706-73 و 706-73-1 فتكون سنتين[1]، ومنها الإتجار بالمخدرات، السرقة المرتكبة في إطار جماعة منظمة، إتلاف الأموال في إطار جماعة منظمة، تزوير العملات، الأفعال الإرهابية، تبيض الأموال، الإحتيال في إطار جماعة منظمة، **الإعتداء على نظم المعالجة الآلية للمعطيات دات الطابع الشخصي التي تنفذها الدولة المرتكبة في إطار جماعة منظمة والمنصوص عليها في المادة 323—4-1 من قانون العقوبات.**

أما البعض الآخر فقد حدد المدة بأمد قصير كالمشرع المصري، حيث حددها بثلاثين يوما قابلة للتجديد لمدة أو مدد أخرى مماثلة طبقا للتحديد الوارد في نص المادتين 95 و 206 إجراءات مصري.

إذا ما إتخدت المراقبة في ظل إحترام ضابط مدة المراقبة وسائر الضوابط المقررة السابقة، ترتب أثر يتعلق بإمكانية الإعتداد بالأدلة الناجمة عنها في إثبات جريمة من الجرائم التي تقع على التعاملات الإلكترونية ونسبتها إلى المتهم، أما إذا لم يراعى بشأنها تلك الضوابط، فيترتب أثر عكسي يتمثل في إستبعاد الأدلة الناجمة عنها وعدم جواز قبولها في الإثبات، علاوة على تحقق المسؤولية الجزائية عن جريمة المراقبة غير المشروعة إذا ما توافرت الشرائط التي يتطلبها القانون لقيام هذه الجريمة[2].

ما تم ذكره يخص الرقابة القضائية، لكن إلى أي مدى يمكن لرب العمل مراقبة الإتصالات الإلكترونية الخاصة بالعاملين لديه والتبليغ عن الجرائم؟ وهذا التساؤل له أهميته القانونية، ذلك أنه إذا كان من حقه ذلك فإن ما يقرره من شهادة على وجود دليل على إرتكاب جريمة معينة يكون صحيحا ويمكن للمحكمة أن تعول عليه في قضائها الصادر بالإدانة.

لقد إختلفت الأراء حول مدى إمكانية السماح لرب العمل في مراقبة الموظف في عمله عند إستعماله جهاز الكمبيوتر في مكان العمل، وعما إذا كان من حقه أن يتداخل في جهاز الموظف أو المستخدم لكي يراقب إتصالاته بطريق الكمبيوتر أو يطلع على ما به من معلومات أو بريد إلكتروني؟ وكان الأمر يدور بين موقفين: أحدهما مؤيد و الثاني معارض لهذه المراقبة.

بالنسبة **للموقف المؤيد** يجسده رأي في **أمريكا**، وفي ذلك قضت المحاكم الأمريكية بأن من حق رب العمل أن يقوم بضبط كمبيوتر متحرك خاص بالعمل وأن يقوم بتسليمه إلى الشرطة، حيث أن الأمر يتعلق بأداة من أدوات العمل، كما أنه لا يتوافر لصالح العمل هنا توقع مقبول لإحترام الحق في الحياة الخاصة.

---

[1]- **Article 100-2** du CPPF Modifié par LOI n°2016-731 du 3 juin 2016 - art. 57 dispose que "Cette décision est prise pour une durée maximum de quatre mois. Elle ne peut être renouvelée que dans les mêmes conditions de forme et de durée, sans que la durée totale de l'interception puisse excéder un an ou, s'il s'agit d'une infraction prévue aux articles 706-73 et 706-73-1, deux ans".

[2]-**د. رؤوف عبيد**، المرجع السابق، ص446.

ولايختلف الأمر في العلاقة بين الموظف الإداري ورئيسه في العمل طالما يتعلق الأمر بجهاز يتبع جهة العمل، فللرئيس الإداري هذا الحق في المتابعة، وبالتالي فإن له أن يقوم بالتبليغ إلى جهات الشرطة والتعاون معهم دون الحاجة إلى صدور إذن بتفتيش هذا الجهاز.[1]

أما بالنسبة للموقف **المعارض** لهذا النوع من المراقبة، فيجسده **القضاء الفرنسي** حيث يعتد بحق العامل في الحياة الخاصة عند إستخدامه لأدوات العمل، فالمستخدم يتمتع بالحق في الحياة الخاصة في مكان وفي أوقات العمل وبصفة خاصة فيما يتعلق بسرية مراسلاته الخاصة، ومن تم ليس من حق رب العمل أن يطلع على المراسلات الشخصية الموجودة في الكمبيوتر الخاص بالمستخدم، ولو كان هذا الكمبيوتر من الأجهزة المخصصة للعمل، ولا يغير من ذلك أن يكون رب العمل قد حظر على المستخدم لدية إستعمال الكمبيوتر في غير أغراض العمل[2].

المطلب الثالث

توسيع الإختصاص الإقليمي لضباط الشرطة القضائية

يتحدد الإختصاص الإقليمي لضباط الشرطة القضائية بمكان إرتكاب الجريمة أو بمكان القبض على أحد المشتبه فيهم أو بمكان إقامة أحدهم، وذلك تحت سلطة وكيل الجمهورية الذي يدير عملهم في مرحلة جمع الإستدلالات، وبإنتداب قاضي التحقيق في حالة فتح تحقيق قضائي.

حيث تنص المادة 37 من قانون الإجراءات الجزائرية الجزائري "**يتحدد الإختصاص المحلي لوكيل الجمهورية بمكان وقوع الجريمة، وبمحل إقامة أحد الأشخاص المشتبه في مساهمتهم فيها أو بالمكان الذي تم في دائرته القبض على هؤلاء الأشخاص حتى ولو حصل هذا القبض لسبب آخر**"، وهو نفس ماجاء في المادة 40 بخصوص الإختصاص الإقليمي لقاضي التحقيق.

وإذا كان عمل ضابط الشرطة القضائية يجب أن يضفى عليه طابع المشروعية، بوجوب إلتزام القائمين على التحري والتحقيق بقواعد الإختصاص المقررة محليا وأن أي تجاوز يكون مصيره البطلان، فإن الإلتزام بالنطاق الإقليمي أحيانا يثير مشاكل خاصة تتعلق بعرقلة الإجراءات المتخذة من قبل ضباط الشرطة القضائية بصدد جرائم معينة، كما هو حال الجرائم الواقعة فيالحيز الإفتراضي عامة والجرائم الواقعة على التعاملات الإلكترونية خاصة. سواء في مرحلة الإستدلالات أو في حالة إنتدابهم بعد فتح تحقيق قضائي، كون هذه

1-Voir :**Albert J. Muick v. Glenayre Electronics** 280 F.3d 741, No. 98 C 3187 (7th Cir., February 6, 2002),available at http://www.internetlibrary.com/cases/lib_case262.cfm

-**René Pépin**, « Le statut juridique du courriel au Canada et aux États-Unis », (2001) 6-2 *Lex Electronica.* disponible en ligne á l'adresse précédente

[2]-Le 2 octobre 2001, la Chambre Sociale de la Cour de Cassation, dans son arrêt NIKON (99-42942) affirmait « que le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée ; que celle-ci implique en particulier le secret des correspondances ; que l'employeur ne peut dès lors sans violation de cette liberté fondamentale prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur. » Crim, **chambre sociale, Audience publique du mardi 2 octobre 2001, N° de pourvoi: 99-42942** .

الجرائم يمكن أن ترتكب في أكثر من نطاق إختصاص داخل الدولة كون الأنترنت ذات وجود عالمي بالمفهوم التقليدي.

وهو ما أدركه المشرع الجزائري، حيث ونظرا للطبيعة الخاصة للجرائم الواقعة على التعاملات الإلكترونية أقر إمكانية تمديد النطاق الإقليمي لضابط الشرطة القضائية إلى خارج الحدود المقررة قانونا لإختصاصه، فجعله ممتد ليشمل الإختصاص الإقليمي للمحكمة الموسع إختصاصها الإقليمي (القطب الجزائي) أو إلى النطاق الإقليمي الوطني أو إلى دائرة إختصاص المجلس القضائي.

حيث أنه وبناء على المواد 16 و 16 مكرر و 40 مكرر 1 و 40 مكرر 2 و 40 مكرر 3 من قانون الإجراءات الجزائية، جعل المشرع من الإختصاص الإقليمي لضباط الشرطة القضائية يتسع ليشمل إختصاص إقليمي لمحاكم أخرى غير المحكمة التي يباشرون مهمتهم في دائرة إختصاصها ليشمل دائرة إختصاص المحكمة الموسع إختصاصها الإقليمي وفقا لأحكام المرسوم التنفيذي رقم 06-348 هذا من جهة.

ومن جهة أخرى وسع المشرع من إختصاص ضباط الشرطة القضائية إلى كامل التراب الوطني وذلك في حالتيــن:

-**الحالة الأولى** : بحسب الصفة الأصلية للمنتمي لجهاز الشرطة القضائية، وهم فئة ضباط الشرطة القضائية من سلك الضباط وضباط الصف في مصالح الأمن العسكري، الذين لهم إختصاص على كافة التراب الوطني في البحث والتحري عن جميع أنواع الجرائم دون إستثناء، وهو ما أشارت إليه المادة 16-6 إجراءات.

-**الحالة الثانية:** بحسب طبيعة الجريمة موضوع البحث، ومن بينها الجرائم الواقعة على نظم المعالجة الآلية، حيث جعل من إختصاص ضباط الشرطة القضائية إختصاصا وطنيا وذلك تحت إشراف النائب العام المختص محليا وإعلام وكيل الجمهورية المختص محليا أيضا.

ويتميز هذا الإختصاص الوطني، بأنه إختصاص عام، يشمل جميع ضباط الشرطة القضائية وأعوانهم مهما كانت جهة إنتمائهم الأصلية.

فضلا عما سبق، منح المشرع الجزائري بموجب المادة 16 مكرر لضباط الشرطة القضائية وتحت سلطتهم أعوان الشرطة القضائية، مالم يعترض على ذلك وكيل الجمهورية المختص بعد إخباره، أن يمددو عبر كامل الإقليم الوطني عمليات مراقبة الأشخاص الذين يوجد ضدهم مبرر مقبول أو أكثر يحمل على الإشتباه فيهم بإرتكاب الجرائم المنصوص عليها في المادة 16 من بينها الجرائم الماسة بنظم المعالجة الآلية، أو مراقبة وجهة أو نقل أشياء أو أموال أو متحصلات من إرتكاب هذه الجرائم أو قد تستعمل في إرتكابها.

كما أتاح المشرع الجزائري تمديد الإختصاص الإقليمي للضباط إلى دائرة إختصاص عادية أخرى، وذلك بموجب الفقرة الثانية والثالثة من المادة 16 من قانون الإجراءات الجزائية، وذلك في حالة **الإستعجال** بدون طلب من السلطة القضائية(قاضي التحقيق) وحالة الإستعجال إذا طلب منهم أداء ذلك من قبل أحد رجال القضاء المختصين قانونا. ففي الحالة الأولى يتم تمديد الإختصاص إلى كافة دائرة إختصاص المجلس القضائي، أما في الحالة الثانية فإن الإختصاص يكون وطنيا شريطة أن يكون بناء على طلب من الجهة

القضائية. وذلك تطبيقا لحكم المادة 13 من قانون الإجراءات الجزائية التي تقرر أنه في حالة فتح تحقيق يتعين على الضبطية القضائية تنفيذ تفويضات جهات التحقيق وتلبية طلباتها، وكذلك تطبيقا للمادة 138 من نفس القانون ومايليها، وينبغي أن يساعدهم ضباط الشرطة القضائية الذي يمارسون وظائفهم في المجموعة السكنية المعنية.

وحالة الإستعجال حصرها جانب من الفقه الجزائي في نطاق الحالات التي يخشى معها ضياع الدليل، كما هو حال الجرائم الواقعة على التعاملات الإلكترونية، ويوسع البعض الآخر من مدلول الإستعجال ليشمل ضرورة البحث والتحري[1].

نخلص مما سبق أن المشرع الجزائري عالج مشكلة الإختصاص الإقليمي لضباط الشرطة القضائية، ففي حين تطلب الإلتزام بالنطاق الإقليمي أحيانا فإنه لم يمانع في إمتداد هذا الإختصاص في أحيان أخرى، وذلك في التحري والتحقيق في الجرائم الماسة بنظم المعالجة الآلية ومن بينها نظم التعاملات الإلكترونية، وهو ما يتماشى وطبيعتها الخاصة حيث يمكن حجب سلوكها وطمس أو تغطية نتائجها عن طريق التلاعب غير المرئي في النبضات أو الدبدبات الإلكترونية التي تسجل المعطيات عن طريقها، وهو ما يتطلب في المقابل ديناميكية وسرعة في تنفيذ الإجراء داخل الإقليم الوطني.

أما إذا تعلق الأمر بالبحث والتحقيق خارج حدود الدولة، كما لو كانت الأدلة المبحوث عنها موجودة في حاسوب خادم خارج حدود الدولة، فإن تمديد الإختصاص حتى ولو كانت حركته عبر الأنترنت يتعارض مع سيادة تلك الدولة التي يقع على أراضيها الخادم أو الملقم ، ويتم حل المشكلة عن طريق التعاون الدولي.

إلا أن تمديد الإختصاص الإقليمي على النحو السابق بيانه يبقى جزءا من حل في إطار الجرائم الواقعة على التعاملات الإلكترونية موضوع ممارسة ضباط الشرطة القضائية لعملهم المعتاد أو المتميز، ووجه الإثارة في هذه الجزئية تتعلق تحديدا بالدراية الفنية والرقمية بمتطلبات البيئة التقنية، إذ يتطلب التحقيق في الجرائم محل الدراسة مهارات متخصصة سواء في تتبع الجاني وتحديد هويته، أو في فحص أدوات التخزين الرقمية وغيرها كثير، ويجب على جهاز الشرطة بإعتباره **الأداة القضائية المحورية** في التحقيق معرفة كيفية تتبع نشاطات أولئك الذين يعملون عبر الأنترنت وكيفية الحصول على المعطيات من مقدمي خدمات الأنترنت، فبعض هذه المعطيات تخضع لقوانين خصوصية فلا يسمح بالحصول عليها إلا إذا كان ذلك تحت غطاء من المشروعية يبرر ذلك.

كما ينبغي على جهاز الشرطة أيضا معرفة طريقة تأمين الأدلة للحفاظ على سلامتها بحيث يمكنها الصمود أمام المحكمة عند الطعن في حجيتها، وأي تدخل في المعطيات الرقمية قد ينتج عنه تغيرها، ولكي تظهر للمحكمة أن المعطيات لم يتم تغيرها تراعي الشرطة في بريطانيا المباديء التالية عند ضبط الأدلة الإلكترونية:

[1]-**د. عبد الله اوهايبيه**، المرجع السابق، ص222.

-ينبغي عدم القيام باي شيء في سياق الحصول على هذه المواد من شأنه ان يغير المعطيات باي طريقة.

2-لا يتعامل المحققون مع المعطيات الأصلية إلا في الظروف الإستثنائية، وعند القيام بذلك ينبغي أن يجري الفحص شخص مختص وان يقدم تفسيرا كاملا إلى المحكمة بهذا الشأن.

3-ينبغي الاحتفاظ بسجل العمليات التي تمت خلال الفحص ومن ثم يمكن استخراج بيان بما تم عند طلبه[1].

لذلك كان من الضروري وإلى جانب دعم التعاون الدولي من خلال تفعيل الإتفاقات الشرطية الدولية، وتفعيل دور المنظمات الدولية للشرطة الجزائية إعداد إدارة خاصة تتعامل مع هذه النوعية من الجرائم وأدلتها على المستوى الوطني، تعتمد على قوة تكوين البناء العلمي والتكنولوجي لأفرادها تتلقى البلاغات وتلاحق المجرمين وتبحث عن الأدلة ضدهم وتقدمهم للمحاكمة.

وهذا ما دعت إليه الإتفاقية الأروبية لجرائم تقنية المعلومات، حيث جاء في المذكرة التفسيرية بيانا لضرورة إنشاء وحدات خاصة كما يلي:"" *كل طرف في الاتفاقية تكون ملزمة بتبني الإجراءات التشريعية و أية إجراءات أخرى ترى أنها ضرورية وفق قانونها الداخلي والأطر القانونية من أجل* ***إنشاء وتأسيس سلطات... مقررة داخل القسم الحالي بغرض التنقيبات أو الإجراءات الجنائية النوعية***"[2].

وفي هذا الإطار أنشأت الجزائر مصلحة مركزية للشرطة القضائية للمصالح العسكرية للأمن العسكري التابعة لوزارة الدفاع الوطني بموجب المرسوم الرئاسي رقم08-52 ، تضطلع المصلحة بمهام معاينة الجرائم **المقررة في قانون العقوبات** وقانون القضاء العسكري وجع الأدلة عنها والبحث عن مرتكبيها مالم يفتح تحقيق قضائي بشأنها، ففي حالة فتح فتح تحقيق قضائي فإن المصلحة تنفد تفويضات جهات التحقيق و تلبي طلباتها[3].

والملاحظ أن إختصاص هذه المصلحة إختصاص عام، يشمل جميع الجرائم دون إستثناء المنصوص عليها في قانون العقوبات، وهو ما ينطبق على الجرائم الماسة بنظم التعاملات الإلكترونية، علما أن إختصاصها المحلي يشمل الإقليم الوطني، إلا أنه تم حل هذه المصلحة بموجب المادة الأولى من المرسوم الرئـــاسي رقم 13-309 [4].

---

[1]- **أيمن رمضان محمد أحمد**، المرجع السابق، ص253.

[2]- Chaque État Partie est tenu d'adopter les mesures législatives et autres qui se révèlent nécessaires, conformément à son droit interne et à son cadre juridique, pour instaurer les pouvoirs et procédures prévus dans la présente section aux fins d'"enquêtes ou de procédures pénales spécifiques.Rapport explicative de la Convention sur la cybercriminalité,op,cit,p25.

[3]-المادة 3 و4 من المرسوم الرئاسي رقم 08- 52 الموافق لـــ 9 فيفري 2008، يتضمن إحداث مصلحة مركزية للشرطة القضائية للمصالح العسكرية للأمن التابعة لوزارة الدفاع الوطني وتحدي مهامها، جريدة رسمية، عدد8، صادرة بتاريخ 13 فيفري 2008.

[4]- المرسوم الرئاسي رقم 13-309 مؤرخ في 8 سبتمبر 2013 ، المتضمن إلغاء المرسوم الرئاسي رقم 08-52 المؤرخ في 9 فبراير 2008، والمتضمن إحداث مصلحة مركزية للشرطة القضائية للمصالح العسكرية للأمن التابعة لوزارة الدفاع الوطني و يحدد مهامها، جريدة رسمية، عدد 45،

كما تم إنشاء بموجب المرســـوم الرئاسي رقم 14-183 **مصلحة التحقيق القضائي لمدريرية الأمن الداخلي بدائرة الإستعلام والأمن،** وتقوم هذه المصلحة بضبط الإجراءات القضائية اللازمة لجمع **الأدلة المعنوية** والمادية المرتبطة بالجرائم والجنح التابعة لإختصاصاتها، ومن بينها الجريمة المنظمة التي تعتبر الجرائم الواقعة على التعاملات الإلكترونية أكثر جاذبية لها خاصة المتعلقة باساءة إستخدام معلومات بطاقة الإئتمان، كما تقوم المصلحة وفي إطار معالجة الآثار القضائية للقضايا المعالجة في المساهمة في الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال وقمعها[1].

هذا وتنفذ هذه المصلحة إنابات وطلبات الجهات القضائية، طبقا للقانون وفي إطار مهامها وصلاحياتها، وبهذه الصفة تباشر التحقيقات قصد جمع المعطيات الضرورية لدراسة الملف القضائي، كما تؤهل لمعالجة ملفات التعاون القضائي المتبادل.

لتبقى الإنطلاقة الحقيقية في مجال التخصص **للمصلحة المركزية لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال** التي تم إنشاؤها بقرار من المدير العام للأمن الوطني في جانفي 2015 لتضاف إلى الهيكل التنظيمي لمديرية الشرطة القضائية، فهذه المصلحة كانت عبارة عن فصيلة شكلت النواة الأولى لتشكيل أمني خاص لمحاربة الجريمة الإلكترونية على مستوى المديرية العامة للأمن الوطني والتي أنشات عام 2011. و من بين أوائل القضايا التي عالجتها وهي قضية قرصنة البنك الكندي من قبل المتهم (ف. محمد) سنة 2009 التي تم التطرق إليها في مواضع مختلفة من هذه الرسالة.

وتدعيما للتخصص بالتكفل بالشكاوى في هذا النوع من الجرائم، تم توسيع التشكيل الأمني بتكوين الفصائل على مستوى أمن 48 ولاية تابعة للمصالح الولائية للشرطة القضائية لأمن الولايات، وذلك بعد عملية إنتقاء لـــ 100 عنصر شرطة ممن تتوفر فيهم شروط الميول، الكفاءة، الإطلاع الدائم على التكنولوجيات الحديثة،الأنترنيت وشبكات التواصل الإجتماعي. وبذلك أصبح للمواطن الجزائري التقرب إلى هذه الفصائل لإيداع الشكاوى المتعلقة بالجرائم الإلكترونية أيا كان نوعها، فيما تتكفل الفصيلة المركزية لمكافحة الجريمة الإلكنرونية على مستوى العاصمة بمتابعة القضايا المعقدة وتقديم الدعم لمختلف الفصائل الولائية.

ولتحقيق الإحترافية أخذت المديرية العامة للأمن الوطني بعين الإعتبار التكوين المتخصّص مع إقتناء أحدث الوسائل والمعدات المستعملة في التحقيقات الجنائية،حيث تم برمجة 10 دورات تكوينية بالداخل في مجال التكنولوجيات الحديثة وتقنيات التحقيق من بداية سنة 2007 إلى غاية 2014 بمشاركة خبراء أجانب وجزائريين لفائدة 402 شرطي،في حين إستفاد أربعة إطارات من ثلاث دورات تكوينية بالخارج[2].

صادرة بتاريخ 18 سبتمبر 2013، ص4. أنظر كذلك : **محمد بكرارشوش،** الإختصاص الإقليمي الموسع في المادة الجزائية في التشريع الجزائري، مجلة دفاتر السياسة والقانون، مجلة جامعية محكمة، العدد 14، جامعة قاصدي مرباح، جانفي 2016، ص318.

[1]-المادة 4-5-6 من المرسوم الرئاسي رقم 14-183 المؤرخ في 13 شعبان 1435 الموافق ل 11 يونيو 2014 المتضمن إنشـــاء مصلحة التحقيق القضائي لمديرية الأمن الداخلي بدائرة الإستعلام والأمن ومهامها وتنظيمها، جريدة رسمية، عدد 32، صادرة بتاريخ 12 يونيو 2014.

[2]-وهو ما كشف عنه عميد الشرطة مصطفاوي عبد القادر رئيس المصلحة في ركن روبورتاج منشور بمجلة الشرطة متاح على الموقع التالي:

وإذا كان نشوء التخصص في مجال الضبط القضائي في إطار الجرائم محل الدراسة ليس أمرا لازما بل طبيعيا في الحقيقة، إلا أن هذا النوع من الجرائم يحتاج إلى أكثر من مجرد التخصص، فهو يحتاج إلى أساليب تقنية في البحث الجنائي لإثبات وقوع هذه الجرائم، وهو ما يطلق عليه بـــ: "**الشرطة العلمية**" والتي تعد من أهم الفروع التابعة لمديرية الشرطة القضائية التي تعمل معها جنبا إلى جنب في حل القضايا الصعبة ومن ضمنها الجرائم محل الدراسة، لما تتوافر عليه من أجهزة واختبارات وهياكل مخبرية لفحص كافة الأثار الجنائية ومنها الرقمية، حيث يحتل **المعهد الوطني للشرطة الجنائية** أو **المخبر المركزي للشرطة العلمية والتقنية** بالسحاولة بالجزائر العاصمة، بمصالحه الـــ 15 المرتبة الثانية إفريقياً والأولى عربياً بين مخابر الشرطة[1]. يتبع المخبر المركزي أربع مخابر جهوية موزعة عبر التراب الوطني وهي: المخبر الجهوي بوهران، قسنطينة، بشار، تمنراست.

وبحكم أن التعامل عبر الشبكة له طابع إلكتروني وبالتالي لا يمكن مراقبة كل المواقع، تم إنشاء هيئة وطنية لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال بمقتضى القانون 09-04، ليتم تنصيبها أواخر 2015[2].

وهي سلطة إدارية مستقلة توضع لدى الوزير المكلف بالعدل، تضم الهيئة لجنة مديرة، مديرية عامة، مديرية للمراقبة الوقائية واليقضة الإلكترونية، مديرية التنسيق التقني، مركز للعمليات التقنية، ملحقات جهوية.

تتولى هذه الهئية وتحت رقابة السلطة القضائية، بتنشيط وتنسيق عملية الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها ومصاحبة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن هذه الجرائم. كما تتولى تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام ولإتصال وتحديد مكان تواجدهم.

كما تكلف بإقتراح عناصر إستراتيجية وطنية للوقاية من الجرام المتصلة بتكنولوجيات الإعلام والإتصال ، تطوير التعاون مع المؤسسات والهئيات الوطنية المعنية بالجرائم المتصلة بتكنولوجيات الإعلام والإتصال، والمساهمة في تكوين المحققين المختصين في مجال التحريات التقنية المتصلة بتكنولوجيات الإعلام والإتصال، والمساهمة في تحديث المعايير القانونية في مجال إختصاصها.

وإلى جانب الجزائر، نجد العديد من الدول أجنبية كانت أو عربية التي كانت سباقة في هذا المجال[1]، فبالنسبة للدول الأجنبية نجد فرنسا مثلا، فبناء على توصية مجلس أروبا رقم R 95 -13 التي دعت إلى

---

http://www.essalamonline.com/ara/permalink/52564.html

[1]-https://ar.wikipedia.org/wiki

[2] -المرسوم الرئاسي رقم 15-261 الموافق ل8 اكتوبر 2015، المحدد لتشكيلة وتنظيم وكيفيات سير الهئية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، جريدة رسمية ، عدد53، صادرة بتاريخ 8 أكتوبر 2015.

إنشاء وحدات خاصة لمكافحة الجرائم الناشئة عن إستخدام تكنولوجيا المعلومات والإتصالات[2] ، قامت بإنشاء عدة وحدات ومراكز متخصصة وغير متخصصة ضمن الشرطة والدرك الوطني لمكافحة هذا الإجرام، ومن ذلك:

---

[1]– لم يتوقف الأمر على المستوى الوطني فحسب, فالبعد الدولي لهذه الجرائم باعتبارها من الجرائم العابرة للحدود, بما يمكن أن تتعدّى آثارها عدّة دول, ممّا يستحيل على الدّولة القضاء عليها بمفردها, لذلك فإنّ الحاجة تدعو إلى ضرورة التّعاون فيما بينها باعتباره إحدى الضّرورات اللّازمة لمواجهة هذه الأنشطة الإجراميّة المستحدثة, ويعدّ التّعاون الشّرطي الدّولي "*la coopèration policiere international*" من أهم صور التّعاون الدّولي في مكافحة الإجرام بصفة عامّة و الإجرام العابر للحدود لا سيما إجرام تقنيّة المعلومات بصفة خاصّة, ويتحقّق هذا التّعاون من خلال عدّة أجهزة من أهمّها: **المنظّمة الدّولية للشّرطة الجنائيّة**,و تهدف هذه المنظّمة إلى تأكيد و تشجيع التّعاون بين أجهزة الشّرطة في الدّول الأطراف على نحو فعّال في مكافحة الجريمة, وذلك عن طريق تجميع المعلومات المتعلّقة بالمجرم و الجريمة من خلال المكاتب المركزيّة الوطنيّة للشّرطة الدّولية الموجودة في أقاليم الدّول المنظّمة إليها, وتبادل هذه المعلومات فيما بينها.

هذا و قد أكّد سكرتير الأنتربول الدّولي"*raymond kendall*"في مؤتمر جرائم الأنترنت المنعقد في لندن في 2000/10/9 على ضرورة تعاون الدّول في مكافحة جرائم تقنية المعلومات بصفة عامة باعتبار هذه الأخيرة تبرز كظاهرة دوليّة, وقد أكد على أنه يجب على المجتمع الدّولي عدم الانتظار إلى حين عقد معاهدات و اتّفاقيات في هذا الإطار بل يجب الشروع و بشكل فوري في مكافحة هذه الجرائم, و يقوم الأنتربول بوضع إستراتيجية جديد لمواجهة جرائم الاعتداء على نظم المعالجة الآلية بالتعاون مع الأمم المتحدة.

و تجدر الإشارة إلى أنه يوجد منظمات أخرى لها دور لا يقل عن دور الأنتربول في مواجهة هذا النوع المستحدث من الإجرام على المستوى الدّولي و نخص بالذّكر منظمة التّعاون الاقتصادي و التّنمية *OECD* و مجموعة الثّمانية الاقتصاديّة *G-8GROUPEOFEIGHT ECONOMIES* حيث قامت بإعداد ملتقى دولي في نهاية نوفمبر 2000في طوكيو لتكوين قوة دوليّة أطلق عليها*DIGITALOPPORTUNITY TASK FORCE* تتمثّل مهامها في تحقيق أمن تكنولوجيا المعلومات.

و على غرار هذه المنظّمة أنشأ المجلس الأوروبي في لوكسمبورغ في عام 1991 شرطة أوروبيّة "الأوربول" و الّتي تّتخذ من لاهاي_هولندا_ مقراً لها, لتكون همزة وصل بين أجهزة الشّرطة الوطنيّة في الدّول المنظّمة و لملاحقة الجناة في الجرائم العابرة للحدود ومنها بطبيعة الحال جرائم الاعتداء على نظم المعالجة الآلية.

في 2002/2/28 تمّ إنشاء "الأورجست" من قبل مجلس الإتّحاد الأوروبي كجهاز يساعد على التّعاون القضائي و الشّرطي في مواجهة الجرائم الخطيرة,حيث يعدّ دعامة في فعاليّة التّحقيقات و المطاردات المتّبعة من قبل السّلطات القضائيّة الوطنيّة, خصوصًا فيما يتعلّق بالأنشطة المرتبطة بجرائم الاعتداء على نظم المعالجة الآلية.

إلى جانب الأنتربول و الأورجست تمّ إنشاء فضاء جماعي من غير حدود سمّي **بشجن** و ذلك من خلال التّوقيع على معاهدة *scengen* في 1985/6/14 و على اتّفاقيّة تطبيق تلك المعاهدة في 1990/6/19 وقد استحدثت هذه الاتّفاقية وسيلتين جديدتين لتعزيز التّعاون الشّرطي الأوربي لمواجهة التّحديّات الأمنيّة التي تفرضها الظّروف الجديدة, منها جرائم الاعتداء على نظم المعالجة الآلية و تتمثّل هاتين الوسيلتين في مراقبة المشتبه فيهم عبر الحدود و ملاحقة المجرمين.

فضلاً عن ذلك قام مركز التّدريب الوطني عن الجرائم التّقنيّة "*nslec*" وهو أحد المؤسّسات التّابعة للإتّحاد الأوروبي بإعداد المشروعات و البرامج التي تهدف إلى مكافحة الجرائم عاليّة التّقنية, ومن أهم هذه المشروعات مشروع فالكون 2001, وأيضاً برنامج أجيس 2004/2003 اللّذان يهدفان إلى التّدريب على مكافحة جرائم الاعتداء على نظم المعالجة الآلية. أمّا على المستوى العربي نجد أنّ مجلس وزراء الدّاخلية العرب أنشأ المكتب العربي للشّرطة الجنائيّة مجاله مكافحة الجريمة وملاحقة المجرمين في حدود القوانين و الأنظمة المعمول بها في كلّ دولة, للمزيد من التفاصيل أنظر على التوالي:

–**د. عمر محمد أبو بكر بن يونس**، الجرائم الناشئة عن استخدام الأنترنت، المرجع السابق، ص814.

-N adine adine L.C thwaites; eurojust, autre brique dans l'édifice de 1 coopération judiciaire en matiere pénale ou solide mortier?, R.S.C.C, n 1 , janvier –mars 2003 , p 45 .

:L'harmonisation des moyens de lutte contre la cybercriminalité , revue de web, realize le22/4/2004, disponible en lingne á l'adresse suivante: http://www.finances-gouv.fr.

د. عفيفي كامل عفيفي، المواجهة الشرطية لجرائم الكمبيوتروالأنترنت, منشور على الموقــع التــالي:

http://www.wadmadani.com/vb/showthread.php?t=26760

[2] Article -16 (Annexe à la Recommandation n° R (95) 13 relative aux problèmes de procédure pénale liés à la technologie de l'information) .dispose que " La création d'unités spécialisées pour la répression d'infractions dont la poursuite requiert une expérience spéciale en matière de technologie de l'information devrait être examinée. Des programmes de formation permettant au personnel de la justice pénale d'approfondir leurs connaissances en la matière devrait être promus".

- ***المكتب المركزي لمكافحة الإجرام المرتبط بتكنولوجيا المعلومات و الاتصالات المعروف اختصارا بـــOCLCTIC)***يعتبر هذا المكتب سلاح الدولة الفرنسية في مكافحة جرائمتقنية المعلومات بصفة عامة, إلى جانب وحدات أخرى, ولقد تم إنشاءه بموجب مرسوم بيوزاري رقم 2000-405 المؤرخ في 15-5-2000 على مستوى المديرية المركزية للشرطة القضائية التابعة لوزارة الداخلية[1].
- فريق التحقيق حول الغش في تكنولوجيا المعلومات المعروف إختصارا بـــ (BEFTI)[2]
- القسم المركزي لقمع الجرائم المعلوماتية المعروف إختصارا بـــ: (BCRCI)[3]
- المصلحة المركزية للإستخبارات الجنائية المعروفة إختصارا بـــ: (SCRC)، المعروف سابقا بـــقسم الأنترنت التابع للمصلحة التقنية للبحوث القانونية و الوثائقية المعروف اختصارا بـــ*(STRJD)*[4]
- *القسم المعلوماتي الإلكتروني التابع لمعهد البحوث الجزائية للدرك الوطني المعروف اختصارا بـــ (IRCGN)*[5]
- *وحدات أقسام الاستعلامات والتحقيقات القضائية المعروفة اختصارا بـــ (BDRIJ)*[6] [7]

---

[1]- Décr. n º 2000-405 du 15 mai 2000 portant creation d'un office central de lutte contre la criminilaté liéé aux technologies de l'information et de la communication.

[2]- la Brigade d'enquête sur les fraudes aux technologies de l'information; a été créée en 1994:

[3]- la Brigade centrale de répression de la criminalité informatiqueest créée en 1994 au sein de la Direction centrale de la police judiciaire et de la sous-direction des affaires économiques et financières

[4]-Le **Service central de renseignement criminel** (**SCRC**), anciennement **Service technique de recherches judiciaires et de documentation** (**STRJD**) ; « *Décret n° 2015-1805 du 28 décembre 2015 modifiant le code de procédure pénale (partie règlementaire) et relatif aux unités de la gendarmerie nationale au sein desquelles les officiers et agents de police judiciaire exercent leurs fonctions habituelles*

[5]L'Institut de recherches criminelles de la gendarmerie nationale. dispose d'une division ingénierie et numérique, au sein de laquelle a été créé en 1992 un département « *informatique-électronique* » ayant pour objectif de répondre aux demandes croissantes en matière de preuves numériques, et un département « *signal image parole* » chargé de traiter les enregistrements audio et vidéo. Ces deux départements réalisent des examens scientifiques et des expertises judiciaires, apportant ainsi un soutien technique de point aux enquêteurs.

[6] -La **Brigade départementale de renseignements et d'investigations judiciaires** (**BDRIJ**) est une unité de la Gendarmerie nationale française chargée de centraliser, d'orienter, de diffuser et d'exploiter les fichiers nationaux concernant les personnes et les véhicules recherchés et d'effectuer des rapprochements judiciaires au profit des unités.

[7]– للمزيد من التفاصيل حول هذه الأقسام, مهامها, أنظر ما يلي:

-Rapp. présenté **par Thierry Bereton** et remis á monsieur le minustre de l'interieure et dela sécuritéintérieure et des libertés locales: Chantier sur la lutte contre la cybercriminalté, 25-02- 2005, disponible en ligne á l'adresse suivante : http;/www.lesechos. fr

-La gendarmerie et la lutte contre la cybercriminalite, disponible en ligne á l'adresse suivante http://www.libertysecurity.org/article226.html

- **M. Robert DEL PICCHIA,;** Rapp. fait *au nom de la commission des Affaires étrangères, de la défense et des forces armées (1) sur le projet de loi,* ADOPTÉ PAR L'ASSEMBLÉE NATIONALE*, autorisant l'approbationde la* **convention** *sur la* **cybercriminalité** ***et du*** **protocole additionnel** *à cette convention, relatif à l'incrimination d'***actes** *de nature* **raciste** *et* **xénophobe***commis par le biaisde* **systèmes informatiques**, disponible en ligne á l'adresse suivante:http://www.senat.fr/rap/104-321/104-3210.html

-La police nationale; la lutte contre la cybercriminalté et les frauds aux cartes bancaires, , disponible en ligne á l'adresse précédente.

-La Convention sur la cybercriminalité, signée par la France le 23 novembre 2001, est entrée en vigueur avec l'adoption du décret du 23 mai 2006, revue de web, realize le 5/11/2009, disponible en ligne á l'adresse suivante; http://www.foruminternet.org/specialistes/veille-juridique/actualites/publication-de-la-convention-sur-la-cybercriminalite-au-journal-officiel.html

-M. Jean-Marc Nesme, rapp. fait au nom de la commission des affaires étrangéres sur le projet de loi (**n° 905**).**autorisant l'approbation de la convention sur la cybercriminalité** disponible en ligne á l'adresse suivante;http://www.assemblee-nationale.fr/12/cr-cafe/04-05/c0405018.asp

وإلى جانب فرنسا نجد النّموذج المعتاد والأكثر شهرة هو"**الإدارة المتخصصة لمتابعة جرائم تقنية المعلومات بمكتب التحقيقات الفدرالي** Fbiفي الولايات المتحدة الأمريكية الذي يضم بداخله مجموعة أشخاص مدربين على كيفية متابعة تلك الجرائم والتحري عنها وضبطها والمحافظة على ما يتم تحصيله من أدلة. وهي إدارة نالت الاعتراف بها كواحدة من أنجح هيئات مكافحة الإجرام التقني.

أما على المستوى العربي، فنجد مثلا مصر أيضا حيث أنشأت هذ الأخرى**إدارة مكافحة جرائم الحاسبات وشبكات المعلومات** وذلك بموجب القرار رقم 13507 لسنة 2002 الصادر عن وزارة الداخلية المصرية، وهذه الإدارة جديدة في تكوينها ونوعيتها تختص بمكافحة مثل تلك الجرائم، وهي في الأصل تابعة للإدارة العامة للمعلومات والتوثيق، وتخضع للإشراف المباشر لمدير الإدارة، وتشرف عليها فنيا مصلحة الأمن العام، ويشمل البناء التنظيمي لهذه الإدارة على ثلاث أقسام و هـــــي:**قسم العمليات:** ويختص بمكافحة الجرائم التي تقع باستخدام أجهزة الحاسب الآلي في مجالات نظم وشبكات وقواعد المعطيات، وإخطار الأجهزة النوعية المختصة بأعمال المكافحة بالمعطيات والمعلومات المتعلقة بالجرائم الجنائية التي يُمكن التوصل إليها من خلال الاتصال بشبكات المعلومات والتنسيق معها ، وإعداد قاعدة معطيات بجرائم المعلومات التي تدخل في نطاق إختصاص الإدارة والأحكام الصادرة فيها.

قسم التـــأمين:ويختص بوضع الخطط والأساليب التي تُستخدم في مجال تأمين نظم المعلومات والشبكات الخاصة بأجهزة الوزارة، وتقديم العون لكافة أجهزة الوزارة التي تطلب تأمين نظم معلوماتها وشبكاتها حماية للثروة المعلوماتية بها، ومتابعة التراخيص التي تصدر للشركات الخاصة في مجال نظم وأجهزة وشبكات المعلومات وذلك بالتنسيق مع الجهات المعنية.

قسم البحـــوث والمساعدات الفنية:ويختص بإعداد البحوث الفنية والقانونية في مجال تأمين نظم وشبكات المعلومات بالحاسبات الآلية، بحث مدى ملاءمة التشريعات الجنائية لمواجهة جرائم المعلومات التي تدخل في مجال عمل الإدارة واقتراح التوصيات، تقديم الدعم الفني لجميع جهات الوزارة في كافة القضايا والوقائع المرتبطة بمجال نظم وبرامج وأجهزة وشبكات المعلومات، توفير كافة المساعدات الفنية وإبداء الرأي والمشورة للجهات سواء من داخل الوزارة أو خارجها للمعاونة في عمليات ضبط الجرائم التي تتم باستخدام الحاسب الآلي.

وتجدر الإشارة إلى أن إدارة مكافحة جرائم الحاسبات وشبكات المعلومات ليست الإدارة الوحيدة المختصة بمكافحة هذه الجرائم، بل هناك عدة جهات تسعى إلى تحقيق هذا الهدف، من قبيل ذلك الإدارة العامة لمباحث الأموال العامة، الإدارة العامة للمعلومات والتوثيق، وتعد هذه الأخيرة من أكثر الإدارات بوزارة الداخلية تعاملا مع الجرائم المعلوماتية، وهي تختص بعملية المتابعة الفنية من خلال التحري عن الجرائم المبلغ عنها من الإدارات الأخرى، كما تقوم بتحديد شخص المتهم من خلال عملية التتبع باستخدام عنوان الأنترنت*IP*الذي يتعامل من خلاله الشخص مع شبكة الأنترنت[1].

[1]–أنظر:**د. أيمن عبد الحفيظ عبد الحميد سليمان**، إستراتيجية مكافحة الجرائم الناشئة عن إستخدام الحاسب الآلي، دراسة مقارنة، رسالة دكتوراه، أكاديمية الشرطة، 2003، ص398 ومابعـــدها.

كما نجد أيضًا الأردن الّتي أنشأت مديريّة الأمن العام **قسم خاص يعنى بجرائم تقنية المعلومات بصفة عامة** ويتولىّ إجراءات المكافحة والاستدلال والتحقيق في الجرائم التي ترتكب بواسطة النظم هدفا أو بيئة لها وذلك عام 1998[1].

إلا أن منطق التخصص في مجال قانون تكنولوجا الإعلام والإتصاللن يكون له دور طالما لم يكن هناك دورا تشريعيا يتولى التخصص القيام بأعبائه، إذ لا يرتبط الأمر بمجرد الإعداد الإداريوالفني لأعضاء التخصص و تفريعاته، بقدر ما يرتبط بوجود تشريعات يتولى التخصص تنفيدها بشكل يحقق الهدف والغاية منها، وإن كانت بعض الدول كفرسا والتي إتبعت نهجها الجزائر قد خطت خطوات في هذا المجال، فلازالت بعض الدول مثل مصريعد قطاع التشريع فيها مشروع قانون مكافحة جرائم تقنية المعلومات، إلى جانب تجريم بعض الأفعال المرتبطة بالتعاملات الإلكترونية في قانون التوقيع الإلكتروني، إلا أنه إقتصرت نصوصه على تنظيم تجريم السلوكات والممارسات الإلكترونية التي لا يوجد ما يجرمها في القانون المصري، والمعروف أن هناك فرق بين القانون الذي يجرم السلوك ويحدد الأفعال المجرمة وعقوباتها وبين قانون الإجراءات الذي يضم مجموعة القواعد القانونية التي تنظم النشاط الذي تباشره السلطات العامة بسبب جريمة إرتكبت و تستهدف به تحديد المسؤول عنها و إنزال العقوبة أو التدبير، فكان لابد من إضافة نصوص قانونية تنظم الجوانب الإجرائية لهده النوعية من الجرائم.

المبحث الثالث

تعاون مقدمي الخدمات مع رجال الضبط القضائي

تسمح الغالبية العظمى من التشريعات بإلزام مقدمي الخدمة بالتعاون مع رجال الضبط القضائي، بتسليم أو كشف ما تحت أيديهم من معلومات والتي يطلب منهم حفظها لمدة معينة، أو التحفظ عليها من أجل الإجابة عن طلب أو أمر. ولعل أن تأطير هذا الإجراء قانونيا، هو إجراء مناسب لإعفائهم من كل مسؤولية عقدية أو غير عقدية، خاصة إذا كان الإلتزام بالتعاون يتجاوز الحدود السابقة إلى الإعتراض في الوقت الفعلي لمعطيات المحتوى بما في ذلك معطيات المستند التي تعد لإثبات ما إذا كان الإتصال مشروعا من عدمه، وكل ما يفيد في تحصيل دليل الكتروني في جريمة وقعت بالفعل أو يرجح وقوعها في فترة وجيزة.

وهو ما دعت إليه لجنة الوزراء للمجلس الأروبي في توصيتها رقم 13 لسنة 1995، بأن تتضمن قوانين الإجراءات الجزائية في الدول الأعضاء منح رجال الضبط القضائي السلطة التي تسمح لهم بطلب

[1]– وقد تم تزويد هذا القسم بمختصين في مجال علوم وهندسة الكمبيوتر، وكما تم تزويده بما يلزم من أجهزة ومعدات وبرمجيات تساعده في عمليات التحقيق في جرائم الكمبيوتر وفي فحص الأجهزة المضبوطة في الجريمة والمحافظة على الأدلة فيها.**وضاح محمود الوضاح، نشأت مفضي المجالي**،جرائم الأنترنت –التعرض للأخلاق و الآداب العامة، الحض على الفجور ، جرائم الإستغلال الجنسي للأطفال، دار المنار، عمان، 2005، ص119.

المعلومات المتواجدة لدى مقدمي الخدمات والتي تفيد في الكشف عن الحقيقة، ويترتب على ذلك القول أن مزودي الخدمات ليسو من أصحاب المهن الملتزمين بسر المهنة"[1].

ولاشك أن تعاون مقدمي الخدمة على النحو السالف بيانه من شأنه أن يوفر مرونة في تعقب الدليل الإلكتروني وضبطه، إلا أن تعدد هذه الجهات قد يمتد إلى **مقدمي خدمات التصديق الإلكتروني** بما يوفر قدرا من التنوع يمكن من خلاله تيسير سبل التوصل إلى المستند الإلكتروني المتضمن لأدلة الإثبات في جرائم التعاملات الإلكترونية، على عكس المشرع الجزائري الذي حدده في متعهد الوصول ومتعهد خدمة الإيواء.

ونظرا لتعلق الأمر بحرمة الحياة الخاصة ذلك كون أن الكثير من المعطيات المتعلقة بمستخدمي شبكة الأنترنت دات **طابع شخصي**، فضلا على أن هذه المعطيات ليست دائما ساكنة بل متدفقة عبر إطار عملية الإتصال، كان لزاما التوجه نحو عدم وضع تكافؤ بين المعطيات نظرا للتفاوت في درجة المساس بالمصالح الفردية، بما يفرض وضع قيود على الإجراءات المتعلقة بالمعطيات تتفاوت صرامتها حسب **نماذج المعطيات**(المعطيات المتصلة بالمرور، معطيات المحتوى، معطيات المشترك.) **وشكلها**(مخزنة أو مسجلة أو في طور الإنتقال).

وبالتالي فانه لا يسمح بالتعاون بين مقدمي الخدمة وبين رجال الضبط بدون قيد أو شرط، بل لا بد من وضع قيود وضوابط لهذا التعاون حسب نموذج وشكل المعطيات ومدى تعلقها بحرمة الحياة الخاصة.

ويتمثل تعاون مزودي الخدمة مع رجال الضبط القضائي في جمع وتسجيل المعطيات المتعلقة بالمحتوى في حينها، التحفظ على المعطيات المعلوماتية المخزنة،تقديم معطيات معلوماتية متعلقة بالمشترك، وهذا ما سنتناوله بالدراسة من خلال المطالب التالية:

المطلب الأول: إعتراض المعطيات المتعلقة بمحتوى الإتصالات الإلكترونية

المطلب الثاني: التحفظ على المعطيات المعلوماتية المخزنة

المطلب الثالث: تقديم معطيات معلوماتية متعلقة بالمشترك

---

[1]-Article 09 dispose que " Sous la réserve des protections ou privilèges prévus par la loi, la plupart des législations permettent aux autorités chargées de l'enquête d'ordonner à des personnes de remettre des objets qui sont sous leur contrôle et qui sont 2 Recommandation n° R (95) 13 requis pour servir de preuve. Le droit de procédure pénale devrait, de la même manière, accorder le pouvoir d'ordonner à des personnes de leur présenter toute donnée spécifique qui se trouve sous leur contrôle, dans un système informatique, dans la forme requise par les autorités chargées de l'enquête"

يرى البعض أن السبب في عدم إعتبارهم من الطائفة المهنية الملتزمة بالسر المهني، في كونهم ليسو من الأمناء الضروريون الذين يأتمنهم الناس على أسرارهم فيفضون إليهم بتلك الأسرار، بل إنهم قد يصادفون معلومات تتعلق بالغيربسبب إدارة أعمالهم المتمثلة في الإشراف على الإتصالات السلكية واللاسلكية أو الإلكترونية، أو بسبب قيامهم بصيانة الخطوط وبالتدقيق على حسن سير الخطوط. **د. غنام محمد غنام**، ذاتية الإجراءات الجنائية في مجال جرائم تقنية المعلومات، بحث مقدم لمؤتمر "مكافحة جرائم تقنية المعلومات "، الإمارات العربية المتحدة ، 26- 30 / 11/ 2006 ، ص116.

المطلب الأول

إعتراض المعطيات المتعلقة بمحتوى الإتصالات الإلكترونية

الأصل أن المعطيات المتعلقة بمحتوى الإتصالات الإلكترونية تدخل ضمن إطار الحق في الخصوصية، ولا يجوز لمقدم الخدمات أو غيره في التشريعات المقارنة أن يقوم باستخدام وسائل للتنصت على محتوى الرسالة الإلكترونية أو المحادثة الفورية بوسائل للإعتراض والتنصت، ولا يتعارض ذلك مع حقهم في معرفة أماكن الأجهزة المتراسلة وفقا لما يعرف IP وذلك حتى يتمكنوا من ممارسة حقهم في الرقابة على الخدمات التي يقدمونها[1]، أو حفظ البعض من المعطيات المتعلقة بحركة السير **إذا كان ذلك لغرض** إعداد الفواتير ودفع الفوائد[2]، أو لضمان أمن الشبكات[43]. إلا أن هذا الأصل يرد عليه إستثناء يتعلق لإعتبارات التعاون مع الجهات القضائية، ذلك أن التكنولوجيا المعلوماتية إن كانت قادرة على نقل كميات ضخمة من المعطيات مستندات كانت أو صورا أو أصوات، فإنها تقدم إمكانيات واسعة للغاية لإرتكاب الجرائم بصفة عامة، وجرائم الإعتداء على التعاملات الإلكترونية بصفة خاصة.

وفي هذا الإطارنصت إتفاقية بودابست في المادة 21 منها تحت عنوان إعتراض معطيات المحتوى، على إلزام مقدم الخدمة في نطاق قدراته الفنية المتوفرة على أن يمنح السلطات المختصة عونه ومساعدته من أجل تجميع أو تسجيل في الوقت الفعلي، المعطيات المتعلقة بمحتوى إتصالات معينة على أرضه، منقولة عن طريق نظام معلوماتي[5]. كما نصت على ذات المعنى الإتفاقية العربية في المادة 29 منها تحت عنوان "إعتراض معلومات المحتوى".

---

[1]- د. **شيماءعبد الغني**، المرجع السابق، ص 219.

[2]-*Aux termes de l'article L. 34-2, second alinéa, du code des postes et des communications électroniques : «* La prescription est acquise, au profit de l'usager, pour les sommes dues en paiement des prestations de communications électroniques d'un opérateur appartenant aux catégories visées au précédent alinéa lorsque celui-ci ne les a pas réclamées dans un délai d'un an courant à compter de la date de leur exigibilité. *»*

[3]-*Disposition introduite à l'article L. 34-1 du code des postes et des communications électroniques par l'article 20 de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure.*

[4]- **Stéphanie Faber et Marion Le cardonnel**, Confidentialité des emails; REVUE SQUIRE PATTON BOGGS; 18 Juin 2015http://larevue.squirepattonboggs.com/Confidentialite-des-emails_a2621.html;
Voir aussi LES DISPARITÉS ENTRE ÉTATS MEMBRES, ENTRAVES À LA COOPÉRATION POLICIÈRE ET JUDICIAIRE,disponible en ligne á l'adresse suivante https://www.senat.fr/rap/l04-201/l04-2014.html#fn12

[5]-**Article 21 – Interception de données relatives au contenu. Du CCB dispose que "**
1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes en ce qui concerne un éventail d'infractions graves à définir en droit interne :
a à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, et
b à obliger un fournisseur de services, dans le cadre de ses capacités techniques:
i à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou
ii à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer, en temps réel, les données relatives au contenu de communications spécifiques sur so territoire, transmises au moyen d'un système informatique.

وعلى ذات النهج كان قد سار المشرع الفرنسي، حيث أجاز إعتراض المراسلات الإلكترونية وإلتقاط المعطيات المعلوماتية بموجب المادة 100 والمادة 706- 95 والمادة 706-102-1 إجراءات، وكذلك فعل المشرع الجزائري، حيث نص هذا الأخير في المادة 3 من القانون رقم 09-04 على أنه مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والإتصالات، يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وضع ترتيبات تقنية لمراقبة الإتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها.

ولما كنا قد فصلنا تارة وأشرنا تارة أخرى في مواقع مختلفة من هذه الرسالة إلى مسألة تنظيم المراقبة الإلكترونية في التشريع الفرنسي، فإننا سنكتفي هنا بما جاء في التشريع الجزائري بالمقارنة مع الإتفاقية العربية وإتفاقية بوداسبت وبعض التشريعات الأخرى كالتشريع الأمريكي، موضحين بذلك ماهية هذا الإجراء(الفرع الأول) وسلطة مقدمي الخدمة في القيام به (الفرع الثاني).

الفرع الأول

المقصود بإعتراض المعطيات المتعلقة بمحتوى الإتصالات الإلكترونية

إذا كانت المراقبة والتجميع والتسجيل تعني وضع شيء تحت الملاحظة، وتسجيل ما يحدث في جو من السرية والحذر على نحو لا يمكن معه الإحساس بوجود مراقبة، فإن هذا المفهوم لا يختلف في نطاق الإتصالات الإلكترونية، كل ما هنالك أنها تتم بإستخدام أجهزة ووسائل الكترونية لتحقيق غرض محدد، وإفراغ النتيجة في ملف إلكتروني وتحرير تقارير بهذه النتيجة.

وإن كان قد أغفل المشرع الجزائري تعريف المراقبة -أو كما يسميه البعض الإعتراض- في القانون رقم 09-04، مكتفيا بوضع تنظيم لهذه العملية في المادة 4 منه، فهو مسلك لا يعتبر بدعا من جانب المشرع فالأغلبية الساحقة من التشريعات المعاصرة تسلك هذا المسلك، في حين عرفها المشرع الأمريكي ضمن الباب الثالث من القانون الفدراليعلى أنها" الإكتساب السمعي أو أي إكتساب لمحتويات أي إتصال سلكي أو إلكتروني أو شفوي بإستخدام أي جهاز إلكتروني، أو ميكانيكي أو أي جهاز آخر"[1] وقد قضي بأن المقصود بكلمة الإكتساب acquisitionأن يتم الإلتقاط أثناء الإتصال نفسه ومن تم تسجيله[2].

وفي مفهوم الإتصالات الإلكترونية أشار المشرع الجزائري فيالفقرة و من المادة 2 من القانون رقم 09-04 إلى أنها تعني"أي تراسل او إرسال أو إستقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية، لتضيف المادة 5 من المرسوم رقم 15-261 المحدد لتشكيلة

[1]-title 18, parti 1, chapter 119, 2510, (4)"intercept" means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.

[2]- **د. شيماءعبد الغني**، المرجع السابق، ص305.

وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة "**بما في ذلك وسائل الهاتف الثابت و النقال**".

كما أشار المشرع الفرنسي إلى المقصود بها ضمن القانون رقم 2004-669 المتعلق بالإتصالات الإلكترونية المعدل لقانون رقم 91-646[1] بموجب الفقرة 2 منه على أنها إنبعاثات،وإرسال أواستقبال علامات أوإشارات أوكتابات أوصور أو أصوات، كهرمغنطيسية[2] "

كما عرف قانون الإتصالات الإلكترونية الأمريكي لسنة 1986 الإتصالات الإلكترونية بأنها كل إنتقال بشكل كلي أو جزئي للإشارات أو الصور أو الأصوات أو المعطيات أو المعلومات أيا كان نوعها، عن طريق الكابل أو الراديو أو النظام الكهرومغناطيسي أو التصوير الكهربائي أو الصور المرئية"[3].

مما سبق نخلص إلى أن الإتصالات الإلكترونية هي "إتصالات **مكتوبة** أو **مرئية** أو **مسموعة** تتخذ تقنية الإلكترون أداة للقيام بدورها، ومن تم فهي تشمل الإتصالات السلكية، الفاكس،البريد الإلكتروني، المحادثات الفورية التي تتم عن طريق تشات أو الفيسبوك أو تويتر أو الفايبر...إلخ ، وإن كان المشرع الجزائري قد حدد المعطيات محل التسجيل من قبل مقدم الخدمة بـــ "المعطيات المتعلقة بالمحتوى" كما ورد ذكرها في المادة 3 "...**وتجميع وتسجيل محتواها في حينها...**"، فهي معطياتلم يأت على بيان لتحديد المقصود بها، كما جاءت إتفاقية بودابست والإتفاقية العربية خالية من ذلك، وعلى العموم يمكن القول أن هذا المصطلح يشير إلى المحتوى "الإخباري للإتصال، بمعنى مضمون الإتصال الفعلي بين طرفيه، أو الرسالة أو المعلومات المنقولة عن طريق الإتصال[4].

وترتيبا على ذلك، يمكن القول أن جميع المعطيات الجوهرية التي يتضمنها المستند الإلكتروني والتي تكون محلا للإعتداء أو تلك التي تستخدم في تزوير التوقيع الإلكتروني أو إعداد برنامج لإتلافه أو تعييبه هي معطيات جوهرية يتعين على رجال الضبط **إلزام مقدمي خدمة التصديق** ومقدمي خدمة الأنترنت تقديمها حتى يتسنى تحليلها والوصول من خلالها للدليل الإلكتروني المؤدي لإدانة المتهم[5].

---

[1] **- LOI n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des telecommunications,** JORF n°162 du 13 juillet 1991**.**

[2]-Article 2 du**LOI n° 2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle (1)** JORF n°159 du 10 juillet 2004 page 12483 texte n° 1 dispose que « 1° Communications électroniques.« On entend par communications électroniques les émissions, transmissions ou réceptions de signes, de signaux, d'écrits, d'images ou de sons, par voie électromagnétique. » ;Article L32 du Code des postes et des communications électroniquesModifié par LOI n°2016-1321 du 7 octobre 2016 - art. 68

[3]- 18 U.S.C.A. § 2510 (2012) "Electronic communications" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system….

[4]-Rapport explicatif de la Convention sur la cybercriminalité, op. cit p 46.

[5]- **أيمن رمضان محمد أحمد**، المرجع السابق، ص273.

وبالرغم من خلو التشريع الجزائري من نص مماثل، إلا أن التشريع العماني قد تضمن نصا يوجب على مقدم خدمات التصديق والعاملين لديه تقديم تسهيلات للسلطة المختصة أو لأي موظفيها للقيام بالمراقبة أو الإشراف أو التفتيش على أي نظام معلوماتي أو مواد أخرى متصلة بالنظام بمقر مقدم خدمات التصديق[1].

بناء على ما سبق ذكره، يمكن تحديد المقصود بهذا الإجراء"**توجيه السلطة المختصة لمقدمي الخدمة الأمر بمراقبة أو إلتقاط الإتصالات الإلكترونية خلال الزمن الفعلي أثناء البث دون علم أطراف الإتصال محل التنقيب**"،وقد عبر المشرع الجزائري عن زمن الإعتراض بعبارة "في **حينها**" وكذلك فعلت إتفاقية بودابست بعبارة "**في الوقت الفعلي**" والإتفاقية العربية بعبارة "**بشكل فوري**"، ومؤدى ذلك أن هذا الإعتراض يطبق على تجميع أدلة المحتويات المتعلقة بالإتصالات في فترة الإنتاج وتجميعها لحظة النقل عبر الإتصال، فارتكاب العديد من الجرائم الواقعة على التعاملات الإلكترونيةيفترض النقل أو إتصال المعطيات بغرض الإنضمام بطريقة غير مشروعة لنظام معلوماتي، أو لبث الفيروسات، ففي هذه الحالة لا يكون من الممكن تحديد الوقت الفعلي للطبيعة الضارة وغير القانونية لهذه الإتصالات دون إعتراض محتوى الإتصال.

الفرع الثاني

سلطة مقدمي الخدمات في إعتراض معطيات محتوى الإتصالات الإلكترونية

إن القائم بعملية مراقبة الإتصالات لإلكترونية قد يكون أحد ضباط الشرطة القضائية ذاته بعد حصوله على إذن بالمراقبة، إذا ما توافرت لديه الخبرة الكافية لإستخدام التقنيات التكنولوجية التي يعتمد عليها في عملية المراقبة بدرجة عالية من الدقة والكفاءة، وقد يتم بالتعاون والإستعانة بمقدمي الخدمات، ويلاحظ أن هذا الإلتزام المفروض على مقدمي الخدمات لا يتم تطبيقه إلا في حدود عملية التجميع والتسجيل أو التعاون والمساعدة. وهو ما أشار إليه المشرع الجزائري صراحة بقوله في المادة 10 "...**يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الإتصالات في حينها...**"

وإذا تعلق الأمر بمعطيات أو إتصالات مخزنة لدى مزود الخدمة فإن ضابط الشرطة القضائية يستصدر إذنا بالتفتيش للإطلاع على تلك الإتصالات المخزنة وضبطها. والملاحظ أن المشرع الجزائري في المادة 10 لم يميز بين نوعي مقدمي الخدمات الملزمين بجمع وتسجيل المعطيات المتعلقة بمحتوى الإتصالات في حينها، كل ما إشترطه أن يتم حدوثهابشكل متزامن مع وقت البث، وليس الحصول على اتصالات الكترونية مخزنة. فعلى سبيل المثال ربما يمضي البريد الإلكتروني أو البريد الصوتي بعض الوقت في حالة تخزين الكتروني قبل أن يتم إسترداده نهائيا بواسطة المرسل إليه، فإذا حصلت السلطات على مثل هذا الإتصال من حالة التخزين الإلكتروني فلا يعد ذلك مراقبة إتصال بالمعنى المقرر في المادة 4 من القانون 09- 04.

[1]- الفقرة 3 من المادة 53 من قانون المعاملات الإلكترونية العماني رقم 69_2008 الصادر في 8 ماي 2008.

ولما كانت عملية مراقبة الإتصالات الإلكترونية لا تخرج عن كونها عملية رقابة وملاحظة سرية تتم بشأن إتصال الكتروني بصورة سرية وفي جو من الكتمان، فهي بذلك إجراء تطفلي يحمل في طياته نوعا من التدخل في الحريات الشخصية للأشخاص، لذا كان من الضروري وجود إجراءات صارمة تضمن تحقيق توازن مناسب بين مصالح العدالة والحقوق الأساسية للإنسان، ولعل من أبرز هذه الإجراءات ضرورة الحصول على إذن قضائي، إلا أن هنالك حالات يكون فيها الإعتراض مشروعا دون صدور هذا الإذن.

أولا- إعتراض معطيات محتوى الإتصالات الإلكترونية بناء على إذن

تدخل معطيات المحتوى ضمن الحق في الخصوصية التي تحميه التشريعات الداخيلة، ولايجوز لمزود الخدمة إستخدام وسائل فنية بغرض جمعها أوتسجيلها أثناء بثها، وإن تم ذلك فيجب أن يتم إجراؤها في إطار من المشروعيـــــة:

أ-الجهة المختصة باصدار الإذن بالمراقبة:

السلطة القضائية هي المختصة عموما بإصدار هذا الإذن، وبمقتضى هذه الضمانة يقوم رجل الضبط القضائي بالحصول على إذن **مكتوب** بالمراقبة من السلطة القضائية المختصة(النيابة العامة أو قاضي التحقيق)، ويتعين على مزود الخدمات عندئذ أن يتعاون معه في إعداد تلك المراقبة، وهو ما نص عليه المشرع الجزائري صراحة في الفقرة 3 من المادة 4 من القانون رقم 09-04.

وان كان الأمر كدلك، فقد خص المشرع النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية وحدهم المنتمين إلى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال إذنا بمراقبة الإتصالات الإلكترونية للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، لمدة 6 أشهر قابلة للتجديد، على أن يكون ذلك بناء على تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها.

وضرورة أن يكون الأمر مصدره القضاء، يرجع إلى رغبة المشرع في حماية حقوق وحريات الأفراد، باعتبار أن القضاء هو الحامي والحارس لها.

ب-حالات الإعتراض:

أقر المشرع مشروعية وضع الإتصالات الإلكترونية تحت المراقبة بناء على إذن من السلطة القضائية المختصة في حالات محددة حصرا وهـــي:

1- **الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة:**
والملاحظ أن ضابط الوقاية من وقوع هذه الجرائم فقط دون أن تكون هناك جريمة قد وقعت يعتبر

السند الشرعي للمراقبة، والمثال على ذلك أن تكون المراقبة لمنع الإعتداء على مستند إلكتروني يتعلق بأسرار عسكرية.

2- **في حالة توفر معلومات عن إحتمال إعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الإقتصاد الوطني:** أي تقوم بها السلطات حتى ولو لم يترتب على هذه الأنشطة ضررا يمثل جريمة يعاقب عليها القانون، وذلك إدراكا من المشرع كون هذه التهديدات لو تحققت تصبح معالجة آثارها جد صعب، خاصة مع توجه الجزائر لتسخير الإقتصاد الرقمي لخدمة الإقتصاد الوطني، خاصة ما تعلق منه **بنظام الدفع الإلكتروني** الذي يعد نواة الإقتصاد الرقمي من جهة، ومن ضمن المفاهيم التي ترتبط بها التعاملات الإلكترونية عضويا من جهة أخرى.

والملاحظ أن هذين الحالتين يدخلان ضمن الرقابة الوقائية، وهذا النوع من المراقبة له أهميته في مجال الضبط الإداري، كما أن له دورا جوهريا في كشف النقاب عن الحقائق، وقد سبق وأن نظم المشرع الفرنسي هذا النوع من المراقبة في القانون رقم 91-646 وحددها في حماية الأمن القومي وحماية المصالح الإقتصادية والعلمية لفرنسا والإرهاب. وهذا النوع من المراقبة كما يسميه الفقه "**بالمراقبة الأمنية**"[1] لا تستهدف الحصول على جريمة وقعت بل الغرض منها الحفاظ على كيان الدولة وبقائها، يصدر الأمر بها من رئيس مجلس الوزراء أو من يفوضه، ويصدر هذا القرار بناء على إقتراح مكتوب ومسبب مقدم من وزير الدفاع أو وزير الداخلية أو الوزير المختص بالجمارك أو من الشخص الذي يفوضه أي منهم[2].

3-**لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية:** وهذا النوع من المراقبة ضبطي قضائي وهو الذي يهمنا، والملاحظ أن المشرع لم يحدد جريمة بعينها على عكس ما فعل في المادة 65 مكرر 5، وهو ما يشمل الجرائم الواقعة على التعاملات الإلكترونية بجميع صورها.

وعلى ذلك، لا يكفي وقوع جريمة من جرائم التعاملات الإلكترونية لتبرير المراقبة، بل يجب فضلا عن ذلك أن تكون هناك فائدة حقيقية ترجى من وراءها في كشف الحقيقة، والمقصود بذلك أن وسائل البحث العادية في كشف غموض الجريمة وتحديد هوية الجناة وضبطهم قد فشلت، أو أن يكون الإستمرار فيها ونجاحها في تحقيق الغرض منها قد أضحى بعيد الإحتمال، وهو مايقتضي وجود قرائن قوية ومقنعة على أن المراقبة ستكشف غموض الجريمة وتساعد على ضبط الجناة. ويترك للسلطة القضائية تقدير مدى فائدة الإعتراض في كشف الحقيقة.

ففي قضية البنك الكندي caisse populaire des jardins ، وبناء على ما كشفت عنه التحريات بأن الفاعلين الدين استعملوا تسميات من بينها إسم المتهم (ف.محمد) ومن خلال عنوان الربط ip address ، وما وصلت إليه الأبحاث على مستوى المتعامل Eepad ، تم وضع ترتيبات تقنية من أجل مراقبة إلكترونية

[1]-**د. محمد أبو العلا عقيدة**، المرجع السابق، ص178.

[2]- Art. 4. Dispose que "- L'autorisation est accordée par décision écrite et motivée du Premier ministre ou de l'une des deux personnes spécialement déléguées par lui. Elle est donnée sur proposition écrite et motivée du ministre de la défense, du ministre de l'intérieur ou du ministre chargé des douanes, ou de la personne que chacun d'eux aura spécialement déléguée.Le Premier ministre organise la centralisation de l'exécution des interceptions autorisées."

بغرض تجميع المعطيات الإلكترونية دات الصلة بالإسم المستعار WALLACEZ وتبين أن صاحب هذا الإسم له عنوان الكتروني www.wallacez a hotmail.com وتم التعرف على الإسم المستعار[1] .

ب-تحديد مدة المراقبة:

ت-والهدف من هذا التحديد هو منع التعسف، ويجد أساسه في الضمانة السابقة المتمثلة في أن المراقبة لا يؤمر بها إلا إذا كانت ضرورية لكشف الحقيقة، وهذه الضرورة تساعد القاضي المختص في تقدير مدة المراقبة.

ورغم أهمية هذه الضمانة في وضع حد مناسب لحماية الحق في الخصوصية، فقد جاء قانون 09-04 خاليا من أي إشاره إليها، وهو نقص يجب تداركه من المشرع.

ث-حدود إستعمال المعطيات المتحصل عليها:

إن المعطيات المتعلقة بمحتوى الإتصالات الإلكترونية لايجوز إستعمالها إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية. تحت طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بالحياة الخاصة للغير.

ثانيا- إعتراض معطيات محتوى الإتصالات الإلكترونية دون إذن

ونميز هنـــا بين الفرضين التالـــيين:

أ-الإعتراض المعتاد لعمل الشبكة:

تقرر بعض التشريعات كالقانون الأمريكي إستثناء خاصا لمقدمي الخدمات يستطيعون بمقتضاه أن يقومو بمراقبة المشتركين في خدماتهم دون حصولهم على إذن بدلك، من خلال معرفة ما يقوم هؤلاء المشتركون به من نشاط التداخل في أجهزة الآخرين أو تخزين مواد مخالفة للقانون، وتسجيل هذه التداخلات والتبليغ عنها لرجال الضبط القضائي(مادة (I)(a) (2) 2511 U S C ss 18)[2]

وبشكل خاص يجب أن يكون هناك سلسلة أشياء جوهرية مترابطة بين المراقبة وبين تهديد حقوق مقدمي الخدمة، وبناء عليه فإنهم لا يستطيعون إستخدام هذا الإستثناء لتجميع دليل على جريمة ليس لها علاقة بحقوقهم[3]، والحقوق الممنوحة لهم والتي يحميها القانون الأمريكي كثيرة منها حقهم في حماية أنظمتهم من

---

[1]- محكمة عنابة، قسم الجنح،حكم رقم 07357/10 ، بتاريخ 28-06-2010، قضية جنحة تصميم وإدخال عمدا وعن طريق الغش لمعطيات للمعالجة الآلية والمتاجرة فيها أدت إلى تعديل معطيات تلك المنظومة وجنحة التقليد وجنحة السرقة، ضد (ف. محمد)، ص6.

[2]- د. **شيماء عبد الغني**، المرجع السابق، ص221.

[3]- **د. عمر محمد بن يونس**، الإجراءات الجنائية عبرالأنترنت في القانون الأمريكي، المرجع السابق، ص386.

إساءة الإستعمال أو من الأضرار بها _استعمال الفيروسات– أو الإستيلاء عليها –سرقة– أو إنتهاك الحق في الخصوصية–الإختراق–.

ومن تطبيقات ذلك ما قضي به من أنه يجوز لمقدمي الخدمات أن يقوموا بالمراقبة الإلكترونية لمكافحة الغش والسرقة الواقعة على الخدمات التي يقدمونها، من ذلك أن يقوم أحد الأشخاص بتقليد خط التلفون المحمول للحصول على خدمة دون دفع الإشتراك، الأمر الذي يقتضي أن يتابع مقدم تلك الخدمة هذا الخط المقلد لتحديد مكانه ومعرفة الفاعل لذلك.

وللسلطات قبول نتائج مراقبة مقدم الخدمة فقط إذا تم الوفاء بمتطلبات معينة تشير إلى أن مقدم الخدمة يراقب و يكشف الإتصالات لحماية حقوقه، وهذه المتطلبات هـــــــي[1]:

– أن يكون مقدم الخدمة مجنيا عليه في جريمة.

– أن يقوم بالمراقبة وبالتبليغ عما يعلمه من جرائم إلى الجهات القضائية حماية لحقوقه وليس قياما بدور المساعد.

–لا تقوم السلطات بطلب توجيه أو حث على مراقبة وكشف الإتصالات لأجل أغراض وأهداف لها.

–ألا تشارك السلطات في المراقبة الفعلية التي تحدث.

ب– الإعتراض بناء على شكوى المشترك:

لقد إختلفت التشريعات في إجازة مراقبة مقدم الخدمات للرسائل الواردة إلى جهاز الشخص المشتكي لديه من مشكلات تخل بعمل هذا الجهاز دون إذن بذلك، وإنقسمت في هذا المجـــال إلـــى إتجاهين:

الإتجاه الأول: ويرى إعتبار مقدم الخدمات مثماثل في عمله مع رجال السلطة العامة، وبالتالي فإنه ليس من حقه القيام بتلك الرقابة وتلك التسجيلات بدون إذن،وهو الإتجاه السائد في كندا، فمن بقوم بذلك فهو يخالف حكم المادة رقم 24 –2 من ميثاق الحقوق والحريات الكندي[2].

أمـــا **الإتجاه الثاني،** فيسمح بالخروج على الأصل وهو حظر مراقبة الإتصالات الإلكترونية إلا بأمر قضائي، وهو الإتجاه الدي يأخذ به القانون الأمريكي إلا أنه يربط ذلكبتوافر شروط معينة:

–أن يسمح المالك أو صاحب الحق لرجال الضبط بوضع الجهاز الخاص به تحت المراقبة.

–أن يتم ذلك في إطار تحقيق جنائي قائم.

–أن تتوافر دلائل كافية على أن تسجيل الإتصالات القادمة من الجهاز الصادر منه الإعتداء يفيد في كشف الحقيقة.

– أن يقتصر رجال الضبط على إعتراض الإتصالات الصادرة من وإلـــى الأجهزة محل التحقيق.

---

[1]– **د. شيماء عبد الغني،** المرجع السابق، ص224. **د. عمر محمد بن يونس،** الإجراءات الجنائية عبرالأنترنت في القانون الأمريكي، المرجع السابق، ص386.

[2]-**René Pépin**, « Le statut juridique du courriel au Canada et aux États-Unis », (2001) 6-*2 Lex Electronica.*disponible en ligne á l'adresse précédente.

ويعرف الباب الثالث منتهك النظام أنه الشخص الذي يخترق حاسوب محمي دون أن يكون مصرح له بذلك" ويستثني هذا التعريف أي شخص معروف لدى مالك أو مشغل الحاسوب المحمي ويكون لديه علاقة تعاقد مع المالك أو المشغل يمكن بمقتضاه الدخول على كل أو جزء من الحاسوب المحمـــي.

ويمكن أن يستخدم إستثناء شكوى المشترك في تركيبته مع سلطات أخرى مثل إستثناء مقدم الخدمة الذي يقوم بمراقبة نظامه ليحمي حقوقه، ربما يستمر في مراقبة النشاط الجنائي وفقا لتوجيه السلطات مستخدما إستثناء شكوى المشترك، وفي مثل هذه الظروف فإن مقدم الخدمة عندئذ يعمل في القانون كـــوكيل للحكومة[1].

المطلب الثاني

التحفظ على المعطيات المعلوماتية المخزنة

لما كانت مشكلة تبخر المعطيات المعلوماتية بما في ذلك المستندات الإلكترونية التي يمكن تعديلها أو تغييرها أو فقدها في بضع ثواني سواء من خلال المحو الروتيني أو نتيجة الإهمال أو ممارسات التخزين غير الدقيقة، أو التغيير العمدي لها لتدمير عناصر الإثبات، فإن **السرعة والسرية** تعدان في غالب الأحيان من العناصر الجوهرية في نجاح التنقيب والتحري، وعلى ضوء ذلك تنص إتفاقية بودابست بموجب المادة 16 منها على ضرورة السماح لكل طرف لسطلته أن يأمر أو يفرض على شخص مابالتحفظ العاجل على المعطيات المعلوماتية المخزنة بما في ذلك المعطيات المتعلقة بحركة السير المخزنة بواسطة نظام معلوماتي وخاصة في وجود أسس للإعتقاد بإمكانية تعرض المعطيات بصفة خاصة للفقد والتعديل.

ولكي يتم حفظ المعلومات المتعلقة بحركة السير المنصوص عليها في المادة 16، نصت المادة 17 على ضرورة أن يقوم كل طرف باتخاذ الإجراءات التشريعية اللازمة لكي يتم : الحفظ السريع لهذه المعلومـــات، والتأكد من أن واحد من مقدميالخدمة أو أكثر قد ساهموا في نقل الاتصـــال. الكشـــف الســـريع للســـلطات المختصة أو الشخص المعين من جانبها عن كمية المعلومات الكافية والمتعلقة بحركة تداول المعطيات بمـــا يسمح بتحديد هوية مقدمي الخدمة والطريق الذي تم الاتصال من خلاله. على أن تخضـــع تلـــك الســـلطات والإجراءات الواردة في هذه المادة لما هو منصوص عليه في المادة 14 و 15 من هذه الاتفاقية.

ولم تذهب الإتفاقية العربية بعيدا عما ذهبت إليه إتفاقية بودابست، حيث قررت في المادة 23 تحت عنوان التحفظ العاجل على المعطيات المخزنة بتمكين السلطات المختصة من إصدار الأمر أو الحصول على التحفظ العاجل للمعلومات المخزنة بما في ذلك معلومات تتبع المستخدمين، وكذلك فعل المشرع الفرنسي في قانون البريد والإتصالات الإلكترونية، فإذا كان الأصل هو حذف المعطيات المتعلقة بالإتصالات الإلكترونية

[1]- **د. عمر محمد بن يونس**، الإجراءات الجنائية عبرالأنترنت في القانون الأمريكي، المرجع السابق، ص226.

بعد نهاية كل إتصال تطبيقا للفقرة 2 من نص المادة **L34-1**[1]، أجاز المشرع ولضرورات البحث أو تقرير أو متابعة تحقيقات جنائية حفظ المعطيات المتعلقة بحركة السير من طرف مقدم الخدمة بمقتضى الفقرة 3 من نفس المادة L. 34-1 من قانون البريد والإتصالات الإلكترونية، وبالرغم من أن فرنسا مرسومها رقم 2006-358 المتعلق بحفظ الإتصالات الإلكترونية[2] جاء سابقا للتوجيه رقم **2006/24/CE** المتعلق بحفظ المعطيات التي تم إنشاؤها أو معالجتها في إطار توفير خدمات الإتصالات الإلكترونية المتاحة للجمهور أو شبكات الإتصالات العامة[3] إلا أنه جاء متطابقا معـــه.

وإلى جانب المشرع الفرنسي، نجد كذلك المشرع الجزائري الذي ألزم مقدمي الخدمات بالحفاظ على المعطيات المتعلقة بحركة السير، حيث نصت المادة 10 من القانون 09-04 على ضرورة تقديم مقدمي الخدمات المساعدة للسلطات المكلفة بالتحريات القضائية بوضع المعطيات المتعلقة بحركة السير تحت تصرف السلطات المذكورة.

وكما هو ملاحظ، فإن هذا الإجراء في التشريع الجزائري بل وفي غالبية الدول، يعد سلطة أو إجراء قانوني جديد كلية في القانون الداخلي، فهو أداة جديدة للتنقيب في مجال الكفاح ضد الإجرام الواقع في البيئة التقنية.

وسنتناول هذا الإجراء من خلال تحديد المقصود به(الفرع الأول)، ثم سلطة مقدم الخدمة في القيام به (الفرع الثاني).

الفرع الأول

المقصود بالتحفظ على المعطيات المعلوماتية المخزنة

لم تحدد التشريعات المقارنة المقصود من هذا الإجراء، وتشير المذكرة التفسيرية لإتفاقية بودابست إلى أن هذا الإجراء ينطبق على المعطيات المخزنة التي سبق تجميعها والإحتفاظ بها عن طريق حائزي المعطيات[4]، فعلى سبيل المثال المراسلة بالبريد الإلكتروني والتي تم إستقبالها بواسطة مزود الخدمة الخاص بالمرسل إليه

---

[1]-**Article L34-1** Modifié par LOI n° 2013-1168 du 18 décembre 2013 - art. 24 dispose que " II.-Les opérateurs de communications électroniques, et notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, effacent ou rendent anonyme toute donnée relative au trafic"

وهذه المعطيات التقنية تتعلق بالمعطيات الإدارية المتعلق بالعميل(الإسم واللقب العنوان، طريقة الدفع...) وأنها تعني المعلومات المتعلقة بإستخدام الشبكات، سواء الإتصالات الهاتفية، البريد الإلكتروني، الدخول إلى موقع انترنت خدمات الرسائل القصيرة sms أو خدمات البريد متعدد الوسائط mmsتمكنمنتحديدجهاتالاتصال،تحديدمكانها،مدةالاتصال. **أنظـــر:**

https://www.senat.fr/rap/l04-201/l04-2014.html#fn11

[2]-**Décret n° 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques ,** JORF n°73 du 26 mars 2006 page 4609

[3]-**Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE.**

[4]- Les mesures de conservation s'appliquent aux données électroniques « *stockées* au moyen d'un système informatique », ce qui suppose que les données existent déjà, ont déjà été collectées et sont stockées, Rapport explicatif de la Convention sur la cybercriminalité , op, cit, p29.

والتي لم يطلع عليها بعد تستقر في حالة تخزين إلكتروني، ففي هذه المرحلة فإن النسخة من الإتصال المخزنة تتواجد فقط كإجراء مؤقت في إنتظار إستقبال المرسل إليه لها من مزود الخدمة، وبمجرد إستلام المرسل إليه المراسلة بالبريد الإلكتروني فإن الإتصال يكون قد وصل إلى وجهته الأخيرة، فإذا إختار المرسل إليه الحصول على نسخة من إتصال سبق الإطلاع عليه من مزود الخدمة فإن النسخة المخزنة على الشبكة لم تعد في حالة تخزين إلكتروني لأن النسخة المعتادة لم تعد في وسيط التخزين. فقد تتبنى الشركة سياسة محو المعطيات بعد كل فترة أو أن المعطيات يتم محوها منهجيا عندما يكون وسيط التخزين مطلوبا من أجل تسجيل معطيات أخرى.

وبشكل عام لا يوجد نصوص تنظم المدة الزمنية التي يجب خلالها على مزودي الخدمات حفظ السجلات الإلكترونية، فبعض مزودي الخدمة يحتفظون بالسجلات لشهور وآخرون لساعات وغيرهم لا يحتفظون بها إطلاقا، ومع ذلك فإن هذه المعطيات لا تكون غالبا مخزنة إلا لفترة قصيرة، حيث أن التشريعات في حمايتها **للخصوصية** يمكن أن تحرم التخزين لفترة طويلة بالنسبة لهذه المعطيات، فالمشرع الفرنسي وتماشيا مع مبدأ تحديد الهدف من معالجة المعطيات ذات الطابع الشخصي، يجيز لمزود الخدمة حفظ بعض المعطيات المتعلقة بالإتصالات الإلكترونية فقط **للأغراض** الفوترة ودفع خدمات الإتصالات الإلكترونية كحد أقصى لمدة سنة يتعلق الأمر بالمعطيات التي تسمح بتحديد هوية المستخدم، بالتجهيزات الطرفية المستعملة، تاريخ ووقت ومدة كل إتصال، الخدمات التكميلية المطلوبة، أو **لغرض** أمن الشبكات لمدة لا تتجاوز 3 اشهر ويتعلق الأمر بالمعطيات المتعلقة تاريخ ووقت ومدة كل إتصال، الخدمات التكميلية المطلوبة والمعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الإتصال[1].

وعلى ذلك فمن الناحية العملية فإن هذا يعني أن هذه المعطيات التي قد تمثل مصلحة للتنقيبات الجنائية يمكن تدميرها أو فقدانها قبل حصول السلطات على الأمر القانوني المناسب لتنفيد الكشف جبرا. وعلى ذلك فإن التحفظ الفوري على المعلومات المخزنة من أهم الإجراءات التقنية اللازمة لتعقب الدليل الإلكتروني في جرائم الإعتداء على التعاملات الإلكترونية، والمحافظة عليه خاصة من خطر الفقد أو التعديل، فضلا عما يستلزمه المحافظة على الدليل من ضرورة تخويل السلطة القائمة على التحقيق صلاحية التحفظ الفوري على تلك المعطيات المخزنة وصولا للتحري الدقيق عن مرتكب الجريمة وملاحقته[2].

وإن كانت إتفاقية بودابست تعطي أهمية لحماية المعطيات التي سبق وجودها وتخزينها من كل ما يعرض لحظر التغيير أو التجريد من صفتها أو حالتها الراهنة، حيث إستخدمت مصطلح "**التحفظ**"، وهو ما يفيد تطلب أن تكون المعطيات مصانة على نحو آمن من كل تغيير أو إتلاف أو محو، وعلى نهجها سار المشرع الفرنسي والإتفاقية العربية، فإن المشرع الجزائري لم يولي أهمية لذلك، حيث إستخدم مصطلح **الحفظ**، وهو ما يشير إلى أرشفة المعطيات فقط، بما يعني تجميعها في الوقت الحاضر وحفظها أو حيازتها في أرشيف لمدة معينة من أجل الإجابة عن طلب أو أمر.

---

[1]- https://www.senat.fr/rap/l04-201/l04-2014.html#fn14

[2]- **أيمن رمضان محمد أحمد**، المرجع السابق، ص265.

وفي تحديد المعطيات المخزنة محل الإجراء، أشارت إتفاقية بودابست صراحة إلى المعطيات المتعلقة بحركة السير أو كما نعتتها المادة 23 من الإتفاقية العربية" "معلومات تتبع المستخدمين" ، بغرض الإشارة إلى الإنطباق الخاص لهذه النصوص على هذا النوع من المعطيات التي بمقتضاها عندما يتم تجميعها والإحتفاظ بها، فإنها لا تكون بصفة خاصة متحفظا عليها إلا **لفترة وجيزة** محددة قانونا، وهو ما أخذ به المشرع الجزائري.

وقد عرفتها إتفاقية بودابست بموجب المادة 1 الفقرة د على أنها "صنف من معطيات الحاسب التي تكون محلا لنظام قانوني محدد، حيث يتم توالد هذه المعطيات من الحواسيب عبر تسلسل حركة الإتصالات لتحديد مسلك الإتصالات من مصدرها إلى الجهة المقصودة، وبذلك فهي تشمل طائفة من المعطيات تتمثل في : مصدر الإتصال ووجهته المقصودة، خط السير ووقت أو زمن الإتصال وفقا لتوقيت غرينتش، حجم الإتصال ومدته ونوع الخدمة المؤداة.

ولم يذهب المشرع الجزائري بعيدا عن ذلك، حين عرفها في الفقرة ه من المادة 2 على أنها "أي معطيات متعلقة بالإتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة بإعتبارها جزءا في حلقة إتصالات، توضح مصدر الإتصال والوجهة المرسل إليها والطريق الذي تسلكه ووقت وتاريخ وحجم مدة الإتصال ونوع الخدمة".

ومن ضمن معطيات المرور، حدد المشرع أنواع من المعطيات التي يلزم مقدم الخدمة بحفظها وتتمثل فـــي:

- المعطيات التي تسمح بالتعرف على مستعملي الخدمة (مثل adresse IP، رقم الهاتف، عنوان البريد الإلكتروني).

-المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للإتصال، بالخدمات التكميلية المطوبة أو المستعملة و مقدميها

-الخصائص التقنية وكذا تاريخ ووقت ومدة كل إتصال، وتلك التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الإتصال وكذا عناوين المواقع المطلع عليها.

وبالنسبة لنشاطات الهاتف، يقوم المتعامل بحفظ المعطيات التي تسمح بالتعرف على مستعملي الخدمة، وكذا تلك التي تسمح بالتعرف على مصدر الإتصال وتحديد مكانه.

ورغم أهمية شمول هذا الإجراء المعطيات المتعلقة بحركة السير(معطيات إلكترونية أو معطيات تلفونية) كونها تساهم في تحديد منبع الإتصال ومصبه الذي من شأنه المساعدة في تحديد هوية أي فاعل أو فاعلين للجريمة التي يتم إرتكابها عن طريق نقل للإتصالات بواسطة نظام معلوماتي، كون هذه الإتصالات يمكن أن تحوي محتوى غير مشروع كتعليمات تحمل إعتداء على المعطيات أو تعيق حسن أداء النظام المعلوماتي، فإننا نرى أن يوسع المشرع الجزائري نطاق هذا الإجراء إلى جميع المعطيات المعلوماتية الموجودة من قبل والتي تم تجميعها وتخزينها،ولاشك أن الوقوف على صور من تلك المعطيات من شأنه أن يؤدي إلى الربط

بين المستند الإلكتروني أو النظام المعلوماتي محل الإعتداء وشخصية مرتكب الجريمة، و يقود إلى دليل يمكن الركون إليه في الإثبات.

أما الوضع في فرنسا، فقد كانت المادة 34-1-1 من قانون البريد والإتصالات الإلكترونية تنص على إلزام مقدم الخدمة بالتحفظ على المعطيات التقنية المتعلقة بتحديد أرقام الإشتراك أو الإتصال في خدمة الإتصالات الإلكترونية، وتعداد جميع أرقام الإشتراك أو الخدمة للشخص المعين، والمعطيات التي تسمح بتحديد مكان التجهيزات الطرفية وتاريخ وساعة الإتصال[1]، وظلت هذه المادة إلى غاية 31 ديسمبر 2008، أين صدرت نسخة جديدة من قانون البريد والإتصالات الإلكترونية والذي دخل حيز التنفيد في 1 جانفي 2010، حيث تم حذف المادة السابقة وتم نقل مضمونها في المادة L34-1وحددت المعطيات المتحفظ عليها في تلك التي تسمح بالتعرف على مستعملي الخدمة المزودة من المشغلين والخصائص التقنية للإتصالات وموقع المعدات الطرفية[2].

ويتعلق الإلتزام حسب المادة L34-1، بمشغلي الإتصالات الإلكترونية، بالإضافة إلى أي من الأشخاص الذين في إطار نشاطهم المهني الرئيسي أو الثانوي يتيح للجمهور ربط الإتصال بالأنترنت عن طريق وسيط الدخول إلى الشبكة، سواء كان ذلك على أساس الدفع أو مجانا[3]. من تم فإن الإلتزام –يقول النائب AlainMarsaud-يشمـــــل[4]:

–الأشخاص الذين يوفرون الخدمة بالدفع والمصنفون "مقاهي الأنترنت".

–الأشخاص الذين يقدمون لزبائنهم في إطار عام أو الزوار الربط الإلكتروني مثل الفنادق وشركات الطيران.

–مقدم خدمة الدخول لشبكة إتصال إلكترونية يمكن الدخول إليها عن طريق WIFI بواسطة إستخدام بطاقات الدفع المسبق التي تمكن الدخول إلى الشبكة ، ولكن أحيانا أيضا بالمجان.

وقد حددت المادة R10-13[5]من قانون البريد والإتصالات الإلكترونية المضافة بموجب المرسوم رقم 2006-358 المقصود بالمعطيات الفنية محل التحفظ من قبل مشغلي الإتصالات الإلكترونية لإعتبارات

---

[1]-وجاءت تلك المادة متوافقة في المعنى مع الفقرة 12 من المادة 3 توصية رقم 1995

Des obligations spécifiques devraient être établies pour les fournisseurs de services qui offrent des services de télécommunication au public via des réseaux de communication publicsou privés, de délivrer l'informationnécessaire, lorsque les autorités compétentes chargées de l'enquête l'ordonnent, pour identifier l'utilisateur.

[2]-Les données conservées et traitées dans les conditions définies aux III, IV et V portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux.

[3]-Les personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit, sont soumises au respect des dispositions applicables aux opérateurs de communications électroniques en vertu du présent article.

[4]-**Emilie Bailly & Emmanuel DAOUD** , WIFI et conservation des données : Les obligations du fournisseur de services disponible en ligne á l'adresse suivante;https://www.cdse.fr/wifi-et-conservation-des-donnees

[5]-**Article R10-13** Modifié par Décret n°2012-436 du 30 mars 2012 - art. 7 I.- dispose que "En application du III de l'article L. 34-1 les opérateurs de communications électroniques conservent pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales :

a) Les informations permettant d'identifier l'utilisateur ;

b) Les données relatives aux équipements terminaux de communication utilisés ;

c) Les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ;

d) Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ;

e) Les données permettant d'identifier le ou les destinataires de la communication.

بحث أوتقرير أو متابعة الجرائم، وهي المعطيات نفسها التي نص عليها المشرع الجزائري في المادة 11، أي فقط المعطيات المتعلقة بحركة السير **les données de traffic**.

والملاحظ أن المعطيات المتحفظ عليها في فرنسا، لا تتضمن المعطيات المطلع عليها(محتويات صفحات الأنترنت التي زارها) أو محتوى المراسلات المتبادلة، مثل موضوع أو نص الإميل، ، فالبريد الإلكتروني لا يزال يحكمه القانون رقم 91- 646 المتعلق بسرية المراسلات التي تتم عن طريق وسائل الإتصال الإلكترونية[1]، وبالتالي فإن القانون الجزائري أصبح يتوافق مع القانون الفرنسي، عندما أجاز إلزام مقدمي الخدمات بالحفاظ على معطيات المرور المخزنة دون أن يمتد هذا الإلتزام ليشمل محتوى المراسلة نفسها.

كما يستبعد المشرع الفرنسي من المعطيات السابقة، أنواع معينة نصت عليها المادة 60-2 في فقرتها الأولى من قانون الإجراءات الجزائية وهي الخاصة بالمعلومات التي يغطيها سرالمهنة، حيث تنص"...بإستثناء المعلومات التي تعتبر من أسرارالمهنة التي أوردها القانون، والمتواجدة في الأنظمة المعلوماتية أو أي أجهزة للمعالجة الآلية..." [2]، كما تستثني نفس المادة بعض الجهات من واجب التعاون وهي التجمعات غير الربحية الدينية أو الفلسفية السياسية والنقابية.

بناء على ما سبق، يمكننا تعريف هذا الإجراء كونه " **قيام مقدم الخدمة بناء على طلب السلطة المختصة بإتخـــاذ جميع الخطوات اللازمة للتحفظ على سجلات المعاملات عبر الوسائل الإلكترونية وأدلـــة أخرى في حيازته في إنتظـــار إتخاذ إجراء قانوني آخر كالتفتيش والضـــبط**".

وإذا كان هذا الإجراء في الجزائر يخص الحفاظ على المعطيات التي تم توالدها عبر تسلسل حركة الإتصالات، وكذلك هو الشأن في فرنسا مع مراعاة أحكام القانون رقم 78-17 (المادة1-34 .L،الفقرة ماقبلالأخيرةمنقانونالبريد والإتصالات الإلكترونية)، فإنه إذا رغب رجل الضبط القضائي في جعل مقدم الخدمة يقوم بتسجيل المعلومات عن إتصالات الكترونية مستقبلية فإنه يجب أن يكون هناك توافق مع نصوص المراقبة الإلكترونية التي تم مناقشتها سابقا.

لكن السؤال الذي يمكن أن يثار في هذا الخصوص هو معرفة ما إذا كانت الرسالة الإكترونية غير المفتوحة والمنتظرة في صندوق الخطابات حتى يقوم المرسل إليه بإدخالها في نظامه المعلوماتي هل يجب أن تعتبر كأنها معطيات معلوماتية مخزنة، وبالتالي تطبق عليها النصوص الخاصة بالتفتيش والضبط والتحفظ،

II.-Pour les activités de téléphonie l'opérateur conserve les données mentionnées au II et, en outre, celles permettant d'identifier l'origine et la localisation de la communication.
III.-La durée de conservation des données mentionnées au présent article est d'un an à compter du jour de l'enregistrement.

[1]-**Article L34-1 du CPCE** Modifié par LOI n°2009-669 du 12 juin 2009 - art. 14 **dispose que "**Elles ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications" voir aussi Internet et wi-fi en libre accès : contrôles de la CNIL; http://www.cil.cnrs.fr/CIL/spip.php?article2625

[2]- **Article 60-2** Modifié par **LOI n°2009-526 du 12 mai 2009 - art. 124 dispose que "**à l'exception de celles protégées par un secret prévu par la loi, contenues dans le ou les systèmes informatiques ou traitements de données nominatives qu'ils administrent.**"**

أم أنها معطيات في مرحلة النقل أو التحويل وبالتالي تطبق عليها النصوص الخاصة بإعتراض المعطيات المتعلقة بالمحتوى؟

حســـم المشرع الأمريكي هذا الأمر، وإستبعد إعتبار هذه الرسالة جزءا من الإتصال، بدليل أنه قام بتعديل القسم 2703 من قانون خصوصية الإتصالات الإلكترونية ECPA ليشمل حماية الإتصالات الإلكترونية المخزنة من بريد إلكتروني ورسائل صوتية غير مفتوحة ومخزنة لدى مزود الخدمة، وقد تم تأكيد هذه القاعدة في العديد من التطبيقات القضائية مثل قضية united states v smith حيث قرر القضاء بأنه لا يمكن مراقبة الإتصالات السلكية وهي في حالة التخزين الإلكتروني[1].

الفرع الثاني

سلطة مقدمي الخدمات في التحفظ على المعطيات المخزنة

"يقتضي هذا الإجراء كما رأينا قيام مقدم الخدمة بناء على طلب السلطة المختصة بإتخاذ جميع الخطوات اللازمة للتحفظ على سجلات المعاملات عبر الوسائل الإلكترونية وأدلة أخرى في حيازتهبإعتباره إجراء أولي يتم تبنيه لإنتظار إتخاد إجراءات قانونية أخرى تستهدف الحصول على المعطيات أو الكشف عنها. وقد تكون معطيات المرور أو بعض نمادج معطيات المرور مشتركة بين مقدمي الخدمات الذين ساهمو في نقل الإتصال، لأغراض تجارية أو أمنية أو تقنية في مثل هذه الحالة، فإن أي من مقدمي الخدمات يمكن أن يكون بحوزته معطيات مرور جوهرية من أجل تحديد المصدر والخط النهائي للإتصال.

ولما كان هدا الإجراء يتضمن التحفظ على جميع المعطيات المعلوماتية المخزنة، فهو بذلك ينطوي حتما على مساس بسرية المعلومات وحرمة الحياة الخاصةومن ثم فقد كان ضروريا وضع ضوابط تساعد كما أشارت المذكرة التفسيرية لإتفاقية بودابست على "**الدفاع عن الحق على الحياة الخاصةللشخص** "[2]، وهي كمايلي:

أولا- توافر حالة الضـــرورة:

ويمكن القول بتوافر حالة الضرورة كلما كانت تلك المعطيات عرضة لخطر الإتلاف أو التلاعب، وتقدير ما إذا كان التحفظ على تلك المعطيات ضروريا من عدمه يتوقف على مدى جدية المبررات التي ترتكن إليها السلطة المصدرة لأمر التحفظ.

---

[1]-United states v smith, 155 f3d 1051-59(9 th cir 1998)

مشار إليه لدى : **د. عمر محمد بن يونس**، الإجراءات الجنائية عبر الأنترنت في القانون الأمريكي، المرجع السابق، ص368 وما بعدها.

[2]-à défendre le droit à la vie privée de la personne; Rapport explicatif de la Convention sur la cybercriminalité ; op; cit; P 32

وفي فرنسا، يجب عملا بأحكام المادة **L34-1** لإحتياجات البحث، ومتابعة الجرائم، أو لأغراض منع الإعتداء على نظم المعالجة الآلية المعاقب عليها في المادة 323-1 إلى 323-3-1 من قانون العقوبات، تاجيل محو المعطيات لمدة سنة لإتاحتها للسلطة القضائية[1].

ثانيا- ضمان سرية إجراء التحفظ:

من أجل إحترام الحياة الخاصة للفرد، ولإعتبارات إحتياجات الكفاح ضد الإجرام، تفرض التشريعات إلتزام السرية بالنسبة لتطبيق إجراء التحفظ على مقدم الخدمة الملزم بالتحفظ على هذه المعطيات في غضون المدة المحددة قانونا، وهكذا يكون ملتزما بضمان سرية تطبيق إجراء التحفظ على المعطيات المخزنة خلال المدة المقررة للسرية، وهذا ما دعت لتبنيه اتفاقية بودابست في الفقرة 3 من المادة 16[2]، وكذلك فعلت الإتفاقية العربية حيث ألزمت بموجب الفقرة 3 من المادة 23 مقدم الخدمة بالإبقاء على سرية الإجراءات طوال الفترة القانونية المنصوص عليها في القانون الداخلي. كما نص المشرع الجزائري بموجب الفقرة 3من المادة 10 على أنه يتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق المنصوص عليها في المادة 301 عقوبات.

ثالثا-أن يكون الغرض من التحفظ جمع الأدلة أوالتحقق من هوية مرتكب جريمة من جرائم التعاملات الإلكترونية:

فلا قيمة لذلك التدبير، مالم يكن من شأن التحفظ على المعطيات الوصول إلى الدليل الإلكتروني في جريمة من جرائم الإعتداء على التعاملات الإلكترونية، وتحديد هوية مرتكبها، وتحديد المعطيات التي يمكن أن تكون محلا للتحفظ يتوقف على إرتباطها بالمعلومات محل الإعتداء[3].

وإن إشترطت بعض التشريعات كما هو حال المشرع الروماني، حتى تخول النيابة العامة سلطة الأمر بالتحفظ على المعطيات، أن يكون الأمر الصادر بالتحفظ مسببا ومن تم أن يكون مكتوبا، وأن يتم إصداره بناء على طلب الجهة المختصة بالتحقيق الجنائي في جريمة من جرائم الإعتداء على التعاملات الإلكترونية[4]، أقام المشرع الجزائري الإزدواجية في الشروط القانونية بينالمعطيات المتعلقة بحركة السير التي تسمح بتحديد

---

[1]- Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales :::: ou pour les besoins de la prévention des atteintes aux systèmes de traitement automatisé de données prévues et réprimées par les articles 323-1 à 323-3-1 du code pénal, et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire ... il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques.

[2]-Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger le gardien des données ou une autre personne chargée de conserver celles-ci à garder le secret sur la mise en œuvre desdites procédures pendant la durée prévue par son droit interne.

[3]- **أيمن رمضان محمد أحمد**، المرجع السابق، ص269.

[4]-المرجع نفسه، ص 270.

الهوية وبين المعطيات المتعلقة بالمحتوى، إذ من حق مقدم الخدمة أن يتعاون مع ضباط الشرطة القضائية بتزويدهم بتلك المعطيات دون الحاجة إلى تسخير بدلك أو **إذن**، على خلاف الوضع بالنسبة للمعطيات المتعلقة بمحتوى الإتصال نفسه.

وإن كنا نرى بأن بعض المعطيات المتعلقة بحركة السير كتلك المتعلقة بالساعة ومدة حجم الإتصال قد لا تكشف إلا القليل عن المعلومات ذات الطابع الشخصي بالنسبة للفرد، إلا أن الأمر على خلاف ذلك إذا تعلق الأمر بزيارة مواقع الواب مثلا إذ يمكن أن تثير حق الخصوصية، فتجميع شتات هذه المعطيات يمكن أن يسمح بالتعريف بالشخص المعني، ومن تم كان الأجدر أن يشترط المشرع لوضع هذه المعطيات تحت تصرف ضباط الشرطة القضائية الحصول على تسخيرة بذلك من السلطة القضائية المختصة، وكيل الجمهورية أو قاضي التحقيق حسب الأحوال.

أما بالنسبة للمشرع الفرنسي فإن المعطيات المتحفظ عليها لا يمكن تقديمها إلا لأشخاص مؤهلين من بينهم:

- ضابط الشرطة القضائية في إطار التحري في الجريمة المتلبس فيها حسب المادة 60-1 إجراءات، وإشترطت الفقرة الثانية من المادة 60-2 إجراءات أن يطلب ضباط الشرطة القضاية من مشغلي الإتصالات السلكية واللاسلكية وخاصة الذين يتيحون إمكانية الوصول إلى خدمات الإتصالات على شبكة الأنترنت(متعهد الوصول) أن يتخدو بدون إبطاء جميع التدابير المناسبة لضمان الحفاظ لمدة لا تتجاوز سنة على **محتوى المعلومات** التي تتم من طرف أشخاص مستعملي الخدمات التي يؤمنها مقدمو الخدمات المعنيون. وذلك بعد منح التسخير بذلك من وكيل الجمهورية وبعد ترخيص من قاضي الحريات والحبس[1].

والملاحظ أن المادة 60-2 إجراءات (60-1 سابقا التي تم إنشاؤها بمقتضى قانون الأمن الداخلي 2003-239[2] وتحويلها بموجب القانون 2004-204[3] وتعديلها بموجب القانون 2009-526[4]) أجازت إلزام مقدم الخدمة بالكشف عن المحتوى وعدم الإقتصار على الكشف عن المعطيات المتعلقة بحركة السير فقط، وعلى مايبدو فإن هذا الحكم جاء مكملا للمادة 29 من قانون الأمن اليومي 15 نوفمبر 2001(**L34-1** من قانون البريد والإتصالات الإلكترونية) الذي ينص على أن حفظ المعطيات لا يمكن بأي حال من الأحوال أن يشمل محتوى الرسالة.

- لوكيل الجمهورية أو لضابط الشرطة القضائية وبإذن من وكيل الجمهورية في إطار التحري الأولي حسب المادة 77-1-1 إجراءات.

---

[1]-L'officier de police judiciaire, intervenant sur réquisition du procureur de la République préalablement autorisé par ordonnance du juge des libertés et de la détention, peut requérir des opérateurs de télécommunications, et notamment de ceux mentionnés au 1 du I de l'article 6 de la loi 2004-575 du 21 juin 2004pour la confiance dans l'économie numérique, de prendre, sans délai, toutes mesures propres à assurer la préservation, pour une durée ne pouvant excéder un an, du contenu des informations consultées par les personnes utilisatrices des services fournis par les opérateurs.

[2]-**Loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure**

[3]**Loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité**

[4]-**LOI n° 2009-526 du 12 mai 2009 de simplification et de clarification du droit et d'allègement des procédures**

♦ قاضي التحقيق أو ضابط الشرطة القضائية المناب في إطار التحقيق حسب المادة 99-3 إجراءات[1].

فهـــــــــؤلاء: لهم أن يطلبو من كل شخص، من كل مؤسسة من كل جهة خاصة أو عامة أو كل إدارة عامة، من المحتمل حيازتهم **معلومات** ذات صلة بالتحقيق، بما في ذلك المتعلقة بنظام المعالجة الآلية أو بمعالجة المعطيات الشخصية أن يسلمهم هذه المعلومات".

رابعا- ضمان أمن المعطيات

أشرنا إلى أنه وعلى خلاف المشرع الجزائري، ألزمتكل من إتفاقية بودابست والإتفاقية العربية مقدم الخدمةبالتحفظ على المعطيات لمدة معينة، وهو ما يعني حماية المعطيات من كل ما يعرضها لخطر التغيير أو الإتلاف أو المحو، و يمكن لمزود الخدمة بناء على تخصصات هذا الأمر أن يتحفظ على الولوج للمعطيات.

هذا ولم تحدد الإتفاقية الطريقة التي من خلالها يجب أن تكون المعطيات متحفظا عليها، وتحديد ما إذا كان التحفظ يمكن أن يشمل أيضا تجميدها. كما أكد المشرع الفرنسي بدوره على ضرورة إحترام المبادي المنصوص عليها في قانون المعلوماتية والحريات ومن ذلك أخذ الإحتياطات المعقولة حسب الأصول العلمية لحماية هذه المعطيات.

خامسا- إلتزام مقدم الخدمة بمدة معينة للتخلص من المعطيات:

لما كان إجراء التحفظ إجراء وقتي فإن الفترة الزمنية التي يتم فيها التحفظ على المعطيات مؤقتة، وقد إختلفت التشريعات في تقدير هذه المدة بحسب أهميتها والتي تسمح للسلطات المختصة فيها بالكشف عنها، فقد حددتها إتفاقية بودابست والإتفاقية العربية بحد أقصى بـــ 90 يوما، ويمكن للأطراف أن يقررو تجديد هذا الإجراء، إلا أنه لم يتم تحديد مرات التجديد أو شروطه أو إطاره أو إجراءاته أو مدى ضرورته في أي بنود من بنود الإتفاقية.

أما بعض التشريعات الوطنية، فقد حددتها كحد أقصى بـــ سنة ، كالمشرع الفرنسي (المادة **R10-13**)[2] من قانون البريد والإتصالات الإلكترونية، بل أن المادة 39-3[3] قد فرضت عقوبات على مقدم الخدمة الذي

---

[1]- voir article 60-1, 77-1-1, 99-3 du code procedure penale ainsi que l **Article L34-1 -1** **Code des postes et des communications électroniques**

[2]- **Article R10-13** Créé par Décret n°2006-358 du 24 mars 2006 - art. 1 JORF 26 mars 2006 dispose que III. - La durée de conservation des données mentionnées au présent article est d'un an à compter du jour de l'enregistrement.

[3]- **Article L39-3 du CPTE** Modifié par Loi n°2004-669 du 9 juillet 2004 - art. 19 JORF 10 juillet 2004 I. - Est puni d'un an d'emprisonnement et de 75 000 euros d'amende le fait pour un opérateur de communications électroniques ou ses agents :

1° De ne pas procéder aux opérations tendant à effacer ou à rendre anonymes les données relatives aux communications dans les cas où ces opérations sont prescrites par la loi ;

2° De ne pas procéder à la conservation des données techniques dans les conditions où cette conservation est exigée par la loi.

لم يقم بمسح تلك المعطيات، وذلك إحتراما للحياة الخاصة، أو عدم إلتزامه بحفظ تلك المعطيات وفق ما نص عليه القانون، سواء بالحبس سنة وغرامة 75 ألف يورو بالنسبة للشخص الطبيعي، و375 ألف اورو بالنسبة للشخص المعنوي تطبيقا للمادة 131-38 من قانون العقوبات.

ولم يذهب المشرع الجزائري بعيدا عما ذهب إليه المشرع الفرنسي، وهو ما يستفاد من عبارة " تحدد مدة حفظ المعطيات المدكورة في هذه المادة بسنة واحدة إبتداء من تاريخ التسجيل"، كما فرض عقوبة الحبس والغرامة في حالة الإخلال بهدا الإلتزام عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية.

المطلب الثالث

تقديم معطيات معلوماتية متعلقة بالمشترك

نصت المادة 18 من إتفاقية بودابست على أنه يجوز للدول الأطراف في تلك الإتفاقية تمكين السلطات المختصة من إلزام مقدمي الخدمات تقديم المعطيات المتعلقة بالمشترك، سواء كانت في حوزته المادية أو تحت سيطرته حيث تكون هذه المعطيات مخزنة بعيدا عن الحيازة المادية لمزود الخدمة، ولكن يمكن السيطرة عليها، ومثال ذلك أن تكون المعطيات مخزنة في وحدة تخزين عن بعد ويتم تقديمها عن طريق شركة أخرى.

والمعطيات محل التقديم هي معطيات ترتبط بالمشتركين وخدماتهم، يشترط فيها أن تكون مخزنة أو موجودة، لكنها لا تضم معطيات لم توجد بعد كالمعطيات المتعلقة بحركة السير أو مضمونها المرتبط بالإتصالات المستقبلية، والتي من خلالها يمكن تحديد:

-نوع خدمة الإتصال المستخدمة، والأوضاع الفنية المنصوص عليها بالنسبة لفترة الخدمة.

-الهوية، العنوان البريدي أو الجغرافي، ورقم تلفون المشترك، ورقم الولوج، والمعطيات المتعلقة بطريقة الدفع (مثل رقم بطاقة الإئتمان أو الحساب البنكي).

-أية معلومات أخرى تتعلق بموقع تجهيزات الإتصال، المتوافرة على أساس عقد أو إتفاق تقديم الخدمة.

والأمر بتقديم هذه المعلومات يتعلق فقط بمزودي الخدمات الذين يحتفظون بهذه المعطيات، وذلك أن البعض منهم لا يحتفظون بأي أثر للمستخدمين بالنسبة لخدماتهم. فضلا عما سبق، يمكن أن يأخذ تعبير المعلومات المتعلقة بالمشتركين شكلا أخر غير شكل المعطيات المعلوماتية، كأن تكون مستندات ورقية.

ونظرا لأن البعض من معطيات المشترك قد تكون سرية، فقد أشارت المذكرة التفسيرية إلى إمكانية إستبعاد طائفة معينة من المعطيات، أو تفرض ضمانات بصدد أنواع معينة من المعطيات المعلوماتية التي تم حيازتها من طرف مقدم الخدمة، فمثلا بالنسبة لمعطيات المشترك المعروف للكافحة يمكن لأي طرف أن يخول رجال السلطة العامة بأن يصدرو أمرا من هذا الطراز، بينما في حالات أخرى فإن الوضع يقتضي صدور أمر من السلطة القضائية كما هو حال بالنسبة لمعطيات المتعلقة بطريقة الدفع.

ولم تذهب الإتفاقية العربية بعيدا عما ذهبت إليه إتفاقية بودابست، حيث نصت في المادة 25 تحت عنوان "أمر تسليم المعلومات" بضرورة تبني كل دولة طرف الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلـــى:

1- أي شخص في إقليمها لتسليم معلومات معينة في حيازة ذلك الشخص والمخزنة على تقنية معلومات أو وسيط تخزين معلومات.

2- أي مزود خدمة يقدم خدماته في إقليم الدولة الطرف لتسليم معلومات المشترك المتعلقة بتلك الخدمات في حوزة مزود الخدمة أو تحت سيطرته.

من خلال ما سبق يتضح أن الأمر بتقديم معطيات متعلقة بالمتشرك هو إجراء أقل تدخلا في الحقوق الشخصية أو الخصوصية من إجراءات الضبط أو التفتيش، بهدف الحصول على معلومات ضرورية تفيد التنقيب أو التحقيق، بمعنى آخر فإن هذا الإجراء هو :عبارة عن إجراء مرن يسمح للسلطات بأن تضعه موضع التنفيذ في حالات كثيرة وعلى وجه الخصوص في الحالات التي لا يكون من الضروري اللجوء إلى إجراء أكثر إجبارا أو أكثر كلفة"[1].

وقد ظهر إتجاه في التشريعات المقارنة نحو السماح لضباط الشرطة القضائية بالإطلاع على الأنواع السابقة من المعطيات، مع إلزام مقدمي خدمات الإتصالات السلكية والإلكترونية بالتعاون معهم، ومن تلك التشريعات قانون الإجراءات الفرنسي الذي ينص في مادته 60-1 المعدلة بالقانون رقم 2016-731[2] على أنه لوكيل الجمهورية أو ضابط الشرطة القضائية و بأي وسيلة، أن يطلب من كل شخص، من كل مؤسسة من كل جهة خاصة أو عامة أو كل إدارة عامة، من المحتمل حيازتهم **معلومات** ذات صلة بالتحقيق، بما في ذلك المتعلقة بنظام المعالجة الآلية أو بمعالجة المعطيات الشخصية أن يسلمه هذه المعلومات خاصة في شكل رقمي دون أن يكون لهؤلاء أن يتمسكو **بدون وجه حق** بالإلتزام بسر المهنة، وعندما يتعلق هذا الطلب بالأشخاص المشار إليهم في المواد 56-1 إلى 56-5 فإن تسليم هذه المعلومات لا يمكن أن يتم إلا بموافقتهم.

وبإستثناء الطوائف المنصوص عليهم في المادة 56-1 إلى 56-5 فإن الإمتناع عن إجابة الطلب السابق في أقرب وقت ممكن معاقب عليه بغرامة قدرها 3750 يورو.

والملاحظ أن المعلومات التي تهم التحقيق في سياق المادة السابقة، قد تكون ملفات (حاملها ورقي) أومعطيات معلوماتية، وإشارة المادة السابقة للمادة 56-1 إلى 56-5، تنويها بذلك إلى شروط االتفتيش والحجز في مكاتب المحاماة في المؤسسات الصحفية، مكتب الطبيب، الموثق، محضر القضائي.

---

[1]-**د. هلالي عبد الله**، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، المرجع السابق، ص214.

[2]-**Article 60-1** Modifié par LOI n°2016-731 du 3 juin 2016 - art. 58 dispose que " Le procureur de la République ou l'officier de police judiciaire peut, par tout moyen, requérir de toute personne, de tout établissement ou organisme privé ou public ou de toute administration publique qui sont susceptibles de détenir des informations intéressant l'enquête, y compris celles issues d'un système informatique ou d'un traitement de données nominatives, de lui remettre ces informations, notamment sous forme numérique, sans que puisse lui être opposée, sans motif légitime, l'obligation au secret professionnel. Lorsque les réquisitions concernent des personnes mentionnées aux articles 56-1 à 56-5, la remise des informations ne peut intervenir qu'avec leur accord."

A l'exception des personnes mentionnées aux articles 56-1 à 56-5, le fait de s'abstenir de répondre dans les meilleurs délais à cette réquisition est puni d'une amende de 3 750 euros.

كما يلزم القانون الفرنسي رقم 719 لسنة 2000 الخاص بحرية الإتصالات بموجب المادة 43-9[1] متعهد الوصول ومتعهد خدمة الإيواء بالمحافظة على معطيات مستعملي خدماتهم وذلك تمهيدا لطلب السلطات منهم تلك المعطيات التي قد تفيد كدليل في جريمة معينة قد وقعت بالفعل.

ويجيز القانون الأمريكي المعروف ب ECPA إطلاع رجال الضبط القضائي في إطار ما يقومون به من جمع الإستدلالات على المعطيات الموجودة في حوزة مقدمي الخدمات والتي تخص مستخدمي شبكة الأنترنت، وهذه المعطيات تتعلق في ثلاث طوائف[2]:

-المعلومات الشخصية الخاصة بالمشترك مثل إسمه رقم تليفونه وعنوانه.

-المعلومات الشخصية الخاصة بالمتعامل مع المشترك، أي كل من يتصل به أو يدخل معه في صفقة.

-المعلومات المتعلقة بمحتوى الملفات (مضمون المحادثات- مضمون الملفات).

و بناء عليه فإن المتشرك في خدمات مقدم الخدمات لا يتمتع بالحق في الخصوصية بالنسبة لهذه الأنواع الثلاثة من المعلومات سابقة الذكر[3].

والوضع يختلف في كل من التشريع المصري والجزائري، حيث لا يجوز أن يصدر رجل الضبط القضائي مثل هدا الأمر، وإنما لسلطة التحقيق، ولاتختلف سلطة النيابة العامة في ذلك عن سلطة قاضي التحقيق، حيث تنص المادة 99 من قانون الإجراءات المصري أنه "لقاضي التحقيق أن يأمر الحائز لشيء يرى ضبطه أو الإطلاع عليه تقديمه، ويسري حكم المادة 284 على من يخالف ذلك الأمر..."، كما أن للمحكمة أن تصدر مثل هذا الأمر فتنص المادة 291 إجراءات على أنه " للمحكمة أن تأمر ولو من تلقاء نفسها أثناء نظر الدعوى، بتقديم أي دليل تراه لازما لظهور الحقيقة، كما تنص المادة 212 إجراءات جزائري على أنّه" *يجوز إثبات الجرائم بأي طريق من طرق الإثبات...*".

ومن المعروف أنه يجوز لقاضي التحقيق أن يأمر بتفتيش منزل غير المتهم لضبط هذه المستندات أو المعطيات المتواجدة لدى الغير، فتنص المادة 91 إجراءات مصري"...ولقاضي التحقيق أن يفتش أي مكان ويضبط فيه الأوراق والأسلحة وكل ما يحتمل أنه إستعمل في إرتكاب الجريمة أو نتج عنها أو وقعت عليه وكل ما يفيد في كشف الحقيقة..."، كما تنص المادة 81 إجراءات جزائري يجوز لقاضي التحقيق أن يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء يكون كشفها مفيدا لإظهار الحقيقة"، كما أن

---

[1]-Art. 43-9. Dispose que "- Les prestataires mentionnés aux articles 43-7 et 43-8 sont tenus de détenir et de conserver les données de nature à permettre l'identification de toute personne ayant contribué à la création d'un contenu des services dont elles sont prestataires."

LOI no 2000-719 du 1er août 2000 modifiant la loi no 86-1067 du 30 septembre 1986 relative à la liberté de communication, JORF n°177 du 2 août 2000 page 11903

[2]- **د. شيماء عبد الغني،** المرجع السابق، ص216.

[3]- وتطبيقا لذلك قضي بأن وضع جهاز pen register لتسجيل أسماء طرفي الإتصال في صدد المحادثات الإلكترونية يجوز لرجال الضبط القضائي أن يقوم به دون شرط الحصول المسبق على إذن قضائي، بإعتبار ذلك منتميا إلى مجال جمع الإستدلالات وليس فيه إخلال بحرمة الحياة الخاصة

The installation and use of the pen register was not a "search" within the meaning of the Fourth Amendment, and hence no warrant was required, Smith v. Maryland, 442 U.S. 735 (1979) available at :https://supreme.justia.com/cases/federal/us/442/735/case.html

لوكيل الجمهورية أن يأذن بتفتيش منزل غير المتهم، فتنص المادة 206 إجراءات مصري على أنه "لايجوز للنيابة العامة تفتيش غير المتهم أو منزل غير منزله إلا إذا إتضح من إمارات قوية أنه حائز لأشياء تتعلق بالجريمة...ويشترط لإتخاذ أي إجراء من الإجراءات السابقة الحصول مقدما على أمر مسبب بذلك من القاضي الجزئي بعد إطلاعه على الأوراق".

كما نجد المادة 44 إجراءات جزائري على أنه "لايجوز لضابط الشرطة القضائية الإنتقال إلى مسكن الأشخاص الذين يظهر أنهم ساهمو في الجناية و أنهم يحوزون أوراقا أو أشياء لها علاقة بالأفعال الجنائية المرتكبة لإجراء التفتيش إلا بإذن.....ويكون الأمر كدلك في حالة الجنحة المتلبس بها أو التحقيق في إحدى الجرائم المدكورة في المادة 37 و40 " ومن بينها الجرائم الواقعة على نظم المعالجة الآلية، وتستكمل المادة 45 إذا جرى التفتيش في مسكن شخص آخر يشتبه بأنه يحوز أوراقا أو اشياء لها علاقة بالأفعال الإجرامية...ولضابط الشرطة القضائية وحده مع الأشخاص السابق دكرهم في الفقرة الأولى أعلاه الحق في الإطلاع على الأوراق أو المستندات قبل حجزها".

كما يلزم القانون الجزائري رقم 09-04 مقدم الخدمة بالمحافظة على المعطيات المتعلقة بحركة السير إلكترونية كانت أو تلفونية وذلك تمهيدا لطلب السلطات المكلفة بالتحريات القضائية منهم تلك المعطيات التي قد تفيد كدليل.

الفصل الثاني

قواعد الإثبات الجزائي والإختصاص القضائي في جرائم الإعتداء على التعاملات الإلكترونية

ينشأ عن وقوع الجريمة حق الدولة في عقاب مقترفيها، بيد أن هذا الحق يتوقف على إثبات ونسبة إرتكاب تلك الجريمة إلى شخص معين، وهو المتهم لذا يتعين على سلطة التحقيق، ومن بعدها سلطة القضاء البحث عن حقيقة هذه الجريمة ومدى صحة نسبتها إلى المتهم من عدمه، وهنا تكمن أهمية العملية الإثباتية.

ويقصد بالإثبات[1] كما يعرفه البعض هو إقامة الدليل لدى السلطات المختصة بالإجراءات الجنائية على حقيقة واقعة ذات أهمية قانونية، وذلك وفق الطرق التي حددها القانون ووفق القواعد التي أخضعها لها.

وتدور القواعد التي تحكم عملية الإثبات الجزائي حول تحقيق هدف أساسي هو تحقيق العدالة الجزائية بالكشف عن الحقيقة، التي تهم المجتمع بأسره[2].ومن ثم فإن الركيزة الأولى لعملية الإثبات الجنائي هي مدى توافر الدليل القاطع الذي بمقتضاه يستطيع القاضي أن يبرر الإدانة أو البراءة التي يحكم بها، فالقاضي لا يكون في إستطاعته الحكم بما يعتقد أنه الحق من غير دليل يستند إليه، ومن هنا جاءت الأهمية القصوى لعملية الإثبات في المواد الجزائية[3].

وقد مرت نظم الإثبات الجزائي بمراحل متعددة مسايرة لمراحل التطور الإجتماعي، ومنها المرحلة السحرية والإحتكام إلى الآلهة أو المرحلة الدينية، ومرحلة الأدلة القانونية ومرحلة الإقتناع الذاتي للقاضي الجزائي وأخيرا مرحلة الأدلة العلمية[4]:

نظام الأدلة القانونية: حيث يقوم المشرع في هذا النظام بتحديد الأدلة التي يجوز للقاضي قبولها في حالة معينة، والقيمة القانونية للدليل إذا توافرت له شروط معينة، فالقاضي يصل إلى إقتناعه من خلال عملية تتوقف على قواعد محددة سلفا من المشرع.

الإثبات في العصرالحديث: هنا المشرع لم يرسم لأطراف الخصومة الجنائية طريقا معينا للإثبات يتقيدون به، بل ترك لهم حرية تقديم ما يرونه موصلا لإقتناع القاضي، وللقاضي أن يستمد إقتناعه من أي منها.

نظام الأدلة العلمية:يقوم هذا النظام على الاستعانة بالأساليب الفنية التي كشف عنها العلم الحديث في إثبات الجريمة ونسبتها إلى المتهم، ويعطى الدور الرئيسي في الإثبات للخبير، وهذا النظام مطبق حاليا إلى جانب نظام الإقتناع القضائي.

وإذا كانت القواعد العامة في الإثبات الجنائي تختلف بإختلاف السياسة التشريعية التي يتبعها المشرع الجنائي، ووفق المباديء التي يعتنقها في هذا المجال، فإن ذلك لا يعني أكثر من أن عامل الإختلاف بين نظم

---

[1]-**د. محمود نجيب حسني**، شرح قانون الإجراءات الجزائية، المرجع السابق، ص405.

[2]-**د. حسنين المحمدي بوادي**، الوسائل العلمية الحديثة في الإثبات الجزائي، منشأة المعارف، الإسكندرية، 2005، ص5.

[3]- **د. جميل عبد الباقي الصغير**، أدلة الإثبات الجزائي والتكنولوجيا الحديثة، (أجهزة الرادار – الحاسبات الآلية – البصمة الوراثية)دراسة مقارنة ، دار النهضة العربية، القاهرة، 2001، ص12.

[4]- أنظر: **د. رمسيس بهنام**، الإجراءات الجنائية تأصيلا وتحليلا، منشأة المعارف، الإسكندرية، 1984، ص698. **د. صوفي أبو طالب**، تاريخ النظم القانونية والإجتماعية، دار النهضة العربية، القاهرة، 1977، ص48.**د.عبد الوهاب حومد**، أصول المحاكمات الجزائية، الطبعة الرابعة، المطبعة الجديدة، دمشق، 1987، ص528 و ما بعدها.**حسن الجوخدار**، أصول المحاكمات الجزائية، الجزء الثاني، الطبعة الخامسة، منشورات جامعة دمشق، 1991، ص124 وما بعدها.**د. محمود نجيب حسني**، شرح قانون الإجراءات الجزائية، المرجع السابق، ص408 وما بعدها. **د. عبد الناصر محمد محمود فرغلي**، المرجع السابق، ص86.

الإثبات في هذا الشأن ليس سوى إختلافا في نهج الإعتراف بالحقيقة، وفي هذا لكل نظرته في الوصول إليها[1].

ويتمثل جوهر العملية الإثباتية في تحويل حالة الشك في الواقعة المراد إثباتها إلى حالة من التقين بحدوثها من خلال التوصل إلى إقناع القاضي بحقيقة ذلك عن طريق ما يقدم في الدعوى من أدلة[2]. ولكي يتمكن القاضي من بناء عقيدته وإقتناعه الذاتيين بما يجعل حكمه هو عنوانا صادقا للحقيقة الواقعية ومعبرا عنها، فلابد في سبيل ذلك أن يعتمد على وسائل معينة تمثل دعائم الإثبات الجزائي كالشهادة والقرائن والخبرة والمعاينة.

وإذا كانت هذه الوسائل لا زالت فعالة في البيئة المادية، فإنه ليست بذات الفعالية في البيئة الإلكترونية التي ترتكب في نطاقها الجرائم الواقعة على التعاملات الإلكترونية المختلفة. فقد تتعرض الكثير من نظم المعلومات بما تحتويه من معلومات(مستندات معلومايتة، معطيات شخصية،....) التي تعتمدها التعاملات الإلكترونية لكثير من المخاطر التي تؤثر على أداء وظائفها والهدف الذي وجدت من أجله، وهذه المخاطر إما أن تكون مادية أو معنوية، وفي هذه الأخيرة يقع الإعتداء غالبا بسبب الإختراق أو التزوير أو التحريف في المعطيات المعالجة بعد إختراق الأمن الإلكتروني لها، سواء تمت هذه الأعمال أثناء إدخال هذه المعطيات أو أثناء تخزينها أو أثناء إخراجها، وما يميزه أنه سريع وغير مرئي فهو يقع على نبضات إلكترونية، وبإمكان الجاني أن يمحو المعطيات التي تستخدم ضده كأدلة في أقل من ثانية، أو إخفاء أفعاله بإستخدام كلمات السر والتشفير.

ولاشك أن كشف ستر هذا النوع من الجرائم يحتاج أيضا إلى **طرق إلكترونية** تتناسب مع خصوصية هذه الجرائم، بحيث يمكنها فك رموزه وترجمة نبضاته وذبذباته إلى كلمات ومعطيات محسوسة ومقروءة تصلح لأن تكون **أدلة إثبات لها**[3]، وتتمثل في "الدليل الإلكتروني" الذي يتشكل من طبيعة الجريمة التي يولد منها.

وإن كان هذا الأخير يمكن الحصول عليه من خلال طرق فنية وعلمية تتناسب مع طبيعته ويمكن بإتباعها إثبات الجرائم التي تقع على التعاملات الإلكترونية، فإنه قد يكون نتاج خبرة أو تفتيش أو غيرها مع الحاجة لتطويرها لكي تقوى على ذلك، مع وضع ما يشبه بروتوكولات لضمان الجودة المستخدمة في مجاله.

والطبيعة الخاصة للجرائم الواقعة على التعاملات الإلكترونية لم تقف عند حد السلوكات التي تتحقق بها وطبيعة الوسط الذي ارتكبت فيه وطرق إثباتها، وإنما تمتد هذه الطبيعة لتشمل البعد العالمي لهذا النوع من الجرائم، فالطبيعة الدولية للأنترنت قد أدت إلى إرتكاب جرائم الإعتداء على التعاملات الإلكترونية عن طريق وحدة طرفية في دولة معينة، بينما تتحقق النتيجة في دولة أخرى. الأمر الذي يثير التساؤل حول الإختصاص القضائي بنظر هذه الجرائم.

---

[1]-**د. عمر محمد أبـــو بكر بن يونس**، الجرائم الناشئة عن إستخدام الأنترنت، المرجع السابق، ص931.

[2]– **د. أيمن عبد الحفيظ**، الإتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، الطبعة الأولى، دار النهضة العربية، القاهرة، 2005، ص 187.

[3]– **د. علي محمود علي حمودة**، المرجع السابق، ص34.

وتماشيا مع تسلسل الأفكار على النحو السابق، فإننا قسمنا هذا الفصل إلى ثلاث مباحث على النحو التالي:

المبحث الأول:طرق الإثبات الجزائي التقليدية في جرائم الإعتداء على التعاملات الإلكترونية

المبحث الثاني: طرق الإثبات الجزائي المستحدثة في جرائم الإعتداء على التعاملات الإلكترونية

المبحث الثالث: الاختصاص القضائي بنظر جرائم الإعتداء على التعاملات الإلكترونية

المبحث الأول

طرق الإثبات الجزائي التقليدية في جرائم الإعتداء على التعاملات الإلكترونية

إذا كان هناك ضرورة لتطوير الإثبات الجزائي بتطوير طرقه أمر في غاية الأهمية بما يتناسب وطبيعة الجرائم الواقعة على التعاملات الإلكترونية الفنية والخاصة، فلا يعني ذلك إستبعاد الطرق التقليدية، إلا أنها قد تكون في حاجة إلى تطوير مستمر لكي يمكنها أن تتناسب مع الطبيعة الخاصة لهذه الجرائم.

وقد سبق وتناولنا بالشرح والتفصيل في موطن متقدم من هذه الدراسة بعضا منها، لذا فنحن نحيل بشأن ذلك إلى ما سبق ذكره ضمن ما تقدم من هذه الدراسة ليقتصر بحثنا من خلال المطالب الثلاثة التالية عـــلى الشهادة والقرائن والخبرة التقنية.

المطلب الأول

الشهادة في مجال جرائم الإعتداء على التعاملات الإلكترونية

تعد الشهادة في الجرائم الواقعة على التعاملات الإلكترونية من الأدلة الهامة التي يمكن تقديمها للمحكمة، لكونها عاملا حاسما يمثل منطق التعامل مع نوعية الجرائم هذه، وإن كانت الشهادة لا تختلف من حيث كيفية الإستعانة بها أو نظام أدائها أو أثرها بين الجرائم التقليدية وتلك الواقعة على التعاملات الإلكترونية، فإنها قد تثير البعض من الإستفسارات في الجرائم الأخيرة، خاصة ماتعلق منها بنطاق الإلتزام بأداء الشهادة، ومدى إمكانية إدلائها عبر الوسائل الإلكترونية ذاتها؟.

وقبل الإجابة على هذا الســؤال، وإستكمالا للإجراءات المنهجية المتبعة في هذا المبحث، سنحاول التطرق للشهادة بصفة عامة، ثم ندخل في رحاب الفروع الأخرى ملقين الضوء على الشهادة في جرائم التعاملات الإلكترونية.

الفرع الأول

التعريف بالشهادة بصفة عامة

إن الشهادة بإعتبارها إجراء من إجراءات التحقيق إنما هي المعلومات التي تتعلق بالجريمة التي يدلي بها الشاهد أمام سلطة التحقيق، وهي الطريق العادي للإثبات الجنائي[1]، فهي إذن تقرير الشخص بما وصل إلى علمه بحاسة من حواسه، البصر، السمع، الشم، أو غيرها[2]، وكثيرا ما يكون للشهادة وخاصة تلك التي يدلي بها فور وقوع الحادث أكبر الأثر في الحكم بالإدانة أو البراءة، وغالبا ما تقوم بدور الدليل في الدعوى بمفردها ودون أن يؤازرها دليل آخر، ومن أجل ذلك عنيت التشريعات بتنظيم أحكام الشهادة وإحاطتها بضمانات متعددة زخرت بها التشريعات الإجرائية المختلفة بغية البعد بها عن كل ما يحتمل التأثير فيها. ولما كانت شهادة الشهود من أهم الأدلة التي يمكن بواسطتها الوصول إلى الحقيقة ومعرفة الجناة، فقد وجب على المحقق أو القاضي عند سؤال الشاهد التثبت من صدق أقواله ومناقشته وأخذ كل ما يدلي به بحيطة وحذر[3].

وللشهادة أهمية بالغة في المجال الجنائي بإعتبارها أهم طرق الإثبات قاطبة، فهي توازي الكتابة ودورها في الإثبات في المجال المدني، فغالبا ما يتم التصرف في التحقيق أو الحكم بالإدانة أو البراءة بناء على شهادة الشهود، بل يمكن أن تكون الشهادة هي الدليل الوحيد في الدعوى الذي يبنى عليه حكم القضاء[4].

الفرع الثاني

الإلتزام بأداء الشهادة في جرائم التعاملات الإلكترونية

إذا كان الشاهد يحمل إلتزامات معينة لا تخرجه عن نطاق الوقائع التي أحاط بها علمه، فإلى أي مدى أصبح هدا النظام صامدا أمام تحديات التقنية؟ أو لم يحن الوقت لإقرار وسيلة قانونية جديدة تحقق ما لم تستطع فكرة الإلتزام بأداء الشهادة أن تأديه؟ هذا ما سنراه من خلال النقاط التالية.

أولا– إلزام الشاهد بالإدلاء بالمعلومات

يقصد بالشاهد في جرائم الإعتداء على التعاملات الإلكترونية الفني صاحب الخبرة والتخصص في تقنية الحوسبة والإتصال، والذي تكون لديه معلومات جوهرية هامة للولوج في نظام المعالجة الآلية للمعطيات إذا

---

[1]- **د. عبد الفتاح بيومي حجازي**، مباديء الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت، المرجع السابق، ص334.

[2]–**د. محمود نجيب حسني**، شرح قانون الإجراءات الجزائية، المرجع السابق، ص441.

[3]- **د. هلالي عبد الله احمد**، إلتزام الشاهد بالإعلام في الجرائم المعلوماتية–دراسة مقارنة–الطبعة الثانية، دار النهضة العربية، القاهرة، 2008، ص34.

[4]–في هذا المعنى أنظر: **د. رؤوف عبيد**، المرجع السابق، ص455.

كانت مصلحة التحقيق تقتضي ذلك، ويطلق على هذا النوع من الشهود مصطلح "**الشاهد المعلوماتي**" تمييزا له عن الشاهد التقليدي[1].

ويرى الفقه أن الشاهد في مجال التعاملات الإلكترونية يمكن أن يكون من إحدى الطوائف التالية[2]:

- **القائم على تشغيل النظام:** وهو المسؤول عن تشغيل النظام والمعدات المتصلة به، ويجب أن تكون لديه خبرة كبيرة في تشغيل الجهاز وإستخدام لوحة المفاتيح في إدخال المعطيات، كما يجب أن تكون لديه معلومات عن قواعد كتابة البرامج.
- **المبرمجون:** وهم الأشخاص المتخصصون في كتابة أوامر البرامج ويمكن تقسيمهم إلى فئتين:

  الفئة الأولى: مخططو برامج التطبيقات.

  الفئة الثانية: مخططو برامج النظم.

حيث يقوم مخططوا برامج التطبيقات بالحصول على خصائص ومواصفات النظام المطلوب من محلل النظم، ثم يقومون بتحويلها إلى برامج دقيقة وموثقة لتحقيق هذه المواصفات، أما مخططوا برامج النظم فيقومون بإختبار وتعديل وتصحيح برامج نظام الحاسب الداخلية، أي أنهم يقومون بالوظائف الخاصة بتجهيز النظام بالبرامج والأجزاء الداخلية التي تتحكم في وحدات الإدخال والإخراج ووسائط التخزين بالإضافة إلى إدخال أي تعديلات أو إضافات لهذه البرامج.

- **المحلل،** وهو الذي يقوم بتحليل خطوات البرنامج وتجميع معطيات النظام، ودراسة هذه المعطيات ثم تحليل النظام أي تقسيمه إلى وحدات منفصلة وإستنتاج العلاقات الوظيفية من هذه الوحدات، كما يقوم بتتبع المعطيات داخل النظام عن طريق ما يسمى بمخطط تدفق المعطيات وإستنتاج الأماكن التي يمكن ميكنتها بواسطة النظام.
- **مهندسو الصيانة والإتصالات[3]:**وهم المسؤولون عن أعمال الصيانة الخاصة بتقنيات الحاســـــــب بمكوناته وشبكات الإتصال المتعلقة بـــه.
- **مدير النظام:** وهو الذي يوكل إليه أعمال الإدارة في النظم المعلوماتية، ويدخل ضمن هذه الطائفة مدخل المعطيات والمعلومات.

بالإضافة إلى هذه الفئات، هناك أشخاص آخرون يعدون بمثابة شهود في جرائم التعاملات الإلكترونية، وهذه الفئة لها دور كبير في توصيل المتعامل الإلكتروني إلى شبكة الأنترنت، وهي ما يصطلح عليها **بالوسطاء الفنيين** السابق دراستهم.

---

[1]– **د. هلالي عبد الله،** إلتزام الشاهد بالإعلام في الجريمة المعلوماتية، المرجع السابق، ص23.**ولنفس المؤلف:** تفتيش نظام الحاسب الآلي وضمانات المتهم المعلوماتي، ص43 وما بعدها. **د. عبد الفتاح بيومي حجازي،** الجوانب الإجرائية لأعمال التحقيق الإبتدائي في الجرائم المعلوماتية، دراسة مقارنة في ضوء القواعد العامة للإجراءات الجنائية، الطبعة الأولى، دار النهضة العربية، القاهرة، 2009، ص612.**د. خالد ممدوح ابراهيم،** فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص263.

[2]– **د. محمد فهمي طلبة وآخرون،** الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني، موسوعة دلتا كمبيوتر، مطابع المكتب المصري الحديث، القاهرة، 1991، ص23 وما بعدها. **د.هلالي عبد الله،** إلتزام الشاهد بالإعلام في الجريمة المعلوماتية، المرجع السابق، ص24. **د. عبد الفتاح بيومي حجازي،** الجوانب الإجرائية لأعمال التحقيق الإبتدائي في الجرائم المعلوماتية، المرجع السابق، ص613.

[3]-**د. عمر محمد أبو بكر بن يونس،** أشهر المباديء المتعلقة بالأنترنت في القضاء الأمريكي، المرجع السابق، ص439.

وتطبيقا لذلك، فإن الشهادة في إطار جرائم التعاملات الإلكترونية من الممكن أن يدلي بها مدخلوا المعطيات العاملون في إحدى الشركات، الذين تم تكليفهم بإرسال الرسائل الإلكترونية إلى الزبائن، إذا تبين فيما بعد أن الشركة كانت تقصد من وراء هذه الرسائل القيام بخداع الزبائن والإستيلاء على أموالهم، دون علم العاملين في الشركة.

إلا أن الأمر ليس بهذه البساطة دائما، فلقد أصبح بامكان برمجيات تكنولوجيا التشفير، والتي يمكن لأي إنسان أن يحملها من شبكة الأنترنت، تحويل أي كمبيوتر شخصي إلى آلة تشفير غير قابلة للإقتحام، ومع التوسع المتزايد لطريق المعلومات السريع سوف تطبق خدمات الأمن على كل أشكال المعلومات الرقمية مثل: المكالمات التلفونية والملفات وقواعد المعطيات، فمادام تم الإحتفاظ بكلمة السر فان المعلومات المخزنة في الكمبيوتر يمكن أن تظل محمية، مما يؤمن أقصى قدر من الخصوصية المعلوماتية[1].

وإن كان الرأي الغالب في الفقه يذهب إلى عدم إلزام المشتبه به على طباعة ملفات المعطيات المخزنة داخل النظام، أو الكشف عن الشفرات أو كلمات السر الخاصة بالدخول إلى هذه المعلومات، أو إجباره على تقديم الأمر اللازم لوقف الفيروس أو القنبلة المنطقية، ذلك أنه لا يجوز إلزام الشخص بإتهام نفسه سواء عن طريق الشهادة أو عن تقديم عناصر الإثبات فضلا عن صعوبات عملية لا يمكن التغلب عليها ، لعل أبرزها أن المتهم يستطيع التذرع بنسيان المعلومة أو عدم إمكان تذكرها أو ما شابه ذلك. فإن التساؤل المثار في هذا المجال هو: **ما مدى إلتزام الشاهد في جرائم التعاملات الإلكترونية بتقديم مثل هذه المعلومات؟** للإجابة على هذا السؤال أهميته حيث أن الخبير المنتدب من الجهة القضائية قد لا يمكنه معرفة الأساليب الفنية التي يمكن إتباعها للكشف عن أدلة تفيد في كشف الحقيقة، وقد لا يعلمها إلا هذا الشاهد[2].

لقد اختلف الفقه المقارن في الإجابة على هذا السؤال بين مؤيد ومعارض، ويمكن بلورة هذا الخلاف في إتجاهين رئيسيين:

الإتجاه الأول: يذهب القائلون بهذا الإتجاه إلى أنه ليس من واجب الشاهد وفقا للإلتزامات التقليدية للشهادة أن يقوم بطبع ملفات المعطيات أو الإفصاح عن كلمات المرور أو الشفرات الخاصة بالبرامج المختلفة. ويجد هذا الإتجاه تجسيده التشريعي والفقهي في كل من ألمانيا[3] و تركيا[4].

الإتجاه الثاني:يرى أنصار هذا الاتجاه أن من الالتزامات التي يلتزم بها الشاهد القيام بطبع ملفات المعطيات، أو الإفصاح عن كلمات المرور أوالشفرات الخاصة بالبرامج المختلفة، ففي هولندا يتيح مشروع قانون الحاسب الآلي لسلطات التحري والتحقيق إصدار الأمر للقائم بتشغيل النظام بتقديم المعلومات اللازمة لإختراقه والولوج إلى داخله، كالإفصاح عن كلمات المرور السرية والشفرات الخاصة بتشغيل البرامج

---

[1]–**بيل جيتس**، المعلوماتية بعد الانترنت، طريق المستقبل، ترجمة عبد السلام رضوان، المجلس الوطني للثقافة والفنون والآداب، العدد 231، الكويت، 1998، ص428.

[2] -**د. شيماء عبد الغني**، المرجع السابق، ص

[3]-**mohrenschloager (Manfred),** Computer Crime and Other Crimes Against Information Technology in germany ridp,1993,p351.

مشارإليـــه لـــدى: د. **هلالي عبد الله أحمد**، إلتزام الشاهد بالإعلام في الجرائم المعلوماتية، المرجع السابق، ص53.

[4]- **ERMAN (sahir),** les crimes informatique et d'autres crimes dans le domaine de la techonologie informatique en Turquie R.I.D.P. 1993.P624.

المختلفة، وإذا وجدت معطيات مشفرة أو مرمزة داخل ذاكرة الحاسب وكانت مصلحة التحقيق تسلتزم الحصول عليها، يتم تكليف القائم على تشغيل النظام المعلوماتي بحل رموز هذه المعطيات[1].

كما يؤيد بعض الفقهاء في فرنسا هذا الإتجاه، ويرون أنه طالما أن المشرع لم ينظم هذه المسالة، فإنه لا مناص من تطبيق القواعد العامة في الشهادة، وعلى ذلك فإن الشهود الذين يقع على عاتقهم الإلتزام بأداء الشهادة يكونوا مكلفين بالكشف عن كلمات المرور السرية التي يعرفونها أو شفرات تشغيل البرامج، ماعدا حالات المحافظة على سر المهنة فإنهم يكونون في حل من هذا الإلتزام.[2]

وفي مقام الموازنة والترجيح بين الإتجاهين السابقين، فلا شك في رجحان الإتجاه الأول، فالقاعدة الأصولية في الجزائر وفي مصر وغيرها من الدول لا تلزم الشاهد بالإدلاء بمثل هذه المعلومات، وإن كانت تلزمه بثلاث إلتزامات أساسية إذا ما تم تبليغه تبليغا صحيحا[3]:

أ-**الحضور أمام الجهة التي إستدعته:**ومضمون هذا الإلتزام أن يحضر الشاهد بنفسه في المكان والوقت المحددين للإستماع إلى شهادته، ثم البقاء فيه حتى يؤذن له بالإنصراف[4]. ويضمن المشرع الوفاء بهذا الإلتزام عن طريق تقرير جزاءات، حيث تنص المادة 97 من قانون الإجراءات الجزائية الجزائري "***كل شخص إستدعي لسماع شهادته ملزم بالحضور و حلف اليمين و أداء الشهادة مع مراعاة الأحكام القانونية المتعلقة بسر المهنة.***

و إذا لم يحضر الشاهد فيجوز لقاضي التحقيق بناء على طلب وكيل الجمهورية استحضاره جبرا بواسطة القوة العمومية و الحكم عليه بغرامة من 200 إلى 2000 دينار غير أنه إذا حضر فيما بعد و أبدى أعذارا محقة و مدعمة بما يؤيد صحتها جاز لقاضي التحقيق بعد سماع طلبات وكيل الجمهورية اقالته من الغرامة كلها أو جزء منها.

ويجوز توقيع العقوبة نفسها بناء على طلب رجل القضاء المذكور على الشاهد الذي يمتنع رغم حضوره عن أداء اليمين أو الإدلاء بشهادته."

أما في حالة التخلف عن الحضور أثناء المحاكمة، وكانت الشهادة تنصب على مخالفة أو جنحة، فتطبق أحكام المادة 223 إجراءات التي أحالت إلى أحكام المادة 97 من نفس القانون، أي إمكانية لجوء قاضي الحكم إلى إستعمال القوة العمومية أو تأجيل القضية لأقرب جلسة ممكنة ويتحمل الشاهد في هذه الحالة كل مصاريف التكليف بالحضور والإجراءات والإنتقال وغيرها، إضافة للعقوبة التي يمكن تسليطها عليه والمتمثلة في الغرامة من 200 إلى 2000 دج.

---

[1]-**kaspersen**, computer crimes and other vrimes against information technology in netherland, RIDP, P479.

مشارإليه لدى: **سليمان احمد فضل**، المواجهة التشريعية والأمنية للجرائم الناشئة عن إستخدام شبكة المعلومات الدولية(الأنترنت)، دار النهضة العربية، القاهرة، 2013،ص 336.

[2]- **Francillon (gaques)**; Les crimes informatiques ET d' autres crimes dans domaine de la technologie informatique en France; RIDP; 1993. P309

[3]- **د. محمود نجيب حسني**، شرح قانون الإجراءات الجنائية، المرجع السابق، ص448 وما بعدها، **براهيمي صالح**، الإثبات بشهادة الشهود في القانون الجزائري، رسالة دكتوراه، كلية الحقوق، جامعة مولود معمري، تيزي وزو، 2012، ص160.

[4]- د.**محمود نجيب حسني**، شرح قانون الإجراءات الجنائية، المرجع السابق، ص448.

إلى جانب المشرع الجزائري ضمن المشرع المصري الوفاء بهذا الإلتزام عن طريق العقوبة والأمر بالضبط والإحضار، وذلك في مرحلة التحقيق الإبتدائي(117 إجراءات) أو في مرحلة المحاكمة (279 إجراءات).

ب-حلف اليمين:يتعين حلف اليمين قبل أداء الشهادة، واليمين تعني أن الشاهد يتخذ الله تعالى رقيبا على صدق شهادته ويعرض نفسه لغضبه وإنتقامه إن كذب فيها، والتكييف القانوني لليمين أنها ضمانة تضفي على الشهادة الثقة التي يتعين أن تتوافر لها كي تكون دليلا يستمد منه القاضي إقتناعه، واليمين ضمانة من وجهة أخرى، ذلك أنها تحيط الشهادة بشكلية خاصة، وهي بذلك تلفت إنتباه الشاهد إلى أهمية ما يقوله وتجعله حريصا على قول الحق[1].وقد نصت على هذا الإلتزام المادة 97 و222 إجراءات جزائية جزائري، كما نص عليه المشرع المصري في المادة 283و119 من قانون الإجراءات الجزائية، ويعفى من هذا الإلتزام بعض الأشخاص الذين يؤدون الشهادة على سبيل الإستدلال، كما لا يحلف اليمين الشهود في مرحلة الإستدلال (29-2 اجراءات مصري).

وقد حدد المشرع الجزائري صيغة اليمين بحيث يؤديها الشاهد حسب المادة 93-2 إجراءات جزائية، ويده اليمنى مرفوعة كمايلي:"أقسم بالله العظيم أن أتكلم بغير حقد ولاخوف وأن أقول كل الحق ولاشيء غير الحق".

ومن جهته أقر المشرع الفرنسي صيغة معينة لليمين، وإن كانت تختلف بإختلاف المحاكم، فهي أمام محاكم الجنح والمخالفات وقضاة التحقيق وطبقا للمواد (103-446-536) كالأتي "الشاهد يقول كل الحق ولاشيء غير الحق"، أما أمام محكمة الجنايات طبقا للمادة 331-3[2] كالتالي "أتكلم بدون حقد و بدون خوف و أقول كل الحق ولاشيء غير الحق".كما حدد من جهته المشرع المصري صيغة اليمين في المادة 283 إجراءات، ولكن هذه الصيغة غير إلزامية، فيكفي حلف الشاهد بأن "**يشهد بالحق**"[3].

وإن كان ليس من الضروري ذكر صيغة اليمين بأكملها في المحضر[4] إلا أنه لابد أن تثبت المحكمة أو المحقق في المحضر حلف الشاهد اليمين، ولكن إذا لم يثبت ذلك في المحضر فيترتب على إغفاله البطلان عند كل من المشرع الفرنسي والجزائري، على خلاف الوضع بالنسبة للمشرع المصري، فالفرض أن الإجراءات قد روعيت وهذا الإفتراض يقبل إثبات العكس، فإذا ثبت عدم حلف اليمين قضي بالبطلان[5].

---

[1]- المرجع نفسه، ص452.

[2]-**Article 331 alinea 3 du CPPF**Modifié par Loi n°2004-204 du 9 mars 2004 - art. 154 JORF 10 mars 2004 dispose que "Avant de commencer leur déposition, les témoins prêtent le serment " de parler sans haine et sans crainte, de dire toute la vérité, rien que la vérité ". Cela fait, les témoins déposent oralement. Le président peut autoriser les témoins à s'aider de documents au cour de leur audition."

[3]- **د. محمود نجيب حسني**، شرح قانون الإجراءات الجنائية، المرجع السابق، ص452.

[4]- الغرفة الجنائية، قرار 26 نوفمبر 1985 ملف 39440، المجلة القضائية، 1990-1، ص242.

[5]- **د. محمود نجيب حسني**، شرح قانون الإجراءات الجنائية، المرجع السابق،ص452.

وما يجدر الإشارة إليه أن أداء الشاهد اليمين من النظام العام مالم يوجد ما يبرر إعفاءه من أدائها، ويتعين على المحكمة مراعاتها تحت طائلة بطلان الإجراء ومعه بطلان الحكم[1].

ت-الإدلاء بالشهادة:وهو من أهم الإلتزامات المفروضة على الشاهد، إذ هو جوهر مهمته، ومن أقواله التي تتمثل فيها شهادته يستمد الدليل[2]، والإدلاء بالشهادة ينطوي على **الإلتزام بالتكلم وواجب قول الحقيقة:**

1-الإلتزام بالتكلم: فإذا حضر الشاهد وحلف اليمين وجب عليه أداء الشهادة، فإن إمتنع يحكم عليه بغرامة من 200 إلى 2000 دج حسب المادة 97 إجراءات جزائري، وبعشرة جنيهات في المخالفات ومائتي جنيه في الجنح والجنايات حسب المادة 284 إجراءات مصري.

لكن ترد عليه عدة إستثناءات، فواجب مساعدة القضاء في كشف الحقيقة يصطدم بعوائق هامة ناشئة عن واجبات أخرى يفرضها القانون نفسه على بعض الفئات من الأشخاص ومن بين هذه الواجبات ما يتعلق بعدم جواز إفشاء السر المهني وعدم جواز إفشاء الموظف لما علم به أثناء قيامه بوظيفته من أمور غير معدة لإطلاع الجمهور عليها[3].

2-الإلتزام بذكر الحقيقة ولاشيء غير الحقيقة: والمقصود بذلك الحقيقةالواقعية لما يكون قد رآه أو سمعه بنفسه، أو أدركه على وجه العموم بحواسه بخصوص واقعة معينة، وإلا عرض نفسه لعقوبة شهادة الزور.

من خلال ما سبق، يتضح لنا أن الشاهد يحمل إلتزامات معينة، ومن ثم فإن الإدلاء بمعلومات لازمة لإختراق نظام معلوماتي معين بحثا عن أدلة الجريمة داخله يخرجه عن نطاق الوقائع التي أحاط بها علمه، وهكذا يصبح الطريق ممهدا لإدخال وسيلة قانونية جديدة تحقق ما لم تستطع فكرة الإلتزام بأداء الشهادة أن تأديه، وهذه الوسيلة هي "**الإلتزام بالإعلام في الجريمة**" ليمثل أهمية عظيمة في إمكانية جمع الأدلة في الجرائم محل الدراسة، كما يلعب دورا وقائيا هاما إذ أن تطبيقه يمنع من ضبط النظام الشبكي بأكمله وعدم عزله عن البيئة المعلوماتية المحيطة به[4].

هذا وقد نصت إتفاقية بودابست في المادة التاسعة عشر في فقرتها الرابعة على أنه يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من أجل تخويل سلطاته المختصة سلطة إصدار الأمر لأي شخص لديه معلومات عن تشغيل النظام أو الإجراءات المطبقة من أجل حماية المعطيات المعلوماتية التي تضمن تقديم كل المعلومات الضرورية على نحو معقول يسمح بتطبيق الإجراءات المشار غليها في الفقرتين 1، 2..."

فهنا نجد أن هذه الفقرة أثارت مسألة في غاية الأهمية تتمثل في إلزام مديري النظام بالتعاون أو تقديم المساعدة اللازمة بحكم اللزوم العقلي والمنطقي للقيام بعملية التفتيش والضبط، إذ أنه بدون تأكيد هذا التعاون فإن السلطات المختصة يمكن أن تمكث في المواقع المراد تفتيشها ومنع الوصول إليها عبر النظام المعلوماتي فترة طويلة من الزمن وهذا الوضع يمكن أن يخلق عبثا إقتصاديا بالنسبة للشركات الشرعية أو لعملائها و

---

[1]-الغرفة الجزائية، قرار 21 ديسمبر 2005، ملف 391134، المجلة القضائية 2/2006 ، ص513.

[2]- **د. محمود نجيب حسني**، شرح قانون الإجراءات الجنائية، المرجع السابق، ص449.

[3]- **د. إدوارد عيد**، موسوعة أصول المحاكمات والإثبات والتنفيذ، الجزء السادس عشر، الإثبات(اليمين-والشهادة)، لبنان، 1991، ص206.

[4]- **د. علي محمود علي حموده**، المرجع السابق، ص48.

كذلك المشتركين الذي يجدون أنفسهم في حالة إستحالة للوصول إلى المعطيات أثناء التفتيش، والمعلومات التي يمكن إلزام مديري النظام بتقديمها هي المعلومات الضرورية التي تسمح بتطبيق إجراء التفتيش والضبط أو تطبيق طريقة مشابهة للدخول والحصول على المعطيات كأن يتعلق الإتصال بكلمات مرور أو إجراء أمني آخر[1].

ولم يذهب المشرع الجزائري بعيدا عما ذهبت إليه إتفاقية بودابست، حيث نص بدوره وبموجب الفقرة الأخيرة من المادة 5 من قانون 09-04 على إمكانية السلطات المكلفة بالتفتيش تسخير كل شخص له **دراية بعمل المنظومة المعلوماتية** محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها، ومما لاشك فيه أن الدخول إلى النظام المعلوماتي في هذه الحالة لا يمثل جريمة لأنه يتم بناء على إذن.

ثانيا- شروط إلزام الشاهد بالإعلام في جرائم الإعتداء على التعاملات الإلكترونية

الإلتزام بالإعلام في جرائم الإعتداء على التعاملات الإلكترونية من شأنه أن يوجب على الشاهد المعلوماتي في هذه النوعية من الجرائم، أن يدلي بما يحوزه من معلومات جوهرية، لازمة للولوج لنظام المعالجة الآلية تنقيبا عن أدلة الجريمة داخله، إلى جهة التحري أو التحقيق أو المحاكمة، ويجب أن يراعي الشاهد المعلوماتي في إعلامه أن يكون مفهوما بسيطا، محددا، دقيقا، صادقا، وأمينا[2].

ولاينشأ إلتزام الشاهد بالإعلام في جرائم الإعتداء على التعاملات الإلكترونية إلا بتوافر ثلاثة شروط وهـــي:

الشرط الأول: وقوع جريمة من جرائم التعاملات الإلكترونية فعلا

كي يلتزم الشاهد المعلوماتي بالإعلام في أي من الجرائم الواقعة على التعاملات الإلكترونية فلابد أن تكون هده الجريمة قد وقعت فعلا، فلا ينشأ هذا الإلتزام بشان جريمة مستقبلة، ولو دلت التحريات أنها حتما ستقع بالفعل فيما بعد، كما أنه لا يكفي مجرد وقوع جريمة من جرائم التعاملات الإلكترونية للقول بقيام هذا الإلتزام، بل لا بد أن تكون مما يعتبرها القانون جناية أو جنحة.

الشرط الثاني: أن يكون لدى الشاهد المعلوماتي معرفة وعلم بالمعلومات الجوهرية المتعلقة بالنظام المعلوماتي محل الواقعة، ويتمثل مضمون هده المعلومات الجوهرية في ثلاثة عناصر وهي:

1-طبع ملفات المعطيات المخزنة في ذاكرة الحاسوب أو حاملات المعطيات الثانوية ويعلم بها جهات التحري والتحقيق.

2-الإفصاح عن كلمات المرور السرية لسلطات التحري والتحقيق.

---

[1]-Rapport explicatif de la Convention sur la cybercriminalité;op;cit; p39

[2]-**د.هلالي عبد الله أحمد**، إلتزام الشاهد بالإعلام في الجرائم المعلوماتية، المرجع السابق، ص59 وما بعدها. **سامح أحمد بلتاجي موسى**، المرجع السابق، ص 296.

3-الكشف عن الشفرات المدونة بها الأوامر الخاصة بتنفيد البرامج المختلفة، حيث أن الأوامر أو الرسائل المكتوبة بالشفرة تحتاج إلى ترجمة لحل هذه الشفرة حتى يمكن فهمها.

الشرط الثالث: أن تستلزم مصلحة التحقيق ضرورة الحصول على هذه المعلومات الجوهرية

حرى بنا أن نشير على أنه لا يكفي كي يلتزم الشاهد المعلوماتي بالإعلام في الجرائم محل الدراسة أن يكون هناك أحد صورها قد وقع حقيقة، وأنها تعد جنحة أو جناية، وأن الشاهد لديه معرفة وعلم بالمعلومات الجوهرية اللازمة والمتعلقة بالنظام المعلوماتي محل الواقعة، بل يجب إضافة إلى ذلك أن يكون من مصلحة التحقيق الحصول على تلك المعلومات الجوهرية لحل لغز الجريمة وكشف المتورطين فيها والتوصل إليهم، ويعني ذلك أن تكون هذه المعلومات لازمة وتفيد في كشف الحقيقة الواقعية للجريمة محل التحقيق.

الفرع الثالث

الشهادة عن بـــعد

يطلق على هذا النوع من الشهادة إسم **الشهادة الإلكترونية الفورية**، وهي تطلق على نوعية من الشهادة لا يكون فيها الشاهد حاضرا جلسة التحقيق (الإبتدائي أو النهائي) بشخصه وإنما تتم عبر وسائل إلكترونية أو رقمية متطورة[1]. ويفترض حدوث هذه النوعية من الشهادة في التحقيق النهائي أمام محكمة الموضوع، حيث يكون الشاهد غير حاضرا جسديا في الجلسة ولكن يمكن الحصول على أقواله بشكل سمعي ومرئي عن طريق الدوائر الإتصالية المتكاملة من مغلقة ومفتوحة[2].

وقد كانت بداية الأخذ بنظام الشهادة الإلكترونية الفورية في القضاء الأمريكي عندما واجه القضاء مشكلة إدلاء الشهادة من قبل أشخاص وضعوا في برنامج حماية الشهود، فقد قررت المحكمة الفيدرالية العليا الأمريكية قبولها لنظام الشهادة الإلكترونية الفورية طالما كانت هناك أسباب في القانون تدعو إليه، ففي قضية إستلزمت إدلاء شخص محصن بسماع شهادته عبر دوائر تلفزيونية مغلقة شريطة أن يكون حضور الشاهد عبر الدوائر المذكورة كما لو كان حاضرا الجلسة بالفعل بحيث يكون كل ما يدور في الجلسة مرئيا له بالمقابل لرؤية من هو في الجلســـة له[3].

ويمـــيز القضـــاء الأمريكـــي بين نوعين من الشهادة الإلكترونـــية المرئية هما:

أولا: الشهادة المرئية ذات الإتجاه الواحد: وفي هذه الحالة لا يرى الشاهد حين يدلي بشهادته سوى الكاميرا المسلطة عليه، فالرؤية تكون من طرف واحد وهو طرف المحكمة[4].

---

[1]-**د. عمر بن يونس**، الجرائم الناشئة عن إستخدام الأنترنت، المرجع السابق، ص954.

[2]-الدوائر المغلقة تعني إنغلاق الدوائرالإتصالية بين جهتين فأكثر يتم تحديدها مسبقا وبحيث لا يستطيع الغير الدخول على هذه الدوائر.

[3]-**Leader, Kathryn**, Closed-Circuit Television Testimony: Liveness and Truth-telling, Law Text Culture, 14, 2010,. Available at:http://ro.uow.edu.au/ltc/vol14/iss1/18

[4]-**د. عمر بن يونس**، أشهر المبادئ المتعلقة بالأنترنت في القضاء الأمريكي، المرجع السابق، ص1012.

ثانيا: الشهادة المرئية ذات الإتجاهين: وفيها يرى الشاهد قاعدة المحكمة، وبالمقابل يراه كل من في المحكمة.

وإختيار أي من هاتين الشهادتين يخضع لتقدير المحكمة، بناء على الأسباب التي تطرحها جهة الإدعاء أو الدفاع وتأخذ المحكمة في الإعتبار مسالة صغر السن[1].

هذا وقد ساير المشرع الجزائري هذا النهج، حيث أخذ بأسلوب الشهادة الإلكترونية عبر الأنترنت قصد تطوير وعصرنة المنظومة القضائية بالجزائر وتماشيا وإرساء مفهوم "**المحاكمة عن بعد**" و"**التقاضي الإلكتروني**"[2]، فقد كان من أهم النقاط التي تناولها قانون عصرنة العدالة رقم 15-03 المؤرخ في 11 فيفري 2015 .

سنحاول من خلال النقاط التالية تحديد شروط اللجوء إلى هذه الشهادة في ظل التشريع الجزائري، ولما كانت هده الوسيلة تحقق نوعا ما الحماية للشاهد فرأينا أنه لا حرج من التطرق إلى هده المسالة خاصة وأن هذا النوع من الحماية تم تعزيزه مؤخرا بموجب الأمر رقم 15-02 في نطاق جرائم محددة، وهو ما يطرح مسالة شمول الجرائم محل الدراسة في نطاقه؟ هذا ما سنعرفه من خلال دراسة شروط الشهادة الإلكترونية(أولا) ثم حماية أمن الشاهد(ثانيا).

أولا- شروط الشهادة عن بعــد

نصت المادة 15 من القانون رقم 15-03 على أنه يمكن لقاضي التحقيق أن يستعمل المحادثة المرئية عن بعد في إستجواب أو سماع شخص وفي إجراء مواجهات بين عدة أشخاص.

يمكن لجهة الحكم أيضا أن تستعمل المحادثة المرئية عن بعد لسماع الشهود والأطراف المدنية والخبراء. .كما نصت المادة 16 على أن إستعمال آلية المحادثة المرئية عن بعد يتم بمقر المحكمة الأقرب من مكان إقامة الشخص المطلوب تلقي تصريحاته، بحضور وكيل الجمهورية المختص إقليميا وأمين الضبط. ويتحقق وكيل الجمهورية من هوية الشخص الذي يتم سماعه ويحرر محضرا عن ذلك.

---

[1]- **د. عمر بن يونس**، الجرائم الناشئة عن إستخدام الأنترنت، المرجع السابق، ص957.

[2]-التقاضي الإلكتروني أو التقاضي لدى دوائر معلوماتية عاليه التقنيةتتضمن هذه الدوائر أنظمة قضائية تعمل وفق آليات تختلف في الشكل والمضمون عن أصول التقاضي المعمول بها لدى غالبية الدول، وقد عرفه القاضي حازم الشرعة على أنه سلطه لمجموعة من القضاة بنظر الدعاوى بوسائل إلكترونية مستحدثة ضمن أنظمة قضائية تعتمد أسلوب البرنامج الحاسوبي عوضا عن الأسلوب الورقي في استقبال اللوائح والطلبات القضائية ونظر الدعوى ضمن برامج حاسوبية تعتمد أسلوب التحديد المسبق لوقائع الجلسات، ويتيح هذا النظام للقضاة وأطراف الدعوى تقديم البينات الخطية والشخصية دون داع للحضور إلى المحكمة، ومن خلال مواقع إلكترونية ضمن الشبكة الخاصة بموقع المحكمة، https://ar.wikipedia.org/wiki/%D8%A7%D9%84%D8%AA%D9%82%D8%A7%D8%B6%D9%8A_%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A_(%D9%83%D8%AA%D8%A7%D8(%A8

وتطبق كندا مند أكثر من عشر سنوات هذا النوع من التقاضي، وهو ما صرح به القاضي خالد خالص حين زيارته لمكتب أكبر المحامين، وهو مكتب لابلان وشركاؤه، حيث إكتشف بهذا المكتب الضخم آلة مرتبطة بقصر العدالة تسمح للمحامي بالقيام بجل الإجراءات إنطلاقا من المكتب عبر شبكة الإكسترانت ولاسيما تتبع الملفات.**خالد خالص**، المحاكم الإلكترونية، مقــال متــاح على المــوقع التالي:
http://www.ahewar.org/debat/show.art.asp?aid=29607

ومما لاشك فيه أن تطبيق هذا الإجراء، سيؤدي إلى تسهيل إجراءات المحاكمة وإختصار الوقت والجهد، وحماية أمن الشاهد، متى توفرت شروط معينة:

1-**أن يتعذر حضور الشاهد ماديا أمام المحكمة:** وهو ما أشار إليه المشرع الجزائري في المادة 14 بنصه "إذا إستدعى بعد المسافة أو تطلب ذلك حسن سير العدالة ...".

2-أن يتم سماع الشهادة الإلكترونية بحضور خبير أو أكثر لضمان إنغلاق الدورات الإتصالية مع الشهود.

3-أن يتم تبليغ الشاهد بأي وسيلة كانت قبل موعد الجلسة بمدة معقولة تقدرها المحكمة.

4- الحصول على إذن الشاهد.

4-أن تضمن الوسيلة المستعملة سرية الإرسال وأمانته، وهو ما أشارت إليه الفقرة الثانية من المادة 14 من القانون 15-03.

ويرى البعض من الفقه[1] أن تأخذ التشريعات بأسلوب الشهادة الإلكترونية لإثبات الجرائم الواقعة في العالم الإفتراضي فحسب، إلا أننا نرى أن تعميم هذا الأسلوب في جميع الجرائم ضمن الشروط المذكورة، كونه يندرج ضمن مفهوم عام وهو "**المحاكمة الإلكترونية**".

ثانيا-حماية أمن الشاهد

نميز في هذا الإطار بين **نوعين** من الحماية: الحماية الجنائية لأمن الشاهد والحماية الأمنية، ففيما يخص الأولى فتعني تجريم وعقاب كل من يتعدى على الشهود بالإكراه والتهديد والحمل على عدم الشهادة أو الشهادة زورا، أما النوع الثاني من الحماية فتعني الإجراءات والتدابير المتخذة بشأن منع الإعتداء على شخص الشاهد أو أسرته بسبب أدائه الشهادة، وذلك خلال مراحل تداول إجراءات الدعوى الجنائية وبعد الإنتهاء منها،والحيلولة دون إستمرار هذا الإعتداء إذا ما وقع على الشاهد أو على أفراد أسرته أو أقاربه[2].

ويتميز التشريع الأمريكي بأنهأول التشريعات التي تضمنت نصوصا قانونية لحماية أمن الشاهد، فقد أراد الكونغرس الأمريكي من خلال الفصل الخامس من قانون الرقابة على الجريمة المنظمة الصادر 1970 و المعدل بقانون 1984 أن يزيد من مقدرة أجهزة العدالة الجنائية في الحصول على الأدلة ضد المشتبه بهم أو المتورطين في إرتكاب الجرائم المنظمة فأعطى المدعي العام الأمريكي سلطة ضم الشهود لبرنامج حماية أمن الشاهد التابع لوزارة العدل بهدف تأمينهم والحفاظ على سلامتهم، في حال وجود إحتمال تعرضهم للمخاطر نتيجة أدائهم للشهادة، ووفقا لما أوجبته المادة 501 من القانون المذكور[3].

---

[1]- **د. محمد طارق عبد الرؤوف الخن**، المرجع السابق، ص310.

[2]- **د. أحمد يوسف السولية**، الحماية الجنائية والأمنية للشاهد، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2007، ص267.

[3]- Bonnes pratiques de protection des témoins dans les procédures pénales afférentes à la criminalité organisée, Office des Nations Unies contre la drogue et le crime Vienne, 2008, p8disponible en ligne á l'adresse suivante: https://www.unodc.org/documents/organized-crime/09-80620_F_ebook.pdf

كما أدخل المشرع الفرنسي نصوصا خاصة تحمي الشاهد بمقتضى قانون الأمن اليومي 2001-1062 المعدل لقانون الإجراءات الجزائية[1] وذلك من المواد 706-57 إلى 706-63 إجراءات جزائية[2]، وكذلك فعل المشرع الألماني والإيطالي والأسترالي والصيني.[3]

وقد سلك المشرع الجزائري نفس المسلك، فتماشيا على ما نصت عليه الإتفاقيات الدولية التي صادقت عليها الجزائر سيما إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، ونظرا للدور المحوري للشهود في مكافحة الجريمة من خلال ما يدلون به من معلومات تساعد في الكشف عن المجرمين وتقديمهم للعدالة، أصدر المشرع الأمر رقم 15-02 المعدل و المتمم للأمر 66-155 المتضمن قانون الإجراءات الجزائية، حيث أضاف بموجبه الفصل السادس من الباب الثاني من الكتاب الأول تحت عنوان"**في حماية الشهود والخبراء و الضحايا**"، حيث نصت المادة 65 مكرر 19 منه "يمكن إفادة الشهود والخبراء من تدبير أو اكثر من تدابير الحماية غير الإجرائية المنصوص عليها في هدا الفصل إدا كانت حياتهم أو سلامتهم الجسدية او حياة او سلامة أفراد عائلاتهم أو أقاربهم أو مصالحهم الأساسية معرضة لتهديد خطير بسبب المعلومات التي يمكنهم تقديمها للقضاء والتي تكون ضرورية لإظهار الحقيقة....".

وبالرجوع للمادة 65 مكرر19 ومايليها نجد أن حماية أمن الشاهد تتم بشتى الوسائل والطرق، إلا أنه قيد نطاقها بجرائم معينة.

أ- وسائل الحماية:

إن المتأمل للمادة 65 مكرر 19 من قانون الإجراءات الجزائية، يجدها تنص على وسائل وطرق عديدة تكفل الحماية للشاهد:

1- تدابير الحماية غير الإجرائية: وهي حسب ما نصت عليه المادة 65 مكرر 20 عدم إفشاء هوية الشاهد وتغيير مكان إقامته ومنحه مساعدة إجتماعية أو مالية، ووضع رقم هاتفي خاص تحت تصرفه، مع تمكينه من نقطة إتصال لدى مصالح الأمن، ووضع أجهزة تقنية وقائية بمسكنه مع تسجيل المكالمات الهاتفية التي يتلقاها أو يجريها بشرط موافقته الصريحة.

فضلا عن ضمان حماية جسدية مقربة له مع إمكانية توسيعها لأفراد عائلته وأقاربه. ووضعه إن تعلق الأمر بسجين في جناح يتوفر على حماية خاصة.

ويمكن أن تتخد التدابير للحماية قبل مباشرة المتابعات الجزائية، وفي أي مرحلة من الإجراءات القضائية، ويتم ذلك إما تلقائيا من قبل السلطة القضائية المختصة أو بطلب من ضابط الشرطة القضائية أو بطلب من الشخص المعني.

---

[1]-**Loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne**

[2] -لمزيدمن التفاصيل حول حماية الشاهد في القانــون الفرنــسي أنظــر:

Stéphane babonneau La protection des témoins en France disponible en ligne á l'adresse suivante; http://www.sba-avocats.com/avocat-droit-penal-la-protection-des-temoins.html

[3]- Bonnes pratiques de protection des témoins dans les procédures pénales afférentes à la criminalité organisée,

2-تدابير الحماية الإجرائية: وهي حسب المادة 65 مكرر23 تتمثل في عدم الإشارة لهويته أو ذكر هوية مستعارة في أوراق الإجراءات، فضلا عن الإشارة إلى مقر الشرطة القضائية أين تم سماعه أو إلى الجهة القضائية التي سيؤول إليها النظر في القضية بدلا من الإشارة إلى عنوانه الحقيقي. مع الإحتفاظ بالهوية و العنوان الحقيقيان للشاهد في ملف خاص يمسكه وكيل الجمهورية.

3-إعتماد الوسائل الحديثة للإدلاء بالشهادة:وهوما قررته المادة 65 مكرر 27 على أنه يجوز لجهة الحكم تلقائيا أو بطلب من الأطراف سماع الشاهد مخفي الهوية عن طريق وضع وسائل تقنية تسمح بكتمان هويته، بمافي ذلك السماع عن طريق المحادثة المرئية عن بعد واستعمال الأساليب التي لا تسمح بمعرفة صورة الشخص وصوته.

4- إتخاد الإجراءات العقابية: لحماية الشهود، يجب التوجه بعقاب كل من يحاول كشف هويتهم أو عنوانهم، وهذا ما أكده المشرع الجزائري بموجب المادة 65 مكرر28 من الأمر رقم 15-02 كمايلي" يعاقب على الكشف عن هوية أو عنوان الشاهد أو الخبير المحمي، طبقا لهذا القسم، بالحبس من ستة اشهر إلى 5 سنوات و بغرامة من 50000 دج إلى 500000 دج

ب-مجال تطبيق الحماية:

حدد المشرع في المادة 65 مكرر19 الجرائم التي يحمى في إطارها الشاهد ومن بينها الجريمة المنظمة". ومن المعروف أن هذا النوع من الجرائم يرتبط بكافة أنواع الممارسات اللاخلاقية، وتعد جرائم التعاملات الإلكترونية من أكثر الجرائم جاذبية للجريمة المنظمة، وتشير الإحصائيات إلى أن أكثر من ثلاثة أرباع أفعال الإعتداء على التعاملات الإلكترونية اليوم ترتبط بالنشاط الإجرامي المنظم خاصة الجرائم المتصلة بالهوية فهي الأكثر شيوعاً وأسرع أشكال الاحتيال على المتعاملين الإلكترونيين على شبكة الإنترنت، سيما من خلال إساءة استخدام معلومات بطاقة الائتمان[1] ، ولاندل على ذلك أكثر من كونها من أوائل القضايا التي عرضت على القضاء الجزائري في قضية البنك الكندي.

المطلب لثاني

القرائن في مجال إثبات الجرائم الواقعة على التعاملات الإلكترونية

قبل أن نلقي الضوء على دور القرائن في إثبات الجرائم الواقعة على التعاملات الإلكترونية، لا بد لنا من التعرض للأحكام العامة للقرائن.

[1]-Norton Cybercrime Report (2012); Transnational Organised Crime Threat Assessment (2010); UNODC Cybercrime Report

مؤتمر الأمم المتحدة الثالث عشر لمنع الجريمة والعدالة الجنائية، الدوحة 16-19 نيسان-أبريل 2015، متـــاح على المـــوقع التـــالي:
http://www.un.org/ar/events/crimecongress2015/cybercrime.shtml

الفرع الأول

التعريف بالقرائن بصفة عامة

تمثل القرائن وسائل إثبات غير مباشرة كونها لا ترد على الوقائع المطلوب إثباتها، على عكس الأدلة المباشرة **كالشهادة** مثلا فهي ترد على هذه الوقائع.

هذا ولم تتطرق أغلب التشريعاتلتعريف القرينة –كما هو حال المشرع الجزائري– بل تركتها للفقه، في حين عرفها المشرع الفرنسي بموجب المادة 1349 من القانون المدني الفرنسي على أنها "النتائج التي يستخلصها القانون أو القاضي من واقعة معروفة لمعرفة واقعة غير معروفة[1]"، وهذا التعريف صحيح في الإجراءات الجزائية[2]. أما على النطاق الفقهي فقد تعددت التعريفات التي سيقت بشأنها، إلا أنها تدور حول مفهوم واحد وهو أن القرينة هي إستنتاج الواقعة المطلوب إثباتها من واقعة أخرى قام عليها دليل إثبات[3].

فالقرينة إذا هي إستنتاج مجهول من معلوم، ويرتكن هذا الإستنتاج إما إلى إفتراض قانوني أو إلى ترابط منطقي بين الواقعتين، ففي الأولى تعد قرينة قانونية أما في الثانية فتكون قرينة قضائية.

والقرائن لها أهمية خاصة في الإثبات، إذ أن بعض الوقائع يستحيل أن يرد عليها إثبات مباشر، فإذا إقتصر الإثبات على الأدلة المباشرة لما كان من الممكن الفصل في الدعاوى، فالقرائن تمكن من إثبات بعض الوقائع عن طريق وقائع أخرى ذات صلة سببية ومنطقية بها. ومثال القرائن في الدعوى الجزائية أن يتهم شخص بسرقة منزل، ولا يكون على هذه الجريمة شهود، وهو غير معترف بها، ولكن ترفع من باب المنزل بصمات تعود له، وتضبط المسروقات في حيازته، فتكون البصمات وضبط المسروقات لديه قرينتين على أنه هو الذي قام بالسرقة[4].

والقرائن تنقسم إلى نوعين قرائن قانونية وقرائن قضائية.

أولا: القرائن القانونية: كقاعدة عامة هي التي نص عليها القانون، أي قام المشرع بعملية استنباط بصددها من واقع ما يغلب وقوعه في طائفة معينة من الحالات، وتتميز بتحديد القانون لها على سبيل الحصر فلا يجوز للقاضي إختراعها من جانبه، وهي تسهل على القضاء والخصوم من حيث سبق إفتراض الأوضاع الدارجة و المعتادة، والإعفاء من عبء إثباتها[5].

---

[1]-L'article 1349 du CCF énonce : "les présomptions sont des conséquences que la loi ou le magistrat tire d'un fait connu à un fait inconnu". Il s'agit d'un raisonnement déductif permettant d'établir une preuve indirecte à partir d'une preuve directe des faits.

[2]–**Jacques Marie Boileux,** Commentaire sur le code civil, imprimeurs de luniversite royale de france, paris,1843,P709.

[3] -**د. محمود نجيب حسني**، شرح قانون الإجراءات الجنائية، المرجع السابق، ص487.

[4] – **د.محمود نجيب حسني**، شرح قانون الإجراءات الجزائية، المرجع السابق، ص ص487،488.

[5]- المرجع نفسه، ص501.

Jacques Marie Boileux, op, cit, p709.

والقرائن القانونية تنقسم بدورها إلى نوعين:

أ-القرائن القانونية القاطعة: وهـــــي التي لا يقبل إثبات عكسها، مقدرا بدلك المشرع أن إحتمال عدم مطابقتها للواقع هو إحتمال ضعيف لا يعبأ به لأجل تحقيق الغاية التي أرادها ولو أدى ذلك إلى حرمان المتقاضي من حق إثبات العكس، ومثال القرينة القاطعة الأحكام التي حازت حجية الأمر المقضي به تكون حجة فيما فصلت فيه من الخصومة، ولا يجوز قبول دليل ينقض هذه القرينة، كون هدا الحكم هو عنوان الحقيقة، وله قوة القضية المقضية[1].

ب-القرائن القانونية البسيطة: فهـــــي غير قاطعة وتقبل إثبات العكس، ومثالها قرينة أن المتهم بريء حتى تثبت إدانته بحكم قضائي مبرم، فيجب أن يعامل على هذا الأساس في جميع مراحل الدعوى.[2]

ثانيا: القرائن القضائية: وتسمى بالقرائن الفعلية أو الموضوعية، وهي التي يستخلصها القاضي بحكم اللزوم العقلي والمنطقي من الوقائع الثابتة في الدعوى، وهذه القرائن لا تدخل تحت حصر بل يترك أمر إستنتاجها للقاضي، ومثالها: وجود بصمات المتهم أو سلاحه في مكان الجريمة، وجود بقعة من زمرة دم المجني عليه على ملابس المتهم تعتبرقرينة على مساهمته في إقتراف الجريمة...إلخ.

وعن حجية القرينة القضائية، إختلف فقهاء القانون في ذلك ويمكننا أن نميز في ذلك بين إتجاهين:

الإتجاه الأول: ويمثله قلة من الفقهاء، حيث يرون أنه لا يجوز الإعتماد على القرائن القضائية وحدها في الإثبات الجزائي وخاصة في الحكم بالإدانة، وأن دور القرائن القضائية يقتصر على تعزيز الأدلة الأخرى المتوافرة في القضية وذلك ما يجعل دورها محدودا وثانويا، ذلك أن القاضي يمكن أن تكون إستنتاجاته خاطئة إعتمادا على الدلائل، كما أن هذه الدلائل وإن كانت تعبر عن أحداث صامتة ولا تعرف الكذب فإنها قد تكون عرضة للتلفيق بقصد التضليل والمغالطة[3].

الإتجاه الثاني[4]: ويمثله غالبية فقهاء القانون، حيث يرون أن القرائن من أهم طرق الإثبات في المواد الجنائية التي يعتمد عليها، سواء لوحدها أو لتعزيز أو مساندة العناصر الأخرى للإثبات وهذا ما يجعلها تمتاز عن غيرها من وسائل الإثبات بالدور الواسع الذي تقوم به، ويبررون إتجاهم هذا كون أن الإثبات الجزائي يتعلق بوقائع مادية عادة ما تتم في الخفاء، وقد تكون القرائن القضائية الدليل الوحيد في الدعوى.

أما عن موقف التشريعات المقارنة، فتتجه غالبيتها إلى إعتبار القرائن القضائية شأنها شأن بقية أدلة الإثبات الأخرى لاتقل أهمية عنها، متروكة لحرية القاضي طبقا لمبدأ حرية القاضي في الإثبات عن طريق إقتناعه الشخصي، فتنص المادة 212 إجراءات جزائري "يجوز إثبات الجرائم بأي طريق من طرق الإثبات ماعدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لإقتناعه الخاص"، ولا

---

[1]- **Franklin Kuty;** Principes généraux du droit pénal belge: Tome II – l'infraction pénale; edition larcier , bruxelles . 2010 , p 462

[2]– **د. حسن الجوخدار**،المرجع السابق ، ص190.

[3]– د. **مأمون سلامة**، الإجراءات الجنائية في التشريع المصري، دار الفكر العربي، القاهرة، 1977، ص160.

[4]–أنظر في هذا الرأي: **محمد طيب عمور**، الإثبات الجزائي بالقرائن القضائية بين الشريعة والقانون، الأكاديمية للدراسات الإجتماعية والإنسانية، العدد9، 2013، ص83.

يختلف التشريع المصري في ذلك عن التشريع الجزائري، وقد أكدت المحكمة العليا على ذلك في قرار لها حيث قضت بأنه" ***يكفي لقناعتها وتكوين عقيدتها وهي غير ملزمة بأن تسترشد في قضائها بقرائن معينة بأن لها مطلق الحرية في تكوين عقيدتها وقناعتها بأية بينة أو قرينة يرتاح إليها ضميرها ويؤدي إلى النتيجة التي إتجهت إليها بمنطق سائغ وسليم كما هو الشأن في واقعة الحال، الأمر الذي يجعل النفي على الحكم من هذه الناحية مجرد محاولة موضوعية في تقدير الدليل"***[1].

الفرع الثاني

دور القرائن في إثبات جرائم الإعتداء على التعاملات الإلكترونية

تحتل القرائن في العصر الرقمي مرتبة خاصة بين سائر وسائل الإثبات الجزائي، ذلك أن الإثبات في الجرائم الواقعة على التعاملات الإلكترونية يتعلق بوقائع حدثت في مسرح افتراضي يتعذر توافر دليل مباشر عليها من شهادة وإعتراف، خاصة مع قيام مرتكبو الجرائم بطمس معالم الجريمة، أو إستخدام أسماء مستعارة تضليلا للعدالة، فلا يجد القاضي إلا بصمات وآثار إلكترونية عقد عليها مفاتيح الغموض فيحاول –عن طريق الخبير– إستنطاقها والإستدلال بها على ما قد يكون لازما أو مرتبطا بها[2]، فإن نجح فإنها تصبح بذلك قرينة على أمر، وقد تكون هده القرينة الدليل الوحيد الذي يمكن التعويل عليه في الوصول إلى إظهار الحقيقة.

ويمكن القول أن المكونات الرقمية (0–1) أو الأدلة المأخودة من النظم المعلوماتيةلهي أقرب إلى القرائن منها إلى أنواع الأدلة الأخرى، والتي يعود تقدير قيمتها إلى قاضي الموضوع.

فمعرفة عنوان الأنترنت الرقمي مثلا ip address يشير إلى الحاسوب الذي إرتكبت بواسطته الجريمة فقط، ولا يؤدي إلى معرفة الفاعل الحقيقي بدقة، وذلك بخلاف الدليل العلمي الناتج عن تحليل الحمض النووي dna أو بصمة الأصبع وغيرها من الأدلة التي تشير إلى الفاعل الحقيقي بدقة متناهية في العالم المادي.

على أنه وبالنظر إلى أن بروتوكول التعريف لا يعد حاسما في الدلالة على مستخدم الجهاز، فإن نظام التفتيش الذي يتم لإستظهار الدليل الإلكتروني لا يمكن أن يكون جازما هو الآخر في شأن مرتكب الفعل، لذلك فإن تساند الأدلة والقرائن يعد من أهم ما يساعد القاضي في بناء قناعته، ومن ذلك أن يبحث القاضي عن آثار رقمية أخرى وأدلة مساندة على إرتكاب الجاني للجرم[3].

ومن أمثلة الأدلة الإلكترونية التي يمكن أن يستنتج منها القاضي دلالة معينة، قيام المخترق للمواقع الإلكترونية حال كونه مبرمجا إذا كانت البرمجية المعدة للعمل عبر الأنترنت تتضمن ذات الأخطاء التي كان

---

[1]- ملف رقم 83421 قرار بتاريخ 9–2– 1991 ، غير منشور ، مشار إليه لدى : د .**العربي شحط عبد القادر**، الإثبات في المواد الجزائية، دار الهدى، الجزائر، 2006، ص197.

[2]–**محمد طيب عمور**،المرجع السابق، ص79.

[3]- **أيمن رمضان محمد أحمد**، المرجع السابق، ص332.

المبرمج ولايزال يقع فيها عند إعداد أية برمجية، أو أن يكون المبرمج له أسلوب خاص جدا في بناء البرمجيات التي تم إستخدامها في إرتكاب جريمة الإحتيال بواسطة البطاقات الإئتمانية فيتم القبض عليه انطلاقا من أن أسلوبه معروفا للجهات الضبطية هنا وتقديمه للمحاكمة على هذا الأساس[1].

كما أن تفتيش البريد الإلكتروني أو السجلات الإلكترونية الموجودة في جهاز الضحية أو المشتبه فيه قد يؤدي إلى إستخلاص بعض القرائن، ومثال ذلك أنه في قضية القرصنة على البنك الكندي، فإن عملية تفتيش أجهزة الإعلام الآلي التي إستخدمت في ذلك، وضبط ما يدل على أن هناك ارتكابا لهده القرصنة، كان إشارة إلى أن حائزها أو مالكها هو مرتكب الجريمة، إذ تم الإستدلال على إرتكاب الحائز للجريمة من خلال وجود آثار رقمية له تفيد إستعمال البريد الإلكتروني والإسم المستعار، وصفحات واب مستعملة في عملية النصب الإلكتروني ورسائل إلكترونية لتحويل مبالغ مالية من رصيد المشتبه فيه، إلا أن المحكمة لم تستند على هذه القرينة لبناء منطق الإدانة، بل إستندت كذلك على إعتراف المتهم كونه هو صاحب الإسم المستعار wallacez

أو قد يتم التعرف على النظام الذي تم إرتكاب الجريمة منه من خلال عنوان الربط IP Adresse ، ويتم ضبط الجاني وبحوزته أدوات تستعمل في فك شفرات التوقيع الإلكتروني أو تزويره.

نخلص مما سبق، إلى أن للقرنية أهمية كبرى في إثبات الجرائم الواقعة على التعاملات الإلكترونية، بل ستكون الغلبة لها، وهو ما سيزيد من أهمية دور القاضي في هذا الإثبات، بحيث يظل القاضي متمتعا بسلطة تقديرية في تقدير هذه الأدلة بحسبان أنها قد لا تكون مؤكدة على سبيل القطع، أو قد يحوطها الشك، فهنا تظهر أهمية هذه السلطة التي من خلالها يستطيع إظهار مواطن الضعف في هذه القرائن، ويستطيع كذلك تفسير الشك لصالح المتهم[2].

المطلب الثالث

الخبرة التقنية في مجال جرائم الإعتداء على التعاملات الإلكترونية

تعتبر الخبرة تجسيد لمبدأ العلم في خدمة العدالة، والإستعانة بها أمر جوازي إلا إذا تعلقت الدعوى بمسألة فنية وعلمية لا يكفي في معرفتها الإختصاص العام، فعندها يصبح اللجوء إليها إجباري كما هو حال الجرائم محل الدراسة. فالجرائم التي تقع على التعاملات الإلكترونية تتنوع بتنوع الوسائل الإلكترونية المستخدمة في إرتكابها، فهي بذلك تتميز بطبيعة فنية متأثرة في ذلك بالطبيعة الفنية لهذه التعاملات ووسائلها، فيصبح بذلك اللجوء إلى الخبرة إجراء ضروري ومهم للحصول على الأدلة بالنسبة لهذا النوع من الجرائم، بل قد يظهر الحاجة إلى اللجوء إليها مند بدء مرحلة التحري نظرا للطبيعة المعنوية لمحل الإعتداء وللطابع المتميز لوسائل إرتكابها.

---

[1]–**د. عمر محمد ابوبكر بن يونس**، الجرائم الناشئة عن إستخدام الأنترنت، المرجع السابق، ص941.

[2]–**د. علي محمود علي حمودة** ، المرجع السابق، ص68.

سنحاول من خلال هدا المطلب إلقاء الضوء على الخبرة التقنية، بعد أن نتطرق إلى التعريف بالخبرة القضائية بصفة عامة.

الفرع الأول

التعريف بالخبرة القضائية بصفة عامة

الخبرة القضائية عموما هي وسيلة قررها المشرع لمساعدة القاضي في تقدير المسائل التي يحتاج إثباتها إلى معرفة خاصة علمية كانت أو فنية[1]. فهي إجراء يتعلق بموضوع يتطلب الإلمام بمعلومات فنية لإمكان إستخلاص الدليل منه، ولذلك فإن الخبرة تفترض وجود واقعة مادية أو شيء يصدر الخبير حكمه بناء على ما تم إستظهاره منه، ومن ثم فإن الخبرة تقوم على حكم الخبير أكثر مما تقوم على جمع الأدلة من قبل المحقق وبحثها[2].

والخبير القضائي هو كل شخص له دراية علمية وفنية متخصصة في مجال ما أو فرع من هذا المجال، تستعين به إحدى جهات التحقيق أو الحكم أو غيرها في مسألة ما، لتقديم الأدلة أو الدلائل أو للكشف عنها أو تفسيرها، وتقييمها، بغية إثبات الوقائع وتحديد مرتكبيها ومدى مسؤوليتهم عنها[3].

وتقدم الخبرة عونا ثمينا لجهة التحقيق وللقضاء ولسائر السلطات المختصة بالدعوى الجزائية في أداء رسالتها، فبدونها يتعذر الوصول إلى الرأي السديد بشأن المسائل الفنية التي يكون على ضوئها كشف جوانب الحقيقة المبنية على الأصول والحقائق العلمية[4]. لذا فقد إهتم المشرع بتنظيم أعمال الخبرة، حيث فصل المشرع الجزائري قواعدها في قانون الإجراءات الجزائية من المادة 143 إلى المادة 156 ، وكذلك فعل المشرع الفرنسي من المادة 156 إلى المادة 169-1 من قانون الإجراءات الجزائية.

والخبرة بهذا المعنى تتميز عن الشهادة في أمور عديدة رغم التشابه بين الخبير والشاهد في كون كل منهما يقرر أمام القضاء الأمور التي شاهدها والتفاصيل التي لاحظها والظروف التي تأثر بها[5]:

-إن الشهادة دليل مباشر بينما قرار الخبير إيضاح أو تقدير للدليل، فالخبير بهده المثابة أقرب إلى الحكم منه إلى الشاهد.

---

[1]-**د. آمال عبد الرحيم عثمان**، الخبرة في المسائل الجنائية، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 1964، ص13.

[2]-**د. مأمون سلامة**، قانون الإجراءات الجنائية معلقا عليه بالفقه وأحكام النقض، الجزء الأول، الطبعة الثانية، مكتبة رجال القضاء، القاهرة، 2005، ص369.

[3]-**عبد الناصر محمد محمود فرغلي**، المرجع السابق، ص141.

[4]-**د. حسين بن سعيد الغافري**، السياسة الجنائية في مواجهة جرائم الأنترنت، المرجع السابق، ص562.

[5]- **عبد الناصر محمد محمود فرغلي**، المرجع السابق، ص148. **د عبد الوهاب حومد**، المرجع السابق، ص656. **د محمود نجيب حسني**، شرح قانون الإجراءات الجنائية، المرجع السابق، ص475.

-إن الشاهد يقرر ما يعلمه عن وقائع رآها أو سمعها بنفسه، بينما الخبير يبدي رأيه فيما يعرض عليه من ظروف لا يعرفها شخصيا، بل يقدم للقاضي آراء وتقييمات وأحكاما توصل إليها بتطبيق قوانين علمية أو أصول فنية، تمكن عن طريقها إشتقاق النتيجة التي إنتهى اليها.

-الشاهد يقدم شهادته بصفته الشخصية فلا يمكن الإستعاضة عنه بغيره، بينما الخبير يقدم رأيه بصفته الوظيفية أو المهنية أو العلمية، في مجال تخصصه، والخبراء يتعددون ويمكن للقاضي أن يختار من يشاء منهم ويمكن أن يستبدل الخبير بغيره من الخبراء.

-الشاهد تحده مصادفة معاينته إرتكاب الواقعة الإجرامية، أما الخبير فتعينه دراساته ومؤهلاته وخبراته السابقة، وقد يجمع الشخص بين صفتي الشاهد والخبير كطبيب شهد إرتكاب قتل وحاول إسعاف المجني عليه قبل وفاته فأتيح له معرفة أسباب وفاته.

وإذا كان للخبرة مالها من أهمية في الجرائم التقليدية، فهي تكشف عن الدليل العلمي الذي يعجز عن كشفه غير الخبير المتخصص، أو توضح الدليل، أو تفسره أو تقيمه، وفقا للأسس والقواعد والنظريات العلمية، وبإستخدام الوسائل والأجهزة والتقنيات العلمية الحديثة[1]، فإن أهميتها تزداد وتصبح ضرورية بل وحتمية في إثبات الجرائم التي تقع على التعاملات الإلكترونية حيث تتعلق بمسائل فنية أية في التعقيد لدرجة يصعب على المتخصصين تتبعها وإستيعابها، ومحل الجريمة فيها غير مادي، والتطور في أساليب إرتكابها سريع ومتلاحق، ولا يكشف غموضها إلا متخصص وعلى درجة كبيرة من التميز في مجال تخصصه، فإجرام الذكاء والفن لا يكشفه إلا ذكاء وفن مماثلين[2].

والواقع أن الخبرة التقنية بدأت تتخذ لنفسها حيزا في مجال إثبات جرائم العالم الإلكتروني بصفة عامة، حتى أصبح يعرف في الفقه المقارن بمصطلح digital forensic أو computer forensic أي المعلوماتية الشرعية[3]

ويمكن تعريف المعلوماتية الشرعية بأنها" إستخدام الطرق العملية لجمع وتعريف وتحليل وتفسير الدليل الإلكتروني المأخوذ من مصادر رقمية، والإحتفاظ به وتوثيقه، على نحو يسهل بناء الحوادث التي تؤدي إلى إكتشاف الجريمة"، أو هو جمع وحفظ وتحليل وتقديم الدليل المتعلق بالحاسوب"[4].

---

[1]- **عبد الناصر محمد محمود فرغلي**، المرجع السابق، ص142.

[2]- **د. محمد أبو العلا عقيدة**، التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، بحث مقدم للمؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية الشرطة، مركز البحوث والدراسات ، دبي خلال الفترة 28/26 أبريل 2003،ص6

[3]-**Simson L. Garfinkel** , Digital Forensics, available at http://www.americanscientist.org/authors/detail/simson-l-garfinkel

[4]- **john r vacca**,Computer Forensics: Computer Crime Scene Investigation (Networking Series) (Charles River Media Networking/Security), 2002, chapter 1, p4.

مشار إليه لدى: **د. محمد طارق عبد الرؤوف الخن**، المرجع السابق، ص331.

الفرع الثاني

مدى الإستعانة بالخبرة التقنية في المراحل المختلفة للدعوى

الأصل أن ندب الخبراء عمل من أعمال **التحقيق الإبتدائي**، وهو ما إستقرت عليه مختلف النظم الإجرائية، كما هو حال النظام الجزائري، وهو ما يستفاد صراحة من نص المادة 143 من قانون الإجراءات الجزائية "لجهات التحقيق أو الحكم عندما تعرض لها مسالة ذلت طابع فني أن تأمر بندب خبير إما بناء على طلب النيابة العامة وإما من تلقاء نفسها أو من الخصوم..."، إلا أن بعض النظم الإجرائية إتجهت إتجاها مغايرا كما هو الحال في مصر، حيث أجازت لمأمور الضبط القضائي في مرحلة جمع الإستدلالات الإستعانة بالخبراء في هذه المرحلة، وهو ما تضمنته المادة 29 إجراءات "لمأموري الضبط القضائي أثناء جمع الاستدلالات أن يسمعوا أقوال من يكون لديه معلومات عن الوقائع الجنائية ومرتكبها وأن يسألوا المتهم عن ذلك ، ولهم أن يستعينوا بالأطباء وغيرهم من أهل الخبرة ويطلبوا رأيهم شفهيا أو بالكتابةولا يجوز لهم تحليف الشهود أو الخبراء اليمين إلا إذا خيف ألا يستطاع فيما بعد سماع الشهادة بيمين".

إلا أن المشرع الجزائري وإن كان قد منح حق الإستعانة بخبير أو أكثر **لجهات التحقيق** أو **الحكم** في مرحلة التحقيق الإبتدائي والمحاكمة، وذلك في المسائل ذات الطابع الفنيإما بناء على طلب النيابة العامة وإما من تلقاء نفسها أو من الخصوم، إستحدث تعزيزا لقدرات النيابة العامةفي معالجة القضايا ذات الطابع التقني كالجرائم الواقعة علىالتعاملات الإلكترونية وظيفة **المساعدين المتخصصين الدائمين** بموجب المادة 35مكرر من الأمر رقم 15-02 المعدل والمتمم لقانون الإجراءات الجزائية، وهم مساعدون يكونون بشكل دائم تحت تصرف النيابة العامة التي تستعين برأيهم وخبرتهم خلال **التحريات الأولية** ومختلف مراحل الدعوى وهو ما من شأنه أن يزيد من نجاعة النيابة العامة، ولعل أن التساؤل الذي يثار هنا: هو ***مالقيمة القانونية للأعمال التي يتم إجراءها في هذه المرحلة، هل تعد خبرة بالمعنى الإجرائي للخبرة القضائية؟ .***

الفرع الثالث

القواعد التي تحكم الخبرة التقنية

قبل التطرق إلى القواعد الفنية الخاصة بأعمال الخبرة القضائية في مجال الإثبات العلمي للجرائم الواقعة على التعاملات الإلكترونية، سنتناول القواعد القانونية العامة المنظمة لأعمال الخبرة القضائية لما لها من أهمية في رسم الخطوط العريضة التي يسير عليها الخبير.

أولا- القواعد القانونية التي تحكم الخبرة التقنية

سنتناول فيما يلي القواعد القانونية التي تحكم عمل الخبير في شتى مجالات الخبرة والتي تنطبق على أعمال الخبرة التقنية في مجال أبحاث الإعتداءات على التعاملات الإلكترونية.

أ- إختيار الخبير التقني:

لكل جهة قضائية تتولى التحقيق أو تجلس للحكم عندما تعرض لها مسألة ذات طابع تقني أن تأمر بندب خبير من تلقاء نفسها أو بناء على طلب النيابة العامة أو الخصوم، ولكن لا يجوز لهؤلاء الآخرين أن يعينوا أو يختاروا الخبير، وهذا ما نصت عليه المادة 143 إجراءات جزائري، على أن يتم اختيار الخبراء من الجدول الذي تعده المجالس القضائية بعد إستطلاع رأي النيابة العامة[1] دون التزام بترتيب معين تبعا لثقة المحقق أو القاضي.

وحتى يتم تقييده في جدول الخبراء القضائيين ينبغي للمترشح أن يستوفي جملة من الشروط حددها المرسوم التنفيدي رقم 95-310[2] في مادته 4، ومن بينها أن تكون **له شهادة جامعية أو تأهيل مهني**، معين في الإختصاص الذي يطلب التسجيل فيه، وبالرجوع للمادة 4 فقرة 7 نجدها تشترط أن يكون قد مارس هذه المهنة أو هذا النشاط في ظروف سمحت له أن يتحصل على تأهيل كاف لمدة لا تقل عن سبع سنوات، ومعنى ذلك يجب أن يكون متمرسا، وهذا مالا يتماشى ومنطق التعامل مع تكنولوجيا المعلومات التي لا ترتبط بمنهج دراسي أو بحثي معين أو مدة زمنية يقضيها المرء دارسا في الجامعات والمعاهد المتخصصة، وإنما ترتبط بمهارات خاصة، ذلك أن أمهر مبرمجي نظم التشغيل لم يتجاوز تحصيله العلمي المرحلة الثانوية، وذات الأمر ينطبق على عتاة الهكرة ومخترقي الأنظمة فإن أعمارهم لا تتجاوز مرحلة التعليم الثانوي والسنوات الجامعية الأولى في أحسن الأحوال[3]، وإن كان الأمر هنا يحتاج إلى مزيد من التأمل القانوني كذلك، ذلك أن عدم التركيز على النواحي التي تجعل الخبرة مرتبطة بركنها الشكلي يصطدم بعقبة أخرى تتعلق بالتقرير المعد من الخبير، فمن المعروف أنه بعد الإنتهاء من أداء المهام الموكلة إليه، فإنه عليه أن يقدم تقريرا يشتمل على وصف ماقام به من أعمال، والنتائج التي ترتبت عليها، ويجب أن يكون هذا الأخير متكاملا لعناصره الشكلية والموضوعية.

وفضلا على أن الأمر لا يحتاج إلى خبرة دارسة في مجال الحوسبة والإتصال، فإن التطور الحادث فيه يجعل من الصعوبة بمكان متابعته على النحو الذي يحقق الإلمام التام والكلي بموضوع هذا الفرع، ومثل هذا الأمر ينبغي أن يدركه المشرع جيدا وإلا وقع تشريعه في خلل عدم التفاعل مع حقيقة وجوهر التعامل مع جرائم التعاملات الإلكترونية بصفة عامة، والوسائل الإلكترونية على رأسها الأنترنت بصفة خاصة، فمثلا أن

---

[1]- المادة 144 من قانون الإجراءات الجزائري.

[2]-المرسوم التنفيدي 95-310 المؤرخ في 10 أكتوبر 1995، يحدد شروط التسجيل في قوائم الخبراء القضائيين وكيفياته، جريدة رسمية، عدد 60، سنة 1995.

[3]-**د. عمر بن يونس**، الدليل الرقمي، المرجع السابق، ص107.

الصراع بين مدى إمكانية تحديد مسار الأنترنت[1] وعدمه يشكل صراعا جوهريا من حيث المبدأ، وإن كان الراجح هو الإتجاه إلى عدم إمكانية تحديد مسار الأنترنت حتى مع إمكانية تحديد هوية IP الحواسيب وأماكن وجودها[2].

ومن ثم نرى أنه لكي يصبح الشخص خبيرا في مجال تكنولوجيا المعلومات يجب أن لا يكون مؤهلا تأهيل علمي ومهني عال فحسب، بل لابد من الإستمرار في عمليتي التعلم والتدريب حتى يتمكن من استلهام وتتبع قواعد التطور السريع في فرع تكنولوجيا المعلومات، ويشق طريقه بنجاح في مجال الجرائم التي ترتكب بالوسائل الإلكترونية والتي تقع على التعاملات الإلكترونية.

تجدر الإشارة إلى أن نظام جدول الخبراء الذي يتميز به النظام القانوني الفرانكفوني غير مقيد على الإطلاق، إذ يمكن ندب خبير ليس مقيد في أي من هذه الجداول، وهذا ما نص عليه المشرع الجزائري صراحة في الفقرة الأخيرة من المادة 144 إجراءات، وإن إستلزم في هده الحالة أن يكون ذلك بقرار مسبب كعدم وجود الخبرة المطلوبة ضمن هذه الجداول[3]، ويبدو أن اتجاهه هذا غير متفرد، فالمشرع الفرنسي وإن نص في الفقرة الأولى من المادة 157 إجراءات على ضرورة إختيار الخبير من الجدول الوطني الذي تعده محكمة النقص أو الجدول الذي تعده المحاكم الإستئنافية وفق الشروط المنصوص عليها في القانون رقم 71-498 من 29 جويلية 1971 المتعلق بالخبراء القضائيين، أجاز بموجب الفقرة الثانية من نفس المادة وبشكل إستثنائي وبقرار مسبب للمحكمة أن تختار خبراء ليسو من هذه الجداول[4].

ومثل هذا النص يتجاوب مع الحال الذي عليه الخبرة في مجال التعاملات الإلكترونية،، فإختيار الخبير في إطارها يتحدد تبعا لنوعية الجريمة المرتكبة وأنواع الوسائل الإلكترونية المستخدمة فيها، وقد لا يتوافر خبير ضمن خبراء الجدول المعتمدين له معرفة تقنية معمقة في سائر قضايا العالم الإلكتروني، وبدلا من إستفادة جهات تحقيق العدالة من الخبير فقد يكون سببا في فقدان الدليل أو تدميره[5].

وعلى خلاف الوضع في التشريع الجزائري، لم يعد في التشريع المصري خبراء الجداول، وذلك بعد أن قفل المرسوم رقم 96 لسنة 1952 الخاص بتنظيم الخبرة أمام جهات القضاء هذه الجداول، ليقوم بأعمال الخبرة أمام جهات القضاء حسب المادة 2 من هذا المرسوم خبراء وزارة العدل ومصلحة الطب الشرعي والمصالح الأخرى التي يعهد إليها بأعمال الخبرة، وكل من ترى جهات القضاء عند الضرورة الإستعانة

---

[1]- يقصد **بمسار الأنترنت**، الحركة التراسلية للنشاط الممارس من خلال الأنترنت، فالحاسوب بمجرد أن يتعرف على المسار، يقوم تلقائيا باختيار البروتوكول التراسلي الذي من خلاله يقوم باستدعاء البيانات، وهذه هي الحركة التي أشار إليها علماء الأنترنت بأنها تتشابه مع شبكة العنكبوت من حيث عدم إنتظام شكل المسار الإتصالي والتواصلي عبرها. **د.عمر بن يونس**، الجرائم الناشئة عن إستخدام الأنترنت، المرجع السابق، ص998.

[2]- د. **عمر محمد بن يونس**، الدليل الرقمي، المرجع السابق، ص108.

[3]-**د. أحمد شوقي الشلقاني**، المرجع السابق، ص260.

[4]-**Article 157** Modifié par Loi n°2004-130 du 11 février 2004 - art. 54 JORF 12 février 2004 **dispose que "** Les experts sont choisis parmi les personnes physiques ou morales qui figurent sur la liste nationale dressée par la Cour de cassation ou sur une des listes dressées par les cours d'appel dans les conditions prévues par la loi n° 71-498 du 29 juin 1971 relative aux experts judiciaires. A titre exceptionnel, les juridictions peuvent, par décision motivée, choisir des experts ne figurant sur aucune de ces listes.

[5]-**د. عبد الفتاح بيومي حجازي**، الدليل الجنائي والتزوير في جرائم الكمبيوتر والأنترنت، المرجع السابق، ص97.

برأيهم الفني من غير من ذكروا. إلا أن هذا المرسوم لم يتضمن نصا يتعلق بخبراء مصلحة تحقيق الأدلة الجنائية أو المعمل الجنائي بصفة عامة.

ومن بين الشروط التي تطلبها المرسوم 96 لسنة 1952 في الخبير حتى يترشح لإكتساب صفة خبير أن يكون حائزا لدرجة البكالوريوس أو ليسانس من إحدى الجامعات المصرية في مادة القسم الذي يطلب التعيين فيه، أو شهادة تعتبر معادلة لهذه الدرجة من معهد علمي معترف به، وهو ما أشارت إليه المادة 18، ونفس الملاحظة التي أدرجناها فيما يخص مسالة التخصص لدى المشرع الجزائري تطرح بالنسبة للمشرع المصري.

هذا وقد أطلق المشرع يد القاضي في حرية ندب خبير أو خبراء[1]، وهدا ما يتجاوب وخصوصية جرائم التعاملات الإلكترونية فطبيعتها الفنية تجعلها موزعة على تخصصات فنية وعلمية دقيقة ومتنوعة، حتى أنه يمكن القول أن الأصل في الخبرة التقنية هو **تعدد الخبراء**، بحيث يجب ألا يكون هناك خبير واحد في الدعوى التي يكون موضوعها الحوسبة والإتصال، هذا من جهة.

ومن جهة أخرى لم يحدد طبيعة شخص الخبير الذي من الممكن أن يكون شخصا طبيعيا أو إعتباريا، كالشركات المختصة في تكنولوجيا المعلومات، ويرى جانب من الفقه[2] أنه يمكن للقاضي الجزائي أن يختار الخبير المعلوماتي من إحدى الفئات التالية:

-**الجهات الخاصة:**إلى جانب الخبرة الفردية، يمكن للقاضي الجزائي أن يلجأ إلى الشركات المختصة في مجال تكنولوجيا المعلومات، التي تضم في الغالب خبراء على مستوى عال من الكفاءة، فهده الشركات كثيرا ما تسعى إلى التعاقد مع أشخاص لهم شهرتهم في هذا المجال، ولو لم يكونوا من أصحاب الدراسات الأكاديمية، فلقد أثبتت التجربة العلمية أن هناك أشخاصا يتمتعون بمهارات فائقة في التعامل مع الوسائل الإلكترونية دون أن يتجاوز تحصيلهم العلمي السنوات الجامعية الأولى، مثل بيل كيتس bill gatesصاحب شركة مايكروسوفت، وهذا الأمر ينطبق أيضا على عتاة الهكرة ومخترقي الأنظمة، الذين لم يتجاوز تعليمهم الثانوية العامة.

-**المؤسسات التعليمية:** قامت العديد من المؤسسات التعليمية بإعداد قاعدة قوية في مجال دراسات تكنولوجيا المعلومات، مثل جامعة ستانفورد ومعهد التكنولوجيا في ولاية ماساشوست الذي قدم للبشرية خبراء على درجة عالية من التميز، ويمكن للقاضي الإستعانة بمثل هذه المؤسسات التعليمية المختصة لإختيار الخبير المعلوماتي.

-**التعاون الدولي:** يمكن للقاضي الجزائي أن يلجأ إلى الخبراء الأجانب من أجل القيام بالخبرة التقنية، غير أن هذا الأمر يتوقف على مدى نشاط المشرع في كل دولة لإبرام إتفاقيات تعاون في هذا المضمار.

وفي الجزائر يمكن للقاضي الجزائري أن يستعين بعدة جهات مماثلة للجهات المذكورة، ككلية الهندسة المعلوماتية، أو الشركات الخاصة التي تعمل في مجال تكنولوجيا المعلومات، أوالهيئة الوطنية للوقاية من

---

[1]-المادة 147 من قانون الإجراءات الجزائية الجزائري.

[2]-**د. عمر بن يونس**، الجرائم الناشئة عن إستخدام الأنترنت، المرجع السابق، ص1035. د. **محمد طارق عبد رؤوف الخن**، المرجع السابق، ص332.

الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته، حيث جعل القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها من مهام الهيئة مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، بما في ذلك من خلال جمع المعلومات والتزويد بها ومن خلال **إنجاز الخبرات القضائية**[1].

كما نص على الخبرة التقنية من خلال الفقرة الأخيرة من المادة 5 "يمكن للسطات المكلفة بالتفتيش تسخير **كل شخص له دراية بعمل المنظومة المعلوماتية** محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها".

ب: حلف اليمين:

يشترط لصحة أعمال الخبير أداء اليمين، وذلك لحمله على الصدق والأمانة في عمله، وبث الطمأنينة في آرائه التي يقدمها، سواء بالنسبة لتقدير القاضي أو لبقية أطراف الدعوى، ولذلك لا يغني عن هذا الإجراء أية ضمانة أخرى من الضمانات[2]، فقد أوجب المشرع الجزائري على **الخبير** أن يؤدي بمجرد قيده بالجدول الخاص بالمجلس القضائي يمينا أمامه بالصيغة المنصوص عليها في المادة 145 إجراءات، وهذا ما كرسته المادة 9-1 من المرسوم التنفيدي 95-310، كما يؤدي **المساعدون المتخصصون** الذين تستعين بهم النيابة العامة اليمين أمام المجلس القضائي الذي يعينون بدائرة إختصاصه لأول مرة وفق الصيغة التي حددتها المادة 35 مكرر من قانون الإجراءات الجزائية.

كما أوجب المشرع المصري بدوره أداء اليمين بموجب المادة 86 من قانون الإجراءات الجزائية.هذا وقد إستقر الفقه والقضاء على أن أداء الخبير لليمين يوم تسلمه العمل يغني عن أدائه اليمين عند مباشرة كل مأمورية وإن كان لا تثريب على المحكمة إن إستحلفته اليمين قبل أداء مأموريته[3].

ت-إلتزام الخبير بأداء أعمال الخبرة بنفسه:

الأصل أن يلتزم الخبير بأداء المهمة المكلف بها وفقا لأمر الندب ولايصح أن يحيل غيره للقيام بها، إلا أن المشرع قد خرج عن هذا الأصل وأجاز للخبير المنوط به أداء العمل أن يستعين باخصائي آخر للمعاونة ، وهذا ما أخذ به المشرع الجزائري في المادة 149 إجراءات، وإن كان قد إشترط أن يكون ذلك بتصريح من القاضي على أن يقوم هؤلاء الخبراء بحلف يمين الخبرة ويرفق تقريرهم مع تقرير الخبراء المنتدبين.

وبالرجوع للمشرع الفرنسي، نجده هو الآخر أجاز إستعانة الخبير بغيره من الإخصائيين، وهو ما أشارت إليه المادة 162 التي جاء نصها كمايلي:" ***إذا طلب الخبراء الإستنارة في مسالة خارجية عن دائرة***

---

[1]-المادة 14 من القانون رقم 09-04 ، والمادة 4 من المرسوم الرئاسي رقم 15-261 المحدد لتشكيل وتنظيم الهئية.

[2]- **د. أحمد ابو القاسم**، الدليل الجنائي المادي ودوره في إثبات جرائم الحدود والقصاص، الجزءالأول، دار النشر بالمركز العربي للدراسات الأمنية و التدريب، الرياض، 1993، ص377.

[3]- **عبد الناصر محمد محمود فرغلي**، المرجع السابق، ص171.

تخصصهم فيجوز للقاضي ان يصرح لهم بضم اخصائيين يعينون باسمائهم ويكونون على الخصوص مختارين لتخصصهم.

ويحلف الأخصائي المعين على هذا الوجه اليمين ضمن الشروط المنصوص عليها في المادة 160.ويرفق تقريرهم بكامله بالتقرير المنوه عنه في المادة 166.[1]

اما بالنسبة للمشرع المصري، وإن كان قد أجاز إستعانة الخبير باخصائي آخر للمعاونة، إلا أنه قصر الأمر على مجرد القيام بالأعمال المادية البحتة، دون أن يشترط حلف اليمين أو أن يكلفه بأداء التقرير الفني في الخبرة المطلوبة.

ث-خضوع الخبير للرقابة القضائية:

يتعين على الخبير أن يتولى مهمته تحت رقابة القاضي الذي عينه وأن يبقى على إتصال دائم به لأجل إحاطته علما بتطورات الأعمال التي يقوم بها، فالخبير هو مساعد للقاضي و معاون فني لا أكثر[2].

ج-رقابة الخصوم لأعمال الخبرة التقنية:

حيث أجاز كل من المشرع الجزائري بموجب المادة 152 من قانون الإجراءات الجزائية، والمشرع الفرنسي بموجب المادة 165 من قانون الإجراءات الجزائية لأطراف الخصومة أثناء إجراء أعمال الخبرة أن يطلبوا إلى الجهة القضائية التي أمرت بها أن تكلف الخبراء بإجراء أبحاث معينة أو سماع أي شخص معين بإسمه قد يكون قادرا على مدهم بالمعلومات ذات الطابع الفني، وهو ما يمثل نوع من رقابة الخصوم لأعمال الخبرة.

ويرى البعض أن الإستعانة بالخبراء المتخصصين نيابة عن الخصوم في الدعوى الجزائية لمراقبة أعمال الخبراء القضائيين المنتدبين، فيه حماية أكثر لحقوق الدفاع، لدورهم المباشر في مراقبة وتوجيه الخبير القضائي فضلا عن التأثير غير المباشر على العمل المطلوب منهم، حيث يضع الأخير في إعتباره عند أدائه لمهمته أنه مراقب من قبل خبير له ذات تخصصه، الأمر الذي يدفعه إلى إتخاذ كافة الإحتياطات اللازمة و تحري الدقة حتى يتجنب النقد سواء أثناء مباشرة مأموريته أو فيما يتعلق بإستخلاص النتائج وتقديم التفسيرات التي ينتهي إليها.[3]

---

[1]-**Article 162**Modifié par Loi n°2004-130 du 11 février 2004 - art. 56 JORF 12 février 2004 **dispose que "** Si les experts demandent à être éclairés sur une question échappant à leur spécialité, le juge peut les autoriser à s'adjoindre des personnes nommément désignées, spécialement qualifiées par leur compétence.Les personnes ainsi désignées prêtent serment dans les conditions prévues à l'article 160.Leur rapport sera annexé intégralement au rapport mentionné à l'article 166.

[2]- **Michaud (Jean)**. Le juge d'instruction et l'expert, Revue de science criminelle et de droit pénal comparé, 1975, n° 3, p. 791

[3]- **د. فتحي محمد أنور عزت**، دور الخبرة في الإثبات الجنائي، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 2007، ص221.

ح-تقديم تقرير الخبرة التقنية:

بعد أن ينتهي الخبير من أداء المهام الموكلة إليه، فإنه عليه أن يقدم تقريرا يشتمل على وصف ماقام به من أعمال، والنتائج التي ترتبت عليها، وأن يودعو التقرير و الأحراز أو ما تبقى منها لدى كاتب الجهة القضائية التي أمرت بالخبرة ويثبت هذا الإيداع بمحضر، فإذا لم يودعوا تقاريرهم في الميعاد المحدد لهم، جاز في الحال أن يستبدل بهم غيرهم، وعليهم إذ ذاك أن يقدمو نتائج ماقامو به من أبحاث كما عليهم أيضا أن يردو جميع الأشياء والأوراق والوثائق التي تكون قد عهد بها اليهم على ذمة انجاز مهمتهم، ومن الجائز ان تتخذ ضدهم تدابير تاديبية قد تصل إلى شطب أسمائهم من جدول الخبراء[1].

ثانيا- القواعد الفنية التي تحكم الخبرة التقنية

للخبير التقني في سبيل تحري الحقيقة أن يقوم بكل ما يمكنه من التوصل إليها، وهو في إطار القيام بعمله أن يستخدم الأساليب العلمية التي يقوم عليها تخصصه،ويرى الفقه الإجرائي[2] أنه يجب على الخبير التقني أن يكون قادرا على القيام بالمهام التالية:

أ- حجز المعطيات

ب-التحفظ على المعطيات

ت-استعادة المعطيات

ث-تحليل المعطيات

ج-إعادة بناء القضية

ح-كتابة التقرير

أ- حجز المعطيات :

من أشهر نظريات العلوم الجزائية المفيدة في إعادة تكوين عناصر الجريمة وعلاقة الجناة بالجريمة، نظرية أو مبدأ **لوكارد لتبادل المواد**، ويقصد به عند أي اتصال بين مادتين لا بد أن يترك كل منها أثر على الاخر[3]. فمثلا إذا أرسل شخص رسالة الكترونية وتحمل مضمونا إحتياليا إلى أحد المتعاملين الإلكترونيين، فإن هذه الرسالة سوف تخزن على المخدمات الموجودة لدى مزود الخدمة مع ساعة بداية الربط وتاريخه Gmt+01وساعة نهاية الربط وتاريخه Gmt+01، إضافة إلى مسار الرسالة وعنوان

[1]-المادة 148 و153 من قانون الإجراءات الجزائية الجزائري، المادة 161 من قانون الإجراءات الجزائية الفرنسي.

[2] -John R. Vacca,Computer Forensics: Computer Crime Scene Investigation, Charles River Media, 2002, isbn,1584500182.chapter 1,p5.

[3]-"Any one, or anything, entering a crime scene takes something of the scene with them, and leaves something of themselves behind when they depart,"
Ephraim Nissan, Computer Applications for Handling Legal Evidence, Police Investigation and case argumentation , volume 1, springer, new York ,2012, p1061.

ورقم النفاذ ونوع الإشتراك ورقم الهاتف، لذلك يجب على الخبير التقني أن يقوم في بادىء الأمر بعملية حجز المعطيات المتعلقة بالجريمة الموجودة لدى مزود الخدمة، إضافة إلى حجز الأجهزة التي تحوي هده المعطيات، والتي تكون بحيازة المشتبه به أو في مسرح الجريمة[1].

ومن أهم مصادر الأدلة في عملية الإثبات العلمي التي يتعين ضبطها بقصد تفحصها[2] فضلا عن الأوراق المكتوبة يدويا والمخرجات الطباعية، جهاز الحاسب الآلي وملحقاته، أقراص الليزر، الشرائط الممغنطة، لوحدة الدوائر، المودم، الطابعات، البطاقات الممغنطة وبطاقات الإئتمان، مع التاكد من أن المكونات الصلبة و البرمجيات تعمل بشكل سليم ومنتظم، وأن جهاز الحاسوب غير مصاب بفيروس يؤثر على نظامه أو على ملفات التشغيل أو التنفيد، لأن ذلك يمكن أن ينال من صحة الدليل الإلكتروني المستخلص عند عرضه على القضاء.

ب-حفظ المعطيات:

فالأولويـــة أن يتم التحفظ على الأدلـــة الموجودة على وسائط التخزين الأصلية (قرص صلب داخلي أو خارجي، قرص مرن، قرص مضغوط ..إلخ)، ذلك أن بدء تشغيل الكمبيوتر أو نفاد بسيط بغرض القراءة يغير الملفات الموجودة على القرص، وهذا هو السبب في وجوب تقديم نسخة كاملة من وسيط أصلي مع إجراءات حجب القراءة، على أن يتم تنفيد التحقيقات والإختبارات على تلك النسخة[3].

ت-إستعادة المعطيات:

يجب على الخبير التقني أن يستعيد المعطيات المحذوفة، وهو أمر ضروري من أجل إعادة بناء القضية، فمثلا يمكن للخبير أن يستعيد جميع الرسائل التي قام الجاني بحذفها عن طريق تتبع الأثر الذي تتركه هذه الرسائل على جهاز التخزين[4].

ففي قضية قرصنة البنك الكندي، أسفرت نتائج الخبرة على المعدات المضبوطة أثناء عملية التفتيش على 3 أجهزة إعلام آلي، عن وجود آثار رقمية أفادت إستعمال البريد الإلكتروني والإسم المستعار wallacez ، و آثار أخرى حول صفحة web المستعملة في عملية النصب الإلكتروني على البنك، وآثار رسائل الكترونية لتحويل مبالغ مالية من رصيد المشتبه فيه على نظام التحويلات wester union .

---

[1]-**Eoghan Casey**; Digital Evidence and Computer Crime: Forensic Science, Computers and the internet, second edition, a cadimic press,2004, p101.

[2]- **عبد الناصر محمد محمود فرغلي**، المرجع السابق، ص388.

[3] -**Michel VILLARD,** La cybercriminalité et l'expertise judiciaire; disponible en ligne á l'adresse suivantehttp://www.lajauneetlarouge.com/article/la-cybercriminalite-et-lexpertise-judiciaire#.WCMyQNThASk

[4]-**محمد طارق عبد الرؤوف الخن**، المرجع السابق، ص335.

والخبير بفضل برامج متخصصة يمكنه تتبع المسار الجغرافي للطلب إتجاه مزود واب، وغالبا ما يتحقق بأن قاعدة المعطيات لمحتوى غير مشروع قد تم ترحيلها للخارج[1].

ث-تحليل المعطيات:

في هذه المرحلة يقوم الخبير التقني بعملية تقييم محتوى المعطيات الرقمية، بحيث **يفحصها بدقة** بفصل الأدلة المتعلقة بالقضية وإستخراجها من المعطيات التي تم الحصول عليها. وعلى الخبير على حسب نوع حاوية المعطيات مراعاة إستخدام نوع الأداة المناسبة لإستخراج الدليل الإلكتروني.

نوع الحاوية أو المعطيات	الأدوات المحتملة
الذاكرة العشوائية RAM	Volatility toolkit, PE Tools.
الأقراص الصلبة أو الذاكرات الخارجية	EnCase, FTK, SleuthKit, … etc.
بيانات الشبكة	Wireshark, Network Miner, Xplico, NetSleuth or any enterprise alternative.
الأجهزة المحمولة والأجهزة اللوحية	Encase Forensics v7 and above

جدول 1 – أمثلة للأدوات المساعدة في عملية إستخراج الأدلة[2]

وبعد عملية الفحص، تأتي عملية التحليل التي تتم على المعطيات التي تم إستخراجها في عملية الفحص، من من أجل تحديد وسائل الجريمة ودوافعها والغرض منها[3].

ج-إعادة بناء القضية:

ويقصد بدلك العملية التي يقوم بها الخبير، بعد تجميع وتحليل المعطيات والمعلومات التي تم الحصول عليها نتيجة البحث، من أجل توضيح ما حصل بين المجرم والضحية أثناء إرتكاب الجريمة، فالدليل الإلكتروني الذي تم الحصول عليه يحتوي على آثار سلوكية للمجرم، مثل الكلمات التي إستخدمها المجرم في تصفح الأنترنت، والمواقع التي قام بتصفحها على الشبكة، وغرف الدردشة التي قام بزيارتها وغير ذلك، فالربط بين هذه السلوكيات يؤدي إلى معرفة وقت ومكان إرتكاب الجريمة، والطريقة التي تمت بها، وكيفية وصول الجاني إلى ضحيته[4].

1-, **Michel** VILLARD, disponible en ligne á l'adresse précédente.

2- **ساري بخاري**، مقدمة لمراحل التحقيق الجنائي وخطواته، مقال متاح على موقع المجتمع العربي المختص بأمن المعلومات التـــالي:
https://www.isecur1ty.org/%D9%85%D9%82%D8%AF%D9%85%D8%A9-

3 **Eoghan Casey**, op,cit, p111.

4 **- ibid,** p-116.

ولكي يتم تطبيق أو تنفيذ كل ما سبق، لا بد أن يكون الخبير مؤهل ذي تخصص فريد في معالجة الأدلة الإلكترونية وفحصها وتحليلها، ويكون كذلك عن طريق إستخدام العديد من الوسائل المساعدة مادية وإجرائية و برامجية[1] منها[2] : برنامج إذن التفتيش، قرص بدء التشغيل، برنامج معالجة الملفات مثل x tree pro gold ، برنامج النسخ مثل lap link، برنامج كشف الدسك مثل ama disk, vieu disk برنامج إتصالات مثل lantastic، بروتكول tcp/ ip.

ح-كتابة التقرير:

يتضمن تقرير الخبرة بين دفته النتائج التي توصل إليها الخبير من خلال عملية البحث، ومن النقاط التي يجب أن يتضمنها التقرير: مواصفات مسرح الجريمة الإفتراضية، ملخص عن عملية الفحص التي تم القيام بها، إعادة رواية أحداث القضية، ملخص النتائج، إقتراحات الخبير المعلوماتي[3].

الفرع الرابـــــع

مدى حجية تقرير الخبير التقني

الخبرة التقنية شأنها شأن بقية أدلة الإثبات تخضع حجيتها لتقدير القاضي ومدى تاثير أعمال الخبرة في الإقتناع الذاتي له، فهو **الخبير الأعلى** في كل ما يستطيع أن يفصل فيه بنفسه، إلا أن البعض يرى بأن الخبير التقني هو القاضي الحقيقي للدعوى، فكل ما يبديه يعد من الحقائق التي تجبر القاضي على الأخذ بها، فالدور الجوهري للخبير في تحديد الأدلة الإلكترونية لا يترك مجالا واسعا للقاضي لتحديد مسار الدعوى، ولذلك يصبح الخبير الملهم الأساسي في القضية[4]. إلا أننا نرى أن إعتماد المحكمة على تقرير الخبير التقني لا يعد مساسا بمبدأ قناعة القاضي الشخصية، ولا يجعل من الخبير القاضي الحقيقي للدعوى، فدور الخبير التقني ليس سوى أحد الأدوار التي تساعد القاضي على فهم القضية، وهذا الدور ليس بجديد على الساحة القضائية، فالقضاء كثيرا ما كان يستند في أحكامه إلى الخبرة التي تجري على البصمات، أو على الحمض النووي وغيرها، فضلا عن ذلك فان بناء الحكم على تقرير الخبرة لا يختلف عن الأخذ بأقوال الشهود وبناء الحكم بالبراءة أو الإدانة على أساس هذه الأقوال، فمحكمة الموضوع هي صاحبة القول الفصل في تقرير الخبرة الذي تقتنع به أولا تقتنع[5].

د. محمد طارق عبد الرؤوف الخن، المرجع السابق، ص338.

[1]– **د. خالد ممدوح إبراهيم**، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص302.

[2]–**د. حسن طاهر داود**، المرجع السابق ، ص228 وما بعدها.

[3]-**Eoghan Casey**, op,cit, p131

د. محمد طارق عبد الرؤوف الخن، المرجع السابق، ص336.

[4]-**د.عمر محمد أبو بكر بن يونـــس** ، الجرائم الناشئة عن إستخدام الأنترنت، المرجع السابق، ص967.

[5]–**د. محمد طارق عبد الرؤوف الخن**، المرجع السابق، ص338.

المبحث الثاني

طرق الإثبات الجزائي المستحدثة في جرائم الإعتداء على التعاملات الإلكترونية

(الدليل الإلكتروني[1])

إن أصبحت الحاجة ملحة لدعم طرق الإثبات في جرائم لا تتعدى حدودها الحيز الإفتراضي، فلقد وفر هذا الأخير بما يحويه من نظم التخزين ونظم التراسل هذا الدعم، من خلال ما يقدمه من ملفات وسجلات وحزم وغيرها تعكس أعمال المهاجم، ويشكل نتاج هذه الأنظمة ما يسمى **بالدليل الإلكتروني** مكرسا بذلك منطق التفاعل المطلوب بين طبيعة الدليل وطبيعة الجريمة التي يولد منها.

فالدليل الإلكتروني يستمد طبيعته من ذات العمليات الإلكترونية التي نتج عنها في حالة الإعتداء عليها، فالتلاعب في المستندات الإلكترونية لا يمكن كشفه بالطرق التقليدية بل بالأدلة الإلكترونية التي قد تتحصل من التقنيات ذاتها، كذلك هو الشأن في تزوير التوقيع الإلكتروني حيث يلزم فك رموز وشفرات معينة بإستخدام التقنيات داتها، وليس بفحص الخطوط وغيرها من الطرق التقليدية.

و إن كان كذلك، فإن هذه الأدلة لها سمات محددة خلقت مصاعب أنقصت من قيمتها ونسبة الإعتماد عليها في الإثبات إن لم يتم إيجاد حلول بشأنها، ولا يحتاج التعامل مع تلك التحديات إلى قانون لتحديد الإجراءات التي يتم إتباعها بشأنها في الجرائم الواقعة على التعاملات الإلكترونية فحسب، بل يمتد أيضا إلى وضع ما يشبه بروتوكولات لضمان الجودة المستخدمة في مجال الدليل الإلكتروني[2].

وعلى هدي ما تقدم، سنتولى في هدا المطلب إستجلاء الدليل الإلكتروني فنحدد مفهومه وخصائصه، ثم في محاولة مستمدة من الواقع حصر مشكلاته، على أن يكون ذلك من خلال المطالب التالية:

المطلب الأول: مفهوم الدليل الإلكتروني

المطلب الثاني: خصائص الدليل الإلكتروني

---

[1]– ولإلكترون electron جسيم أولي elementary particle مستقر ذو شحنة كهربائية سالبة هي أصغر شحنة يمكن أن توجد في الطبيعة، ولذلك اتُخذت واحدة كمية الكهرباء، وليست شحنة أي جسم سوى مضاعفات لها. أما كتلة الإلكترون فهي أصغر كتل الجسيمات المستقرة، وهي تعادل ما يقرب من جزء واحد من 1850 جزءاً من كتلة ذرة الهدروجين ، وقد أمكن التعرف عليه عام 1897 على يد أحد العلماء عدما تمكن من قياس النسبة بين شحنة الكترون إلى كتبته، والإلكترونيات فرع من علم الفيزياء والهندسة يتناول التحكم في إنسياب الشحنات الكهربائية في وسائل معينة لتحقيق أغراض مفيدة، وتستخدم المكونات الإلكترونية في مدى واسع من المنتجات مثل أجهزة الراديو والتلفاز والحواسيب: أنظر **الموسوعة العربية**، إصدار هيئة الموسوعة العربية، دمشق، 2001، ص324.

والبعض يطلق عليه الدليل **الرقمي**، وترجع تسمية الدليل الرقمي إلى أن المعطيات داخل الوسط الافتراضي سواء كانت صوراً أو تسجيلات أو نصوص تأخذ شكل أرقام على هيأة الرقمين (1 أو 0) و يتم تحويل هذه الأرقام عند عرضها لتكون في شكل صورة أو مستند أو تسجيل، **د. ممدوح عبد الحميد عبد المطلب، زبيدة محمد قاسم، عبد الله عبد العزيز**، نموذج مقترح لقواعد إعتماد الدليل الرقمي للإثبات في جرائم الكمبيوتر، منشور ضمن أعمال مؤتمر"الأعمال المصرفية والالكترونية "، الجزء الخامس، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، في الفترة من 10–5/12/ 2003 م ،ص2237.

[2]- **Padova (Yann)**. Un aperçu de la lutte contre la cybercriminalité en France, Revue de science criminelle et de droit pénal comparé, 2002; p 772

المطلب الأول

مفهوم الدليل الإلكتروني

تستند عملية الإثبات الجزائي في الجرائم الواقعة على التعاملات الإلكترونية على الدليل الإلكتروني كونه يتفق وطبيعة الوسط الذي إرتكبت فيه هذه النوعية من الجرائم، وللوقوف على تحديد مفهومه لا بد لنا من التعرض لتعريفه (الفرع الأول)، ثم دراسة أهم تقسيماته(الفرع الثاني).

الفرع الأول

تعريف الدليل الإلكتروني

قبل الخوض في موضوع الدليل الإلكتروني، يتوجب علينا أن نتناول مفهوم الدليل الجنائي بشكل عام، بإعتباره الأصل، ولايمكن التطرق للفرع دون المرور على الأصل.

أولا- التعريف بالدليل الجنائي بشكل عام

الدليل في اللغة:هو المرشد،ومايتم به الإرشاد، وما يستدل به، والدليل :الدال والجمع أدلة[1]، وكذلك يعني تأكيد الحق بالبينة، والبينة هي الدليل أو الحجة.

الدليل إصطلاحا: هو ما يلزم من العلم به شيء آخر، وغايته أن يتوصل العقل إلى التصديق اليقيني بما كان يشك في صحته، أي التوصل به إلى معرفة الحقيقة[2].

أما الدليل في الإصطلاح القانوني، فقد تعددتالتعاريف التي رصدها الفقه للدليل، منها أنه الوسيلة التي يستعين بها القاضي للوصول إلى الحقيقة التي ينشدها، والمقصود بالحقيقة في هذا السياق كل ما يتعلق بالوقائع المعروضة عليه لإعمال حكم القانون عليها[3]. كما عرفه البعض أنه ما يؤدي إلى كشف الحقيقة أو

[1]- **د جميل صليبيا**، المعجم الفلسفي، الطبعة الأولى، دار الكتاب اللبناني، بيروت،1970، ص23.

[2]–**د. أحمد أبو القاسم**، الدليل الجنائي ودوره في إثبات جرائم الحدود والقصاص، المرجع السابق، ص177.

[3]– **د. أحمد فتحي سرور**، الوسيط في قانون الإجراءات الجنائية، الطبعة الثانية، دار النهضة العربية، القاهرة، 1981، ص418.

هو ما يولد اليقين في النفس بصحة أمر أو بعدم صحته[1]. كما عرفه البعض على أنه"مجموعة الوقائع المادية والمعنوية التي تفيد في كشف أية جريمة وإظهار الحقيقة فيها"[2].

تأسيسا على ما سبق، يمكن القول أن الدليل هو "معلومة يقبلها المنطق والعقل يتم الحصول عليها في ***إطار من الشرعية الإجرائية لإثبات صحة إفتراض أو لرفع أو خفض درجة اليقين الإقناعي في واقعة محل خلاف***" [3]. **وهو أداة اثبات[4] عموما.**

والدليل في المواد الجنائية أهمية عظيمة في كونه هو الذي يدعم الحقيقة ويكشف وقوع الجريمة ويحدد مرتكبها، وهو الذي يحول الظن والتخمين إلى تأكيد ويقين، فالحقيقة في معناها العام تعني معرفة حقيقة الشيء بأن يكون أو لا يكون، وهذا لا يتحقق إلا بالدليل بحسبان أنه المعبر عن هذه الحقيقة.[5]

ثانيا– تعريف الدليل الإلكتروني

يعرف البعض الدليل الجنائي الإلكتروني بأنه "**يشمل جميع المعطيات الرقمية التي يمكن أن تثبت أن هناك جريمة قد إرتكبت، أو توجد علاقة بين الجريمة و الجاني أو توجد علاقة بين الجريمة و المتضرر منها،** [6]وهناك من يعرفه بأنه"**برامج الحاسوب ومعطياته التي تستخدم للإجابة عن الأسئلة الهامة حول الحادثة الأمنية**"[7]، **او أنه الدليل الذي يجد له أساسا في العالم الإفتراضي يقود إلى الجريمة**[8]، أنه"***الدليل المأخوذ من أجهزة الكمبيوتر وهو يكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة وهي مكونرقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات والأشكال والرسوم وذلك من أجل اعتماده أمام أجهزة إنفاذ وتطبيق القانون*** ."[(9)]وهناك من يعرّفه بأنّه" ***معلومات يقبلها المنطق و العقل و يعتمدها العلم, يتم الحصول عليها بإجراءات قانونية وعلمية بترجمة المعطيات الحسابية المخزنة في أجهزة النظم***

---

[1]– **د. عوض محمد عوض**، دراسات في الفقه الجنائي الإسلامي، دار المطبوعات الجامعية ، الإسكندرية، 1977، ص283.

[2]–**د لواء فهد إبراهيم الدوسري**، ضبط الآثار والأدلة المادية والجرمية الأبعاد القانونية، ورقة مقدمة لجامعة نايف العربية للعلوم الأمنية، متاحة على المـــوقع الإلكتروني التالي:
http://repository.nauss.edu.sa/bitstream/handle/123456789/58291/%D8%A7%D9%84%D8%A3%D8%AF%D9%84%D8%A9%20%D8%A7%D9%84%D9%85%D8%A7%D8%AF%D9%8A%D8%A9.pdf?sequence=1

[3]– **د. أحمد أبو القاسم**، الدليل الجنائي ودوره في إثبات جرائم الحدود والقصاص، المرجع السابق، ص184.

[4]–مفهوم الإثبات أوسع وأشمل من مفهوم الدليل، فالإثبات يشمل مجموعة من الإجراءات الشكلية والموضوعية والقواعد اللازمة لكشف الحقائق و تحقيق العدالة، والدليل مجموعة من الحقائق التي تقدم للمحكمة لتبرئة أو لإدانة المتهم، أنظر: **د. أحمد أبو القاسم**، المفهوم العلمي والتطبيقي للدليل الجنائي المادي، مجلة مركز بحوث الشرطة، العدد السابع والعشرون، يناير 2005، ص152.

[5]–**Jean-Pierre Gridel;** Le droit des preuves au défi de la modernité ; actes du colloque du 24 mars 2000,p.133

[6]- The term **digital evidence** encompasses any and all **digital** data that can establish that a crime has been committed or can provide a link between a crime and its victim or a crime and its perpetrator, Eoghan Casey, op, cit, p668.

[7]-**Michael G. Solomon** and others, computer forensics jump start, published by wiley- default,2005,chapter-3,p4.

[8]–**د.عمر محمد أبو بكر بن يونـــس** ، الجرائم الناشئة عن إستخدام الأنترنت،المرجع السابق، ص969.

[9]– **د. خالد ممدوح إبراهيم**، الدليل الالكتروني في جرائم المعلوماتية، بحث منـــشور على الموقـــع التـــالي :
http://kenanaonline.com/users/KhaledMamdouh/posts/79345

المعلوماتية وملحقاتها وشبكات الاتصال ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بجريمة أو جان أو مجني عليه[1]"

أما التعريف المقترح للدليل الإلكتروني من قبل المنظمة الدولية لأدلة الحاسوب IOCE بأنه المعلومات المخزنة أو المتنقلة في شكل ثنائي، و يمكن أن يعتمد عليها في المحكمة[2].

ولم يذهب الفريق العلمي العامل على مستوى الأدلة الإلكترونية بعيدا عن التعريف الذي إقترحته هذه المنظمة، **حيث عرف الدليل الإلكتروني على أنه المعلومات المخزنة أو المتنقلة في شكل ثنائي دات قيمة إثباتية**"[3].

من خلال إستقراءنا للتعريفات السابقة، نلاحظ أنها وإن حاولت إستيعاب هذا النوع المستحدث من الأدلةــ إلا أن هناك بعض الملاحظات ينبغي الإشارة إليها في هذا المقام تتمثل فيمايلي :

1-هناك من التعريفات من حصرت عملية تجميع وتحليل محتوى الدليل الإلكتروني وفحصه بالبرامج فحسب، إلا أنه وإن كان صحيحا أن البرامج قادرة على القيام بمعالجة الدليل من مرحلة التبليغ عن وقوع الجريمة لغاية عرض الدليل أمام المحكمة، مرورا بجمعه وحفظه وتحليله وتوثيقه وإنتاج تقريره، مثل برامج:

EnCase (Guidance Software Corporation).
FTK Forensic Tool Kit (Access Data Corporation).
iLook LEO and iLookPI (Perlustro Corporation)
SMART (ASR Data, Data Acquisition and Analysis, LLC)

إلا أن فهم مضمون الدليل الإلكتروني يعتمد فضلا عن البرامج إلى إستخدام أجهزة وأدوات خاصة مختلفة بطريقة تقنية وإستنادا للقانون والمعايير الخاصة به، ومن أشهر هذه الأدوات:

Voom Technologies ،intelligent Computer Solutions ،Weibetech ،Logicube ،Tableau[4]

2-هناك من التعريفات من حصرت مصادر الدليل في الحاسب الآلي، إلا أنه تعريف منتقد، ذلك أنه وإن كانت الحواسيب تعتبر مصدرا غنيا بالأدلة الإلكترونية وخاصة تلك الحواسيب الشخصية التي تعد بمثابة أرشفة سلوكية للأفراد إلا أن هناك من المصادر لا تقل أهمية عنها، سواء كانت من **نظم التخزين** كالهواتف او **نظم التراسل** كمخدمات شبكة الأنترنت التي تحوي الكثير من المعلومات حول أنماط سلوك الأشخاص في وقت محدد كمعرفة المواقع الإلكترونية التي سبق زيارتها وغرف الدردشة التي تم الدخول إليها والرسائل الإلكترونية المرسلة والمستقبلة...إلخ هذا من جهة.

ومن جهة أخرى حصرت صفة الدليل الإلكتروني فقط في الدليل المأخوذ من مصدره، وهذا المنطق يؤدي إلى القول أن مخرجات الأجهزة الإلكترونية لا تكون لها قيمة إثباتية مادامت في الوسط الإفتراضي الذي نشأت فيه أو بواسطته، وهذا غير دقيق.

1-**د. محمد الأمين البشري**،التحقيق في جرائم الحاسب الآلي والأنترنت، جامعة نايف العربية للعلومالأمنية، الرياض، 2004، ص234.

[2]-Digital evidence is information stored or transmitted in binary form that may be relied on in court, **Eoghan Casey**, op, cit,p261

[3]-***Digital evidence or electronic evidence*** is any probative information stored or transmitted in digital form **Adv. Prashant Mali , Electronic Evidence/ Digital Evidence & Cyber Law in India, available at https://www.linkedin.com/pulse/electronic-evidence-digital-cyber-law-india-adv-prashant-mali-**

-[4]**أحمد حمو وآخرون**، الأدلة الإلكترونية من الناحيتين القانونية والتقنية،_دراسة تحليلية مقارنة- دون دار النشر، فلسطين، 2015، ص22.

–التعريفات السابقة إعتنقت مبدأ الحياد التقني، حيث أنها لم تحصر الدليل الإلكتروني وفق هيئة معينة، وحسنا فعلت، فالدليل الإلكتروني دليل متنوع يمكن أن يكون معطيات غير مقروءة كما لو كان ناتج مراقبة عبر الشبكات والملقمات أو الخوادم، وقد يكون مفهوما كما لو كان مستندا إلكترونيا، كما يمكن أن يكون صورة ثابتة أو متحركة أو معدة بنظام التسجيل السمعي المرئي أو تكون مخزنة في نظام البريد الإلكتروني[1]، ففي كل هذه الحالات فـــإن المعطيات التي يتشكل منها الدليل الإلكتروني تأخذ شكل أرقام (0–1) داخل الحيز الإفتراضي(النظام التراسلي، نظام التخزين)، ليتم تحويلها عند عرضها في شكل صورة أو مستند أو تسجيل.

ولذا فإننا بالإستفادة مما سبق نرى تعريف الدليل الإلكتروني بأنه" **المعلومات التي يتم الحصول عليها من الحيز الإفتراضي (نظام تخزين–نظام تراسل) وتكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية يتم معالجتها بتقنيات خاصة لينتج عنها هيئات معينة يتم ربطها بين الجريمة والجاني والمجني عليه بطرق لا تتعارض مع القانون.**

وهذا التعريف للدليل الإلكتروني يلزمنا التمييز بين الأثر الفيزيائي والأثر الإلكتروني للمعلومات في نظم المعالجة الآلية[2]، فالآثار الفيزيائية تكون موجودة على القرص الصلب على شكل كهرومغناطيسي، أو موجودة بشكل مؤقت في ترانزستورات الذاكرة المؤقتة، أو موجودة في الأطياف الكهرومغناطيسية في الكوابل، وهي لا يمكن رؤيتها من قبل المحققين، أما الآثار الإلكترونية فهي عبارة عن تفسير لهذه الاثار الفيزيائية بواسطة أدوات وبرمجيات خاصة.

كما يجب التنويه إلى أن الإثبات بالدليل الإلكتروني لا ينحصر نطاق العمل به في الجرائم محل الدراسة، إذ يتعداه لإثبات جميع الإعتداءات الواقعة في الحيز الإفتراضي (النظام التراسلي–نظام التخزين)، ومثل هذا الأمر يقودنا إلى القول بأن الدليل الإلكتروني يصلح لإثبات جميع الجرائم التي لا صلة لها بهذا العالم إلا من حيث الوسيلة كتهريب المخدرات أوغسل الأموال عن طريق النظم المعلوماتية[3]، كما يصلح لإثبات الإعتداءات التي تقع على العناصر المعنوية لنظم المعالجة الآلية بكافة تطبيقاتها كالدخول غير المصرح به إلى النظم والتلاعب بالمعلومات، إلا أن أهميته تزداد في الوقت الحالي بعد أن إعترفت الكثير من التشريعات بالمستندات الإلكترونية ومنحتها الحجية في الإثبات، كذلك هو الشأن بالنسبة للتوقيع الإلكتروني، كما أجازت التعامل ببطاقات الإئتمان ومدت حمايتها الجزائية إلى الجانب المعنوي الذي تتكون منه المنظومات المعلوماتية معترفة بصلاحيتها لتكون محل لإرتكاب العديد من الجرائم.

والدليل الإلكتروني على النحو السابق وإن كان الحصول عليه يتم وفق تدابير تقنية تتماشى وطبيعته كالتحفظ على المعطيات وإعتراض معطيات المحتوى تمهيدا للكشف عنه، فإنه قد يكون نتاج إجراءات تقليدية كالخبرة والتفتيش والضبط مع ضرورة تطويرها لكي تتناسب مع الطبيعة الخاصة لهذه الجرائم كما سبق وأن رأينا.

---

[1]–**د. عمر بن يونس**، الدليل الرقمي، المرجع السابق، ص47.

[2]–**أحمد حمو وآخرون**، المرجع السابق، ص 7.

[3]–أ. **طارق محمد الجملي**، الدليل الرقمي في مجال الإثبات الجنائي، ورقة عمل مقدمة للمؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، الفترة من 28–29 /2009/10 ، طرابلس، ص09.

نخلص مما سبق، أن الدليل الإلكتروني ظاهرة مستحدثة برزت نتيجة الإرتباط بين الظاهرة الرقمية ذات الطبيعة التقنية الناجمة عن نظم التخزين والتراسل، وبين الإثبات الجزائي، فهذه الأدلة الإلكترونية لها مظهرها المميز حقيقة عن الأدلة التي يمكن تحقيقها في العالم المادي، من حيث كونها من الأدلة القابعة في العالم الإفتراضي المبني على الكيفية المعنوية غير الملموسة، وهذا الأمر يشكل قالب الدليل الإلكتروني في تكنولوجيا المعلومات.

الفرع الثاني

تقسيمات الدليـــــل الإلكتروني

تختلف الجرائم الواقعة على التعاملات الإلكترونية عن الجرائم التقليدية، في كون الأولى تتم في بيئة غير مادية عبر نظام المعالجة الآلية بجناحيه الحوسبة والإتصال، حيث يمكن الجاني عن طريق نبضات إلكترونية رقمية لا ترى أن يخترق مواقعها ويعبث بمعطياتها، وذلك في وقت قياسي قد يكون جزءا من الثانية، مما يصعب الحصول على دليل مادي بخصوصها، فكل ما يتم الحصول عليه غالبا هو آثار معلوماتيّة رقميّة يتركها مستخدم الشّبكة المعلوماتيّة أو الانترنت، ويظهران في شكل رئيسي هو الشّكل الرّقمي. لأنّ المعلومات داخل نظام المعالجة الآلية سواء كانت في شكل نصوص أو أحرف أم أرقام أم أصوات أو صور أو فيديو أو برامج تتحوّل إلى طبيعة رقميّة, حيث ترتكز تكنولوجيا المعلوماتيّة على تقنيّة التّرقيم الّتي تتعلّق بترجمة أو تحويل أيّ مستند معلوماتي مؤلف من نصوص أو صور أو أصوات أو معطيات إلى نظام ثنائي في تمثيل الأعداد قوامه الرقمان الصفر والواحد[1].

كما أن الدليل الإلكتروني ليس على صورة واحدة، بل له خصيصة التنوع نظراً لما تتمتّع به طبيعته من ضرورة توافقه مع الواقعة الإجراميّة، وفي هذا الإطار نلمس نوعين من المحاولات في تقسيمه، البعض منها فقهي والثاني تابع لوزارة العدل الأمريكية، وهو ما سنتناوله فيمايلي:

أولا- المحاولات الفقهية لتقسيم الدليل الإلكتروني

قسم البعض من الفقه[2] الدليل الإلكتروني إلـــى الأقسام الرئيسية التالية:

1- أدلة تقنية خاصة بأجهزة الحاسب الآلي وشبكاته.

---

[1]-النظام الثنائي الرقمي*binary*اعتمد أساسا للكمبيوتر الرقمي، ويمكن من هذا النظام تحويل كافة الأرقام العشرية والحروف والأشكال إلى نظام ثنائي، ويمكن من جهة أخرى الاعتماد على المكافئ له سواء كان نظام ثنائي أو نظام الست عشر، مشار إليه لدى: **د. ممدوح عبد الحميد عبد المطلب**, إستخدام بروتوكول (*tcp/ip*) في بحث وتحقيق الجرائم على الكمبيوتر،المرجع السابق, ص7.

[2]-**د.ممدوحعبدالحميدعبدالمطلب**،البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، مصر، 2006، 88. مشار إليه لدى: **د.عبد الناصر محمد محمود فرغلي و د. عبيد سيف سعيد المسماري**. ورقة بحث مقدمة للمؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، دراسة تطبيقية مقارنة، الرياض المنعقد في الفترة:2-1148/11/04 ه الموافق ل 12-2007/11/14, ص13.

2- أدلة تقنية خاصة بالانترنت.

3- أدلة تقنية خاصة ببروتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات.

4- أدلة خاصة بالشبكة العالمية للمعلومات.

والملاحـــظ أن هذا التقسيم الذي إعتمده هذا الإتجاه من الفقه، يتماشى مع تقسيمه للجرائم عبر الكمبيوتر[1]،والتي يعتبرها جرائم لها علاقة بالكمبيوتر والشبكة المعلوماتية والأنترنت، فهي لذلك تشمل نوعين من الجرائم:

جرائـــم الشبكة العالميةweb computer crime: وهي جرائم يستخدم فيها كل من الكمبيوتر والشبكة والأنترنت كوسيلة مساعدة لإرتكاب الجريمة، وإن كان إستخدام الكمبيوتر والأنترنت لا يعتبر من طبيعة الفعل الإجرامي، إلا أن جهاز الكمبيوتر مع ذلك يظل محتفظا بآثار رقمية يمكن أن تستخدم للإرشاد عن الفاعـــل.

-**جرائم الكمبيوتر** computer crime: وهي تشمل الجرائم التي يكون الكمبيوتر فيها محلا للفعل الإجرامي نفسه، سواء شمل ذلك المكونات المادية أو المعنوية أو قاعدة المعطيات والمعلومات التي قد يكون على الشبكة العالمية، وتشمل تلك الجرائم إنتهاك الملكية الفكرية، جرائم القرصنة، والهاكرز الفيروسات وغيرها.

إذا ما لاحظنا التقسيمات السابقة، فإننا نرى ودون عناء، بأنها تقسيمات غير دقيقة ومنضبطة علىالإطلاق، ذلك أن أدلة الشبكات ذاتها هي عبارة عن حلول وبرمجيات وبروتوكولات مدمجة في نظام الكمبيوتر، ويعدهذا المعيار غير صحيح البتة إذا ما علمنا أن شبكة المعلومات العالمية هي الأنترنت.

كما قسمها البعض من حيث طبيعتها إلـــــى[2]:

1-أدلة مرتبطة بوظائف الجهاز الرقمي: وهذا النوع من الأدلة الإلكترونية يمكن إجمالها فيمايلي:

-المعطيات التي أنشات بواسطة الجهاز الرقمي بشكل تلقائي، حيث تعتبر هذه المعطيات من مخرجات الجهاز الرقمي التي لم يساهم الإنسان في إنشائها مباشرة مثل: ملفات الدخول، التي يتم فيها حفظ جميع التغييرات التي تحصل في قاعدة المعطيات log filesوسجلات الهاتف phone recordوفواتير أجهزة السحب الآلي ATM BILLS.

-المعطيات المحفوظة بالإدخال داخل الجهاز الرقمي، وهي المعطيات المكتوبة والتي يساهم الإنسان بإدخالها قبل أن يقوم بحفظها داخل الجهاز الرقمي، مثل البريد الإلكتروني، ورسائل غرف المحادثة على الأنترنت.

-المعطيات التي يتم حفظ جزء منها بالإدخال ويتم إنشاء جزء آخر منها بواسطة الجهاز الرقمي، مثل أوراق العمل المالية في برنامج exelوالتي تكتسب محتواها بالإدخال قبل أن تتم معالجته تلقائيا بأدوات البرنامج ذاته و إعطائه محتوا جديد من خلال إجراء عمليات حسابية على المدخلات.

---

[1]-**د. ممدوح عبد الحميد عبد المطلب**،إستخدام بروتوكول (*tcp/ip*) في بحث وتحقيق الجرائم على الكمبيوتر، المرجع السابق، ص6.

[2]-**ميسرة خالد الحمد**، الدليل الرقمي ومعايير جودته في الإثبات الجنائي، الطبعة الأولى، مركز الكتاب الأكاديمي، عمان، 2014، ص30. **طارق محمد الجملي**، المرجع السابق، ص6.

2-أدلة مرتبطة بسلوك المجرم

وهذا النوع من الأدلة ينشأ دون إرادة الشخص، أي أنها أثر يتركه الجاني دون أن يكون راغبا في وجوده، ويسمى هذا النوع من الأدلة بالبصمة الرقمية، وهي ما يمكن تسميته بالآثار المعلوماتية الرقمية وهي تتجسد في الآثار التي يتركها مستخدم الشبكة المعلوماتية بسبب تسجيل الرسائل التي يرسلها أو يستقبلها، وكافة الإتصالات التي تتم من خلال الجهاز الرقمي أو شبكة المعلومات الرقمية[1].

وفي الواقع فإن هذا النوع من الأدلة لا يشكل بالضرورة مادة للحفظ من قبل من صدر عنه، غير أن الوسائل الفنية الخاصة تمكن من ضبطها ولو بعد مرور زمن على إنشائها، فالإتصالات التي تجري عبر شبكة المعلومات، والرسائل الإلكترونية التي يرسلها أو التي يتلقاها الشخص، وأية تحركات رقمية يمكن أن يتم السيطرة عليها والتحكم بها لاحقا بالوسائل الفنية.

والملاحظ أن هذا التقسيم الذي إعتمده الفقه مأخوذ من تقسيم وزارة العدل الأمريكية للدليل الإلكتروني.

ثانيا-محاولات وزارة العدل الأمريكية لتقسيم الدليل الإلكتروني

وفقا لوزارة العدل الأميركية (2002)، فإن الدليل الإلكتروني يمكن تقسيمه إلـــى ثلاث مجموعات وهيكالتالي:

1-السجلات المحفوظة في الحاسوب: وهي الوثائق المكتوبة والمحفوظة مثلالبريد الالكتروني وملفات برامج معالجة الكلمات ورسائل غرف المحادثة علىالانترنت.

2 _السجلات التي تم إنشاؤها بواسطة الحاسوب: وتعتبر مخرجات برامج الحاسوبوبالتالي لم يلمسها الإنسان مثل*log files*وسجلات الهاتف وفواتير أجهزة السحب الآلي*.ATM*.

3-السجلات التي جزء منها تم حفظه بالإدخال وجزء آخر تم إنشاؤه بواسطةالحاسوب: ومن الأمثلة عليها أوراق العمل المالية التي تحتوي على مدخلات تم تلقيمهاإلى برامج أوراق العمل مثل*Excel*ومن ثم تمت معالجتها من خلال البرنامج بإجراءالعمليات الحسابية عليها.

والقضاء الأمريكي يأخذ بهذا التقسيم، فسجلات الحاسوب المقبولة إستثناء أمام القضاء الأمريكي هي المعدة في هيئة ملفات text وفقا للمادة 803-6 من قواعد الإثبات الفدرالية، ويتم التمييز في إطارها بين سجلات الحاسوب المخزنة وسجلات الحاسوب المتوالدة، والفرق بينهما يتوقف على ما إدا كان الشخص أو الآلة تصنع محتويات السجلات، فالسجلات المخزنة على الحاسوب والتي تشير إلى وثائق تحتوي على كتابات شخص أو عدة أشخاص وحدث وصارت في شكل إلكتروني أو مراسلات البريد الإلكتروني أو ملفات معالجة الكلمات أو رسائل غرف المحادثة على الأنترنت، وعلى العكس تحتوي سجلات الحاسوب المتوالدة على مخرجات برامج الحاسوب التي لم تمسها أيد البشرية مثل سجلات الدخول على الأنترنت ومصدرها مزود خدمة الأنترنت، وسجلات الهاتف وايصالات ATM ، فهي تميل إلى أن تكون سجلات حاسوب متوالدة،

[1]-**Henry, J.F**, "Testimony before permanent Subcommittee On Governmental Affairs, The UnitedStates Senate, Ninety, Ninth Congress, 1984.available athttp://www.igc.apc.org/nemesis/aclu/nudishallof shame/henry.html

وهي لا تحتوي على معطيات بشرية، ولكن فقط مخرجات برنامج الحاسوب المصمم لمعالجة مدخلا الحاسوب تم تعريفها بلغة جبرية[1].

وهناك نوع ثالث من السجلات يجمع بين التدخل الإنساني ومعالجة الكمبيوتر: كما لو أدخل متهم معطيات معينة وطلب من الكمبيوتر أن يقوم بمعالجتها توصلا إلى نتائج يسمح بها البرنامج المستخدم، كمن يتهرب من الضرائب فيقوم بتسجيل معطيات غير صحيحة عن دخله وربحه طالبا من الكمبيوتر حساب الضريبة المستحقة[2].

والذي يلاحظ على هذا التقسيم أنه يقصر مفهوم الدليل الإلكتروني على المعلومات التي يتم إستخراجها من الحاسب الآلي، والتي تكون على شكل **نصوص**، وهو ما يتعارض ومفهوم الدليل الإلكتروني من كونه قالب يحتوي في داخله مجموعة المعطيات الرقمية، تصلح منفردة أو مجتمعة لكي تكون دليلا للإدانة أو للبراءة، تتضمن نصوصا وصورا وسمعيات ومرئيات وغيرها.

تلك كانت أهم محاولات تقسيم الدليل الإلكتروني، ولأننا أوردنا ملاحظات حول كل منها، فإننا نكتفي بالقول أن تقسيم الدليل الإلكتروني يستدعي مرونة كبيرة كونه من الأدلة المتطورة بطبيعتها بتطور الجرائم محل الدراسة حتى يصلح لإثباتها، وتطور البيئة ذاتها التي يعيش فيها هذا الدليل والذي يكاد يكون تلقائيا يتسع لإمكانية شمول مظاهر رقمية جديدة.

وليس المقصود بالتطور إكتشاف أدلة جديدة، وإنما تطور وسائل الحصول عليه، وفي كل الأحوال يبقى الدليل إلكترونيا، فإن إتخذ مظهرا آخر فإن إعتراف القانون به يكون مؤسسا على طابع إفتراضي مبناه أهمية الدليل الإلكتروني ذاته وضرورته، إلا أنه لكي يحدث تواصل بين القانون والدليل المذكور فإنه يلزم إتخاذ مسلك الإفتراض من حيث إعتباره دليلا أصليا[3].

المطلب الثاني

خصائص الدليل الإلكتروني

نظرا للطبيعة الخاصة للجرائم الواقعة على التعاملات الإلكترونية التي إستمدتها من طبيعة البيئة الإفتراضية التي وقعت في إطارها، فإن دليل إثباتها يتميز بجملة من الخصائص التي تميزه عن الدليل الجنائي التقليدي، سواء من حيث طابعه التقني(الفرع الأول) أو بعده المادي والإلكتروني(الفرع الثاني)، أوصعوبة التخلص منه(الفرع الثالث).

---

[1]-**عمر محمد أبو بكر بن يونس** ، الإجراءات الجنائية عبر الأنترنت في القانون الأمريكي، المرجع السابق، ص422. ولنفس المؤلف:**الجرائم الناشئة عن إستخدام الأنترنت**، المرجع السابق، ص981.

[2]– **د. شيماء عبد الغني**، المرجع السابق، ص409.

[3]–**د.عمر محمد بن يونس**، مذكرات في الإثبات الجنائي عبر الأنترنت، ندوة الدليل الرقمي، مرجع سابق، ص12.

الفرع الأول

الطبيعة التقنية للدليل الإلكتروني[1]

فالدليل الإلكتروني دو طابع تقني كونه مستنبط من البيئة التي يعيش فيها وهي البيئة التقنية، وهي في إطـــار جرائم الإعتداء على التعاملات الإلكترونية ممثلة في الحيز الإفتراضي(النظام التراسلي، نظام التخزين) وهي بيئة المكان الإفتراضي والزمان الإفتراضي، هذه البيئة ممثلة في الأقراص بأنواعها بالإضافة إلى معالجـــات حركة البرامج والذاكرة، وكل قطعة يمكن أن تقوم بدور في هذا الشأن بما في ذلك القطع المرنة التي لا يعمل النظام بدونها، مثل نظام التشغيل والبرمجية التي تعمل على تنفيد أوامر تشغيل الملفات التي وضعها الإنسان، فضلا عن نظام الحزم التراسلية التي يمكن من خلالها التوصل إلى الدليل الإلكتروني[2].

وهذا يعني أنه كدليل يحتاج إلى بيئته التقنية التي يتكون فيها، لكونه من طبيعة تقنية المعلومات، ولأجـــل ذلك فإنما ينطبق على الدليل العلمي ينطبق على الدليل الإلكتروني، فالدليل العلمي يخضع لقاعدة لزوم تجاوبه مع الحقيقة كاملة وفقا لقاعدة في القضاء المقارن "أن القانون مسعاه العدالة أما العلم فمسعاه الحقيقة".

وإدا كان الدليل العلمي له منطقه الذي يجب ألا يخرج عليه من حيث يجب عدم تعارضه مع القواعد العلمية السليمة، فإن الدليل الإلكتروني له ذات الطبيعة، إذ يجب ألا يخرج عما توصل إليه العالم الرقمي وإلا فقد معناه.

الفرع الثاني

البعد المادي والإلكتروني للدليل الإلكتروني

إذا كان مبدأ لوكارد ينطبق على أي تواصل يحدث في مسرح الجريمة بين المتهم والضحيةـــ أو بين الأشخاص ومسرح الجريمة، فإنه ينطبق على الجرائم الواقعة على التعاملات الإلكترونية، ليس فقط في الركن المادي لها كلوحة المفاتيح حيث يترك بصماته مثلا، وإنما يحدث إنتقال بين الدليل المادي والإلكتروني، أي حصول تعاون بين البعدين التقليدي والإلكتروني في التحقيق الجنائي، وبالتالي فإن وسائل التحقيق التقليدية تعمل بشكل مشترك مع وسائل التحقيق الرقمية في فهم الجرائم محل الدراسة وتحليلها.

---

[1]-**د.عمر محمد بن يونس**، الدليل الرقمي، المرجع السابق، ص45. **ولنفس المؤلف:** الجرائم الناشئة عن إستخدام الأنترنت، المرجع السابق، ص977.

[2]-**د.عمر بن يونس**، الدليل الرقمي، المرجع السابق، ص32.

الفرع الثالث

صعوبة التخلص من الدليل الإلكتروني[1]

على خلاف الأدلة التقليدية التي كثيرا ما كانت أجهزة العدالة تعاني من مسألة التخلص منها ، كالتخلص من الأوراق التي تحمل إقرارات معينة بتمزيقها أو حرقها، والتخلص من الشهود بقتلهم أو تهديدهم بعد الإدلاء بشهادتهم، ففي هذه الحالات يكون من الصعب إن لم يكن مستحيلا إسترجاع أو إسترداد هده الأدلة، فإن الأمر مختلف[2]فيما يخص الدليل الإلكتروني، حيث يصعب التخلص منه، وهذه الميزة من أهم مزايا الدليل الإلكتروني على الإطلاق وهو في ذلك يتشابه مع الدليل الجيني أو ما يطلق عليه بـــ DNA.

هذه الخاصية لا تسري على الدليل الإلكتروني فقط، بل على كافة ما يتعلق بهيكلة الحوسبة والرقمية، ذلك أنه كلما حدث إتصال بتكنولوجيا المعلومات في معنى إدخال معطيات إلى ذلك العالم input فإنه من الصعب التخلص منها ولو كان ذلك باستخدام تعليمات delete أو erase أو حتى في حالة إعادة تهيئة القرص الصلب format وغيرها[3]، لا تشكل عائقا يحول دون إسترجاع هده الملفات كليا أو جزئيا التي تم إلغائها أو إزالتها من الحاسوب، والأمر نفسه فيما لو تم إتلافه، أو إخفائه، حيث يمكن إصلاحه وإظهاره، ذلك أنه هناك الكثير من البرامج المتخصصة التي يتم بمقتضاها إسترداد هذه المعطيات، كبرنامج photorecو recuva, Pandora recovery , glary undelete .[4]وهذا يؤكد مبدل لوكارد كون الأثر الإلكتروني لا يمكن إخفاءه بالكامل.

بل أنّ نشاط الجاني لمحو الدّليل(فعل الجاني لمحو الدليل) يشكّل دليلاً، فنسخة من هذا الفعل يتمّ تسجيلها في الكمبيوتر ويمكن استخلاصها لاحقًا كدليل إدانة ضدّه.

المطلب الثالث

مشكلات الدليل الإلكتروني

لقد زادت الطبيعة الخاصة للدليل الإلكتروني من أهمية الإستعانة بالخبرة كإجراء مهم للحصول على الدليل الإلكتروني إزاء نقص معرفة رجال إنفاذ القانون للجوانب التقنية لنظم التخزين والتراسل، إلا أنها في المقابل

---

[1]-**د. ممدوح عبد الحميد عبد الطلب, زبيدة محمد جاسم وعبد الله عبد العزيز**، نموذج مقترح لقواعد إعتمـــاد الدليل الرقمي للإثبات في الجرائم عبر الكمبيوتر، المرجع السابق، ص2240. **د.عمر محمد بن يونس**، الدليل الرقمي، المرجع السابق، ص47 وما بعدها.

[2]

[3]–فقد قضي "عندما يتم حذف ملف حاسوبي فإن محتوى الملف يمكن إسترداده، ذلك أن المساحة التي كان يشغلها الملف تظل كما هي متاحة، ومالم يتم شغلها من قبل ملف آخر فإن الملف الذي تم حذفه يمكن إسترداده بإستخدام أداة إستردادية للملفات المحذوفـــة، كذلك يمكن التعرف على تاريـــخ نشـــــأة الملف وآخر تعديل عليه وآخر مـــرة تم فتحه فيها":د.**عمر بن يونس**، الدليل الرقمي، المرجع السابق، ص47.

[4]–لمزيد من التفاصيل حول هذه البرامج أنظـــر المـــوقع التـــالي:

http://www.arabes1.com/2016/03/best-files-Data-Recovery-Software-free.html

جعلت من عملية الإنفاق تتسع إلى أبعد مدى، فإذا توافرت منظمات متخصصة كالجامعات والمعاهد وأمكن توافر تقنية رقمية في هذا الصدد، فإن التكاليف يمكن أن تكون أقل من أن يتم عرض الأمر على شركات أو منظمات أجنبية في الخارج مما يجعل التكاليف تخضع للسعر العالمي المقرر في اللوائح المالية لتلك المنظمات[1]، ومن ذلك شركة sirchie[2].

ولاتقف مشكلات الدليل الإلكتروني عند حد إرتفاع تكاليف الحصول عليه، بل تتعداها إلى مشاكل أخرى البعض منها ذات طبيعة موضوعية داخلية(الفرع الأول) والأخرى إجرائية على المستوى الدولي(الفرع الثاني).

الفرع الأول

مشكلات الدليل الإلكتروني على المستوى الداخلي

ويقصد بها المشكلات التي تتعلق به تحديدا من حيث تكوينه، سواء من حيث نطاق تخزينه، أو ظرفيته أو عدم رؤيته أو طبيعته الهشة، أو مشكلة الأصالة.

أولا- الدليل الإلكتروني والتخزين الرقمي:

معلوم أن التخزين هو البيئة التي تتصف بها الحوسبة والإتصالات بإعتبار أنها تعد إمتيازا في هذا المجال، فالبيئة الرقمية تعد مجالا حيويا ضخما يمكنه تخزين مليارات المعطيات، والقدرات التخزينية في البيئة الرقمية، وهي تستوعب هذا الكم الهائل من المعطيات لم تتفاعل كليا مع القانون الجزائي، حيث لم يتم التوصل تماما إلى إمكانية قيامها بعملية فرز ذاتية داخلية للملفات البريئة وتلك المجرمة والتي تعد موضوعا للدليل الجنائي الإلكتروني، وذلك على الرغم من وحدة التفاعل الرقمي الجبري في العملية التي يقوم بها الحاسوب بإستخدام االلوغارثميات، بل وأبعد من ذلك ففي بعض الحالات يمكن أن يكون الملف البريء ستارا للملف المجرم[3].

وهذا الذي سلف شكل هاجسا في إطار القواعد التقليدية، وبما يعني أن مثل هذا الأمر يعطي الحق في التفتيش العام الذي ينتهك حق الخصوصية للمتهم أو الحائز للنظام، ولكي يمكن الخروج من هذا المأزق لا بد من وضع غطاء من المشروعية يبرر ذلك، وعلى ذلك نرى أنه يتعين على المشرع أن يتدخل لسن قاعدة

---

[1]-**د. عمر بن يونس**، الجرائم الناشئة عن إستخدام الأنترنت، المرجع السابق، ص984.

[2]- هي عبارة عن شركة تتولى تقديم حلول عالية الجودة للتحليل الرقمي للمختبر الجنائي، والتي تساعد التحقيقات بدءا من مسرح الجريمة وحتى قاعات المحاكم، بما يشمل تقديم الأساليب اللازمة لإستخلاص المعلومات من الأجهزة الإلكترونية المختلفة، فضلا عن طرق التغليف اللازمة لضمان النقل الآمن للجهاز إلى مختص الفحص الرقمي. http://www.sirchie.com/

[3]-**د.عمر محمد أبو بكر بن يونس** ، الإجراءات الجنائية عبر الأنترنت في القانون الأمريكي، المرجع السابق، ص24.

قانونية إجرائية ينظم فيها الوضع القانوني لتفتيش وضبط المعطيات التي لم يتم معرفة موقعها أو إسم الملف المخزن داخل النظام.

ثانيا– الدليل الإلكتروني دليل ظرفي:

ذلك أن برتوكول IP وحدة معلوماتية تحتوي معلومات عن الحاسوب وليس عن الأشخاص، ولذلك فمن الصعوبة إثبات أن شخصا محددا أحدث الفعل غير المشروع، إذ من الممكن ألا يكون هو مرتكب الجريمة حقا كما لو كان حاسوبه مسروقا أو مؤجرا أو أن يكون عنوانه الرقمي مسروقا أو مختلسا أو أن يكون أحد إستخدمه إحتيالا، ففي هذه الحالة يمكن إستخدامه **كقرينة قضائية** ضد مالك الجهاز إلى أن يثبت العكس، وقد يحتاج الأمر إلى مثابرة من جهات الإستدلال والتحقيق لكي يتوافر لها دليل مادي كالإعتراف أو الشهادة أو الخبرة...[1].

لذلك فإن منطق التعامل مع الأدلة الإلكترونية، يحتاج إلى البحث في الأدلة التقليدية في ذات الوقت، ويلزم هنا أن يكون كل منهما يقطع بوجود الآخر، حتى في فرضية عدم إعتبار هذه القاعدة قاعدة مطلقة[2].
كما أن ظهور بعض الأنظمة كنظام IPV[3] وعمليات التخفي أثناء التجوال عبر الشبكة وإستخدام الشبكة من مقاهي الأنترنت التي تقوم عادة بإعادة تشكيل الأجهزة قد زاد في صعوبة تعقب المعطيات غير المشروعة.

حتى أن السباق بين الشركات التي توفر خدمة الدخول على الأنترنت في مجال إسترجاع المعلومات، وبالتالي تسليم معطيات تسجيل الدخول التي تم الحصول عليها مند فترة وجيزة يمكن أن يكون قد فات الآوان على الإستفادة منه،في هذا الخصوص تم تبني التوجيه رقم CE-24-2006 [4] الصادر عن البرلمان الأروبي والمجلس المنعقد في 15 مارس 2006 حول حفظ ومعالجة المعطيات في إطار توفير خدمات الإتصالات الإلكترونية المتاحة للجمهور أو شبكات الإتصالات العامة التي تلزم موردي خدمة الدخول على الأنترنت بتخزين معطيات الحركة على هذه المواقع وتحديدها لفترة تزيد عن 6 أشهر، وذلك من قبل 26 دولة في الإتحاد الأروبي، ففي بلجيكا فإن معطيات حركة السير يتم الإحتفاظ بها لمدة 12 شهرا إبتداء من تاريخ الإتصال، وكذلك هو الشأن في ألمانيا، بلغاريا، إيطاليا وغيرها[5]، أما الوضع في فرنسا فقد كان قد صدر المرسوم رقم 2006–358 المؤرخ 24 اذار/مارس 2006 المتعلق بحفظ الرسائل الالكترونية الذي أعقب القانون رقم 2006–64 المؤرخ 23 كانون الثانى/يناير 2006 بشأن مكافحة الارهاب، والذي جاء متوافقا مع التوجيه السابق.

---

[1]- **د. عمر محمد أبو بكر بن يونس** ، الدليل الرقمي، المرجع السابق، ص64.

[2]– **د.عمر محمد أبو بكر بن يونس** ، الجرائم الناشئة عن إستخدام الأنترنت، المرجع السابق، ص994.

[3]–البروكسي، أو الشبكة الافتراضيـــة الخاصةVPN، تُظهر عنوان آي بي مختلف لاتصالك بالإنترنت، وعادة ما يكون عنوانًا مستعارًا من منطقة مختلفة في البلد أو العـــالم.

[4]- **Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE**

[5]- https://www.senat.fr/rap/l04-201/l04-2014.html

وعلى ذات النهج سار المشرع في الجزائر، حيث ألزم مقدم الخدمة بحفظ المعطيات المتعلقة بحركة السير بموجب المادة 11 من القانون رقم 09-04.

ثالثا-الدليل لإلكتروني دليل غير مرئي:

ذلك أن المستندات والمعطيات المحفوظة في النظم أو التي تتداول عبرها والتي من خلالها تتم التعاملات الإلكترونية، تكون في هيئة رموز ونبضات الكترونية، والجرائم التي ترتكب عليها تعتمد في موضوعها على الرموز السرية والتشفير مما يصعب أن تخلف وراءها أثار مرئية، فكل ما تتركه التقنية هو 0 ،1 تدور في السجلات إلكترونية داخل النظام.وهو ما يصعب من قدرة الجهات التي تتعامل مع هذه الجرائم في فحص وإختبار المعطيات محل الإشتباه[1] .

رابعا-الدليل الإلكتروني من الأدلة الهشة بطبيعتها:

إذ أنه يمكن أن يتعرض لصدمات التعديل فيه على أية شاكلة، سواء كان مقصودا من قبل الجاني، أو غير مقصود من قبل المحقق أو الخبير المعلوماتي أثناء عملية جمعه، أو كان ذلك خلال فترة حفظه.

فإن كانت عملية الحفظ تتواجد مع عملية حفظ العتاد الذي يحمله، فإن هذا الأمر يصبح سهلا أو صعبا بحسب البيئة التي يتواجد فيها باستمرار، ففي حين تكون سهلة المنال في حالة التخزين فإنها تصبح صعبة في حالة التحفظ على البيئة الرقمية ككل حال وجود الدليل الإلكتروني في بيئة حركية(نظام التراسل)[2] وهي البيئة التي تميز التعاملات الإلكترونية، فما يحكم التعامل الإلكتروني أصالة هو النظام التراسلي.

ولا يدق هذا المشكل خلال فترة حفظ الدليل الإلكتروني مما قد ينال من صحته عند عرضه على القضاء، بل يتعداه إلى المرحلة السابقة عليه وهي الحصول عليه، إذ يمكن أن يحصل هناك خطأ في الحصول عليه بسبب خطأ في إستخدام الأداة المناسبة بسبب خلل في الشفرة المستخدمة أو إستخدام مواصفات خاطئة مما ينتج عنه خطأ في إستخلاص الدليل الإلكتروني[3]. ولاشك أن الخبرة تلعب دورا مهما في هذه الحالة.

فمثلما يخضع الدليل الإلكتروني لقواعد قانونية تحكم طرق الحصول عليه، فإنه يخضع لوسائل تقنية تمكن من التأكد من مصداقيته، كإستخدام فكرة التحليل التناظري من خلال مقارنة الدليل الإلكتروني بالأصل المدرج بالنظام المعلوماتي،. ذلك أنه من القواعد المهمة في التعامل مع الأدلة والآثار الإلكترونية، أنه لا يجوز أن يتم الفحص على النسخة الأصلية للدليل، حيث يتم عمل نسخة طبق الأصل بإستخدام أدوات خاصة، وترك النسخ الأصلية لفحص أي تغير يمكن أن يكون قد طرأ على الدليل أثناء عملية التحليل والمعالجة[4]. أو

---

[1] -**د. علي محمود علي حمودة** ، المرجع السابق، ص16.

[2] – **د. عمر محمد أبو بكر بن يونس** ، الدليل الرقمي، المرجع السابق، ص168.

[3] – **طارق الجملي**، المرجع السابق، ص26.

[4] -**Eoghan Casey**, op, cit, p25.

د. طارق عبد الرؤوف الخن، المرجع السابق، ص343. **د. ممدوح عبد الحميد عبد المطلب**،إستخدام بروتوكول (*tcp/ip*) في بحث و تحـــــقيق الجرائم على الكمبيوتر، المرجع السابق، ص8.

إستخدام الدليل المحايد للتأكد من سلامته من العبث، أما للتاكد من سلامة الإجراءات المتبعة في الحصول عليه فيتم إستخدام مايعرف باختبارات(داو بورت)[1] من خلال إخضاع الأداة المستخدمة لإختبارات السلبيات الزائفة وإختبار الإيجابيات الزائفة.

خامسا- مشكلة الأصالة في الدليل الإلكتروني:

إن الأصالة في طابعها الإلكتروني ليست سوى تعداد غير محدود لأرقام ثنائية موحدة في الصفر والواحد (0،1) فالصورة في العالم الإلكتروني مثلا ليس لها ذلك الوجود المادي الذي نعرفه في شكل ورقي بل مجموعة من الأرقام التي ترجع إلى أصل واحد هو الرقم الثنائي المشار إليه.

إن الأصالة لها طابعها الخاص حين التعامل مع الدليل الإلكتروني، فطبيعة هذا الأخير لا تعبر عن قيمة أصلية بمجرد رفع محتواه من النظم حيث يتواجد في كل مكان يتم إستدعائه منه، وتطرح مشكلة الأصالة نفسها بقوة، إذا ما علمنا أن الدليل المستنبط في هذا الإطار مستوحى من قاعدة مجهولة، أو خوادم غامضة ليس من السهولة التوصل إليها، كما يمكن إزالة الدليل الإلكتروني عن بعد ويكون ما تبقى منه هو نسخة فقط يمكن التوصل إليها.

إن بحث موضوع الأصالة على المستوى القانوني جعل المشرع المقارن يعتمد منطق إفتراض أصالة الدليل الإلكتروني، فالإفتراض هنا كان قانونيا فقط.

وقد كان التشريع الأمريكي من أوائل التشريعات التي إهتمت بموضوع الأصالة في الدليل الإلكتروني، وقد برز ذلك عند وضع قانون الإجراءات المدنية الفيدرالي، فقد قامت اللجنة التحضيرية بتعديل تعريف الوثيقة لكي ينضم إليها إعترافا بالمعلومات الرقمية، كما تم وضع نص صريح في قانون الإجراءات الجزائية في القاعدة 1001 بند 3 حيث يسمح إستثناء بقبول الدليل الإلكتروني بإعتباره مستندا أصليا مادام أن المعطيات صادرة من كمبيوتر أو جهاز مماثل وسواء كانت هذه المعطيات مطبوعة أو مسجلة على دعامات أخرى ومقروءة للعين المجردة و تعبر عن المعطيات الأصلية بشكل دقيق، ويستتبع ذلك أن مخرجات النظام تتساوى من حيث الأصالة مع الكتابة المادية على الرغم من أن طبيعة الكتابة على النظام تجعل من المخرجات مجرد نسخ للأصل الموجود رقميا في النظام المعلوماتي أو نظام الإتصالات الإلكترونية[2].

والواقع من الأمر أن الصراع التكنولوجي على أشده في هذه الناحية بالنسبة للدول التي لم تأخذ حقها في تقنين هذا النوع من الأدلة، وهو صراع قد يأخذ الوضعية الجوهرية حين عرضه على القضاء، ومثل هذا الأمر جعل المشرع الجزائري يتبنى منطق الإفتراض القائم في طبيعة الدليل الإلكتروني، حين إعتبر ناتج المراقبة الإلكترونية، نسخ المعطيات محل التفتيش ولو عن بعد مهما كان شكلها صورا أو مستندات أو غيرها دليلا يقبل طرحه على القضاء ليقول كلمته فيه حتى لو كانت تتميز بالصفة الرقمية أصالة.

---

[1]- ترجع أصول هذا الاختبار (اختبارات داو برت) للحكم الذي أصدرته المحكمة العليا الأمريكية في قضية داو بورت ضد ميريل دو للصناعات الدوائية 1993 ، **د. ممدوح عبد الحميد عبد المطلب، زبيدة محمد قاسم، عبد الله عبد العزيز**، مرجع السابـــق،ص2248.

[2]-**د عمر محمد أبو بكر بن يونس** ، الجرائم الناشئة عن استخدام الأنترنت، المرجع السابق، ص986.

الفرع الثاني

مشكلات الدليل الإلكتروني على المستوى الدولي

لا تقف مشكلات الدليل الإلكتروني به تحديدا من حيث هو، بل تمتد لتشمل ضبطه والبحث عنه خارج حدود الدولة في نطاق إقليمي لدولة أخرى، وهذا كلّه يصطدم بمشاكل الحدود والولايات القضائيّة، لما ينطوي عليه من مساس بسيادة هذه الدولة الّتي عبر من خلالها نشاط المجرم وهو في طريقه للهدف،أو حيث قد توجد أدلّة الجريمة.

وإن كانت الدول قد أصدرت تشريعات نظمت التعاملات الإلكترونية، وضمنتها نصوصا جزائية وإجرائية، تعالج كيفية الحصول على الدليل الإلكتروني في تلك الجرائم، فإنها تبقى بذلك غير كافية لمواجهة هذه الجرائم المستحدثة، فالطبيعة الديناميكية للدليل الذي يصلح لإثباتها والتي إستمدها من الطبيعة الدولية لهذه الجرائم جعل منها شأنا دوليا، فمساحة مسرح الإعتداءات المعلوماتية لم تعد محلية بل أصبحت دولية، مما تطلب وجود تعاون دولي لتسهيل الإجراءات الجزائية بين الدول والتغلب على عقبة السيادة. وذلك عن طريق الإتفاقيات والمعاهدات الدولية التي تمثل قانونا عاما في هذا الصدد.

ومن أولى الإتفاقيات التي تعمل على التعاون الدولي في مجال مكافحة هده الجرائم إتفاقية بودابست لسنة 2001، فقد وضعت هذه الإتفاقية إطارا عاما **للتعاون الدولي** في هذا الشأن بموجب الباب الثالث، حيث جاء متضمنا في ذلك مباديء تتعلق بتسليم المجرمين، وأخرى تتعلق بالمساعدة المتبادلة وبالإجراءات المتعلقة بطلبات المساعدة المتبادلة في حالة عدم وجود إتفاقيات دولية واجبة التطبيق، والمساعدة المتبادلة بشأن الإجراءات التحفظية.

أما عن الجهود العربية فقد أسفرت هي الأخرى عن ميلاد الإتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر سنة 2010 وذلك لتعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة هذهالجرائم، ولدرء أخطارها حفاظا على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها، وقد خصصت الفصل الرابع منها للتعاون القضائي والقانوني.وقدصادقت عليها الجزائر بمقتضى المرسوم الرئاسي رقم 14–252 المؤرخ في 8 سبتمبر 2014، وأصبحت مطالبة بالإلتزامات التي تفرضها الإتفاقية على الدول الموقعة عليها في شأن التعاون لمكافحة الجريمة المتصلة بتكنولوجيات الحوسبة والإتصال.

وإلى جانب الإتفاقيات الدولية، فإن التعاون القضائي الدولي من أهم صور التعاون الدولي في مجال الجرائم العابرة للحدود ومنها الجرائم الواقعة على التعاملات الإلكترونية، ولعل من أهم آلياته هو المساعدة القضائية المتبادلة لما لها من دور في التوفيق بين حق الدولة في ممارسة إختصاصها الجزائي داخل إقليم

الدولة وحقها في توقيع العقاب[1].فالحراك الدولي الذي يتميز به الجناة والإستفادة من التكنولوجيات المتقدمة هما عاملان من ضمن عوامل أخرى تجعل من الضروري أكثر من أي وقت مضى أن تلجأ سلطات إنفاذ القانون والسلطات القضائية إلى التعاون في العمل وتقديم المساعدة إلى الدولة صاحبة الولاية القضائية على المسالة المعنية.

وبغية تحقيق هذا الهدف تعمد الدول إلى تشريع قوانين تجيز لها تقديم ما يلزم للتعاون على الصعيد الدولي، كما تلجأ بإزدياد إلى إبرام معاهدات بشأن تبادل المساعدة القضائية في المسائل الجزائية. وهو ما أنتهجته الجزائر، فبالرجوع إلى المادة 16 من قانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الحوسبة والإتصال ومكافحتها، نجدها تنص "في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المشمولة بهذا القانون وكشف مرتكبيها، يمكن للسلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني"، وذلك إذا لم يكن من شأنها المساس بالسيادة الوطنية أو النظام العام[2].

كما حثت الإتفاقية العربية لمكافحة الجرائم المتصلة بتكنولوجيات الحوسبة والإتصال على تقديم المساعدة والتنسيق فيما بين الدول لغايات التحقيقات أو الإجراءات المتعلقة بالجرائم في هذا الشأن أو لجمع الأدلة الإلكترونية[3]. وهو نفس ما فرضته الإتفاقية الأروبية بمقتضى المادة 25.

وللمساعدة القضائية المتبادلة بين الدول الأطراف في الجرائم الواقعة على التعاملات الإلكترونية مجالات عديدة:

أولا- المساعدة المتبادلة في مجال الإجراءات التحفظية:

وهي من الإجراءات الهامة على المستوى الدولي للحفاظ على الدليل الإلكتروني إلى حين إستكمال الإجراءات المتطلبة لإستخراجه. ومن أهم هذه الإجراءات التحفظ العاجل على المعطيات المخزنة، وهو ما كرسته المادة 37 من الإتفاقية العربية والمادة 29 من اتفاقية بودابست، حيث بمقتضى هذه الآلية يحق لأي دولة أن تطلب من دولة أخرى الحصول على التحفظ العاجل على المعلومات المخزنة في النظام الموجود في أراضي الدولة المطلوبة إليها على وجه السرعة، بخصوص ما تريد الدولة الطالبة للمساعدة أن تقدم طلبا بشأنه للمساعدة المتبادلة للبحث وضبط وتأمين وكشف المعلومات. وهو ما أشار إليه المشرع الجزائري في المادة 17 من القانون رقم 09-04 والذي عبرت عنه بـــ "...أو **إتخاد أي إجراءات تحفظية وفقا...**"

---

[1]-د. **أحمد إبراهيم مصطفى سليمان**، الإرهاب والجريمة المنظمة، دار الطلائع للنشر والتوزيع والتصدير،القاهرة، 2006، ص394.

[2]-المادة 18 من القانون 09-04 المؤرخ في 14 شعبان 1430 الموافق لـــ 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الحوسبة والاتصال ومكافحتها،جريدة رسمية، عدد 47، لسنة 2009.

[3]-المادة 32 من الإتفاقية العربية لمكافحة الجرائم المتصلة بتكنولوجيات الحوسبة والإتصال، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، جريدة رسمية، عدد57، لسنة2014.

وقد وضعت إتفاقية بودابست سقفا زمنيا لصلاحية طلب التحفظ وحددته بـــ 60 يوما على الأقل، وهي نفس الفترة التي حددتها الإتفاقية العربية محددة بذلك في طلب الحفظ أن يشمل السلطة التي تطلب الحفظ وموجباته، والجريمة موضوع التحقيق وملخصا للوقائع، فضلا عن المعلومات التي يجب حفظها وعلاقتها بالجريمة.

ويثور التساؤل حول مدى تلبية الدولة إجراء حفظ معطيات تخص جرائم واقعة على تعاملات إلكترونية غير مجرمة لديها؟

لقد أجابت عن هذا التساؤل المادة 29 من إتفاقية بودابست[1] والمادة 37 من الإتفاقية العربية، عندما نصتا على أنه عند إستلام الطلب من الطرف الآخر، يقوم الطرف المطلوب منه بإتخاذ كافة الإجراءات الملائمة وذلك لسرعة التحفظ على المعطيات المحددة وفقاللقانون الوطني، ولأغراض الإستجابة للطلب، فلا يشترط **وجود إزدواجية التجريم للقيام بالحفظ.**

ولضمان توافر المساعدة الفورية لتنفيذ التحفظ على المعطيات، كان لزاما أن يكون هناك **نظام إتصال** يسمح للجهات القائمة على التحقيق بالإتصال بالجهات الأجنبية، وهو ما شجعت عليه إتفاقية بودابست بموجب المادة 35 والإتفاقية العربية بموجب المادة 43.

وفضلا عن التحفظ على المعطيات كإجراء تحفظي، كرست إتفاقية بودابست بموجب المادة 30 والإتفاقية العربية بموجب المادة 38 لتيسير المساعدة القضائية في الجرائم الواقعة على التعاملات الإلكترونية الكشف السريع عن المعطيات المارة المحفوظة المتعلقة بإتصال معين وتتبع نفس الإجراءات المتبعة في التحفظ على المعطيات المخزنة، وإذا ما إكتشفت الدولة التي قدم لها طلب التحفظ أن مزود الخدمة في دولة أخرى قد ساهم في نقل الإتصال، فإنه يجب على الدولة التي تحفظت على المعطيات أن تكشف عن سرية هذه المعطيات للطرف الذي قدم الطلب بهدف التعرف على مقدم الخدمة ومسار الإتصال.

ثانيا- تبادل المعلومات:

حرصت المادة 26 من إتفاقية بودابست والمادة 33 من الإتفاقية العربية على التأكيد على واجب الدولة التي تمتلك معلومات هامة في مساعدة دولة أخرى أثناء التحقيقات أو تداول الدعوى الجزائية في الحالات التي لا تدرك فيها سلطات التحقيق في الدولة التي تجري التحقيقات أو الملاحقة وجود هده المعلومات، دون حاجة لتقديم طلب بالمساعدة المتبادلة في تلك الحالة.

وهو ما نص عليه المشرع الجزائري بموجب المادة 17 من القانون رقم 09-04 : "تتم الإستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو....وفقا للإتفاقيات الدولية ذات الصلة والإتفاقيات الدولية الثنائية و مبدأ المعاملة بالمثل".

[1]-Article26- 3 dispose que " Après avoir reçu la demande d'une autre Partie, la Partie requise doit prendre toutes les mesures appropriées afin de procéder sans délai à la conservation des données spécifiées, conformément à son droit interne. Pour pouvoir répondre à une telle demande, la double incrimination n'est pas requise comme condition préalable à la conservation".

ثالثا- الإنابة القضائية الدولية:

ويقصد بهذا الإجراءطلب إتخاذ إجراء قضائي من إجراءات الدعوى تتقدم به الدولة المطلوب منها إتخاذ الإجراء لضرورة ذلك في الفصل في مسألة معروضة على السلطة القضائية في الدولة الطالبة ويتعذر عليها القيام بها بنفسها، والهدف من هذا الإجراء هو تسهيل الإجراءات الجزائية بين الدول والتغلب على عقبة السيادة التي تكون عائقا تمنع الدولة الأجنبية من مباشرة إجراءاتها القضائية داخل إقليم الدول الأخرى مثل سماع الشهود وإجراء التفتيش[1].

وتستلزم الإنابة الدولية القضائية إرسال الملف الخاص بالدعوى الجزائية بمرفقاته من مستندات ووثائق ومحاضر التحقيق التي أجريت بمعرفة السلطة القضائية في الدولة المطلوب فيها إتخاذ بعض إجراءات التحقيق. وهي بذلك تتشابه إلى حد كبير مع الندب" **الإنابة القضائية الداخلية**[2]".

وعادة ما تكتفي الدول بمسالة تنظيم الإنابة الدولية القضائية للاتفاقيات الدولية، والمعمول به هو الإعتماد على الآليات التقليدية في تسلم الإنابة القضائية ألا وهو "**الطريق الدبلوماسي**" المعروف بالبطء وكثرة شكلياته، وهو ما يتعارض وطبيعة الجرائم محل الدراسة من كونها تتم بالسرعة نظرا للسرعة ذاتها للبيئة التي تنشا فيها ألا وهي البيئة التقنية، ولذلك فإن مكافحتها تقتضي ردود سريعة خشية التلاعب في المعطيات التي قد تشكل دليلا ضد المتهم.

ولذلك، حثت إتفاقية بودابست في فقرتها 3 من المادة 25 والإتفاقية العربية في فقرتها 3 من المادة 32 الدول الأطراف على تنفيد إجراءات الإنابة بوسائل سريعة في حالات الإستعجال مثل الفاكس والبريد الإلكتروني، بشرط ضمان سلامة المعلومات المتبادلة بين الطرفين بمافيها إستعمال وسائل التشفير عند الضرورة وتعزيز ذلك بطلب رسمي لاحقا.

وهو ما إعتمده المشرع الجزائري في الفقرة الثانية من المادة 16 من القانون رقم 09-04 حين نص "..يمكن في حالة الإستعجال، ومع مراعاة الإتفاقيات الدولية ومبدأ المعاملة بالمثل، قبول طلبات المساعدة القضائية المدكورة في الفقرة أعلاه، إذا وردت عن طريق وسائل الإتصال السريعة بما في ذلك أجهزة الفاكس أو البريد الإلكتروني و ذلك بقدر ما توفره هذه الوسائل من شروط أمن كافية للتأكد من صحتها."

---

[1]-**د. جميل عبد الباقي الصغير**، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت، المرجع السابق، ص83. **د. حسين بن سعيد الغافري**، السياسة الجنائية في مواجهة جرائم الأنترنت ، المرجع السابق، ص646.

[2]- **د. سليمان أحمد فضل**، المرجع السابق، ص425.

المبحث الثالث

الاختصاص القضائي بنظر جرائم الإعتداء على التعاملات الإلكترونية

ساهم التطور المذهل في الوسائل الإلكترونية في تجاوز حدود الدولة، وقد أثر تقارب الحدود الجغرافية من إقليم إلى آخر على أساليب إرتكاب الجريمة، فقد أصبح من الممكن أن ترتكب السلوكات غير المشروعة من خلال وحدة طرفية في دولة بينما يكون الجاني موجودا في دولة أخرى.

وقد ترتب على الطبيعة التقنية الممتدة لشبكة الأنترنت أن الإختصاص بنظر تلك الجرائم سوف ينعقد لأكثر من دولة، مما يؤدي إلى التنازع الإيجابي بين قوانين تلك الدول. فهل يمكن إعمال تلك القواعد التقليدية على الإعتداء على التعاملات الإلكترونية إذا ما إرتكبت عبر الأنترنت؟

بل حتى وإن تم حسم مسالة الإختصاص، فالمشكل يطرح بشأن الأدلة الكامنة في هده البيئة، ومامدى القوة الثبوتية التي تتمتع بها، ومدى حرية قاضي الموضوع بالإقتناع بها؟

على ضوء ما تقدم سوف نقسم دراسة هذا المبحث إلى ثلاثة مطالب على النحو التالي:

المطلب الأول: الإختصاص القضائي الدولي بنظر جرائم الإعتداء على التعاملات الإلكترونية
المطلب الثاني:الإختصاص القضائي الداخلي بنظر جرائم الإعتداء على التعاملات الإلكترونية
المطلب الثالث: حجية الدليل الإلكتروني أمام القضاء الجزائي

المطلب الأول

الإختصاص القضائي الدولي بنظر جرائم الإعتداء على التعاملات الإلكترونية

إن طبيعة الأنترنت التي تعتمد عليها التعاملات الإلكترونية خلقت عالما جديدا لا يعترف بالحدود الجغرافية و السياسية للدول، الأمر الذي أثر بدوره على أساليب إرتكاب الجرائم الواقعة عليها، فقد أصبح من الممكن أن ترتكب العديد من السلوكات غير المشروعة من خلال وحدة طرفية في دولة بينما يكون الجاني موجودا في دولة أخرى، كما أن مفهوم النشاط الجرمي يقترن في الجرائم التي تعتمد على شبكة الأنترنت بمفاهيم الإباحة والتجريم لكل دولة.

فالمشكلة التي تشترك فيها جرائم التعاملات الإلكترونية مع غيرها من الجرائم الواقعة في العالم الرقمي، هو كون المستند المعاقب عليه قد يمر عبر أجهزة العديد من الدول، مع عدم وجود أي رقابة أو سيطرة من أي جهة، في غياب نص خاص يحدد المحكمة المختصة.

بالرجوع للقواعد العامة التي تنظم إنعقاد الإختصاص العالمي للمحاكم الوطنية في الفصل في الدعاوى، نجد أن هذه المسالة تنظمها القواعد العامة لتطبيق القانون الجزائي من حيث المكان، والتي تحكمها مباديء ثلاثة: مبدأ الإقليمية(الفرع الأول) مبدأ الشخصية (الفرع الثاني) مبدأ العينية(الفرع الثالث)، فإلى أي مدى يمكن تطبيق هذه المبادئ على جرائم الإعتداء على التعاملات الإلكترونية؟.

الفرع الأول

مبدأ إقليمية القانون الجزائي وجرائم التعاملات الإلكترونية

يعني مبدأ إقليمية القانون الجزائي أن الإقليم الخاضع لسيادة الدولة هو الذي يحدد نطاق تطبيق النصوص الجنائية الوطنية، سواء في ذلك النصوص الموضوعية أو النصوص الإجرائية.

ويستند هذا المبدأ إلى عدة مبررات منها فكرة سيادة الدولة على إقليمها، إذ أن تطبيق القانون الجزائي إقليميا هو من أهم مظاهر السيادة على الإقليم، فالقانون الجزائي هو الذي يضمن حماية الحقوق الدستورية و القانونية، كما أن محكمة مكان إرتكاب الجريمة أقدر على جمع الأدلة والإحاطة بجميع ظروفها وشهودها و فاعلها، كما أن محاكمة الجاني في مكان إرتكاب الجريمة يحقق الردع العام، ويقضي على الإضطراب الإجتماعي الذي أحدثته الجريمة بالمجتمع[1].

ومن حيث المبدأ فإن قانون الدولة يطبق متى وقعت في إقليم الدولة الجريمة كاملة أو أحد العناصر المكونة لها[2] أو كان من الممكن أن تقع النتيجة الإجرامية، أو أن يقع أحد أفعال الإشتراك في ذلك الإقليم، ولاقيمة في ذلك للأعمال التحضيرية، كما لاقيمة لما يلي ارتكاب الجريمة كإخفاء متحصلات الجريمة، وفي الجرائم التي تحتمل الإستمرار أو ترتكب بجملة أفعال، فإن الإختصاص بشأنها قد يكون لقانون وقضاء أكثر من دولة[3].

ولمبدأ إقليمية القانون الجنائي نتيجتان: الأولى إيجابية: وهي أن يكون للقانون الجزائي تطبيق شامل على كافة الجرائم المرتكبة على إقليم الدولة، الأمر الذي يؤدي بالضرورة إلى عدم تطبيق القوانين الجزائية الأجنبية على هذه الجرائم، أما النتيجة الثانية فسلبية، وهي تقضي بعدم تطبيق القانون الجزائي على أية جريمة ترتكب خارج حدود الدولة[4].

ويعتبر مبدأ الإقليمية مبدأ عام وجامع للاختصاص التشريعي والقضائي للدولة، فهو بمثابة الحل المبدئي الأول عند تطبيق القانون الجزائي في المكان، ولهذا إعتمدته أغلب التشريعات من ذلك المشرع الجزائري في المادة

---

[1]–**د. محمود نجيب حسني**، شرح قانون العقوبات اللبناني، القسم العام، الطبعة الثالثة، منشورات الحلبي الحقوقية، بيروت، 1998، ص180.**د. عبود السراج**، شرح قانون العقوبات، القسم العام، المطبعة الجديدة، دمشق، 1990، ص165.

[2]– **د.أحمد شوقي عمر أبو خطوة**، شرح الأحكام العامة لقانون العقوبات، دار النهضة العربية، 2003، ص92.**د. محمد صبحي نجم**، قانون العقوبات القسم العام، دار الثقافة،2000،ص65.

[3]– **د. باسم شهاب**، مباديء القسم العام لقانون العقوبات، ديوان المطبوعات الجامعية، وهران،2007، ص35.

[4]–د.**محمود نجيب حسني**،شرح قانون العقوبات اللبناني، القسم العام، المرجع السابق، ص180.

3 من قانون العقوبات حيث نصت "**يطبق قانون العقوبات على كافة الجرائم التي ترتكب في أراضي الجمهورية**"، كما نصت المادة 586 إجراءات"**تعد مرتكبة في الإقليم الجزائري كل جريمة تكون عمل من الأعمال المميزة لأحد أركانها المكونة لها قد تم في الجزائر**".

ويستفاد من النصوص السابقة أن أحكام هذا التشريع تسري على جميع الجرائم التي تقع داخل النطاق الإقليمي للقطر الجزائري بغض النظر عن جنسية مرتكبها سواء كان وطنيا أم أجنبيا، كما يستفاد أن العبرة في تحديد إقليمية القاعدة الجنائية هي بوقوع الجريمة كاملة أو جزء منها في القطر الجزائري.

كما أخد به المشرع الفرنسي في المادة 113-2 من قانون العقوبات التي تنص" **يطبق القانون الفرنسي على الجرائم المرتكبة على إقليم الجمهورية وتعتبر قد إرتكبت على إقليم الجمهورية إذا كان أحد عناصر الجريمة قد وقع على هدا الإقليم**"[1].

كما أخد المشرع المصري بهذا المبدأ بموجب المادة 1 من قانون العقوبات المصري ***"تسري أحكام هذا القانون على كل من يرتكب في القطر المصري جريمة من الجرائم المنصوص عليها فيه"*** وأيضا نصت المادة 2-1 ***"تسري احكام هذا القانون على الأشخاص الآتي ذكرهم: اولا من ارتكب في خارج القطر فعلا يجعله فاعلا او شريكا في جريمة وقعت كلها او بعضها في القطر المصري"***

إن موضوع الإختصاص في الجرائم الواقعة على التعاملات الإلكترونية وفي غياب إطار تشريعي يحكمه يتم التعامل معه وفق قواعد الإختصاص الإقليمي، وفي الحقيقة فإن تطبيق مبدأ الإقليمية على جرائم التعاملات الإلكترونية لا يثير أية صعوبة إذا كانت جميع عناصر الجريمة قد وقعت على إقليم واحد، وإذا كانت هذه الجرائم متتابعة الأفعال، فيكفي في هذه الحالة أن يتحقق جزء من حالة الإستمرار أو فقرة من فقرات التتابع، ومثال ذلك قيام الجاني بإعداد برنامج بقصد إتلاف توقيع إلكتروني، أو الإستيلاء على مستند إلكتروني، البقاء غير المشروع داخل نظام المعالجة الآلية، حيث أنها تعتبر من الجرائم المستمرة[2].

وعادة لا تتضمن نصوص قانون العقوبات مايفيد تحديد الإقليم، فهي أمور يعنى بها القانون الدولي العام، وفي إطاره يمكن تحديد إقليم الدولة على أنه الإقليم البري وحدده بالحدود السياسية للدولة، والإقليم البحري و يشمل المياه الإقليمية للدولة، وأخيرا الإقليم الجوي وهو طبقات الجو الذي يعلو الإقليمين البري والبحري للدولة. فضلا عن الإقليم الإعتباري وهو السفن والمركبات الهوائية أينما وجدت.

إن العبرة في تحديد إقليم النص القانوني هي بتحقق الركن المادي في الإقليم كاملا أو جزء منه، وقد ساير القضاء الأمريكي ذلك النهج حيث طبقت محكمة واشنطن مبدأ إقليمية النص الجنائي في قضية سكوت

---

[1]-Article 113-2 du CPF **dispose que''**La loi pénale française est applicable aux infractions commises sur le territoire de la République.L'infraction est réputée commise sur le territoire de la République dès lors qu'un de ses faits constitutifs a eu lieu sur ce territoire.**''**

[2]- **أيمن رمضان محمد أحمد**، المرجع السابق، ص365.

ليفين، والتي إرتكبت بعض أجزائها داخل الدولة، حيث قضت بمعاقبته بالسجن 96 شهرا بتهم الدخول غير المشروع على برنامج النظام المعلوماتي لعدد 120 عميل بشركة little rock والدخول غير المشروع على حساب إثنين من العملاء، والتسبب في عرقلة العدالة وذلك بإنشاءه برنامج مكنه من فض مفاتيح التشفير الخاصة بتلك الشركة، والحصول على معطيات العملاء السرية لما يجاوز مليون عميل وأرقام حسابهم وهواتفهم ومحال إقامتهم، و تمكن بذلك من الدخول على الحساب الخاص ببعض العملاء، والإستيلاء على أرصدتهم[1].

وفي سياق الحديث عن الإقليم هناك سؤالا يتبادر للإدهان فيما يخص المساحات من الأنترنت الخاضعة لإدارة الدول ، فإدا أخدنا الجزائر كمثال فإنها تنتهي باللاحقة dz، فهل تعتبر بذلك جزء من الإقليم الإعتباري الجزائري؟

هناك من يرى –ويحق[2]– بأن الإجابة على هذا السؤال تكون بالإيجاب للسببين التاليين:

1–أن المبررات المتعلقة بسيادة الدولة على إقليمها، والتي دفعت المشرع الجزائي إلى إعتبار الطائرات الجزائرية إمتداد للإقليم الجزائري متوفرة في ذلك النطاق العلوي الجزائري على الأنترنت، الذي يخضع لإدارة الحكومة الجزائرية (المنتهي بـــ: dz)، فهذا النطاق يحمل العلم الجزائري أو الجنسية الجزائرية، وبالتالي فإن إعتباره بحكم الإقليم الجزائري يتفق مع فلسفة المشرع الجزائري.

2–هناك مبررات عملية تدفع لاعتبار النطاق العلوي الجزائري على الأنترنت بحكم الأرض الجزائرية، وهي أن هناك جرائم من الممكن أن ترتكب عبر هذا النطاق دون أن تطولها قواعد الإختصاص الجزائي الدولي الجزائري مثاله: إذا أنشأت شركة فرنسية موقعا إلكترونيا لها على النطاق العلوي الجزائري المنتهي ب dz ثم قامت عبر هذا الموقع بالإحتيال على بعض التونسيين الموجودين بتونس، فإن هذه الجريمة لا تخضع للقانون الجزائي الجزائري لأن قواعد الإختصاص الدولي لا تسمح بذلك، مع العلم أن الجريمة **تمت عبر النطاق الوطني الجزائري على الأنترنت.**

كما أن تطبيق مبدأ الإقّليمية على الجرائم محل الدراسة يصطدم بالعديد من العقبات، من أهمها أنها جرائم يصعب تحديد مكان وقوع الفعل الجرمي فيها، لأن طبيعتها الخاصة تتجاوز المعايير التقليدية، فمن الصعوبات التي تثيرها هذه الجرائم أنها متعدية الحدود يتجاوز فيها السلوك المرتكب المكان بمفهومه التقليدي، مما يستتبع ــ ولو نظرياً ــ عدم إمكان خضوعها لسلطان قانون جنائي معين، حيث يمكن أن يتوزع السلوك المادي للجريمة في أكثر من دولة، من ذلك أن يقوم شخص في فرنسا بالدخول على موقع إلكتروني تجاري لتعديل معطيات مسجلة في قاعدة معطيات في الجزائر، و يكون بالتالي قانون كل دولة

[1]-Computer crime intellectual property section united states department of justice.disponible en lingne á l'adresse suivantehttps://www.justice.gov/criminal-ccips

[2]-**طارق عبد الرؤوف الخن**، المرجع السابق، ص218.

تحقق فيها جزء من الجريمة قابلا للتطبيق، وهو ما يؤدي إلى **تنازع إيجابي** في الإختصاص بين أكثر من تشريع ومن تم أكثر من دولة لملاحقة نفس السلوك الجرمي.

تضمنت إتفاقية بودابست بإعتبارها الإطار المرجعي الدولي الذي يمكن اللجوء إليه عندما يتعلق الأمر بالجرام الواقعة في العالم الإفتراضي، جملة معايير يتم بمقتضاها تنسيق الأطراف حدود صلاحيتها[1]، إلا أنها في الأصل لم تخرج عن المعايير التقليدية، لتطرح في الأخير منطق التشاور بين الأطراف لتحديد الإختصاص القضائي الأكثر ملائمة للمحاكمة، مما جعل مسالة الإختصاص تطرح وبشدة كل مرة.

وماقيل بشأن إتفاقية بوابست يقال بشأن الإتفاقية العربية، فبالرجوع للمادة 30 منها نجدها لم تخرج عن الضوابط التي أقرتها الإتفاقية الأروبية فيما يخص سريان الإختصاص القضائي، وإن كانت هذه الأخيرة قد حلت مشكلة تنازع الإختصاص بموجب المادة 30 الفقرة الأخيرة، حيث قدمت الدولة التي أخلت الجريمة بأمنها أو بمصالحها ثم الدولة التي وقعت الجريمة في إقليمها ثم الدولة التي يكون الشخص المطلوب من رعايها وإذا إتحدت الظروف **فتقدم الدولة الأسبق في طلب التسليم.**

وعلى ذلك فإننا نرى أنه من الضروري إيجاد قاعدة إجرائية تحكم مسالة الإختصاص في هذه الفئة بما يتناسب وطبيعتها، على نحو ما ذهب إليه الإجتهاد القضائي الفرنسي فيما يخص بعض الفئات المستهدفة من الجرائم الواقعة في العالم الإفتراضي، حيث تم تحديد مفهوم جديد **لمكان إرتكاب الجريمة** يتماشى وطبيعة هذه الجرائم.

كما هو الحال في جرائم الصحافة المرتكبة عبر الأنترنت، حيث تم الإحتكام على معيار محل تمركز الموقع الذي نشرت الأقوال أو المعلومات بواسطته[2] ، كما ظهرت معايير جديدة ترتبط بالجرائم الماسة بحقوق

---

[1]- Article 22 du CCB dispose que "1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pourétablir sa compétence à l'égard de toute infraction pénale établie conformément aux articles 2à 11 de la présente Convention, lorsque l'infraction est commise:a sur son territoire; oub à bord d'un navire battant pavillon de cette Partie; ouc à bord d'un aéronef immatriculé selon les lois de cette Partie; ou d par un de ses ressortissants, si l'infraction est punissable pénalement là où elle a étécommise ou si l'infraction ne relève de la compétence territoriale d'aucun Etat.
2 Chaque Partie peut se réserver le droit de ne pas appliquer, ou de n'appliquer que dans descas ou des conditions spécifiques, les règles de compétence définies aux paragraphes 1.b à 1.d du présent article ou dans une partie quelconque de ces paragraphes.
3 Chaque Partie adopte les mesures qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction mentionnée à l'article 24, paragraphe 1, de la présente Convention, lorsque l'auteur présumé de l'infraction est présent sur son territoire et ne peut être extradé vers une autre Partie au seul titre de sa nationalité, après une demande d'extradition.
4 La présente Convention n'exclut aucune compétence pénale exercée par une Partie conformément à son droit interne.
5 Lorsque plusieurs Parties revendiquent une compétence à l'égard d'une infraction présuméevisée dans la présente Convention, les Parties concernées se concertent, lorsque cela estopportun, afin de déterminer la mieux à même d'exercer les poursuites

[2]-صدر قرار عن الغرفة الجنائية بمحكمة النقض الفرنسية بتاريخ 8 ديسمبر 2009 اعتبر فيه " أن مكان ارتكاب الجريمة هو المكان الذي تم فيه التلفظ بالتهديد (توجيه التهديد) وليس في الدول التي نقل الخبر فيها عبر التلفاز أو الصحافة المكتوبة أو الإلكترونية والتـــي من خلالها علم الشخص " les juges retiennent que le lieu de commission de l'infraction est celui où les menaces ont été proférées et non pas les pays où elles ont ensuite été rapportées par la voie télévisée ou de presse écrite ou électronique et par lesquelles l'intéressé a pu en prendre connaissance ;**Cour de cassation chambre criminelle**, **N° de pourvoi: 09-82120 09-82135**
كما إعتبرت محكمة باريس في إحدى قراراتها الصادرة بتاريخ 13 نونبر1998 أنها صاحبة الإختصاص في إحدى الجرائم المرتبطة بالصحافة والتي تقع في العالم الإفتراضي حيث جاء فيه " وحيث أن النص المخالف قد تم نشره على موقع أجنبي يمكن الوصول إليه ورؤيته من خلال الولاية الإقليمية لمحكمة باريس وبالتالي فهي من لها الولاية في التحقيق والمتابعـــة".
Tribunal de grande instance de Paris, 13 novembre 1998; n daffaire 9727603115,http://juriscom.net/wp-content/documents/tgiparis19981113.pdf

الملكية الفكرية ، كما هو الحال في جرائم التقليد عبر الأنترنيت حيث يرجع الإختصاص إما لمحكمة المكان الذي إرتكب فيه التقليد وإما مكان نشره، أو معيار إمكانية الوصول للموقع كأساس لإختصاص المحكمة في حالة الإعتداء على حق من حقوق المؤلف من خلال الأنترنيت[1].

بالإضافة إلى هذه المعايير تم إيجاد معايير أخرى مرتبطة أيضا بالجرائم المرتكبة ضد الأحداث حيث أن الإختصاص في هذا النوع من الجرائم ينعقد لمكان ارتكاب الجريمة، ومكان ارتكاب الجريمة هذا يأخذ المعايير التالية والتي يتم تقديمها بالأسبقية وهي [2]:

- المكان الذي شوهد فيه وجود الموقع غير المشروع أو الذي تم فيه مشاهدة الصور والنصوص ذات الطبيعة غير المشروعة.
- المكان الذي يوجد فيه خادم الإيواء إذا ظهر بعد المعاينات الأولى أن الموقع يمكن تحديده من خلال التراب الإقليمي.

وفي إطار الجرائم محل الدراسة ونظرا لطبيعتها الخاصة وإمكانية تحقق النتيجة في أكثر من دولة، نرى ضرورة تبني حل أكثر مرونة يأخذ في الإعتبار هذه الطبيعة، ونرى فيما يذهب إليه البعض[3]: من الفقه أنه من المستحسن تحديد مكان واحد وهو **مكان وقوع النشاط** أي **مكان الجهاز الخادم، بالإضافة على مكان تواجد المتهم عند قيامه بتحميل المعطيات المعاقب عليها**، للأسباب التـــالية:

Pierrat Emmanuel, « Les infractions de presse sur l'internet », *LEGICOM, 1*/2000 (N° 21-22), p. 71-78.
URL : http://www.cairn.info/revue-legicom-2000-1-page-71.htm
DOI : 10.3917/legi.021.0071

[1]–حيث صدر قرارين عن محكمة النقض الفرنسية، الأول بتاريخ 9 ديسمبر 2003 قبلت من خلاله إختصاص محكمة فرنسية للنظر في إصلاح الضرر الناتج عن تقليد علامة تجارية في موقع إسباني ولكنـــه قابل للوصول إليه من فرنسا ورفضت الدفع المثار من أجل عدم إختصاص القضاء الفرنسي" ، و الثاني بتاريخ 5 أبريل 2012 اعتبرت فيه أن التقليد المتنازع بشأنه تم نشره على موقع للأنترنت يمكن الوصول إليه من فرنسا وبالتالي فإن القضاء الفرنسي هو صاحب الإختصاص في النازلة "، و في نفس الإتجاه ذهبت محكمة الإستئناف بباريس من خلال القرار الصادر عنها بتاريخ 25 شتنبر 2007 حيث إعتبرت " أن القانون الجنائي الفرنسي هو المطبق والقضاء الفرنسي هو المختص في واقعة التقليد التي قام بها موقع إيطالي و رفضت الدفع المثار بعد إختصاص المحاكم الفرنسية على اعتبار غياب أي فعل مكون للجريمة تحقق في الأراضي الفرنسية وأن الطرف المدني الوحيد هو من جنسية إيطالية".

- Mathias Kuhn, L'accessibilité du site Internet comme fondement de la compétence du juge dans le cas d'atteinte au droit d'auteur par le biais d'Internet.disponible en lingne á l'adresse suivante: https://www.lepetitjuriste.fr/propriete-intellectuelle/laccessibilite-du-site-internet-comme-fondement-de-la-competence-du-juge-dans-le-cas-datteinte-au-droit-dauteur-par-le-biais-dinternet/

[2]-**Myriam Quéméner & Yves charpenel** , cybercriminalité – droit pénal appliqué- Economica paris France,2010, p .161

د.**يوسف قجاج**، إشكالية الإختصاص في الجريمة الإلكترونية، مقـــال متـــاح على الموقـــع الإلكتروني التـــالي:
http://www.hespress.com/opinions/256777.html

[3]–**د. شيماء عبد الغني**، المرجع السابق، ص378.

- سهولة معرفة مكان تواجد الجهاز بينما يصعب أحيانا معرفة صاحب المستند الذي يبثه عبر موقع ربما سجل هذا الموقع بإسم وهمي أو بدون إسم محدد، وربما يقيم في الخارج و يستدعي الأمر لرفع الدعوى في مكان إقامته السفر إلى الخارج و متابعة إجراءات الدعوى في الخارج.
- رفع الدعوى أمام محكمة الجهاز الخادم يجيز التعويض عن الضرر عن سائر الأضرار التي تحققت في أماكن مختلفة من العالم، على خلاف الحال عند رفع تلك الدعوى أمام إحدى المحاكم التي تصل إليها شبكة الأنترنت، و يمكن الدخول إلى الموقع فيها، حيث أن ذلك لا يجيز سوى التعويض عن الضرر الذي تحقق في هذا المكان وحده دون غيره.
- رفع الدعوى أمام محكمة الجهاز الخادم يسمح للمحكمة بأن تصدر أمرا إلى متعهد الإيواء بمنع الدخول إلى الموقع الذي يتضمن رسائل مؤثمة أو ضارة للآخرين.

لكن ماذا لو أن الجهاز الخادم الذي تم ارسال إليه المواد المعاقب عليها متواجد خارج البلاد وكان دور المتهم المتواجد في الإقليم أنه شريك وليس فاعل؟ سيما وأن أغلب جرائم الإعتداء على التعاملات الإلكترونية تتم من خلال تشكيل منظم يستهدف المساس بسرية التعاملات الإلكترونية؟

تأخذ الكثير من الدول بنظرية إستعارة الإجرام في تحديد إختصاص قضائها، بمعنى أن قضائها لا يختص بمحاكمة الشريك في الجريمة التي وقعت في الخارج وكان هذا القضاء غير مختص أصلا بمحاكمة الفاعل الأصلي، ومع ذلك فإن الجزائر وفرنسا قررتا إختصاص قضائها لمحاكمة الشريك في الحالة السابقة، حيث نص قانون العقوبات الفرنسي على هذا النوع من الإختصاص في المادة 113-5 من قانون العقوبات الفرنسي "**يطبق القانون الفرنسي على كل من يرتكب فعل في اقليم الجمهورية يجعله شريكا في جناية او جنحة وقعت في الخارج إدا كانت الجناية أو الجنحة يعاقب عليها القانون الفرنسي والقانون الأجنبي وكانت ثابتة بموجب حكم نهائي من القضاء الأجنبي**"[1]. كما نصت المادة 586 من قانون الإجراءات الجزائري "**كل من كان في إقليم الجمهورية شريكا في جناية او جنحة مرتكبة في الخارج يجوز ان يتابع من أجلها ويحكم عليه فيها بمعرفة جهات القضاء الجزائرية إذا كانت الواقعة معاقبا عليها في كلا القانونين الأجنبي والجزائري بشرط ان تكون تلك الواقعة الموصوفة بأنها جناية او جنحة قد ثبت ارتكابها بقرار نهائي من الجهة القضائية الأجنبية**".

والملاحظ أن نص المادة 113-5 عقوبات فرنسي يتفق مع نص المادة 586 اجراءات جزائري، في كون أن الإختصاص يقوم بتوافر شريطين أساسين:

1- أن يكون الفعل معاقبا عليه في القانون الوطني والأجنبي.

2- أن يكون قد صدر حكم نهائي أجنبي يقرر وقوع الجريمة الأصلية في الخارج.

[1] **Article 113-5 dispose que "** La loi pénale française est applicable à quiconque s'est rendu coupable sur le territoire de la République, comme complice, d'un crime ou d'un délit commis à l'étranger si le crime ou le délit est puni à la fois par la loi française et par la loi étrangère et s'il a été constaté par une décision définitive de la juridiction étrangère".

ومثل هذا النص يساعد كل من الجزائر وفرنسا في مجال الجرائم الواقعة على التعاملات الإلكترونية في التوسع في إختصاص المحاكم الوطنية بالجرائم محل الدراسة.

الفرع الثاني

مبدأ شخصية القانون الجزائي وجرائم التعاملات الإلكترونية

إن الأخد بمبدأ إقليمية النص الجنائي على الإطلاق يعطي الفرصة للإفلات من العقاب إذا ارتكبت الجريمة خارج حدود الدولة ثم عاد إليها دون أن يعاقب بالخارج، وكذلك إذا ما تم الإعتداء على أحد رعايا الدولة خارج إقليم الدولة فلا تستطيع الدولة معاقبة الجانيوفق مبدأ الإقليمية، لذلك جاء مبدأ شخصية النص الجزائي ليعطي إتساعا كبيرا لتطبيق النص الجنائي على الجناة، ويكون مناط تطبيق القاعدة الجنائية هو جنسية مرتكب الجريمة أو المجني عليه فيها بأن يكون حاملا لجنسية الدولة[1].

ومن تم فإن لهذا المبدأ جانبان: إيجابي وسلبـــي[2]:

فالجانب الإيجابي مؤداه تطبيق القانون الجنائي للدولة على مرتكبي الجرائم الذين ينتمون إلى جنسيتها بصرف النظر عن مكان وقوع جريمتهم، وأيا كانت جنسية المجنيعليه في هذه الجريمة.ويطلق عليه مبدأ الشخصية الإيجابي.

الجانب السلبي: مؤداه تطبيق القانون الجنائي للدولة على كل جريمة تقع على أحد رعاياها حتى لو وقعت من أجنبي وإرتكبت خارج إقليمـــها ويطلق عليـــه مبـــدأ الشخصية السلبية.

على غرار أغلبية التشريعات –كالتشريع المصري[3]–، لم يعتد المشرع الجزائري بمبدأ شخصية النص الجزائي في وجهه السلبي، فجنسية المجني عليه ليست معيارا يحدد سلطان النص الجنائي من حيث المكان، ولكنه إعتد بمبدأ شخصية النص الجنائي في وجهه الإيجابي ، مميزا في ذلك بين فيما إذا كانت الواقعة التي إرتكبها الجاني جناية أو جنحة، وما يهمنا في هذا المقام هو الجنح كون أن اغلب الجرائم الواقعة على التعاملات الإلكترونية ذات وصف جنحوي، وفي هذا الإطار فقد نصت المادة 583 إجراءات المقابلة للمادة 113–6 عقوبات فرنسي" ***كل واقعة موصوفة بانها جنحة سواء في نظر القانون الجزائري ام في نظر تشريع القطر الذي ارتكبت فيه يجوز المتابعة من اجلها و الحكم عليها في الجزائر اذا كان مرتكبها جزائريا و لا يجوز ان تجري المحاكمة او يصدر الحكم الا بالشروط المنصوص عليها في الفقرة الثانية من المادة***

---

[1]- **د. مأمون سلامة**، شرح قانون العقوبات، القسم العام، دار النهضة العربية، القاهرة، 1991، ص77.

[2]–**د.محمود نجيب حسني**، شرح قانون العقوبات اللبناني_القسم العام_، المرجع السابق، ص 201–202.

[3]– نصت المادة 3 من قانون العقوبات المصري " كل مصرى إرتكب وهو فى خارج القطر فعلاً يعتبر جناية أو جنحة فى هذا القانون يعاقب بمقتضى أحكامه إذا عاد إلى القطر وكان الفعل معاقباً عليه بمقتضى قانون البلد الذى إرتكبه فيه، كما نصت المادة 4 منه "لا تقام الدعاوى العمومية على مرتكب جريمة أو فعل فى الخارج إلا من النيابة العمومية ، ولا تجوز إقامتها على من يثبت أن المحاكم الأجنبية برأته ثم أسند إليه أو أنها حكمت عليه نهائيا واستوفى عقوبته.

582" وعليه وبإستقراء المادة **582** نجد إنه يشترط لتطبيق المادة **583** شروط معينة يلزم توافرها لتطبيق القانون الجزائري على الجرائم الواقعة على التعاملات الإلكترونية استنادا إلى مبدأ الشخصية وهي:

-يجب أن يكون الجاني جزائريا وقت إرتكابه الجريمة وعند عودته للجزائر.

-ان ترتكب الواقعة في الخارج.

-عودة الجاني إلى الجزائر فلا يحاكم غيابيا.

-لم يثبت أنه قد حكم عليه نهائيا في الخارج، وأن يثبت إذا ما أدين أنه قد قضى العقوبة أو سقطت عنه بالتقادم أو العفو. وعليه إذا كانت العقوبة المحكوم بها لم تنفد كلها، فإن ذلك لا يحول دون إعادة محاكمة الجاني مرة ثانية، على أن تحسب للمحكوم عليه عند تنفيد العقوبة المدة التي قضي عليه بها في الخارج و نفدها بالفعل.

-أن تكون الجريمة من جنح الإعتداء على التعاملات الإلكترونية وفقا للقانون الجزائري أو قانون الدولة التي ارتكبت على إقليمها الجريمة، ولاشك أن غالب التشريعات الأجنبية تعاقب على بعض الإعتداءات التي تنال من التعاملات الإلكترونية.

- في حالة أن تكون الجنحة مرتكبة ضد الأفراد فلا يجوز أن تجري المتابعة إلا بناءا على طلب من النيابة العامة بعد إخطارها بشكوى من قبل الشخص المتضرر أو ببلاغ من سلطات القطر الذي ارتكبت الجريمة فيه.

وإذا كان المشرع الجزائري قد طبق مبدأ شخصية النص الجنائي في جانبه الإيجابي فقط، بما يضمن حسن سلوك الرعايا الجزائريين في الخارج، فارض عليهم إحترام القانون الأجنبي فضلا عما تحققه مساءلتهم عن جرائمهم من تعاون دولي مطلوب في مكافحة الإجرام.

فإن المشرع الفرنسي وعلاوة على شقه الإيجابي، قد طبق جانبه السلبي بمقتضى المادة 113-7 من قانون العقوبات الفرنسي ***"يطبق القانون الفرنسي على كل جريمة يرتكبها فرنسي أو أجنبي خارج فرنسا إذا كان المجني عليه فرنسيا لحظة وقوع الجريمة"[1].***

وقد طبق القضاء الفرنسي هذا المبدأ عندما قام أحد الموظفين بنسخ ملفات من شبكة الأنترنت، وتخزينها على الحاسب المملوك له، حيث إرتكبت الجريمة خارج إقليم فرنسا إلا أن القضاء أعمل مبدأ الشخصية وأدانه بتهمة إخفاء أشياء مسروقة[2].

---

[1]-**Article 113-7 du CPF dispose que "**La loi pénale française est applicable à tout crime, ainsi qu'à tout délit puni d'emprisonnement, commis par un Français ou par un étranger hors du territoire de la République lorsque la victime est de nationalité française au moment de l'infraction."

[2]- **أيمن رمضان محمد أحمد**، المرجع السابق، ص369.

وقد طبق القضاء اليمني مبدأ شخصية النص الجنائي في قضية سرقة مبلغ 3040627 بإستخدام الكمبيوتر من شركة كنديان نكسن بتروليم يمن، حيث تمكن المتهمون في هذه الجريمة من سرقة مال منقول مملوك لتلك الشركة، بأن قام المتهم الأول الذي يعمل في الشركة بإستخدام جهاز الكمبيوتر الخاص بأحد زملاءه و فتح نظام الحوالات مستخدما كلمة السر الخاصة بزميله، وكلمة السر المكملة الخاصة بالموظف الأجنبي، وسحب مبلغ ثلاثة مليون وأربعون ألف وتسعمائة وسبعة وعشرون دولار أمريكي من حساب الشركة المجني عليها طرف بنك أوف أمريكا، وتحويلها على دفعات إلى عدة بنوك في ماليزيا إلى حساب المتهمين الثاني والثالث، و قد تم تحويلها إلى البنوك في اليمن إلى حساب المتهم الرابع، وقد قام المتهمون لإتمام الجريمة بتغيير

كما قضت محكمة ولاية جورجيا بمعاقبة كليفيناد هوليو بالسجن ووضعه تحت المراقبة لمدة ثلاث سنوات وتعويض قدره 300000 دولا الزم بسداده لستي بنك لإستيلائه على مبلغ 384000 دولار، فقد قام بالدخول غير المشروع على معطيات المجني عليه وتمكن من الحصول على معطيات التشفير الخاصة بفيزا كارد الخاصة به، تم تمكن من تزويره وتوصل بدلك إلى الإستيلاء على ذلك المبلغ من خلال السحب النقدي المباشر[1].

وكما هو الشأن "في قانون العقوبات الجزائري والمصري فقد أوجد قانون العقوبات الفرنسي قيودا على تحريك الدعوى الجنائية في الجرائم التي تقع في خارج فرنسا، فقد نصت المادة 113-8 من قانون العقوبات الفرنسي على أنه "***في الجرائم المنصوص عليها في المادتين 113-6 113-7 لا يجوز إقامة الدعوى الجزائية إلا بناء على طلب من النيابة العمومية، ويجب أن يكن ذلك الطلب مسبوقا بشكوى من المجني عليه أو من خلفه أو بناء على بلاغ رسمي من سلطات الدولة التي حدثت الواقعة داخل إقليمها***".

وقد نصت المادة 113-9 ***على أنه "في الحالات المنصوص عليها عليها في المواد 113-6 113-7 لا ترفع الدعوى الجنائية ضد الشخص الذي ثبت أنه قد حوكم نهائيا في الخارج عن ذاتالوقائع، وفي حالة الإدانة ثبت أنه قضي العقوبة أو سقطت بالتقادم***"

ويلاحظ مما سبق أن المشرع الفرنسي يسوي بين إستيفاء العقوبة وبين سقوطها بالتقادم من حيث الأثر المتمثل في منع تحريك الدعوى الجنائية عن الجريمة المرتكبة في الخارج.

إن تطبيق مبدأ شخصية النص الجزائي على الجرائم الواقعة على التعاملات الإلكترونية يصطدم بالعديد من العقبـــات أهمـــها:

- أن هذا المبدأ يعتمد على تحديد جنسية مرتكب الفعل، إلا أنه من أحد المشاكل التي تطرح للكفاح ضدّ الإجرام في عالم الشّبكات هو صعوبة تحديد فاعل الجريمة، سيما وأن الدليل الإلكتروني تقف حدوده عند التعرف على عنوان بروتوكل الأنترنت وفي أفضل الفروض إلى الحاسوب والخادم والمضيف والشّبكات التي إرتكبت الجريمة به.

-كما أن محاكمة المجرم الموجود في دولة أجنبية أمر يحتاج إلى إجراءات طويلة ومكلفة، وتشمل المحاكمة هنا جميع اجراءات الضبط والقبض والتحقيق والتقديم والمحاكمة، وتنفيد الأحكام التي تصدر في الخارج.

-إن الدول التي وقعت على اتفاقيات لتسليم المجرمين يعد قليل جدا بالمقارنة بعدد الدول التي تتصل بالأنترنت.

أسمائهم الحقيقية بوثائق إثبات شخصية مزورة. وقد إرتكبت الأفعال المكونة للركن المادي للجريمة خارج إقليم الجمهورية اليمنية، في ماليزيا، إلا أنه وتطبيقا لمبدأ شخصية النص الجنائي إختص القضاء اليمني بنظر الدعوى حيث قضي بإدانة المتهمين. وذلك عملا بنص المادة 41 من القانون رقم 40 لسنة 2006 والتي تنص على معاقبة" كل من يرتكب فعلا يشكل جريمة بموجب أحكام القوانين النافدة بواسطة إستخدام الوسائل الإلكترونية:**صالح الماوري**، تعزيز قدرات الموارد البشرية في عمليات التحقيق والإدعاء والمحاكمة في الجرائم المتصلة بالكمبيوتر-أعمال الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، 19-20 نيسان، يونيو 2007، المملكة المغربية، ص78.

[1]- U.S department of justice central district of california debra wong yang united states ***attorney*** thom mrozek, public affairs officer

https://www.dol.gov/sites/default/files/ebsa/about-ebsa/our-activities/newsroom/criminal-releases/graf2.pdf

– إذا لم يكن القانون الوطني يجرم الفعل الذي أحدث الضرر، فإن على المتضرر أن يسافر إلى دولة مرتكب هذا الفعل لإقامة دعواه هناك، والأشد من ذلك أنه حينما يسافر قد لا يكون القانون الأجنبي يجرم الفعل الذي ألحق به الضرر مما يوقع المجني عليه في ظلم شديد[1].

لدا نرى بأنه يجب أن يكون هنالك جهود دولية لإيجاد أداة **قانونية** على غرار القانون الدولي الخاص لتطبق على الجرائم الإلكترونية بصفة عامة والجرائم الواقعة على التعاملات الإلكترونية بصفة خاصة.

الفرع الثالث

مبدأ عينية القانون الجزائي وجرائم التعاملات الإلكترونية

لاشك أن لكل دولة من الدول مجموعة من المصالح الأساسية التي تمثل جوهر كيانها ووجودها، ولها من أهم هذه المصالح، مصلحة الدولة في حماية أمنها الداخلي والخارجي ومصالحها السياسية والإقتصادية، وهذه المصالح قد يتم الإعتداء عليها من خارج إقليم الدولة صاحبة الشأن ومن أشخاص لا يحملون جنسيتها، لذلك وجدت الدولة لزاما عليها الركون إلى مبدأ جديد **هو مبدأ العينية**[2].

يعني مبدأ العينية تطبيق القانون الجنائي للدولة على الجرائم التي تشكل إخلالا بمصالحها الأساسية أو الجوهرية، وذلك بصرف النظر عن مكان وقوع الجريمة وأيا كان جنسية فاعلها[3]. فالمعول عليه هنا هو طبيعة هذه الجرائم.

لقد توجه المشرع الجزائري ذات توجه العديد من التشريعات –كالمشرع الفرنسي في المادة 113–10 والمصري المادة 2–2 عقوبات– فأخذ بمبدأ العينية في جرائم معينة وردت على سبيل الحصر، وهي الجرائم المنصوص عليها في المادة 588 من قانون الإجراءات الجزائية ***"كل اجنبي ارتكب خارج الإقليم الجزائري بصفة فاعل اصلي أو شريك جناية أو جنحة ضد سلامة الدولة الجزائرية أو تزييفا لنقود أو أوراق مصرفية وطنية متداولة قانونا بالجزائر تجوز متابعته و محكامته وفقا لأحكام القانون الجزائري إذا القي القبض عليه في الجزائر أو حصلت الحكومة على تسليمه لها".***

والملاحظ أن هذه المادة حصرت الجرائم التي يؤول الإختصاص فيها للقضاء الجزائري في تلك المرتكبة ضد أمنها، أو المتعلقة بتزييف النقود الوطنية أو الأوراق المصرفية.

وتطبيقا لذلك فإن بعض هذه الجرائم يمكن أن ترتكب عبر تكنولوجيا الإعلام والإتصال، فإذا شخص في الخارج قام بإختراق النظام المعلوماتي لوزارة الدفاع الجزائرية عبر الشبكة بقصد الحصول على معلومات سرية، يكون مرتكبا لجريمة التجسس، أو إرتبط الإعتداء على التوقيع الإلكتروني بجريمة من جرائم الإعتداء

---

[1]-**د حسين بن سعيد الغافري**، السياسة الجنائية في مواجهة جرائم الأنترنت، المرجع السابق، ص584.

[2]– **عمر عبيد محمد الغول**، نطاق تطبيق القانون الجنائي من حيث المكان وفقا للمعطيات التكنولوجية المعاصرة، دراسة مقارنة، رسالة دكتوراه، جامعة القاهرة، 2009، ص193.

[3]–**د.عبود السراج**، المرجع السابق، ص175.**د. محمود نجيب حسني**، شرح قانون العقوبات اللبناني–القسم العام– المرجع السابق، ص197.

على أمن الدولة من جهة الداخل أو الخارج، فإن القانون الجزائري المنظم للتعاملات الإلكترونية هو الذي يطبق، والمثال لدلك أن يكون المستند الإلكتروني الذي تم الإعتداء عليه يتعلق باسرار عسكرية يتم إفشاؤها.
كما ينعقد الإختصاص للقضاء الجزائري في حالة تزييف النقود الإلكترونية سواء أخدت شكل البطاقات البلاستيكية أو تلك التي يتم التعامل بها عبر الأنرنت(النقود الشبكية).

لكن في المقابل، فإن المادة 15 من القانون المتضمن الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال وسعت من إختصاص المحاكم الجزائرية وذلك في النظر في الجرائم المتصلة بتكنولوجيات الإعلام والإتصال المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للإقتصاد الوطني، دون أن يدرج **شرط القبض عليه** في الجزائر أو **تسليـــــــمه**.

المطلب الثاني

الإختصاص القضائي الداخلي بنظر جرائم الإعتداء على التعاملات الإلكترونية

في حالة إختصاص القضاء الوطني دوليا بنظر الدعوى الجزائية، فإنه يتعين طرح الدعوى لتنظر أمام المحكمة المختصة، ومن خلال عرضنا لمجال تجريم الإعتداء على التعاملات الإلكترونية تبين لنا من خلال العقوبات التي قررها المشرع لمختلف مظاهر السلوك المادي المنشيء للمسؤولية الجزائية، هي الحبس أقل من 5 سنوات والغرامة أو بإحدى هاتين العقوبتين ومن تم تعد هذه الجرائم من قبيل الجنح كاصل عام ، ومن تم إنعقاد الإختصاص بالنظر في هذه النوعية من الجرائم لمحاكم الجنح. إلا إدا كان الإعتداء على التعاملات الإلكترونية يشكل جناية فإن الإختصاص في هذه الحالة ينعقد لمحكمة الجنايات، كماهو الحال لو كان المستند الإلكتروني رسمي وتم تزويره، ففي هذه الحالة تشكل الواقعة جناية تزوير مستند إلكتروني رسمي أو إستعماله فيما زور من أجله.

إلا أنه ومع إتساع رقعة الدولة وإستحالة جمع الإختصاص في محكمة واحدة كانت الحاجة إلى تنظيم القضاء على أساس معيار يحدد المحكمة المختصة من المكان بعد أن يتم تحديد إختصاصها بالنوع والدرجة.
والأصل أن الإختصاص المحلي للجهات القضائية يتحدد بمكان وقوع الجريمة ومحل إقامة احد الأشخاص أو بالمكان الذي تم في دائرته القبض على هؤلاء.

إلا أنه ونظرا للطبيعة الخاصة للجرائم الواقعة في البيئة التقنية بصفة عامة والجرائم الواقعة على التعاملات الإلكترونية بصفة خاصة وخروجها عن طابع الكلاسيكية وتعقيدها وسرعة تحركها داخل الإقليم وخارجه، وما يتطلبه إثباتها من وسائل وتحكم في التكنولوجيا الحديثة، خطى المشرع الجزائري في خطوة سابقة من نوعها نحو **التخصص** في المعالجة القضائية لهذه النوعية من الجرائم، كانت في صورة إختصاص إقليمي موسع في المادة الجزائية في مختلف مراحل عمر الدعوى، بدأ من التحقيق الأولي إلى الحكم، وذلك بمقتضى التعديل الذي أُجري على نصوص المواد 37 و40 و329 من قانون الإجراءات الجزائية المتضمن

بالقانون رقم 14/04 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم له،متجها في ذلك إلى إرساء "فكرة الأقطاب الجزائية" بدل القضاء المتخصص كون هذا الأخير يقوم على تخصص القضاة والأجهزة القضائية المتخصصة، هذه الأخيرة التي تتطلب إمكانيات مادية وبشرية ضخمة، ليشكل بذلك الجانب البشري حجر الزاوية لفكرة الإقطاب القضائية[1].

وتجسيدا لهذا التوجه، صدر المرسوم التنفيذي رقم 06-348 المؤرخ في 5 أكتوبر 2006، المتضمن تمديد الإختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق[2]، المعدل بموجب المرسوم التنفيذي رقم 16-267 الموافق لـــ 17 أكتوبر 2016.

وعلى ذلك سنحاول من خلال هذا المطلب دراسة التنظيم القانوني لهذه الأقطاب في الجزائر بإعتبارها سابقة في هذا المجال، والآلية التي إعتمدها المشرع في إسناد الإختصاص النوعي (الفرع الأول) والإقليمي (الفرع الثاني).

الفرع الأول

الإختصاص الإقليمي للأقطاب الجزائية المتخصصة

إن فكرة إنشاء أقطاب جزائية متخصصة جاءت إنعكاسا لوضعية العدالة في الجزائر والتوجهات الطموحة نحو إصلاحها وتعزيز مكانتها وتطوير أدائها، وقد جاء في إتفاقية التمويل الجزائرية الأروبية لمشروع دعم إصلاح العدالة في الجزائر أن: هذا المشروع يهدف إلى دعم التخصص وتكوين القضاة داخل وخارج الوطن للإستجابة للمتطلبات المستجدة الناتجة عن التزايد المستمر للمنازعات التي يجب عليهم الفصل فيها، ونظرا لأهمية التخصص القضائي فقد عقد له عدة مؤتمرات دولية منها: مؤتمر روما سنة 1958، مؤتمر نيس 1972، ريودي جانيرو 1978، وقد أكدت هذه المؤتمرات أن التخصص في مجال القضاء له أهمية كبيرة ودور فعال في رفع مستوى العمل القضائي، ولنظام التخصص جانبين : تخصص القضاة وتخصيص جهات القضاء[3].

وبناء عليه قام المشرع الجزائري بموجب القانون رقم 14-04 بتعديل قانون الإجراءات الجزائية، حيث وسع من الإختصاص المحلي لوكيل الجمهورية وقاضي التحقيق والمحكمة إلى دائرة إختصاص محاكم أخرى بخصوص جرائم معينة تتميز بالخطورة والتعقيد يتطلب مكافحتها كفاءة مهنية عالية من بينها "**المساس بنظم المعالجة الآلية للمعطيات.** ليأتي بعدها المرسوم التنفيذي رقم 06-348 المعدل بالمرسوم **رقم 16-267**

---

[1]-**د. عمار بوضياف**، النظام القضائي الجزائري، دار الريحانة، الجزائر، 2003، ص229-230.

[2]- قد بدأت الأقطاب القضائية المتخصصة العمل بالفعل سنة 2008، حيث تم فعلا إعطاء إشارة الإنطلاق الرسمي للأقطاب الجزائية المتخصصة في كل من الجزائر العاصمة يوم 26 فيفري 2008، وهران يوم 5 مارس 2008، أما تدشين مقرالقطب الجزائي المتخصص لمحكمة ورقلة وإعطاء إشارة الإنطلاق الرسمي لنشاط هذا القطب فقد كانت يوم 19 مارس 2008، **محمد بكرارشوش**، المرجع السابق، ص 307.

[3]- **د.عمار بوضياف**، المرجع السابق، ص229.

الموافق ل 17 أكتوبر 2016، ليحدد 4 محاكم وسع من إختصاصها الإقليمي ليشمل دوائر إختصاص محاكم أخرى، وهي محكمة سيدي أمحمد بالجزائر العاصمة، محكمة قسنطينة، وهران ، ورقلة.

+**محكمة سيدي محمد:**يمتد الإختصاص المحلي لمحكمة سيدي أمحمد إلى محاكم المجالس القضائية لـــ: الجزائر، شلف ،الأغواط، البليدة، البويرة ،تيزي وزو، الجلفة، المدية، المسيلة، بومرداس، تيبازة، عين الدفلى.

+ **محكمة قسنطينة:** تمديد الإختصاص المحلي لمحكمة قسنطينةإلى محاكم المجالس القضائية لـــ: قسنطينة و أم البواقي وباتنة وبجاية وتبسة وجيجل وسطيف وسكيكدة وعنابة وقالمة وبرج بوعريريج والطارف وخنشلة وسوق أهراس وميلة.

+**محكمة ورقلة:** تمديد الإختصاص المحلي لمحكمة ورقلة لـــ: ورقلة، أدرار، تمنراست، ايليزي، بسكرة، الوادي، غرداية.

+**محكمة وهران:** تمديد الإختصاص المحلي لمحكمة وهران لـــ: بشار، تلمسان، تيارت، تندوف، سعيدة، سيدي بلعباس، مستغانم، معسكر، البيض، تيسمسيلت، النعامة، عين تموشنت، غليزان.

وفي حالة حصول إشكال في الإختصاص فإن الفصل فيه يعود لرئيس المجلس القضائي الذي تقع في دائرته إختصاص المحكمة التي تم تمديد إختصاصها ، ولايكون أمره قابلا لأي طعن.

زيادة على قواعد الإختصاص السابقة، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والإتصال المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجة للأقتصاد الوطني، مع ما يتطلبه الأمر من تعزيز التعاون والمساعدة القضائية الدولية المتبادلة وفقا للإتفاقيات الدولية ذات الصلة والإتفاقيات الدولية الثنائية ومبدأ المعاملة بالمثل.

إن المتأمل للنصوص القانونية السابقة يجد أن هذه المحاكم عادية[1]، إلا أن تخصصها في جرائم معينة كتلك الواقعة على نظم المعالجة الآلية بمختلف تطبيقاتها مع تعميق فكرة تخصص القضاة، يظهر أن المشرع يتوجه نحو إنشاء محاكم خاصة في المجال الجنائي إلى جانب محاكم القانون العام، مما يحقق تقريب العدالة من المتقاضين وسرعة التقاضي.

[1]–في إجابة لوزير العدل في الجلسة العامة التي عقدت بمجلس الأمة بتاريخ 10 ماي 2005 عن سؤال يتعلق بالفرق بين المحاكم الخاصة والأقطاب القضائية أكـــد أن هذه الأخيرة لا تعتبر محاكم خاصة وأن مبرر إنشاؤها هو طبيعة القضايا التي يستدعي التحقيق والفصل فيها توافر وســائل مـــادية ضخمة وبشرية متخصصة، وعلى ضرورة التعامل مع هذه الأقطاب كمحاكم القانون الـــعام: مجلة مجلس الأمة، العدد21، اوت 2005، ص23، كما أثير نقاش لدى المجلس الدستوريحول مطابقة القانون العضوي المتعلق بالتنظيم القضائي للدستور فيما يخص المواد 24،25،26 منه المتضمنة إنشاء الأقطاب القضائية، حيث أكد أن القانون العضوي قد أخل بالمبدأ الدستوري المستمد من المادتين 122 و123 من الدستور: أنظر: **محمد بكرارشوش**، المرجع السابق، ص312 وما بعدها.

الفرع الثاني

الإختصاص النوعي للأقطاب الجزائية المتخصصة

نظم المشرع الجزائري الإختصاص النوعي للأقطاب الجزائية المتخصصة من خلال تمديده الإختصاص المحلي لكل من وكيل الجمهورية وقاضي التحقيق إلى دائرة إختصاص محاكم أخرى عندما يتعلق الأمر بجرائم محددة من بينها المساس بنظم المعالجة الآلية للمعطيات.

أولا- الإختصاص المحلي لوكيل الجمهورية

يحدد المشرع الجزائري الإختصاص المحلي لوكيل الجمهورية في المادة 37 من قانون الإجراءات الجزائية بمكان وقوع الجريمة وبمحل إقامة أحد الأشخاص المشتبه في مساهمتهم فيها أو بالمكان الذي تم في دائرته القبض على أحد هؤلاء الأشخاص حتى لو حصل هذا القبض لسبب آخر.

ليعود المشرع بموجب الفقرة الثانية من نفس المادة المعدلة بموجب القانون 04-14 ليوسع الإختصاص الإقليمي لوكيل الجمهورية ليشمل إختصاص محاكم أخرى عن طريق التنظيم، كلما تعلق الأمر بالتحري والتحقيق بشأن جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف.

وطبقا للمادة 40 مكرر 1 يتعين على ضابط الشرطة القضائية أن يخبر وكيل الجمهورية فورا لدى المحكمة الكائن بها مكان الجريمة ويبلغه بأصل وبنسختين من إجراءات التحقيق، ويرسل هذا الأخير فورا النسخة الثانية إلى النائب العام لدى المجلس القضائي التابعة له المحكمة المختصة ذات الإختصاص الموسع.

وللنائب العام إذا إعتبر أن الجريمة تدخل ضمن إختصاص المحكمة أن يطالب بالإجراءات فورا، وفي جميع مراحل الدعوى.

ثانيا- الإختصاص المحلي لقاضي التحقيق

عملا بنص المادة 40 من قانون الإجراءات الجزائية المعدلة بالقانون رقم 14-04 المؤرخ في 10 نوفمبر 2004، فإن الإختصاص المحلي لقاضي التحقيق يتحدد بالمكان الذي وقعت فيه الجريمة أو الذي يقيم فيه المتهم أو الذي قبض فيه عليه.

إلا أنه أجازت الفقرة الثانية من نفس المادة تمديد الإختصاص المحلي إلى دائرة إختصاص محاكم أخرى عن طريق التنظيم، في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف.

بل أن المادة 47-4 من قانون الإجراءات الجزائية أجازت لقاضي التحقيق عندما يتعلق الأمر بالجرائم الواقعة على نظم المعالجة الآلية أن يقوم بالتفتيش في أي مكان على إمتداد التراب الوطني، وإذا كان هذا ينطبق على التفتيش المادي، فإن المادة 5 من القانون 09-04 أجازت التفتيش عن بعد ببرامج الدخول.

ثالثا- المحكمة كقطـــب جـــزائي متخصـــص

يتحدد الإختصاص المحلي لمحاكم الجنح حسب المادة 329 من قانون الإجراءات الجزائية بمكان وقوع الجريمة أو محل إقامة أحد المتهمين أو شركائهم أو محل القبض عليهم ولو كان هذا القبض لسبب آخر.
كما تختص المحكمة بالنظر في الجنح والمخالفات غير القابلة للتجزئة أو المرتبطة.
إلا أنه ونظرا للطبيعة الخاصة والمعقدة لبعض الجرائم ومنها الواقعة على نظام المعالجة الآلية، وسع المشرع من الإختصاص المحلي لعدد من محاكم الجنح إلى إختصاص محاكم مجالس قضائية، وذلك بمقتضى الفقرة الأخيرة من نفس المادة المضافة بالقانون 04-14، حيثأجاز بموجبها تمديد الإختصاص المحلي للمحكمة إلى دائرة إختصاص محاكم أخرى عن طريق التنظيم.

وتطبيقا للمواد 37 و40 و329 من قانون الإجراءات الجزائية، جاء المرسوم التنفيذي رقم348/06 المؤرخ في 05 أكتوبر 2006 والمعدل بموجب**المرسوم رقم 16-267 الموافق ل 17 أكتوبر 2016** لتمديد الإختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق في الجرائم المتعلقة بالمتاجرة بالمخدراتوالجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف.

والملاحظ أن هذه الأقطاب تختص فقط في الجرائم الواقعة على نظم المعالجة الآلية بتطبيقاتها المختلفة موقع إلكتروني، منظومة توقيع إلكتروني....، ومن ثم فتستبعد ما عداها والتي تندرج تحتها العديد من الجرائم التي تقع على التعاملات لإلكترونية كالتعامل في المعطيات الشخصية، تزوير المستند الإلكتروني... وهو ما يجب أن يتداركه المشرع، من ضرورة أن يشمل الإختصاص جميع الجرائم الواقعة في البيئة التقنية على نحو مافعل في المادة 15 من القانون المتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، أيــن وسع من إختصاص المحاكم الجزائرية بالنظر في جميع الجرائم المتصلة بتكنولوجيات الإعلام والإتصال المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجة للإقتصاد الوطني.

المطلب الثالث

حجية الدليل الإلكتروني أمـــــام القضـــــــــاء الجزائي

إذا تم إحالة الدعوى الجزائية للمحكمة المختصة ، تبدأ مرحلة جديدة هي المحاكمة، وما يهمنا في هذا المجال هو كيف سيتعامل القاضي مع الأدلة ذات الطبيعة الإلكترونية عند عرضها على شكل صورة أو مستند أو تسجيل، خاصة أن **جانبا** من هذه المعلومات لايدخلها أو ينظمها الأشخاص، وإنما يخلقها الجهاز نفسه ضمن عمليات المعالجة وفي إطار تقنيات البرمجيات القائمة على الذكاء الإصطناعي، كسجلات الدخول إلى الأنترنت القائمة على الكيفية المعنوية، **وجانب آخر** من المعلومات يمكن التلاعب بها بما يجعل مضمونها مخالفا للحقيقة، وهو ما يطرح التساؤل عن القوة الثبوتية التي يتمتع بها هذا الدليل، وما مدى حرية القاضي بالإقتناع به لبناء الحكم على أساس البراءة أو الإدانة؟

وتظهر أهمية إعتراف القانون بالأدلة ذات الطبيعة الالكترونية ، خاصة مع إحتمال ظهور أنشطة جرمية عديدة في بيئة الاعمال والتجارة والبنوك الالكترونية في مسألة إنكاره، فنكون بصدد فرد إرتكب جريمة ومع ذلك برز العجز واضحا في إدانته وإستمر طليقا يراه المجتمع مذنبا والقانون عاجزا عن إدانته.

ولا يثير الدليل الإلكتروني مشكلات تتعلق بالإثبات في المواد الجزائية فحسب، بل حتى في المواد المدنية إذا ما توقف الفصل في الدعوى الجزائية على إثبات معاملة الكترونية بموجب دليل الكتروني، وهو ما يطرح عدة تساؤلات في حالة ما إذا ثار نزاع حول صحته.

وعلى ذلك سوف نتناول حجية الدليل الإلكتروني في المواد الجزائية في الفرع الأول، وحجيته في المواد المدنية في الفرع الثاني.

الفرع الأول

حجية الدليل الإلكتروني في المواد الجزائية أمام القضاء الجزائي

مع أن الأدلة ليست سوى وسائل تهدف إلى للتوصل للحقيقة، ويمكن من حيث المبدأ إقامتها أمـــام القضـــاء الجزائي وتأسيس إقتناع القاضي عليها، مادامت مشروعة، إلا أن قبول ما يكون منها مستمدا مـــن الوســـائل الإلكترونية تصادفه صعوبات قانونية وعملية عديدة، خاصة في الأنظمة الإجرائية الإثباتية المختلفة.

أولا- حجية الدليل الإلكتروني في النظام اللاتيني

في ظل**نظام الإثبات الحر**الذي تأخذ به القوانين ذات الصياغة اللاتينية، فإن القانون لا يرسم طرقا محددة للإثبات يتقيد بها القاضي الجنائي، بل يترك حرية الإثبات لأطراف الخصومة في أن يقدموا ما يرون أنه

مناسب لإقتناع القاضي، ويترك للقاضي في أن يلتمس تكوين إعتقاده من أي دليل يطرح أمامه، وفي أن يقدر القيمة الإقناعية لكل منها حسبما تتكشف لوجدانه.[1]

وفي ظل هذا النظام، تتناول بعض التشريعات مسالة قبول الأدلة الكترونية، في حين يطبق البعض الآخر منها القواعد العامة عليها.

ففي فرنسا، أقر المشرع الفرنسي المبدأ العام في الإثبات وهو "حرية الإثبات" بموجب المادة 427 من قانون الإجراءات الجزائية حيث نصت " ما لم يرد نص مخالف، يجوز إثبات الجرائم بجميع طرق الإثبات، ويحكم القاضي بناء على إقتناعه الشخصي"[2].وهذا النّص وإن كان مخصصاً لمحاكم الجنح، إلاّ أنّ مبدأ حريّة الإثبات يطبّق أمام جميع أنواع المحاكم الجزائيّة، إلاّ إذا نصّ القانون على خلاف ذلك.

والواقع أن الفقه الفرنسي يدرس حجية الدليل الإلكتروني ضمن مسألة أوسع وأعم هي مسألة قبول الأدلة الناشئة عن الآلة أو الأدلة العلمية، مثل الرادارات والأجهزة السينمائية وأجهزة التصوير وأشرطة التسجيل و أجهزة التصنت، أما القضاء فقد قبل هذه الأدلة إذا ما إستوفت شروطا معينة كأن يتم الحصول عليها بطريقة شرعية ونزيهة وأن يتم مناقشتها حضوريا من قبل الأطراف[3].

كذلك هو الوضع في التشريع الجزائري، حيث أقر هذا الأخير مبدأ حريّة الإثبات الجزائي في المادة 212 من قانون الإجراءات الجزائية حيث نصّت على أنّه" يجوز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك, وللقاضي أن يصدر حكمه تبعاً لاقتناعه الشّخصي"، مدرجا هذه المادة ضمن الفصل الأول من الباب الأول من الكتاب الثاني تحت عنوان "في طرق الإثبات"، وهو بذلك قد قطع من كون هذه المادة تطبق أمام جميع الجهات القضائية الجزائية.

أما بخصوص الدليل الإلكتروني، فقد نظم المشرع الجزائري طرق الحصول عليه في القانون رقم 09-04 والذي يستفاد من نصوصه **إعتماد وقبول** المشرع للدليل الإلكتروني سواء كان **صور أو تسجيلات رقمية أو مستندات كدليل إثبات**، وهو مايستفاد من المادة 4 المنظمة لمراقبة الإتصالات الإلكترونية سواء كانت كتابات أو صور أو أصوات أو معلومات مختلفة، والمادة 5 و6 المتعلقة بتفتيش وحجز المعطيات المخزنة المفيدة في كشف الحقيقة، والمادة 11 المتعلقة بحفظ المعطيات المتعلقة بحركة السير، وذلك وفق ضوابط إجرائية معينة.

أما المشرع المصري، و إن لم يورد أي نص ينظم الأدلة الإلكترونية، إلا أنه إعمالا لنص المادة 291 من قانون الإجراءات الجزائية المصري التي نصت": للمحكمة أن تأمر ولو من تلقاء نفسها أثناء نظر الدعوى، بتقديم أي دليل تراه لازما لظهور الحقيقة"، والمادة 302 التي نصت "يحكم القاضي في الدعوى حسب العقيدة التي تكون لديه بكامل حريته ومع ذلك فلا يجوز أن يبني حكمه على دليل لم يطرح أمامه في الجلسة...."فإن الدليل الإلكتروني يخضع للسلطة التقديرية للقاضي في الأخذ به أو رفضه.

---

[1]-**د. موسى مسعود أرحومة**، المرجع السابق، ص 25

[2]-Article 427 du CPPF dispose que " Hors les cas où la loi en dispose autrement, les infractions peuvent être établies par tout mode de preuve et le juge décide d'après son intime conviction."

[3]- **د. هلالي عبد الله أحمـــد**، حجية المخرجات الكمبيوترية في المواد الجنائية، الطبعة الثانية، دار النهضة العربية، القاهرة، 2008، ص43.

ومن تم وتطبيقا لما سبق، فإن للقاضي الجزائي **دور إيجابي** في توفير وقبول وتقدير الدليل الجنائي بما في ذلك الدليل الإلكتروني، في مقابل إنحصار دور المشرع:

أ- الدور الإيجابي للقاضي الجزائي في توفير الدليل الإلكتروني:

حيث أن الدعوى الجزائية تشكل نشاط القاضي، فهو القائم على إدارتها، وعليه أن يصل إلى معرفة الحقيقة كما وجدت في الواقع، فهو ملزم قانونا بالبحث عن الأدلة اللازمة لظهور الحقيقة ولا يكتفي في سبيل ذلك بما يقدمه الخصوم أو ما يتفقون عليه من أدلة كما هو الشأن في الخصومة المدنية[1].

وتطبيقا على الجرائم الواقعة على التعاملات الإلكترونية، فإن القاضي الجزائي يستطيع من أجل الوصول إلى الحقيقة أن يطلع على جميع المعلومات التي تخص مستخدم الأنترنت وهو متصل بها: كالمعلومات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الإتصال وكذا عناوين المواقع المطلع عليها، تاريخ ووقت ومدة كل اتصال، الرسائل الإلكترونية التي أرسلها، رقم الدخول والمعطيات المتعلقة بالفاتورة أو الدفع المتوافرة على أساس عقد والتوقيع عليها، عنوانه البريدي أو الجغرافي، المعلومات اللازمة لتحديد هوية من قاموا بإنشاء موقع معين على الأنترنت...[2]

ومن مظاهر الدور الإيجابي للقاضي الجزائي في توفير الدليل الإلكتروني أنه بإمكان القاضي الجزائي أن يأمر مدير النظام بأن يقدم المساعدة اللازمة عقلا من أجل السماح بتطبيق إجراء التفتيش أو الضبط، متى ما قدر ضرورة وملائمة هذا الإجراء.

ب-الدور الإيجابي للقاضي الجزائي في قبول الدليل الإلكتروني:

تعد مرحلة قبول الدليل الإلكتروني الخطوة الثانية بعد البحث عن الدليل وتقديمه، ومع تنظيم كل من المشرع الفرنسي والجزائري للدليل الإلكتروني، وفي غياب نص صريح بقبول الدليل الإلكتروني في التشريع المصري، فيعد **مقبول** مبدئيا في إثبات الجرائم الواقعة على التعاملات الإلكترونية، إذا ما تم الإحترام فيه على **ضابط المشروعية** وفق القواعد العامة التي تكفل وجوده، وذلك قبل الوصول إلى مرحلة تقديره.

وبناء على ذلك، نستطيع القول أن للقاضي أن يقبل المستندات الإلكترونية المخزنة في النظم المعلوماتية والشفرات المكونة لرموز تشفير التوقيع الإلكتروني، والمعطيات المتحفظ عليها أو التي تم إعتراضها، أرقام الكود السرية لبطاقات الإئتمان ... فكل هذه أدلة الكترونية وإن كان يستلزم هنا التحفظ على منظومة التخزين كونها حرز لا زم هنا كونه يشكل البيئة للدليل الإلكتروني، فطبيعة هذا الأخير تجعل من البيئة التي يحيا فيها أمرا لازما بدونها لا يمكن الإعتماد عليه، وهو ما أشارت إليه المادة 6 من القانون 09-04 بقولها"...يتم نسخ

[1]-**د. حسن سعيد عبد اللطيف**، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الأنترنت، الطبعة الأولى، دار النهضة العربية، القاهرة، 1999،ص 140.

[2]-TGI Paris, référé, 2 février 2004, Métrobus c/ Ouvaton , disponible en lingne á l'adresse suivante : http://juriscom.net/2004/02/tgi-paris-refere-2-fevrier-2004-metrobus-c-ouvaton/

المعطيات محل البحث والمعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز..."[1].

وتطبيقا لذلك قضت محكمة ولاية نيو جرسي بمحاكمة جاسون صلاح عرابة بالسجن 30 شهرا وإلزامه برد مبلغ 504490 دولار بتهمة الولوج داخل النظام المعلوماتي وتدمير الموقع الإلكتروني لشركتي جيرسي و كراستوفير للملابس الرياضية المنافسة له وذلك بالإستيلاء على البرامج والرموز الخاصة بهما مما ألحق بهما أضرارا بالغة[2].

ت- الدور الإيجابي للقاضي الجزائي في تقدير الدليل الإلكتروني:

ما من شك في أن نظرية الإثبات هي المحور الذي تدور عليه قواعد الإجراءات الجزائية مند لحظة وقوع الجريمة إلى حين إصدار الحكم النهائي بشأنها، وهذا الحكم لا يمكن إصداره إلا من خلال العملية القضائية التي يمارسها القاضي الجزائي طبقا للسلطات الممنوحة إليه. وأبرز هذه السلطات هو ما يتعلق بجانب تقدير الأدلة، فمن خلال عملية التقدير هذه يتم الوصول إلى الحقيقة التي يعلنها الحكم الجنائي والذي يمثل عنوانا لها.

والسائد في الفقه، أن سلطة القاضي الجنائي في تقدير الأدلة يحكمها مبدأ حرية القاضي الجنائي في تكوين قناعته، وأن هذا المبدأ يؤدي إلى نتيجتين هما:

1-حرية القاضي في قبول الأدلة

2-حرية القاضي في تقدير الأدلة

و إن كنا نسلم مع إجماع الفقه[3] بالنتيجة الثانية دون الأولى، كون هذه الأخيرة مسالة قانونية لا مجال لإعمال سلطة القاضي التقديرية فيها، حيث أن المشرع قد حسم هذه المسألة بتحديده النموذج القانوني للدليل القابل للإثبات، فمتى ما توفرت فيه شروط هذا النموذج طبقا لمبدأ الشرعية الإجرائية، وجب على القاضي إخضاعه لعملية تقديره، أما الثانية فهي مسالة تتعلق بقيمة الدليل لإثبات الحقيقة وهي مسالة موضوعية محضة، للقاضي أن يمارس سلطته التقديرية فيها، بل هي المجال الطبيعي لهذه السلطة حيث أنها تتعلق بقيمة الدليل في الإثبات وصولا للحقيقة.

وقد أقرت معظم التشريعات الحديثة مبدأ الإقتناع القضائي، حيث أقره المشرع الجزائري بموجب المادة 307 من قانون الإجراءات الجزائية وهي مستوحاة من المادّة 353 من القانون الإجراءات الفرنسي

---

[1]- كما قضت محكمة النقض الفرنسية من أن أشرطة التسجيل الممغنطة التي يكون لها قيمة دلائل الإثبات يمكن أن تكون صالحة للتقديم أمام القضـــاء الجنائي" أنظـــر :**د. علي حسن محمد الطوالبة**، المرجع السابق، ص196.

Cass,crim,28 avr,1987,bull,crim n 173

[2]-U.S department of justice central district of california debra wong yang united states ***attorney*** thom mrozek, public affairs officer,disponible en lingne á l'adresse suivantehttps://www.dol.gov/sites/default/files/ebsa/about-ebsa/our-activities/newsroom/criminal-releases/graf2.pdf

[3]- د. **فاضل زيدان محمد**، سلطة القاضي الجنائي في تقدير الأدلة، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن، 2006، ص93، **د.محمود نجيب حسني**، شرح قانون الإجراءات الجنائية، المرجع السابق، ص438، **د.عبد الوهاب حومد**، أصول المحاكمات الجزائية، المرجع السابق، ص334.

حيث تنص على "... *إن القانون لا يطلب من القضاة أن يقدموا حسابا على الوسائل التي بها قد وصلوا إلى تكوين اقتناعهم, ولا يرسم لهم قواعد بها يتعين عليهم أن يخضعوا لها على الأخص تقدير تمام أو كفاية دليل ما, ولكنّه يأمرهم أن يسألوا أنفسهم في صمت أن يبحثوا بإخلاص ضمائرهم في أيّ تأثير قد أحدثته في إدراكهم الأدلّة المسندة إلى المتّهم و أوجه الدّفاع عنها و لم يضع لهم القانون سوى هذا السّؤال الّذي يتضمّن كلّ نطاق واجباتهم: هل لديكم اقتناع شخصي*"[1]. كما أنّ الاقتناع القضائي كرّسته أيضًا صراحة المادة 212 من قانون الإجراءات الجزائية.

وقد ورد المبدأ ذاته في المادة 302-1من قانون الإجراءات الجزائية المصري حيث نصت على أنه" يحكم القاضي في الدعوى حسب العقيدة التي تكونت لديه بكامل حريته، وتؤكد هذا المبدأ أيضا المادتين 291-1 و المادة 300 من نفس القانون.

وإعمالا لهذا المبدأ، فإن الدليل الإلكتروني لا يحظ بقوة حاسمة في الإثبات، وإنما هو مجرد دليل لا تختلف قيمته ولا تزيد حجته عن سواه، ومن تم يصح للقاضي أن يؤسس إقتناعه على الدليل الإلكتروني كما يصح أن يهدره تبعا لإطمئنانه، ولا يجوز مطالبة القاضي أو إلزامه بالإقتناع بالدليل الإلكتروني ولو لم تكن في الدعوى أدلة سواه.

إلا أن إعتبار الدليل الإلكتروني من تطبيقات الدليل العلمي بما يتميز به من حياد وموضوعية وكفاءة في إقناع القاضي، هذه السمات قد تدفع إلى القول بأن بمقدار إتساع مساحة الأدلة العلمية بمقدار ما يكون إنكماش وتضاؤل دور القاضي الجنائي في التقدير. إلا أن هذا التصور ليس في محله، ويذهب الفقه[2]إلى التمييز بين أمرين:القيمة العلمية القاطعة للدليل، الظروف والملابسات التي وجد فيها هذا الدليل.

فتقدير القاضي لا يتناول القيمة العلمية القاطعة للدليل، ذلك أن قيمة الدليل تقوم على أسس علمية دقيقة، ولاحرية للقاضي في مناقشة الحقائق العلمية الثابتة. أما مايتعلق بالظروف والملابسات التي وجد فيها هذا الدليل، فإنها تدخل في نطاق تقديره الشخصي لأنها من طبيعة عمله، ومن ثم فللقاضي الجزائي أن يطرح الدليل المستخرج من النظام عندما يجد أن وجوده لا يتفق منطقيا مع ظروف الواقعة، فمجرد توفر الدليل العلمي لا يعني أن يحكم القاضي مباشرة بالإدانة أو البراءة دون البحث بالظروف والملابسات، فالدليل العلمي ليس ألية أعدت لتقرير إقتناع القاضي نحو مسالة غير مؤكدة.

---

[1]-**Article 353 du cPPF**Modifié par LOI n°2011-939 du 10 août 2011 - art. 12dispose que "Avant que la cour d'assises se retire, le président donne lecture de l'instruction suivante, qui est, en outre, affichée en gros caractères, dans le lieu le plus apparent de la chambre des délibérations :

" Sous réserve de l'exigence de motivation de la décision, la loi ne demande pas compte à chacun des juges et jurés composant la cour d'assises des moyens par lesquels ils se sont convaincus, elle ne leur prescrit pas de règles desquelles ils doivent faire particulièrement dépendre la plénitude et la suffisance d'une preuve ; elle leur prescrit de s'interroger eux-mêmes dans le silence et le recueillement et de chercher, dans la sincérité de leur conscience, quelle impression ont faite, sur leur raison, les preuves rapportées contre l'accusé, et les moyens de sa défense. La loi ne leur fait que cette seule question, qui renferme toute la mesure de leurs devoirs : " Avez-vous une intime conviction ? ". "

[2]- **د. هلالي عبد اللاه أحمـــد**، حجية المخرجات الكمبيوترية في المواد الجنائية، المرجع السابق، ص46، **د.جميل عبد الباقي صغير**، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، المرجع السابق، ص22. **د. محمد طارق عبد الرؤوف الخن**، المرجع السابق، ص364.

ونحن نؤيد فيما ذهب إليه الفقه، فالقاضي ليس له أن ينازع فيما إستقرت عليه تقنية المعلومات من الناحية العلمية، وإنما له أن يقدر الظروف والملابسات التي أحاطت بهذا الدليل، ويساعده في هذا التقدير الأدلة التقليدية التي توجد عادة إلى جانب الدليل الإلكتروني، فله أن يرفض الدليل إذا لم يقتنع بظروف الواقعة وملابستها.

بناء على ذلك يمكن القول أن التطور العلمي في مجال الأدلة لا يتعارض مع سلطة القاضي الجنائي في تقديرها، بل أنها جعلت من الإقتناع أكثر جزما ويقينا، كما أنها ساعدت على التقليل من الأخطاء القضائية، والإقتراب إلى العدالة بخطوات أوسع.

الفرع الثاني

حجية الدليل الإلكتروني في النظام الأنجلو أمريكي

إن كان الدليل الإلكتروني لا يصادف عقبات بالنسبة لحرية القاضي في تقديره في ظل النظام الأنجلوأمريكي حيث يعبر عليها بـــ "الإدانة دون شك معقول"، فإنه يجد صعوبات في التقدم به، ذلك أن الدول التي تكون تشريعاتها ذات أصل أنجلوأمريكيفإن الدليلتحكمة قواعد خاصة لقبوله أمام المحاكم،هو تطبيق قاعدة **إستبعاد شهادة السماع**، وقاعدة **الدليل الأفضل**.

ففي الولايات المتحدة الأمريكية فإن القانون الفدرالي الأمريكي للأدلة يطبق على الأدلة المستخلصة من الحاسوب والمسماة بـــ"**سجلات الحاسوب**، وهو مايثير مسألة مقبولية الدليل الإلكتروني في إطار القاعدتين السابقتين:

أولا– قاعدة إستبعاد شهادة السماع

شهادة السماع يكون الشاهد الذي يدلي بها قد نما إلى سمعه إن أمرا حدث، فهو لم يشاهد أو يشارك بإحدى حواسه في الواقعة التي تنظرها المحكمة في الجلسة، وإنما نما إلى سمعه فقط ما حدث بشأن هذه الواقعة. ومثل هذه الشهادة مرفوضة على إستثناء في الأنظمة الأنجلوأمريكية. ومن بين هذه الإستثناءات: المعطيات والمعلومات التي يتم الحصول عليها من الكمبيوتر.

والأصل أن الدليل الإلكتروني يشكل شهادة سماعية كون هذا الدليل يتضمن جمل وكلمات أدخلها شخص إلى جهاز الكمبيوتر، سواء تمت معالجة تلك المعطيات أو لا، في هذه الحالة يتعين إثبات أن الدليل الإلكتروني يشكل **إستثناء على قاعدة الشهادة السماعية** حتى يتم الإعتداد بها كحجة في الإثبات[1]. وفي هذا الإطار ينبغي التمييز بين أنواع سجلات الحاسوب التي قسمتها المحاكم الفدرالية الأمريكية [2]:

---

[1]- **د. شيماء عبد الغني**، المرجع السابق، ص402.

[2]–**د. عمر محمد بن يونس**، الإجراءات الجنائية عبر الأنترنت في القانون الأمريكي، المرجع السابق، ص 433 ومابعدها.

- ✓ سجلات الحاسوب المخزنة: وهي تحتوي على معطيات بشرية مثل المخرجات من برنامج الكتابة من الكمبيوتر، فهي تعتبر شهادة سماعية مثلها في ذلك مثل الكلمات أو التقريرات التي يسجلها الإنسان على الأجهزة المختلفة، وقبل ان تقبل المحكمة بالسجلات فإنه يجب ان يثبت لها أن المعطيات الموجودة في السجل قد تم إعدادها في ظروف تهدف إلى ضمان صحتها والثقة بها.
- ✓ سجلات الحاسوب المتوالدة: الجهاز هو الذي يقوم بتدوين المعطيات التي تصلح أن تقدم مباشرة إلى المحكمة كمعطيات الدخول على المواقع وملفات تسجيل الإتصالات، فهي ليست من قبيل شهادة السماع، وتتوقف قيمتها الثبوتية على ما إذا كان الجهاز يعمل بطريقة صحيحة أم لا.
- ✓ توجد هناك فئة ثالثة: تجمع بين سجلات الحاسوب المتوالدة وسجلات الحاسوب المخزنة، ومثاله إستخدام المشتبه فيه في قضية إحتيال جدول لمعالجة أشكال مالية ذات علاقة بنموذج إحتيال، سوف يتم إشتقاق سجل الحاسوب الذي يحتوي على مخرجات البرنامج من كل من المعطيات الإنسانية و معالجة الحاسوب، وإن كان جزء منها يعد شهادة سماع ، إلا أنها لا تعتبر شهادة سماع، حتى وإن كان يجب توافر لصحة المستند الإلكتروني شرطين: فمن ناحية توافر الشرط اللازم لصحة الشهادة السماعية، كما أنه يجب التأكد من عمل الجهاز نفسه على نحو صحيح.

وبناء عليه فإن النيابة العامة إذا إستندت إلى مستند إلكتروني في دعوى جزائية يتعين عليها أن تقدم الدليل على أن الجهاز يعمل بطريقة صحيحة[1]، ومع ذلك تذهب أحكام القضاء الأمريكي على أنه لا يلزم أن يثبت صحة عمل الكمبيوتر من جانب الخبير[2].

ثانيا- قاعدة الدليل الأفضل

فضلا عما سبق، تتجه التشريعات ذات الأصل الأنجلوأمريكي إلى تطبيق **قاعدة الدليل الأفضل**، والتي تقضي: أنه لأجل إثبات محتويات كتابة أو سجل أو ورقة فإن أصل الكتابة أو السجل أو الورقة يكون عادة مطلوبا[3]، وقد قررها القانون الأمريكي في المادة 1002 من قانون **الإثبات الأمريكي** والتي جاء نصها "باستثناء ماهو مقرر في هدا القانون أو بقانون خاص يصدر عن الكونجرس، فإن عند إثبات مضمون الكتابة والتسجيل والورقة فإنه يلزم توافر **أصل الكتابة والتسجيل والصورة**[4]".

وقاعدة الدليل الأفضل التي تعبر عن أصالة الدليل تقف حائلا أمام الدليل الإلكتروني، لأن ما يتم تقديمه إلى المحكمة ليس الملفات الإلكترونية المخزنة في الحاسوب وإنما نسخ من هذه الملفات.

---

[1]-**United States v.simpson** 152 F.2d 1241, 1250 (10 th Cir 1998)available at :http://openjurist.org/152/f3d/1241/united-states-v-simpson

[2]-united states v moore ,923f2d910,915 (1st Cir 1991)united states , v,Whitaker,127 f,3d 595 ,601(7th cir 1997)united states v miller , 771 f 2d 1219, 1237 (9 th cir 1985) .

مشار إليه لدى:**د. شيماء عبد الغني**، المرجع السابق، ص410.

[3]-**د.عمر بن يونس**، الإجراءات الجنائية عبر الأنترنت، المرجع السابق، ص440.

[4]**Rule 1002 of** Federal Rules of Evidence provides that:to prove the content of a writing , recording, or photograph, the original writing recording or photograph is required except as otherwise provided in these rules or by act of congres"available at:
https://en.wikibooks.org/wiki/Federal_Rules_of_Evidence

وعليه ومع ظهور المستندات المعلوماتية إستدعى الأمر تغيير هذه القاعدة لكي تتلائم مع عصر المعلومات، وهذا ما فعله المشرع الأمريكي حاسما بذلك المسالة للدليل الإلكتروني[1]، حيث طور المادة 1001 لتشمل الدليل الإلكتروني بشكل موسع، بحيث سمحت بالإعتراف بالمواد المكتوبة writings والمسجلة recordingوالإلكترونية electronics لكي تحظى بذات الإهتمام الذي تحظى به الأدلة الأخرى في المحاكم، وبالتالي قام المشرع باستخدام مدلول موسع لمصطلح الأصالة حال التعرض للدليل الإلكتروني، بحيث قام بتعريف الأصالة في الوثائق الإلكترونية صراحة لتشمل المناهج المغناطيبسية والميكانيكية والإلكترونية حال رصد الحروف والكلمات والأرقام أو ما يعادلها أو يتساوى معها[2].

كما توسع المشرع الأمريكي في مدلول عرض الدليل الإلكتروني بموجب المادة 1001(3) والتي نصت على مايلي:"**إذا كانت المعطيات مخزنة في حاسوب أو آلة مشابهة، فإن أي مخرجات مطبوعة منها أو مخرجات يمكن قراءتها بالنظر إليها وتعكس دقة المعطيات تعد معطيات أصلية**""[3]. **لذلك فإن مخرجات الطابعة لمعطيات الحاسوب تفي دائما بأفضل قاعدة للدليل.**[4]

وبناء عليه، فإنه في ظل القانون الأمريكي فإن مخرجات الطابعة نتيجة معالجة الملف من خلال سلسلة العمليات الإلكترونية والآلية تعتبر دليلا أصليا كاملا ولاحاجة لجلب الحاسوب إلى قاعة المحكمة، كما سمح ذات القانون بموجب المادة 1006 بتقديم ملخص للأدلة الإلكترونية إدا كانت الأدلة على شكل عدد كبير من الصفحات يصعب تقديمها للمحكمة[5].

نخلص مما سبق، أن الدليل الإلكتروني مقبول في الأنظمة القانونية المختلفة، وإن كان النظام الأنجلو أمريكي قد أورد شروطا لقبولها نظرا لطبيعة هذا النظام. إلا أن هناك ضوابط معينة تحكم الدليل يلتزم بها القضاة، وهذه الضوابط مناطها مبدأ قرينة البراءة وما يتفرع عنه من نتائج وآثار وما يستتبع ذلك من ضرورة توافر شروط معينة في ألأدلة الإلكترونية حتى يمكن الحكم بالإدانة[6] وتتمثل فـــــي:

-شرعية الأدلة الإلكترونية

- وضعية الأدلة الإلكترونية

---

[1] - **د.عمر محمد بن يونس**، الجرائم الناشئة عن إستخدام الأنترنت، المرجع السابق، ص988.

[2]Rule 1001(1) of Federal Rules of Evidence **provides that** : **(1) Writings and recordings.** "Writings" and "recordings" consist of letters, words, or numbers, or their equivalent, set down by handwriting, typewriting, printing, photostating, photographing, magnetic impulse, mechanical or electronic recording, or other form of data compilation, available at: https://en.wikibooks.org/wiki/Federal_Rules_of_Evidence

[3]-**Rule 1001(3) of Federal Rules of Evidence provides hat** "If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an "original".

[4]-While strictly speaking the original of a photograph might be thought to be only the negative, practicality and common usage require that any print from the negative be regarded as an original. Similarly, practicality and usage confer the status of original upon any computer printout. *Transport Indemnity Co. v. Seib,* 178 Neb. 253, 132 N.W.2d871 (1965).

[5]- **Rule 1006 of Federal Rules of Evidence provides that**The contents of voluminous writings, recordings, or photographs which cannot conveniently be examined in court may be presented in the form of a chart, summary, or calculation. The originals, or duplicates, shall be made available for examination or copying, or both, by other parties at reasonable time and place. The court may order that they be produced in court.

[6]- **د. محمد أحمد المنشاوي**، سلطة القاضي الجنائي في تقدير الدليل الإلكتروني، مجلة الحقوق، المجلد 36، العدد 2، جامعة الكويت، 2012، ص555، **د. علي محمود علي حمودة** ، المرجع السابق، ص62.

-يقينية الأدلة الإلكترونية

و إذا كان ذلك كذلك، فإننا نرى دعوة المشرع العربي عموما إذا ما أخذ حضه في تقنين هذه النوعية من الأدلة كما هو حال المشرع الجزائري، أن يشترط فضلا عن الشروط العامة السابقة، أن يكون الدليل الإلكتروني **مؤمن أو موثوق** حتى يمكن تقدير قيمته من قبل المحكمة، بأن يتوافر فيه:

- **شرط الصحة والمطابقة:** ويطلق عليه البعض من الفقه" مفهوم **سلسلة الرعاية**" [1]:ويقصد بذلك أن الدليل الإلكتروني مند لحظة جمعه وحتى لحظة تقديمه إلى المحكمة لم يطرأ عليه أي تغيير، ولايوجد أي إحتمال للعبث فيه، وأنه تمت مراعاة سلامته حتى يبقى بنفس الحالة التي وجد عليها.
- **شرط الدقة:** أنتكون الأجهزة الحاسوبية أو المنظومات المعلوماتية المستمد منها هذا الدليل تعمل على نحو سليم.

إلا أنه يثور التساؤل فيما لو تمسك المتهم بعدم صحة الدليل الإلكتروني الذي يحتج به كدليل إدانة ضده أو بتعرضه للتغيير؟

إن الدفوع المتعلقة بهذه الشروط، يجب أن لا تنال من قيمة الدليل الإلكتروني إذا جاءت على شكل**تخمين،** دون أن يوجد دليل يدعمها، وهو ما حسمه القضاء الأمريكي، فقضي بأن مجرد الإدعاء بتعديل المعطيات المحفوظة على النظام يعتبر قولا مرسلا لا ينهض للمساس بحجية المعطيات التي يتكون منها الدليل الإلكتروني[2].

الفرع الثاني

حجية الدليل الإلكتروني في المواد المدنية

قد يفترض للفصل في الدعوى الجنائية بالإدانة أو البراءة على وجود علاقة مدنية أو انتفاءها، وهذه العلاقة ليست في ذاتها ركنا للجريمة، ومن ثم ليست مسألة جنائية، بل هي "**مفترض**" لها، ومن تم كان لها كيانها القانوني الذاتي، فتظل لها طبيعتها غير الجنائية على الرغم من إفتراض الجريمة لها، والمثال الواضح لذلك جريمة خيانة الأمانة التي تفترض وجود عقد أمانة يربط بين الجاني والمجني عليه، فهذا العقد مسألة مدنية وهو سابق على إرتكاب فعل الإختلاس أو التبديد أو الإستعمال الذي تقوم به الجريمة، ومن ثم يخضع إثباته **للقواعـد الـمدنية**[3]، وفي هذا الإطار يفرض القانون إعداد دليل كتابي لإثبات التصرفات القانونية

---

[1]- **Eoghan Casey**, op,cit,p78,

د. طارق عبد الرؤوف الخن، المرجع السابق، ص357.

[2]- كما قضى أيضا بأنه لايلزم للقول بصحة معطيات السجل الإلكتروني وقبولها كدليل أن يكون نظام الحاسب خاضعا لحماية تقنية لبرنامج حماية معين والقول بغير ذلك من شأنه حجب القوة التدليلية عن سجلات الحاسب الآلي، فمجرد إحتمال تعرض تلك المعطيات للتغير ليس دليلا على عدم صحة ما نتج عن ذلك الدليل.

United states v .moor ,923f2d910,915 (1 st Cirl 1990).

مشار إليه لدى: **أيمن رمضان محمد أحمد**، المرجع السابق، ص279.

[3]– **د. محمود نجيب حسني**، شرح قانون الإجراءات الجنائية، المرجع السابق، ص431.

المدنية متى كانت غير محددة القيمة أو تجاوزت قيمتها مبلغا معينا (1500 يورو [1]في القانون المدني الفرنسي، 100000 دينار جزائري حسب المادة 333 من القانون المدني الجزائري).

لقد أصبح التعاقد عبر الأنترنت من أسمى وسائل التعاملات الإلكترونية التي تعتمد أساسا على تبادل المعلومات من خلال **المستند الإلكتروني** الموقع توقيعا إلكترونيا الذي تتبلور فيه حقوق طرفي التعاقد في صيغة نمطية بين الحواسيب الخاصة بالأطراف المتعاقدة المرتبطة ببعضها من خلال شبكة الأنترنت، سواء من خلال مواقع الواب أو منتديات الحوار والمحادثة أو بالبريد الإلكتروني.

وإن كان ذلك كذلك، فقد كان لهذا التطور التكنولوجي–كما رأينا_ أثر مباشر في الكثير من الدول كفرنسا والجزائر ومصر التي عمدت إلى عملية تقييم شاملة لنظمها القانونية في ضوء مفرزات تقنيات المعلومات والإتصال وتحدياتها، من أجل الوقوف على مدى تواؤم النصوص القانونية القائمة على ما أفرزته وسائل الإتصال الحديثة خاصة شبكة الأنرنت، بإعتبار أن القواعد التقليدية للإثبات تتعامل مع عناصر الكتابة والتوقيع وغيرها من مفاهيم ذات مدلول مادي، وقد أسفرت عملية التقييم المذكورة إلى إتخاذ تدابير تشريعية تهدف إلى الإعتراف بوسائل الإثبات الإلكترونية التي تتم وفق شروط فنية وتقنية من شأنها أن تكفل موثوقيتها والإطمئنان إليها، والتوجه نحو الإعتراف بحجية الكتابة والمستند الإلكتروني على قدم المساواة مع الكتابة والمستند الورقي، والإقرار بصحة التوقيع الإلكتروني ومساواته في الحجية مع التوقيع الخطي.

وفي صدد الحديث عن الإثبات بالدليل الإلكتروني للتعاملات الإلكترونية، ونظرا لأن القواعد المتعلقة بالدليل الكتابي قد صيغت معالمها في إطار الإحتكار الورقي لدعامة كتابية، فإن تطبيقها يطرح تساؤلات أخرى تتعلق بحالة إنكار التوقيع الإلكتروني، وتنازع الأدلة الكتابية متى تم تقديمها على دعامات ذات طبيعة مختلفة، وهو ما سنتناوله تباعا من خلال دراسة مسالة إنكار التوقيع الإلكتروني المرتبط بالمستند الإلكتروني(أولا)، ثم دراسة سلطة القاضي في الترجيح بين الدليل الكتابي والدليل الإلكتروني عند التعارض(ثانيا).

أولا– إنكار التوقيع الإكتروني المرتبط بالمستند الإلكتروني

طبقا للقواعد العامة في الإثبات، لايرد إنكار الخط أو التوقيع إلا على المحررات العرفية دون المحررات الرسمية، بالنظر إلى أن حجية هذه المستندات تتوقف على إعتراف أو عدم إنكار من تنسب إليه، في حين تعتبر المحررات الرسمية حجة بذاتها نظرا لتدخل موظف عام في تحريرها، ولا يجوز إثبات العكس في بعض ما ورد فيها إلا بطريق الطعن بالتزوير.

والإشكال الذي ينبغي طرحه في هدا المقام هو هل ***يجوز إنكار التوقيع الإلكتروني المرتبط بالمستند الإلكتروني خاصة إذا لم يكن مستند على شهادة التصديق الإلكتروني، ورأت المحكمة أن الفصل في***

[1]–بموجب المرسوم رقم 2004–836 الصادر في 20 أغسطس المعدل للمرسوم رقم 80–533 الصادر في 15 يوليو 1980، المتعلق بتطبيق المادة 1341 من التقنين المدني الفرنسي.

الدعوى يتوقف على إثبات صحة هذا التوقيع وليس في وقائع الدعوى و مستنداتها ما يكفي لتكوين عقيدتها في هذا الشأن؟

من خلال دراستنا للتنظيم القانوني للتوقيع الإلكتروني في الباب الأول من هذه الدراسة، رأينا أن معظم التشريعات إعتدت بالمستندات العرفية الإلكترونية في الإثبات باعتبارها دليلا كتابيا يتمتع بذات الحجية المقررة للمستند العرفي الورقي، متى ما إستوفت بعض الشروط، فالمشرع الفرنسي إشترط موثوقية وسيلة التوقيع المستخدمة في تحديد هوية الموقع على نحو يضمن إرتباطه بالمستند وبضمان سلامة المعطيات أثناء تبادلها و خلال حفظها، ورأينا أن أثر شهادة التصديق الإلكتروني التي يصدرها مقدم خدمة التصديق ينحصر أثرها في نقل عبء الإثبات عند إنكار التوقيع الإلكتروني، وذلك تماشيا مع أحكام التوجيه الأروبي، حيث فرق بين نوعين من التوقيعات الإلكترونية:

- التوقيع الإلكتروني المتقدم: المستند على شهادة تصديق الكتروني وهو يحوز الحجية كدليل إثبات بقوة القانون، و يكون ملزما للقاضي كونه يتمتع **بقرينة قانونية** بسيطة على صحته.

وفي هدا الصدد فإن من شان قرينة موثوقية التوقيع الإلكتروني أن تقلب عبء الإثبات إلى عاتق من ينكر نسبة التوقيع الإلكتروني له، بأن يقيم الدليل على عدم موثوقية وسيلة التوقيع الإلكتروني كي يقدم للقاضي العناصر التي تبرر قلب هده القرينة ولا يكتفي في هذه الحالة بمجرد الإنكار[1]، ويترتب على نجاحه في ذلك نقل عبء الإثبات على عاتق من يتمسك بالوثيقة الممهورة بتوقيع الكتروني.

- توقيع إلكتروني بسيط: وإن كان لا يتمتع بقرينة قانونية بسيطة إلا أنه لا ترفض حجيته في الإثبات ، ولكن إن أنكره الشخص المنسوب إليه كان على الطرف الآخر المدعي وجوده إثبات جدارة وأمان الوسيلة التي إستخدمت في إنشائه[2].

وعلى غرار قانون التوقيع الإلكتروني المصري، جاء قانون التوقيع الإلكتروني الجزائري، خاليا من أية إشارة إلى الإجراءات أو الشروط الواجب إتباعها في حالة إنكار التوقيع الإلكتروني من قبل من ينسب إليه، وهو ما يوجب علينا في المقابل الرجوع إلى القواعد العامة في هذا الصدد.

وبإستقراء نصوص قانون الإجراءات الإدارية والمدنية والمتعلقة بمضاهاة الخطوط، ونقصد بذلك المادة 164 وما بعدها، سواء تعلق الأمر بالخط أو التوقيع، يتضح لنا انه لا يمكن تطبيقها على التوقيع الإلكتروني، نظرا لأن المدلول اليي توحي به كلمة "الخطوط" تدل للوهلة الأولى على إستعمال أداة مادية لوضع حروف أو أي علامات أو رموز عادية، وهو ما يعني أن تلك القواعد صيغت معالمها في العالم الورقي مما يصعب تطبيقها على المستندات والتوقيعات الإلكترونية.

ومع ذلك وبتطبيق تلك القواعد على التوقيعات الإلكترونية الواردة على المستندات الإلكترونية العرفية، فإنه يجوز لمن يحتج عليه بتوقيع إلكتروني أن ينكر صدوره منه ، مما يلقي بعبء الإثبات على عاتق من

---

[1]- **د. تامر محمد سليمان الدمياطي**، المرجع السابق، ص 817.

[2]- **عيسى غسان الربضي**، المرجع السابق، ص184، **د. تامر محمد سليمان الدمياطي**، المرجع السابق،ص 137.

يتمسك بالمستند المرتبط به، ويجوز للمحكمة أن تلجأ إلى أهل الخبرة ممثلين في خبراء تكنولوجيا المعلومات لتبيان ما إذا كان مايدعيه الخصم صحيح أم لا.

وفي هذه الحالة يفقد المستند الذي يرد عليه التوقيع قوته في الإثبات بصورة مؤقتة إلى حين البت في هذا الطعن، والقول بدلك يهز الثقة في المستندات الإلكترونية التي يرد عليها التوقيع الإلكتروني، التي تتحقق فيها عوامل الأمان والسلامة التي تجعلها تحظى بالحجية اللازمة، حيث يضفى تدخل مقدمي خدمات التصديق الإلكتروني مصداقية على صحة التوقيعات عن طريق التحقق من صحة التوقيع وإصدار الشهادات بذلك، بشكل يؤدي إلى الإطمئنان إلى صدور التوقيع الإلكتروني ممن نسب إليه، وهو أمر لا يتحقق في مجال المستندات والتوقيعات التقليدية.

وما قيل بخصوص المشرع الجزائري يقال بخصوص المشرع المصري، فبالرجوع لقانون التوقيع الإلكتروني نجده قد جاء خاليا من أية إشارة إلى الإجراءات أو الشروط الواجب إتباعها في حالة إنكار التوقيع الإلكتروني من قبل من ينسب إليه، مكتفيا في هذا الصدد بالإحالة إلى قواعد إثبات صحة المستندات في قانون الإثبات التي تفقد التوقيع حجيته في حالة إنكاره بصورة مؤقتة. وهي بذلك دعوة لكلا المشرعين كما سبق و أن أبدينا من ضرورة إنشاء **قرينة قانونية على صحة التوقيع الإلكتروني** –على غرار المشرع الفرنسي والمشرع الجزائري في قانون عصرنة العدالة في المادة 5 منه فيما يتعلق بالتوقيع على الوثائق والمحررات القضائية –، من شأنها أن تفترض صحة المستند الإلكتروني، إذا ما روعي في إنشائه الضوابط و الإشتراطات الواردة في القانون، وتؤدي إلى قلب عبء الإثبات على عاتق من يدعي خلاف ذلك، وبذلك لن يكتفي من يشهد عليه المستند الإلكتروني بمجرد إنكاره او إنكار توقيعه بل سيقع عليه أن يثبت صحة دعواه، بشكل يضفي الثقة في هذه المستندات والتوقيعات.

ثانيا–سلطة القاضي في الترجيح بين الدليل الكتابي والدليل الإلكتروني عند التعارض

لم يتعرض المشرع الجزائري لهذه المسالة خاصة من جانب الدليل الإلكتروني، أما المشرع الفرنسي فقدإستحدث بموجب القانون رقم 230–2000 في 30 مارس 2000، نص المادة 1316–2 من القانون المدني، الذي منح بمقتضاها للقاضي في حالة التعارض بين الأدلة الكتابية سواء كانت إلكترونية أو ورقية، سلطة فض التعارض وذلك بأن ألقى على عاتقه مهمة تحديد الدليل الكتابي الذي يجعل الحق المدعى به الأقرب إلى الإحتمال عن غيره من الأدلة الكتابية أيا كانت الدعامة التي تثبت عليها الكتابة، وذلك ما لم يوجد نص قانوني او إتفاق صحيح بين الأطراف على خلافه[1].

والملاحظ أن النص لم يضع معايير ملزمة للقاضي يستخدمها في عملية الترجيح في طبيعة الدعامة التي تقع عليها، وإنما أتاح له مباشرة هذا الترجيح بما له من سلطة في تقدير ظروف كل حالة على حدة

[1]-**Article 1316-2** Créé par Loi n°2000-230 du 13 mars 2000 - art. 1 JORF 14 mars 2000 dispose que"lorsque la loi n'a pas fixé d'autres principes, et à défaut de convention valable entre les parties, le juge règle les conflits de preuve littérale en déterminant par tous moyens le titre le plus vraisemblable, quel qu'en soit le support".

ليصل إلى المستند الذي يقدر أنه ألأكثر ترجيحا عن الآخر[1]. مالم توجد قاعدة قانونية أواتفاق يتعلق بتنظيم إثبات علاقتهم التعاقدية يقضي بخلاف ذلك ويمنح الأولوية لمستند على آخر.

ومن تم قضاء القاضي بخلاف ما ورد في المستند الإلكتروني لمجرد أن الكتابة فيه وردت في شكل الكتروني هو ما يتنافى ومبدأ افتراض المساواة بين المستند الورقي والإلكتروني بحسب الأصل متى توافرت الشروط التي يتطلبها القانون في كل نوع منهما.

ولا يوجد في القانون المصري ما يحول دو إقرار نفس السلطة للقاضي، ذلك أنه وإن لم يتضمن قانون التوقيع الإلكتروني نصا مشابها للنص الفرنسي، إلا أنه وإعمالا للقواعد العامة في الإثبات، يملك القاضي سلطة الترجيح بين الأدلة الكتابية في حالة تعارضهما مادام القانون لم يلزمه بإتباع معايير معينة.

إلا أننا نرى أن المنازعات المتعلقة بالأدلة الكتابية ورقية أو إلكترونية لابد أن تخضع لتنظيم خاص بها، وهي دعوة للمشرع المصري والجزائري ليأخذ حضه في تقنين هده المسالة خاصة وأن المجتمع فيهما لم يصل بعد إلى مرحلة الإلمام الكامل بمفردات التطور التقني، وما يتطلب ذلك من ضرورة إلمام القضاة بالقواعد الفنية والتقنية المرتبطة بالمستندات الإلكترونية، والفصل في المنازعات التي تنشأ بينها.

[1]-**د. تامر محمد سليمان الدمياطي**، المرجع السابق، ص834.

الخاتمة

الخاتمـــــة

كان موضوع الرسالة الحماية الجزائية للتعاملات الإلكترونية، هذه التعاملات التي لا يمكن أن ينشا الإستثمار فيها في فراغ قانوني دون إقرارها وضبطها بقانون يبين قواعد إبرامها وإثباتها وتنفيذها وإنهائها من جهة، وضمان السلامة المعلوماتية والحماية الجزائية والتي بدونهما لا يمكن الحديث عن إستقرار التعاملات الإلكترونية من جهة أخرى.

فالإنتقال من مرحلة التعامل الورقي إلى مرحلة التعامل الرقمي في مجال التعاملات والتقدم في هذا الإطار يتطلب توفير بنية قانونية قوية ومرنة بما في ذلك تعزيز وتطوير الجانب العقابي من خلال إستحداث نصوص جزائية تكون قادرة على مواجهة هذه الطائفة المستحدثة من الجرائم ومعاقبة مرتكبيها، والقول بغير ذلك من شأنه تهديد حقوق المتعاملين وتقليل الإستفـــادة من التعامل الإلكتروني. وهذا ما سعت إليه التشريعات المقارنة(التشريع الفرنسي، الجزائري، المصري...) من خلال إعداد بعض الأنظمة ذات العـــلاقة كقوانين جرائم تقنية المعلومات والتوقيع والتصـــديق الإلكـــتروني والإقتصاد الرقمي.

و إذا كانت حماية التعاملات الإلكترونية تتطلب مبدئيا تجريم الإعتداءات التي تطال آلية قيامها ومضمونها، فإن هذه الحماية لا تكفي لتحقيق حماية شاملة وكاملة لمعطيات التقنية الحديثة في تبادل المعطيات، دون تحديث قواعد التحقيق والإثبات والإختصاص بما ينسجم وهذه النوعية من الجرائم، وتطوير آليات التعاون الدولي على المستوى الإجرائي.

وهكذا تحددت إشكالية هذا البحث في تحليل السياسة التي إتبعتها وتبنتها مختلف التشريعات للحماية من هذه الجرائم ومكافحتها.

وفي سبيل معالجة هذه الإشكالية كنا قد قسمنا الرسالة إلى بابين، حيث تناولنا في الباب الأول الجوانب الموضوعية للحماية الجزائية للتعاملات الإلكترونية، ثم تناولنا في الباب الثاني الجوانب الإجرائية للحماية الجزائية للتعاملات الإلكترونية، وكان جل إهتمامنا أن نضع تشريعنا الوطني في الميزان بالنسبة للتشريعات التي وفرت حماية جزائية متطورة لهذا النوع من التعاملات في مواجهة الوسائل الإجرامية الناشئة عن تكنولوجيا الحوسبة والإتصال.

ولعله من الواجب علينا في نهاية هذه الدراسة، أن نضع ضمن إطار واحد النتائج التي تم التوصل إليها في مختلف جوانب الرسالة، ثم نعرض لأهم التوصيات التي يمكن الإستفادة منها في تفعيل النظام القانوني لحماية التعاملات الإلكترونية بهدف مواكبة التطورات العلمية الحديثة كمـــايلي:

أولا- أهـــــم نتائـــج الدراســـة

1- بالنسبة لحماية مواقع التعاملات الإلكترونية، فقد تبين لنا أن مختلف القوانين أولت إهتماماتها بمسألة حماية هذه المواقع عن طريق تجريم الإعتداءات التي تطال نظم المعالجة الآلية بصفة عامة، وذلك إيمانا منها بعجز النظم القانونية القائمة التي تتناول الجرائم التقليدية عن حماية هده النظم ومعلوماتها، كما هو حال المشرع الجزائري والمشرع الفرنسي مدرجة الحماية لها ضمن نطاق جرائم الأموال لما لها من قيمة إقتصادية، أمـــا الوضع في بعض الدول العربية، كما هو حال مصر فقد أقر المشرع المصري حماية خاصة لنوع معين من المعلومات ونظم معالجتها، ومن قبيل ذلك ما نصت عليه الفقرة **ه من المادة 23 من قانون التوقيع الإلكتروني**"؛

2- بالنسبة لأنماط تجريم الإعتداء على مواقع التعاملات الإلكترونية فقد تعـــــــــددت:

أ- فقد يتخذ الإعتداء على نظام المعالجة الآلية صورة الدخول غير المشروع الذي يتحقق بأي "**تفاعل ناجح مع النظام**" **ضد ارادة المسؤول عنه, أو المسيطر عليه من يملك تنظيمه**". والذي يندرج ضمن إطاره الإعتراض غير المشروع والإلتقاط غير المشروع للمعلومات أثناء إنتقالها بإعتبار أنها في النهاية تمثل إنتهاكا لإتصال معلوماتي بين النظم المختلفة أثناء عملها،وقد يتخذ صورة البقاء غير المشروع ، وهذا ما نص عليه كل من المشرع الجزائري والمشرع الفرنسي؛

ب-كما إتضح لنا أن السلوك الإجرامي يمكن أن يرتبط بالمساس بسلامة نظام المواقع كما هو الحال بالنسبة لجريمة إعاقة وإفساد نظام المعالجة الآلية، وهو ما نص عليه المشرع الفرنسي وذلك على خلاف المشرع الجزائري، فنهج هذا الأخير لم يكن موفقا عندما وردت نصوصه خالية من ذلك، ذلك أن تجريم هذا السلوك بنص مستقل ضرورة تلحها العلاقة التكاملية فيما بين جريمة التلاعب بالمعلومات وجريمة إفساد نظام المعالجة الآلية حتى لا يفلت المجرم من العقاب، فالإعاقة يمكن أن تنطوي على التلاعب بالمعلومات والتلاعب بالمعلومات يمكن أن ينطوي على إعاقة، ومع ذلك فمن الممكن أن يكون تحقق أحدهما دون الآخر ممكن في الواقع العمـــلي؛

ت- إن كان المشرع الجزائري قد جرم التلاعب بالمعلومات الموجودة داخل نظام المعالجة الآلية بالإدخال أو التعديل، فإن نهج المشرع الفرنسي كان أكثر توسعا حين جرم فضلا عن ذلك فعل حيازة أو نقل أو إستخراج أو إعادة إنتاج بغش المعطيات بموجب التعديل الذي أدخله على قانون العقوبات بالقانون رقم 2014-1353 وهي أفعال كلها تنطوي تحت التلاعب بالمعلومات المعالجة آليا، والصياغة التي جاء بها المشرع سدت بفعالية الفراغ الذي كان موجودا بصدد جريمة **سرقة المعلومات السرية** في نطاق الأعمـــال؛

ث-إن كان نهج المشرع الفرنسي كان أكثر توسعا في جريمة التلاعب بالمعلومات، فقد جاء ضيقا حين جرم التعامل في معلومات صالحة لإرتكاب جريمة فحسب، ولم يتعداها للتعامل في معلومات متحصلة من جريمة، هذه الأخيرة التي إنفرد بها المشرع الجزائري ولعل ذلك ينم عن سياسة هذا الأخير في الحماية، حيث ضيق من نطاق الأشخاص الذين يمكن أن يتعاملوا في

المعلومات المتحصلة من جرائم الاعتداء على نظم التعاملات الإلكترونية للحفاظ على ما تبقى من سريتها؛

3- بالنسبة لدراسة **الضوابط المعنوية** فقد تبين لنا أن أغلب التشريعات الجزائية المقارنة قد تطلبت القصد الجنائي صراحة، من ذلك مثلا ما نص عليه المشرع الجزائري صراحة بموجب المادة 394 مكرر 1"...كل من ادخل بطريق الغش معطيات..."، أما مكانة القصد الخاص فبتتبعنا لمنهج المسؤولية الجزائية في مجال الإعتداء على مواقع التعاملات الإلكترونية في التشريعات الجزائية المقارنة، تبين لنا أن المشرع اكتفى غالبا لتمام الركن المعنوي بتوافر القصد العام، وهو مسلك محمود نظرا لما أفرزه التطبيق العملي من وجود صعوبات تتعلق بالإثبات ما يؤدي إلى إفلات الجاني من العقاب؛

4- في نطاق منهج **تقرير وإختيار الجزاء**، فقد تبين لنا أن التشريعات الجزائية المقارنة قد ساهمت كثيرا بموجب هذا المنهج في تحقيق كثير من جوانب العدالة، حينما قررت نظام حماية جزائي يتميز بأنه واسع من حيث **نطاق المتابعة**، حيث شمل من حيث الأشخاص الذين يشاركون في التحضير لجنح نظام التعاملات الإلكترونية في إطار إتفاق جنائي وهدا في كل من التشريع الجزائري(المادة 394 مكرر 5 عقوبات) والفرنسي (المادة 323-4 عقوبات)، ومن حيث الأفعال أعمال البدء بالتنفيذ (المادة394 مكرر 7عقوبات جزائري والمادة 323-7 عقوبات فرنسي)،**وصارم من حيث العقوبات**، من خلال تشديد العقوبات الأصلية المتمثلة في الحبس والغرامة الموقعين على الأشخاص الطبيعية وذلك متى كانت المعلومات الّتي تم العدوان عليها تتعلق بمواقع الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، حسب المادة 394مكرر 3 عقوبات جزائري، أو كانت الإعتداءات ضد نظام للمعالجة الآلية للمعطيات ذات الطابع الشخصي التي تنفذها الدولة حسب الفقرة 3 من المادة 323-1 والفقرة 2 من المادة 323-2 والمادة 323-3 عقوبات فرنسي.أو أن الجرائم تم ارتكابها من جماعة منظمة ضد نظام للمعالجة الآلية للمعطيات ذات الطابع الشخصي التي تنفذها الدولة حسب المادة 323-4-1 عقوبات ؛

5 بالنسبة لأنواع **الوسطاء** في التعاملات الإلكترونية فقد تبين لنا أنهم على فئتين: **الفئة الأولى** وتشمل الوسطاء النظاميين وهم مقدم خدمة التصديق، الوسيط الإلكتروني، تخصصهم يكون في واسطة تعامل إلكتروني قانوني وليس فني ذلك أن هذا الدور الأخير منوط **بالفئة الثانية:** وتشمل الوسطاء الفنيون وهو الوسطاء في خدمة الأنترنت ينحصر دورهم في تمكين المستخدم من الدخول إلى شبكة الأنترنت والتجول فيها والإطلاع على مايريد وهؤلاء دورهم فني بحث قائم على التعاطي مع الأجهزة والبرامج وتشغيلها، وليس قائما على التوثيق والتصديق؛

6 -بالنسبة **للمسؤولية الجزائية للوسيط الفني**، فقد تبين لنا أنه وعلى خلاف المشرع المصري، فقد تبنت بعض التشريعات المقارنةضوابط قانونية خاصة ومتوازنة أرست فيها النظام القانوني لمقدمي خدمات الإنترنت، من حيث تحديد طبيعة عملهم والتزاماتهم، ومسؤولية كل منهم في مواجهة السلسلة المعلوماتية المتواصلة عبر الشبكة، حيث أقر المشرع الفرنسي أن أفعال مقدمي خدمات

الإنترنت الخاطئة لا يُمكن أن تدخُل في نطاق التجريم إلاَّ إذا ثبت علمهم الفعلي بالمضمون الإلكتروني غير المشروع، وعلى الرغم من علمهم هذا لم يتخذوا الإجراءات اللازمة لشطبه، أو على الأقل لمنع وصول الجمهور إليه. وهو بهذا جاء متفقاًمع الاتجاه العام للتوجيه الأُوروبي حول "التجارة الإلكترونية" الدي تبنىنظام "**عدم المسؤولية أو المسؤولية المشروطة**، ولم يذهب المشرع الجزائري بعيدا عن هدا النهج حين قررأن مسؤولية مقدم الخدمة لا تقام إلا إذا لم يحترم الأمر أو الحكم الصادر عن السلطة القضائية أو الإعذار الموجه إليه من الهئية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، والقاضي باتخاد الإجراءات اللازمة لمنع الوصول الى المعلومات المتنازع فيها؛

7 – تتعدد **صور تهديد المعطيات الشخصية** في بيئة التعاملات الإلكترونية بداية من قواعد معطيات الحاسب حيث يسهل التلاعب بالمعلومات الرقمية وتحليلها وتركيبها وإرسالها و تخزينها ومن السهل إستخدامها وإحداث إساءة بها بغرض ما أو بـــدون غرض، إلى تكنولوجيا جمع المعلومات وما تمثله من مخاطر حقيقة على خصوصية المعطياتكإستعمال ملفات تعريف الارتباط**cookies**" ، **الويب باجز(Web Bugs)** ؛

8 –إن منهج تقرير **الحماية الجزائية لمعطيات المتعامل الشخصية** من مخاطر المعالجة الآلية في نطاق التعاملات الإلكترونية يعتبر أداة قانونية ملائمة تولد الثقة في تعامل الأشخاص بالوسائل الإلكترونية، ولتحقيق المعادلة بين وجوب توفير المعلومات الضرورية لمجابهة المتطلبات الإقتصادية والإجتماعية والثقافية ومسايرة نسق التنمية الذي يفترض الإستغلال الأمثل لما تتيحه الوسائل الإلكترونية من إمكانيات، وبين وجوب توفير كل الضمانات لحماية المعطيات الشخصية من كل إنتهاك أو إستغلال، فقد تدخلت بعض التشريعات بموجب نصوص عامة لحمايتها جزائيا سواء من السلوكات المتعلقة بالمعالجة الآلية ، أو تلك المرتبطة بإستخداماتها، أو تعلق الأمر بإنتحال الهوية الرقمية للمتعامل الإلكتروني، وهو الوضع في التشريع الفرنسي. وفي المقابل أظهرت الدراسة أن هناك نقصا لدى الدول العربية في إصدار تشريعات أو تنظيمات قانونية تتعلق بكيفية معالجة المعطيات الشخصية وحمايتها، وإن كانت الجزائر ومصر قد أصدرتا قانون للتوقيع الإلكتروني وتضمنا بعض صور من الحماية، إلا أنها تبقى قاصرة من حيث شمولها لكل الأفعال، كما أنهما لم يتطرقا إلى إنشاء سلطة الرقابة الرسمية المختصة بالسهر على حماية المعطيات الشخصية ، وإلى تلقي التصاريح وإعطاء التراخيص لمعالجة المعطيات الشخصية، وصلاحية سلطة الرقابة التحقيقية،

ومن جهة أخرى أظهرت الدراسة أن هناك البعض من التشريعات من جمعت بين الإتجاهين حيث أقرت أحكاما خاصة للمساس بالمعطيات الشخصية بصفة عامة، كما أنها تناولت حماية الخصوصية المعلوماتية ومايتعلق بها من معلومات يتم تداولها أثناء التعاملات الإلكترونية من خلال قوانين التعاملات الإلكترونية كما هو حال المشرع التونسي؛

9 –بالنسبة **لحقيقة المستند لإلكتروني** فقد تبين لنا أن نهج المشرع الفرنسي كان له خصوصيته في **تنظيمه وتحديد قيمته الثبوتية**، حيث حدد مفهومه ضمن توسيعه صيغة النص الخاص بالدليل الكتابي في القانون المدني، معتمدا على مبدأ النظير الوظيفي بين الدليل الورقي والمعلوماتي، وهو نفس النهج الذي إتبعه المشرع الجزائري، وذلك على خلاف المشرع المصري الذي وضع نصوص خاصة في هذا الإطار ضمن قانون التوقيع الإلكتروني؛

10 – إن إقرار **مبدأ التكافؤ بين المستندات الإلكترونية والمحررات الورقية** من حيث قبولها وحجيتها في الإثبات من قبل التشريعات المختلفة كان متوقف على إستفاءها شروط معينة: الكتابة الإلكترونية، التوقيع الإلكتروني، كشف هوية الشخص مصدر المستند الإلكتروني حفظ المستند الإلكتروني بطريقة تضمن سلامته، إمكانية إسترجاع المستند الإلكتروني المحفوظ، وكانت النتيجة المترتبة أن المساس بهذه المستندات يشكل **فعل مجرم**؛

11 – أظهرت الدراسة عدم وجود نظام قانوني واضح في الجزائر ومصر ينظم عملية حفظ المستندات الإلكترونية، ويحدد شروطها وضوابطها الفنية والتقنية، ويبين الجهات المنوط بها حفظ المستندات الإلكترونية، بإعتبار الحفظ عاملا رئيسيا لضمان سلامة المستندات الإلكترونية، إلى جانب كونه شرطا جوهريا لحجيتها في الإثبات؛

12 –بالنسبة **لأنماط تجريم الإعتداء على المستند الإلكتروني**، فقد تبين لنا حرص مشرعي الدول المختلفة على وضع الضمانات الكفيلة بحرية التعاملات الإلكترونية أن تم تجريم أفعال الإعتداء على المستند الإلكتروني سيما وقد بدا الدخول على الأنترنت وسيلة سهلة في إرتكابها. ورغم تعدد أنماط التجريم فقد أمكننا تأصيلها في طائفتين: **الأولـــى** تتضمن الأفعال الماسة بسرية المستند الإلكتروني كالدخول غير المشروع إلى نظام المعالجة الآلية والنفاذ إلى المستند الإلكتروني سواء خلال تبادله أو أثناء حفظه، وهدا ما كرسه المشرع الجزائري والفرنسي في قانون العقوبات،والمشرع المصري في قانون التوقيع الإلكتروني. و**الثانيـــة** تشمل الأفعال الماسة بحجيتة في الإثبات كما هو الحال في جريمة إتلاف المستند الإلكتروني أو تزويره؛

فبالنسبة **لإتلاف المستند الإلكتروني** فقد أسفرت الدراسة إلى أن التشريعات قد إختلفت فيما بينهما حول طريقة تجريم إتلافه، ففي حين حرصت بعض التشريعات على النص على ذلك بصورة مباشرة، كما هو حال المشرع المصري في قانون التوقيع الإلكتروني، لم تفرد أغلبية التشريعات نصوصا خاصة تجرم فيها إتـــلاف المستند الإلكتروني بشكل مباشر، كما هو حال المشرع الفرنسي والجزائري، بل أمكن تمديد الحماية له بصورة تبعية من خلال بسط الحماية على نظام التشغيل ومعطيـــاته ؛

أما بالنسبة **لتزوير المستند الإلكتروني**، فقد تبين لنا أن مظاهر تغيير الحقيقة بصورة معنوية المجال الأكثر خصوبة لنمو التزوير المعلوماتي كظاهرة جرمية مستحدثة، ذلك أن من طبيعة المستندات الإلكترونية أنها تقبل التعديل والتحوير دون أن يحمي وعائها أثرا لحك أو تحشية أو محو

ذي علامات بارزة و ظاهرة. كما إتضح لنا أن بعض التشريعات قد كفت عناء البحث عن حماية المستند الإلكتروني من التزوير المعلوماتي، كما هو حال المشرع الفرنسي الذي عمد إلى التوسع في تجريم التزوير في قانون العقوبات ليستوعب حالات التزوير العادي في المحررات إلى جانب تزوير المستند الإلكتروني، وكذلك فعل المشرع المصري بموجب نص خاص ضمن قانون التوقيع الإلكتروني لسنة 2004، وذلك على خلاف المشرع الجزائري، ذلك أنه وإن أقر التوقيع الإلكتروني المشفر الرقمي كحل تقني لمسالة تحريف مضمون المستند الإلكتروني، فإن معالجته الجزائية للأمر جاءت جزئية من خلال قانون التوقيع الإلكتروني، حيث عاقب على إعطاء معلومات مزورة ، كما عاقب على من يقوم **باستعمال بيانات انشاء توقيع الكتروني** موصوف خاصة بالغير، كما عاقب في قانون عصرنة العدالة كل شخص يستعمل بطريقة غير قانونية العناصر الشخصية المتصلة بإنشاء التوقيع الإلكتروني يتعلق بتوقيع شخص أخر". كما أدرج ضمن قانون العقوبات جريمة التلاعب بالمعلومات التي يحتويها نظام المعالجة الآلـــية؛

13- بالنسبة **لفكـــرة التوقيع الإلكتروني،** إنتهت الدراسة إلى أن مختلف التشريعات قد إتجهت صوب التعويل على الوظيفة التي يؤديها وهي **التوثيـــق** لإثبات الهوية، ورغم إتباعها مبدأ الحياد التكنولوجي، فقد إنتهت الدراسة إلى أن تقنية التوقيع الرقمي المعتمد على التشفير اللامتماثل تعد أفضل وسائل التوقيع الإلكتروني في الوقت الراهن، كونها تكفل أداء الوظائف التي يؤديها التوقيع، فضلا على أن إستخدام تقنيات التشفير في إنشاء هذه التوقيعات يكفل لها مزايا لا يستهان بها في مجال حماية سرية المستندات والحفاظ على سلامتها**(السلامة)**،كما يسمح بتحديد مصدر التغييرات غير المصرح بها، كما يثبت هوية أطراف التعامل الإلكتروني، بل أنه يضمن عدم الإنكار من الموقع على أساس أن التوقيع تم إنشاءه وفق بيانات فريدة**(عدم الإنكار)**؛

14- أظهرت الدراسة إلى أن التشريعات المقارنة قد وسعت من نطاق تطبيق التوقيع الإلكتروني ليشمل جميع التعاملات التي يجوز إتمامها إلكترونياً سواء كانت مدنية أو إدارية أو تجارية بشرط أن تكون موقعة إلكترونياً وفقاً للشروط والضوابط القانونية، وإن كان المشرع الجزائري قد إستثنى من ذلك بعض التعاملات الإلكترونية الحكومية و أخضعها لقانون مستقل، وهي تلك المتعلقة بقطاع العـــدالة؛

15- ربطت مختلف التشريعات المقارنة مسالة حجية التوقيع الإلكتروني في الإثبات ومن تم **إضفاء الحماية القانونية عليه** بفكرة واحدة وهي **موثوقية** ذلك التوقيع من الناحية الفنية، حيث تتعلق هذه الشروط بالإرتباط، وبالتصميم وبالإنشاء.وعلى خلاف الوضع في فرنسا، وجدنا أن كل من المشرع الجزائري والمصري، لم يقرا صراحة وجود قرينة على **موثوقية** وسيلة التوقيع الإلكتروني المستخدمة رغم إشارتهما إلى ضوابط تحقق شروط الحجية؛

16- حرصت مختلف التشريعات المقارنة على تنظيم المركز القانوني لمزود خدمة التصديق على التوقيع الإلكتروني وفرض شروط معينة فيمن يقدم هذه الخدمة، إيمانا منها أن ذلك يعد **أحد أهم عناصر الحماية الوقائية للتوقيع الإلكتروني،** فبقدر إلتزامه بقدر ما تتضاءل المخاطر الناجمة عنه.

وقد جسد المشرع الجزائري مناخ الثقة بموجب **مخطط ثقة وطني**، ومن بين النماذج الموجودة في العالم اختار مخططا هيكليا يضم سلطة وطنية للتصديق الإلكتروني وهيئتين تؤطران التصديق الإلكتروني للفرعين الحكومي والإقتصادي، وخلصنا إلى أن المشرع اتبع الإزدواجية في جهة التصديق الإلكتروني حسب نوع المتدخـــل؛

17-**شهادة التصديق الإلكتروني** عبارة عن **مستند** في شكل إلكتروني صادرة عن جهة تصديق مختصة، تعتمد على تكنولوجيا رياضية معقدة وهي تقنية شفرة المفتاح العام والمفتاح الخاص، ويرجع ذلك إلى أن هذه التقنية من أقوى الوسائل الحديثة، لا تقتصر على أداء وظائف حماية البيانات فقط، بل تمتد كذلك إلى المساهمة في تدعيم وسيلة الإثبات الإلكتروني من خلال تحديد هوية مرسل المستند والموافقة على مضمونه وعلى توقيع ذوي الشأن الكترونيا، والتأكد من سلامته، ومن ثم ضمان عدم قابليته للإنكـــار؛

18-حرصت أغلب التشريعات المقارنة على تجريم **جملـــة من الأفعال الماسة بالتوقيع الإلكتروني** سواء منها المرتكبة من طرف المتعاملين الإلكترونيين، أو من الغـــير؛ سواء في إطار النصوص العامة أو في النصوص الخاصة؛

19-بشأن دراسة الضوابط المادية بشأن تجريم الإعتداء على التوقيع الإلكتروني، تبين مدى تشدد المشرع وحرصه في تقرير أقصى حماية ممكنة للمصالح ذات الأهمية، عن طريق التجريم المبكر للسلوك الإجرامي و إعتراض خطواته قبل أن يصل إلى مرحلة الضرر الفعلي ؛

20-إن نهج المشرع الجزائري لم يكن موفقا عندما وردت نصوصه خالية من تجريم إصدار شهادة التصديق الإلكتروني دون ترخيص بمزاولة النشاط من الهيئة المختصة، وتتبع أهمية هذا التجريم من كونه يشكل الإطار القانوني الرادع الذي يضمن عدم إصدار الشهادات دون ترخيص، بسبب الآثار الخطيرة التي تترتب على هذه الشهادة في حق الغير، حيث يكون مضمونها التسليم بصحة بيانات التوقيع أو بيانات المعاملة المطلوب صدور شهادة التصديق عنها، ومما لا شك فيه أن هذا السلوك يشكك في الثقة التي يجب توافرها في التعاملات الإلكترونية، والتي لأجلها صدر تشريع مثل التوقيع الإلكتروني؛

21-إهتمت القوانين بمعالجة مسالة **حماية البيانات المشفرة**، حيث نجد المشرع الجزائري يعاقب ضمن المادة 68 على كل من يفشي أو يستعمل بيانات إنشاء توقيع إلكتروني موصوف خاصة بالغير، وبيانات الإنشاء حسب الفقرة 3 من المادة 2 هي بيانات فريدة، من بينهـــا مفاتيح التشفير الخاصـــة وعلى ذلك فنص المـــادة يشملهـــا؛

22-كل التشريعات المقارنة أغفلت النص صراحة على تجريمصنع أو حيازة أو الحصول أو توفير أو الوضع تحت التصرف تجهيزات، أدوات برامج معلوماتية أو معطيات مصممة أو معدة لإعداد توقيع إلكتروني، رغم أن النص على هذه الصورة يعد من أحد أهم التجريمات في نطاق بيئة

التعاملات الإلكترونية، وتنبع أهمـــية هذا التجريم من كونـــه يقر حماية جزائية وقائية تستهدف منع الجريمة قبل وقوعها والقضاء على الشر في شرنقته، ذلك أن معالـــجة آثارهـــا جد صعب؛

23-بالنسبة **لجريمة تزوير التوقيع الإلكتروني**، فقد إتضح أنه وعلى خلاف المشرع المصري الذي نص صراحة في قانون التوقيع الإلكتروني على هذا التجريم،خلالقانون الجزائري من نص صريح على ذلك، إلا أنه أمكن تدارك ذلك من خلال معاقبته على كل من يقوم بحيازة أو باستعمال بيانات إنشاء توقيع الكتروني موصوف خاصة بالغير. فالجاني هنا يتصرف على أساس أنه صاحب التوقيع الإلكتروني، ويقوم باستعماله في التصرفات المختلفة التي يتحملها المتعامل الشرعي من خلال إنتحـــال شخصيته التي يمثلهـــا التوقيـــع الإلكتـــروني؛

24-أظهرت الدراسة من خلو نصوص قانون التوقيع الإلكتروني في التشريعات المقارنة من العقاب على الشـــروع، ولما كانت تلك الجرائم جنح ومن تم يتطلب النص على تجريم الشروع فيها، فإن الشروع في ارتكاب البعض منها والتي يتصور فيها الشروع، يبقى بمنأى عن التأثـــيم الجنـــــائي؛

25-أظهرت الدراسة أن **وسائل الدفع الإلكتروني** أهم صور تطبيقات التوقيع الإلكتروني، على اعتبار أن هذا النوع من الدفع متمم للتعاملات الإلكترونية المبرمة عن بعد وتتلازم معها، وهو لا يتم ولا يوثق إلا عن طريق الـــتوقيع الإلكتروني، ومن صورها آلية الدفع ببطاقة الإئتمـــان؛

26-أظهرت الدراسة كذلك أنه وإن كانت كل من الجزائر ومصر من أوائل الدول التي ضمت جهودها إلى المجتمع العربي، بمصادقتها على الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، إلا أنهما لم ينتهيا إلى وضع أداة وطنية لمواجهة الإستخدام غير المشروع لبطاقة الإئتمان، وذلك على خلاف المشرع الفرنسي الذي كانت له خصوصيته في هذا المجال، حيث نضم الجرائم المتصلة بإستخدام بطاقة الإئتمان من خلال الفصل 3 من الكتاب الأول من التقنين النقدي والمالي تحت عنوان الجرائم المتعلقة بالشيكات وأدوات النقد غير المادي من خلال المادة س163-3 وما بعدها. فجرم بموجبه فضلا عن تزوير وتقليد البطاقة وإستعمال أو محاولة إستعمال بطاقة مقلدة أو مزورة، وقبول التعامل ببطاقة مقلدة أومزورة، التعامل في معلومات أو أدوات صالحة لإرتكاب جريمة تزوير أو تقليد بطاقة الإئتمـــان وهو في حقيقته تجريم للأعمال التحضيرية التي يكون من شأنـــها الإعتداء على البطاقة بالتزوير أو التقليد وهو ما يعكس صورة من الحماية الجزائية الوقائية التي تستهدف منع الجريمة قبل وقوعها تبررها خطورة الأفعـــال؛إلا أنه لم يستحدث نصوصا خاصة لتجريم الإستخدام غير المشروع للبطاقة في ماعدا هذه الحالات، وهذا المنهج أمكن تبريره بأن أغلب حالات الإستخدام غير المشروع لها تخضع للقواعد العامة في قانون العقوبات كما هو الشأن في حالة إستخدام الحامل لبطاقتة الملغاة أو منتهية الصلاحية(جريمة الإحتيال)، في حين البعض الآخر لا يخضع لأي تكـــييف كما لو قدم الحامل البطاقة للتاجر لشراء سلعة مع عدم وجود رصيـــد كاف.

27- أظهرت الدراسة أن جريمة الدخول غير المشروع في نظام المعالجة الآلية إستطاعت أن تسد ثغرات عديدة في القانون، إذأن المشرع وإن نحى جانبا العديد من الأفعال التي فات عليه تجريمها بموجب نصوص صريحة، فلا يفلت المجرم من العقاب بل يعاقب إستقلالا عن هذه الجريمة ذاتهـــا؛

28-أصبح من المقرر في التشريعات المختلفة(الجزائري، الفرنسي...) جواز التفتيش لضبط المعطيات المخزنة على الرغم من طبيعتها المعنوية حاسمة بذلك الخلاف الفقـــهي، فضلا عن تقريرها نظام **التفتيش عن بعد** و**التفتيش عبر الحـــــدود**؛

29-أظهرت الدراسة ضرورة التمييز بين إعتراض الإتصالات الإلكترونية أثناء تبادلها، وقواعد تفتيش الإتصالات الإلكترونية المخزنة في الجهاز الخادم بعد وصولها أو وصول الرســـالة الإلكترونية؛

30-أظهرت الدراسة كذلك أنه وإن كان المشرع الجزائري قد أطـــر بصرامة التسرب الكلاسيكي الذي يسمح بالدخول في تواصل مع الأشخاص المشتبه بهم. فإن المشرع الفرنسي وعلاوة على ذلك كرس **التحقيق تحت إسم مستعار**. حيث أن هذه التقنية من التسرب تستخدم للبحث عن دليل الجريمة، في الشبكات الرقمية يصطلح عليه **بالتســـــرب الرقمـــي**؛

31-نظرا لخصوصية الجرائم الواقعة على التعاملات الإلكترونية إستثنت بعض التشريعات تطبيق بعض ضوابط التفتيش، لتبقي**على شرط الحصول على الإذن وإحترام السر المهني**، وهو ما إنتهجه المشرع الجزائري حين أقر جواز الخروج على قاعدة الحضور والتوقيت وكان في ذلك موفقا، إلا أنه في المقابل حصر نطاق الإستثناء في تلك الجرائم الواقعة على نظم التعاملات الإلكترونية؛

32-يتمتع الشخص بالحق في الخصوصية على بريده الإلكتروني، فلا يجوز الإطلاع عليه أو إعتراضه بدون رضاء صاحبه إلا بشروط يجب أن يحددها القانون مستهديا بما يحدث بالنسبة للبريد العادي؛

33- يعتبر إعتراض وتسجيل المعطيات المتعلقة بالمحتوى من أهم الإجراءات التقنية اللازمة لتعقب الدليل الإلكتروني والمحافظة عليه من الضياع أو التعديل، فضلا عما يستلزمه المحافظة على الدليل الإلكتروني من ضرورة التحفظ على المعطيات المخزنة، وهو ما إستحدثـــه المشـــرع الفرنسي والجزائري، وإن حصر هذا الأخير المعطيات المخزنة محل التحفظ في المعطيات المتعلقة بحركة السير فقط، وإغفاله تحديد مدة المراقبة رغم أهمية هذه الضمانة في وضع حد مناسب لحماية الحق في الخصوصـــية؛

34-أظهرت الدراسة أن هناك قصورا واضحا في التشريع الجزائي الإجرائي المصري في مواجهة ظاهرة جرائم تقنية المعلومات، إذ أنه لازال يخضع هذه الجرائم للنصوص التقليدية، وقد سبق الإشارة إلى أن مشروع قانون جرائم تقنية المعلومات المصري إقتصرت نصوصه على تنظيم تجريم السلوكات والممارسات الإلكترونية التي لا يوجد ما يجرمها في القانون المصري، والمعروف أن هناك فرق بين القانون الذي يجرم السلوك ويحدد الأفعال المجرمة وعقوباتها وبين قانون الإجراءات الذي يضم مجموعة القواعد القانونية التي تحدد سبل المطالبة بتطبيق القانون على

مرتكبي الجرائم ويحدد الأجهزة القضائية وشبه القضائية وإختصاصاتها والإجراءات المتبعة التي تهدف إلى الوصول للحقيقة، فكان لابد من إضافة نصوص قانونية تنظم الإجراءات الإلكترونية.

35-دعت إتفاقية بودابست لمكافحة جرائم تقنية المعلومات إلى إنشاء وتأسيس سلطات بغرض التنقيبات أو الإجراءات الجنائية النوعية، وهذا ما إستجابت له فرنسا والعديد من الدول الأجنبية والعربية ومنها الجزائر حيث أنشأت ما يسمى **المصلحة المركزية لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال،** فضلا عن الهيئة الوطنية لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال"، فقرار إنشاء هذه الهيئة يعد خطوة أولى بإعتراف وجود إجرام تقني ووجود إرادة سياسية لمحاولة مكافـــحته؛

36-فيما يخص **الخبرة** التقنية فقد تبين لنا أنه يمكن للقاضي الجزائي أن يستعين بعدة جهات لمساعدته في إختيار الخبير المعلوماتي، ككلية الهندسة المعلوماتية، او الشركات الخاصة التي تعمل في مجال تكنولوجيا المعلومات، أو الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته، حيث جعل المشرع الجزائري من مهام الهيئة مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والإتصال بما في ذلك تجميع المعلومات و**إنجـــاز الخبرات القضائية**؛

37-أظهرت الدراسة إلى أنه لا يمكن إلزام الشاهد بالإدلاء بمعلومات لازمة لإختراق نظام معلوماتي معين بحثا عن أدلة الجريمة داخله، كون ذلك يخرجه عن نطاق الوقائع التي أحاط بها علمه، في مقابل ذلك نص كل من المشرع الجزائري والفرنسي على إمكانية السلطات المكلفة بالتفتيش تسخير كل شخص له **دراية بعمل المنظومة المعلوماتية** محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها، ومما لاشك فيه أن الدخول إلى النظام المعلوماتي في هذه الحالة لا يمثل جريمة لأنه يتم بناء على إذن؛

38-إستحدث المشرع الجزائري وقصد تطوير وعصرنة المنظومة القضائية بالجزائر وتماشيا وارساء مفهوم "**المحاكمة عن بعد**" و"**التقاضي الإلكتروني**، الشهادة الإلكترونية والتي يمكن اللجوء إليها لإثبات الجرائم الواقعة على التعاملات الإلكترونية، فقد كان من أهم النقاط التي تناولها قانون عصرنة العدالة رقم 15-03، فسماع الشاهد عن بعد يساعد المحكمة على تقدير قيمة الشهادة أحسن من الإكتفاء بتلاوة أقوال الشاهد السابقة؛

39- يمكن تعريف الدليل الإلكتروني بأنه " المعلومات التي يتم الحصول عليها من الحيز الإفتراضي (نظام تخزين-نظام تراسل) وتكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية يتم معالجتها بتقنيات خاصة تقوم بتجميع وتحليل محتواه وفحصه لينتج عنها هيئات معينة يتم ربطها بين الجريمة والجاني والمجني عليه بطرق لا تتعارض مع القانـــون؛

40- أهم ميزة للدليل الإلكتروني تكمــن في صعوبة التخلــص منه، حيث يمكن إسترجاعه بعد محوه, إصلاحه بعد إتلافه، وإظهــاره بعد إخفــائه؛

41-أظهرت الدراسة أنه بالنسبة للدليل الإلكتروني لا بد أن يكون هناك بروتوكول لتحديد كيفية تجميعه وحفظه، فضلا عن إستخدام أدوات خاصة لإستخلاصه من المعلومات التي يتم تخزينها في الأجهزة دون الإضــرار بســلامتها، لأن ذلك يمكن أن ينال من صحة الدليل الإلكتروني المستخلص عند عرضه على القضاء؛

42- أظهرت الدراسة أن الطبيعة العابرة للحدود لجرائم الإعتداء على التعاملات الإلكترونية والتغير المطرد في هذا المجال أثار فكرة تنازع الإختصاص القضائي بين القاضي الجزائي الوطني والأجنبي في حالة تأسيس الإختصاص على مبدأ الإقليمية، وقد توصلنا من خلال دراستنا بوضع معيار لفض هذا التنازع بأن يؤول الإختصاص إلى المحكمة الواقع في دائرتها **مكان وقوع النشاط أو مكان الجهاز الخـــــــادم**؛

43-خطى المشرع الجزائري في خطوة سابقة من نوعها نحو **التخصص** في المعالجة القضائية لهذه النوعية من الجرائم، كانت في صورة إختصاص إقليمي موسع في المادة الجزائية في مختلف مراحل عمر الدعوى، إلا أنه حد من هذا التوسع حين حصره في الجرائم الواقعة على نظام التعاملات الإلكترونية فــقط؛

44-الدليل الإلكتروني مقبول في الأنظمة القانونية المختلفة، ويمكن للقاضي للجزائي الأخذ به سواء في إطــار الإدانــة أو الــبراءة، إذا توافرت فيه الشروط التالية:

أ- شرعية، وضعية، يقينية الأدلة الإلكترونيـــــة

ب-شرط الصــحة والمــطابقة، وشــرط الــدقة

45- أظهرت الدراسة إلى أن الدليل الإلكتروني لا يثير مشكلات تتعلق بالإثبات في المواد الجزائية فحسب، بل حتى في المواد المدنية إذا ما توقف الفصل في الدعوى الجزائية على إثبات معاملة إلكترونية أحاطها المشرع بضمانات منها ضرورة توافر دليل الكتروني، وهو ما يطرح عدة تساؤلات في حالة ما إذا ثار نزاع حول صحــته؛

46-بالنسبة لمسألة حجية التوقيع الإلكتروني المصدق عليه في المسائل الجزائية، ورغم كون التصديق يقوم دليلا على صحة التوقيع، فإن قانون التوقيع الإلكتروني في كل من الجزائر ومصر لم يعط كل منهما أية حجية له في المسائل الجزائية، وبناء عليه فإن المستند الإلكتروني الموقع توقيعا مصادقا عليه يعد كباقي الأدلة الإلكترونية الأخرى، حيث يخضع لتقدير القاضي من حيث الظروف والملابسات التي وجد فيها هذا المستــند؛

47-أظهرت الدراسة أن الدول مهما سنت من قوانين ومهما غلظت من عقوبات، فإنها لن تستطيع مواجهة هذه الجرائم بمفردها، نظرا لكون هذه الجرائم من الجرائم العابرة للحدود التي لا يقف أمامها أي عائق جغرافي، وهو ما يفرض التعاون الدولي في تطبيق تلك القوانـــين؛

ثانيا- التوصيـــات

1- إعتبار إتفاقية بودابست مدخلا هاما لمساعدة دول العالم وخاصة الدول العربية في مكافحة جرائم تقنية المعلومات بصفة عامة وجرائم الإعتداء على التعاملات الإلكترونية بصفة خاصة، بصورة شاملة وفعالة لما تتضمنه من تدابير وقواعد وإجراءات جزائية متطورة إضافة إلى آليات متعددة للتعاون الدولي والمساعدة القانونية المتبادلة، لهذا نتمنى من الدول التي لم تصادق بعد على هذه الإتفاقية أن تقدم على هذه **الخطـــوة الإيجابيـــة**، لأن من شأن تصديق أي بلد على هذه الإتفاقية ذات النزعة الدولية أن يساهم إلى حد بعيد في مكافحة الإجرام التقني على مستواه، ولكن نشير إلى مسألة هامة وهي عدم كفاية الإنضمام إلى هذه الإتفاقية بل لابد من العمل على تسخير جميع الطاقات و الوسائل للتطبيق السريع والفعال لهذه الآلية وذلك إنطلاقا من إدخال تعديلات على القوانين الداخلية لكل دولة تتماشى مع أحكام الإتفاقية ومن ثم التطبيق الفعـــال للقوانين الجديدة أو المعـــدلة؛

2- التاكيد على سيادة القانون وإحترام كافة التشريعات القانونية وتطبيقها على الجميع دون إستثناء، وضرورة المراجـــعة الدورية للتشريعات الجزائية القائمة وإزالـــة أي غموض أو ثغـــرات فيها ومن قبـــيل ذلـــك:

أ- أهمية تجريم الدخول المصرح به المتجاوز للغرض الذي منح من أجله التصريح بنص خاص, منعا للاعتداء على مبادئ التفسير في القانون الجزائي بإدراج هاته الحالة ضمن جريمة الدخول غير المصرح به، ودرء للمخاطر الناجمة عن إفلات مرتكبيها من العقـــاب؛

ب-على الرغم من قناعة الباحث بإمكانية تطبيق نص الدخول غير المصرح به على الإعتراض غير المشروع للمعلومات أثناء إنتقالها إلا أننا نوصي المشرع الجزائري بأن يتدخل لتجريمه لأن الأمر سيبقى محل خلاف وجدال بين الفقهاء، ولن يحسم إلا بنص صريح من لدن المشرع، خاصة وأنه قد نضم مراقبة الإتصالات الإلكترونية كعمل من أعمال التحقيق؛

ت-حبذا لو يحذو المشرع الجزائري حذو المشرع الفرنسي وينص على تجريم إعاقة الأنظمة بنص مستقل دون ترك ذلك للقضاء ليرى إن كانت تسري عليه النصوص المتعلقة بالتلاعب بالمعلومات أم لا، ذلك أنه يمكن أن يكون هناك تعدي على المعلومات دون أن يترتب على ذلك إعاقة، وقد يحدث إعاقة باستخدام وسيلة منطقية دون أن يترتب على ذلك إتلاف للمعلومات، مع تبيانه الحكم فيما لو ترتب على فعل التعطيل توقيف مصلحة ذات منفعة عامـــــة؛

ث-أهمية تشديد العقوبة في جريمة الدخول غير المصرح به في حالة ما إدا تم ذلك بالإعتداء على نظم الحماية الفنـــية؛

ج-ضرورة تدخل المشرع المصري ببعض النصوص التي تتفق مع التقدم التكنولوجي لتحديد مسؤولية الوسيط الفني في التعامل الإلكتروني عن جرائم الإعتداء على التعاملات الإلكترونية؛

ح- التأكـــيد على كون أنظـــمة معالجة المعطيات ذات الطابع الشخصي هي في خدمة الإنسان الذي يجب أن تحترم حرياته الأساســـية وحقوقه، ولاسيما الحياة الخاصة، مع الأخذ بالإعتبار ضرورة

المساهمة في التطور الإجتماعي والإقتصادي، ولذلك نهيب من المشرع الجزائري الإستجابة للإملاء الدستوري (المادة 46) والمبادرة إلى إصدار تشريع يتعلق بكيفية معالجة المعطيات الشخصية وحمايتها، ولجهة حرية نقل هده المعطيات، وكذلك هو الأمر بالنسبة للمشرع المصري؛

خ- حبذا لو يتدخل المشرع الجزائري لـــحفظ تزوير المستند الإلكتروني في قالب تجريمي مستحدث، يبين تدرج العقـــوبة حســـب طبيعة المستند الإلكتروني الـــمزور؛

د- ضرورة إصدار النظام اللازم المتعلق بتنظيم كيفية حفظ الوثيقة الموقعة الكترونيا، فبدونه يبقى التعامل عبر الوسائط الإلكترونية حبرا على ورق ؛

ذ- حبذا لو يتدخل المشرع الجزائري ويحذو حذو المشرع المصري وينص على تجريم إصدار شهادة تصديق إلكتروني دون الحصول على ترخيص بمزاولة النشـــاط؛

ر- بالنسبة لجريمة إفشاء بيانات إنشاء توقيع إلكتروني خاصة بالغير فإننا نقترح على المشرع الجزائري تشديد العقوبة في حالة ما إدا كان مرتكب الجريمة من موظفي الجهة المرخص لها بإصدار الشهادات، وذلك بكشف مفاتيح التشفير المودعة لدى جهة التصديق؛

ز- نهيب كلا المشرعين الجزائري والمصري التدخل لتجريم صنع أو حيازة أو الحصول أو توفير أو الوضع تحت التصرف تجهيزات، أدوات برامج معلوماتية أو معطيات مصممة أو معدة لإعداد توقيع إلكتروني؛

س- نهيب كلا المشرعين الجزائري والمصري التدخل لتجريم الشروع في الجرائم الواقعة على التوقيع الإلكتروني التي يتصور فيهـــا الشروع؛

ش- نهيب كل من المشرع الجزائري والمصـــري التدخل لتجريم السرقة المعلوماتية على أن يراعى في التجريم إعتباريـــن:

- أن يكون التجريم بنص عام يتسع ليشمل الصور المختلفة التي يمكن أن تنطوي عليها السرقة في البيئة التقنية أو الرقمية بدلا من إفراد نصوص خاصة لكل صورة من هذه الصور.
- تقوم الجريـــمة ولو لم يتم حرمان الحائز الشرعي منها، بل يكفي أن يقتصر الأمـــر على مجرد المشاركة في الحيازة والانتفاع فحســـب؛

ص- على الرغم من قناعتنا بكفاية نصوص قانون العقوبات على بعض حالات الإستخدام غير المشروع لبطاقة الإئتمان، إلا أنه بإعتقادنا أنه من الأفضلأن يقوم المشرع بوضع قانون خاص ذا طابع مرن متوجه مباشرة إلى صور الإستخدام غير المشروع لبطاقة الإئتمان المختلفة واصفا بذلك صور هذه الجرائم وصفا مميزا وبشكل خاص،لأن الأمر سيبقى محل خلاف وجدال بين الفقهاء حول التكييف القانوني الصحيح لهذه الحالات، ولن يحسم إلا بنص صريح من المشرع،

ولا داعي لنحاول تطبيق النصوص الجزائية العادية على كل جرائم بطاقة الإئتمان، كون هذه الجرائم لها طابـــع خاص ومتجدد من وقت لآخـــر؛

3- نهيب من التشريعات المقارنة وضع نص قانوني ينص على جواز تفتيش جميع الملفات في حال عدم معرفة إسم الملف أو مكـــان وجوده؛

4- تنظيم الوضع القانوني للرسالة الإلكترونية غير مفتوحة والمنتظرة في صندوق خطابات مقدم الخدمة، ولا تترك لإجتهاد المحاكم لمعرفة ما إذا كانت معطيات مخزنة وبالتالي تطبق عليها القواعد الخاصة بالتفتيش والتحفظ أم أنها معطيات في مرحلة النقل والتحويل وبالتالي تطبق عليها القواعد الخاصة بإعتراض معطيات المحتوى؛

5- نهيب من المشرع الجزائري التدخل لتوسيع إستثناء تطبيق ضوابط التفتيش على جميع الجرائم الواقعة في البيئة التقنية بما يشمل جميع الجرائم الواقعة على التعاملات الإلكترونية لإتحادها في العلة؛

6- حبذا لو يتدخل المشرع الجزائري ويوسع من المعطيات محل التحفظ من قبل مقدم الخدمة لتشمل جميع المعطيات المخزنة ولا يقصرها على المعطيات المتعلقة بحركة السير، وأن يكون تعاونه مع رجال الضبط القضائي بتزويدهم بهذه المعطيات بعد الحصول على إذن بذلك من السلطة القضائية المختصة؛

7- على الرغم من قناعتنا بإمكانية تكييف التسرب الكلاسيكي كحيلة إجرائية مع الرقمية، فإننا نوصي المشرع الجزائري بأن يكرسه كواقع قانوني درءا للخلاف، بتأطيره **التسرب الرقمي** على نحو ما فعل المشرع الفرنسي ؛

8- ضرورة وضع نص يوجب على مقدم خدمات التصديق والعاملين لديه تقديم تسهيلات للسلطة المختصة أو لأي موظفيها للقيام بالمراقبة أو الإشراف أو التفتيش على أي نظام معلوماتي أو مواد أخرى متصلة بالنظام بمقر مقدم خدمات التصديق؛

9- ضرورة النص على إعتبار **النطاق العلوي** الجزائري على الأنترنت (المنتهي بـــ: dz) الذي يخضع لإدارة الحكومة الجزائية جزءا من الإقليم الجزائري أو بحكم الأرض الجزائرية.

10- ضرورة تدخل المشرع بتوسيع الإختصاص للأقطاب الجزائية للنظر في جميع الجرائم المتصلة بتكنولوجيات الحوسبة والإتصال في الجزائر، وتعميق التفكير حول فكرة التخصص بالنسبة لدوائر المحاكم الإقتصادية في مصر المنوط بها نظر جرائم الإعتداء على التعاملات الإلكترونية مع تأهيل قضاتها فنيا.

11- فيما يتعلق بالدليل الإلكتروني ، وإن كنا نرى ترك مسالة تقدير الدليل الإلكتروني لقناعة القاضي الجزائي أسوة بالقواعد العامة، إلا أننا نقترح النص التالي" يعود للمحكمة تقدير قيمة الدليل الإلكتروني شريطة أن يكون **مؤمن أو موثوق** بأن يتوافر فيه: **شرط الصحة والمطابقة، وشرط السلامة**، وتفترض الموثوقية في الدليل الإلكتروني إلى أن يثبت العكس".

12- ضرورة تدخل المشرع المصري وتحديث أساليب التحري والتحقيق في مجال القواعد الإجرائية من خلال تحديث الأساليب الإجرائية القائمة وإستكمالها على نحو يكفل توفير سلطات ملائمة وكافية لجهات التحري والتحقيق والإدعاء أســوة بالمشرع الفرنسي والجزائــري؛ بما في ذلك تنظيم التعاون الهيكلي والمنتظم بين أجهزة إنفاذ القانون وبين القطاع الخاص بما في ذلك مقدمي الخدمة في مجال الاتصالات الإلكترونية وذلك عبر منحهم دورا إيجابيا ومساعدا للسلطات العمومية في مواجهة الجرائم والكشف عن مرتكبيها, وذلك من خلال تحديد التزاماتهم لا سيما التزامهم بالتحفظ على المعطيات المخزنة لديهم؛

13- العمل على وضع مواقع إلكترونية مخصصة للتبليغ عن جرائم تقنية المعلومات بصفة عامة وإرسالها إلى الجهات المختصة وهو ما يصطلح عليه "**بالبلاغ الرّقمي**", وهو ما انتهجته العديد من الدّول و على رأسها فرنسا, مثل موقع الدرك الوطني التالي:

,http://www.defense.gouv.fr/sites/gendarmerie

أو إلى عنوان بريده الإلكتروني التالي:

judiciaire@gendarmerie.defense.gouv.fr

14- إستكمال الأسس التشريعية للتعاملات الإلكترونية، فالجانب النظامي للتعاملات الإلكترونية لا يقتصر على إصدار نظام للتواقيع والتصديقات الإلكترونية، وإن كان ذلك مهما بل لا بد من تعديل بعض الأنظمة الأخرى بما يتوافق مع متطلباتها، من ذلك التأطير التشريعي للمعلوماتية في المجال التجاري بما في ذلك التحويل الإلكتروني للأموال، تأسيس الشركات عن بعد، المقاصة الإلكترونية...

وختاما نقول إن أهم ما قد يحافظ على إستقرار التعاملات الإلكترونية وأمنها هو تشريع قانون، ولكن أيضا ضمان تطبيقه بالإضافة لقابليته للتعديل بناء على ما قد يجد من إنتهاكـــات، حتى لا نكون كمن يستيقظ بعد أن يأخذ القطار سرعته، فلا هو يستطيع إيقافه، ولاهو يستطيع اللحاق به.

وهكذا يكون البحث قد إكتملت عناصره، فإن كان فيه كمال فهو لله سبحانه وتعالى، وإن إعتراه النقص فهو مني، ولم لا وأنا بشر أجتهد فأخطيء وأصيب، فإن أصبت فأجري على الله، وإن أخطأت فأدعوه ألا يحرمني أجر المجتهدين.

واسأل الله أن يهدينا إلى سواء السبيل، وأن يجعل عملي هذا خالصا لوجهه الكريم، وأن ينفع به، إنه نعم المولى ونعم النصير، وآخر دعوانا أن الحمد لله رب العالمين.

♦♦تمت بحمد الله♦♦

قائمة المراجـــــع والمصـــادر

أولا –النصوص القانونيـــة

أ– الدوليـــــة

1. Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Série des traités européens - n° 108, Strasbourg, 28.I.1981.
2. **Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.**
3. Loi type de la Commission des Nations Unies pour le droit commercial internationalsur le commerce électronique (1996)
4. **Convention sur la cybercriminalité**, Budapest, 23.XI.2001*Série des traités européens - n° 185.*
5. **Directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications** *Journal officiel n° L 024 du 30/01/1998 p. 0001 – 0008*.
6. Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques, j.o nº l013 du 19-01-2000..
7. Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique») Journal officiel n° L 178 du 17/07/2000.
8. Loi type de la Commission des Nations Unies pour le droit commercial internationalsur les signatures électroniques (2001).
9. DIRECTIVE 2002/58/CE DU PARLEMENT EUROPÉEN ET DU CONSEIL du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques.
10. **Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE.**

11. Directive 2007/64/CE du Parlement européen et du Conseil du 13 novembre 2007 concernant les services de paiement dans le marché intérieur modifiant les directives 97/7/CE, 2002/65/CE, 2005/60/CE ainsi que 2006/48/CE et abrogeant la directive 97/5/CE.
12. DIRECTIVE 2009/136/CE DU PARLEMENT EUROPÉEN ET DU CONSEIL du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) no 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs.
13. Règlement (UE) n ° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE.

ب-الوطنـــــية

❖ بالنسبة للجزائـــــــر

1. دستور الجمهورية الجزائرية الصادر بموجب إستفتاء 28 نوفمبر 1996، جريدة رسمية ، عدد76، الصادرة في 8 ديسمبر 1996، وآخر تعديلاته لغاية 2016(معدل بالقانون رقم 16-01 المؤرخ في 6 مارس 2016، جريدة رسمية ، عدد 14، الصادرة في 7 مارس 2016).
2. قانون الإجراءات الجزائية الجزائري الصادر بموجب الأمر رقم 66-155 المؤرخ في 18صفر 1386, الموافق لـــ 8 يونيو1966, وآخر تعديلاته لغاية 2015 (معدل بالأمر رقم 15-02 المؤرخ في 23 يوليو 2015، جريدة رسمية، العدد40، الصادرة في 23 يوليو 2015).
3. قانون العقوبات الجزائري الصادر بموجب الأمر رقم 156/66 المؤرخ في 18 صفر 1386, الموافق لـــ8 يونيو 1966, المتضمن قانون العقوبات، وآخر تعديلاته لغاية 2016(معدل بالقانون رقم 16-02 المؤرخ في 19 يونيو 2016 . جريدة رسمية، العدد37، الصادرة في 22 يونيو 2016).
4. أمر رقم75-58 المؤرخ في 20 رمضان عام 1395الموافق لـــ 26 سبتمبر 1975، المتضمن القانون المدني،الجريدة الرسمية، العدد78،الصادرة في 30 سبتمبر 1975، المعدل والمتمم بموجبالقانون رقم 05-10 المؤرخ في 13 جمادى الأولى عام 1426الموافق لـــ20 يونيو 2005، الجريدة الرسمية، العدد 44، الصادرة في 26 يونيو 2005.
5. المرسوم التنفيدي 95-310 المؤرخ في 10 أكتوبر 1995، يحدد شروط التسجيل في قوائم الخبراء القضائيين وكيفياته، جريدة رسمية، عدد 60، الصادرة في 1995.

6. مرسوم تنفيدي رقم 98–257 ، مؤرخ بتاريخ 25غشت 1998، المتضمن شروط وكيفيات إقامة خدمات أنترنات وإستغلالها، جريدة رسمية، عدد 63، صادرة بتاريخ 26 غشت 1998.
7. مرسومتنفيذيرقم 07 - 162 مؤرخفي 13 جمادى الأولىعام 1428 الموافق 30 مايوسنة 2007 يعدل ويتمّمالمرسومالتنفيذيرقم 01 - 123 المؤرخ في 15 صفرعام 1422 الموافق 9 مايوسنة 2001 والمتعلقبنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية،الجريدة الرسمية، العدد 37، الصادرة في 7 يونيو 2007.
8. المرسوم الرئاسي رقم 08– 52 الموافق ل 9 فيفري 2008، يتضمن إحداث مصلحة مركزية للشرطة القضائية للمصالح العسكرية للأمن التابعة لوزارة الدفاع الوطني وتحدي مهامها، الجريدة الرسمية، عدد8، الصادرة في 13 فيفري 2008.
9. القانون رقم 09–04 المؤرخ في 14 شعبان 1430 الموافق لـــ 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها جريدة رسمية، رقم 47، الصادرة في 16 أوت 2009.
10. قانون رقم 14–03 مؤرخ في 24 ربيع الثاني 1435 الموافق ل24 فيفري سنة 2014، المتعلق بسندات ووثائق السفر.
11. المرسوم الرئاسي رقم 14–183 المؤرخ في 13 شعبان 1435 الموافق ل 11 يونيو 2014 المتضمن إنشـــاء مصلحة التحقيق القضائي لمديرية الأمن الداخلي بدائرة الإستعلام والأمن ومهامها وتنظيمها، الجريدة الرسمية، عدد 32، صادرة في 12 يونيو 2014.
12. مرسوم رئاسي رقم 14–252 مؤرخ في 13 دي القعدة عام 1435 الموافق ل 8 سبتمبر 2014، متضمن التصديق على الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، جريدة رسمية، عدد57، لسنة 2014.
13. قانون رقم 15–03 المؤرخ في 1 فبراير 2015، المتعلق بعصرنة العدالة، جريدة رسمية، العدد 06، الصادرة في 10 فبراير 2015.
14. قانون رقم 15–04 المؤرخ في 1 فبراير 2015، المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، جريدة رسمية، عـــدد 06، الصادرة في 10 فبراير 2015.
15. المرسوم الرئاسي رقم 15–261 الموافق ل8 اكتوبر 2015، المحدد لتشكيلة وتنظيم وكيفيات سير الهئية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، جريدة رسمية ، عدد53، صادرة بتاريخ 8 أكتوبر 2015.

16. المرسوم التنفيذي رقم 16–135 مؤرخ في 17 رجب 1437 الموافق ل 25 أبريل 2016، يحدد طبيعة السلطة الحكومية للتصديق الإلكتروني وتشكيلها وتنظيمها وسيرها، جريدة رسمية، عدد 26، صادرة في 28 أبريل 2016.

17. مرسوم تنفيذي رقم 16–134 مؤرخ في 17 رجب عام 1437 الموافق ل25 أبريل 2016، يحدد تنظيم المصالح التقنية والإدارية للسلطة الوطنية للتصديق الإلكتروني وسيرها ومهامها، جريدة رسمية، عدد 26، صادرة في 28 أبريل 2016.

❖ **بالنسبة لفرنســـــا**

1 la loi**n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.**

2 La loi nº88-19 du 5 janvier 1988, relative á la fraude informatique.

3 **LOI n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des telecommunications,** JORF n°162 .du 13 juillet 1991

4 **Loi n° 91-1382 du 30 décembre 1991 relative à la sécurité des chèques et des cartes de paiement** .JORF n°1 .du 1 janvier 1992 .

5 Loi n° 2000-230 du 13 mars 2000, portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, J.O.R.F numéro 62, 14 mars 2000.

6 Décr. n º 2000-405 du 15 mai 2000 portant création d'un office central de lutte contre la criminilate liéé aux technologies de l'information et de la communication.

7 **LOI no 2000-719 du 1er août 2000 modifiant la loi no 86-1067 du 30 septembre 1986 relative à la liberté de communication,** JORF n°177 .du 2 août 2000 .

8 **LOI n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne.** JORF n°266 .du 16 novembre 2001 .

9 **Décret n°2001-272 du 30 mars 2001, pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique, J.O**RF. numéro 77 ,31 mars 2001.

10 **Décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information**: JORF n°92 .du 19 avril 2002 .

11 La loi nº 2003-239du 18 mars 2003 pour la sécurité intérieure en france.

12 -**Loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité**

13 la LOI no 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique J.O n° 143. du 22 juin 2004 (len)destine a transposer la directive europeene 200o/31/ec du 18 juin 2000 (directive sur le commerce electronique).

14 laLoi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et

modifiant la loi 78-17 du 6 janvier 1978 relative À l'informatique, aux fichiers et aux libertés.

15 **LOI n° 2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle (1)** JORF n°159 .du 10 juillet 2004.

16 Décret n°2005-972 du 10 août 2005 modifiant le décret n° 56-222 du 29 février 1956 pris pour l'application de l'ordonnance du 2 novembre 1945 relative au statut des huissiers de justice ;

17 **Décret n° 2005-973 du 10 août 2005 modifiant le décret n° 71-941 du 26 novembre 1971 relatif aux actes établis par les notaires ,**JORF n°186 .du 11 août 2005 .

18 Décret n° 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques , JORF n°73 .du 26 mars 2006

1 Code pénal,104e édition , Dalloz, paris, 2009.

19 Code de procédure pénale**,** Dalloz, paris, 2009

20 Ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations.

21 LOI n° 2009-526 du 12 mai 2009 de simplification et de clarification du droit et d'allègement des procédures

22 LOI n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet JORF n°0135 .du 13 juin 2009

23 Ordonnance n° 2009-866 du 15 juillet 2009 relative aux conditions régissant la fourniture de services de paiement et portant création des établissements de paiement

24 Décret n°2009-934 du 29 juillet 2009 pris pour l'application de l'ordonnance n°2009-866 du 15 juillet 2009 relative aux conditions régissant la fourniture de services de paiement et portant création des établissements de paiement, J.OR;F. du 31 juillet 2009.

25 Ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques , JORF n°0197 .du 26 août 2011 .

26 LOI n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure

27 **LOI n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme ,**JORF n°0263 .du 14 novembre 2014.

28 LOI n° 2009-526 du 12 mai 2009 de simplification et de clarification du droit et d'allègement des procédures

29 LOI n° 2015-912 du 24 juillet 2015 relative au renseignement

30 **LOI n° 2015-993 du 17 août 2015 portant adaptation de la procédure pénale au droit de l'Union européenne**

31 Décret n° 2015-1805 du 28 décembre 2015 modifiant le code de procédure pénale (partie règlementaire) et relatif aux unités de la gendarmerie nationale au sein desquelles les officiers et agents de police judiciaire exercent leurs fonctions habituelles

32 LOI n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé; JORF n°0022 .du 27 janvier 2016

33 **Ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations** JORF n°0035. du 11 février 2016

34 **LOI n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale**

35 **LOI n° 2017-86 du 27 janvier 2017 relative à l'égalité et à la citoyenneté ,** jORF n°0024. du 28 janvier 2017.

❖ بالنسبة لبقية الـــدول الأخرى

1. –القانون رقم58 لسنة 1937، المتضمن قانون العقوبـــات **المصري** وآخر تعديلاته لغاية 2003.
2. القانون رقم 150 لسنة 1950، المتضمن قانون الإجراءات الجنائية **المصـــري** وآخر تعديلاته لغايـــة 2003.
3. قانون رقم 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات **المصري**، جريدة رسمية، عدد 17، صادرة في 22 أبريل لسنة 2004.
4. قراررئيسجمهورية**مصر**رقم 276 لسنة 2014،بشأنإنضماممصر إلى الإتفاقية العربية لمكافحة جرائم تقنية المعلومات.
5. قرار رقم 109 لسنة 2005، بتاريخ 15–5–2015 ، بإصدار اللئحة التنفيذية لقانون التوقيع الإلكتروني المصري وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات.
6. قانون رقم 83 لسنة 2000، مؤرخ في 9 أوت 2000، المتعلق بالمبادلات والتجارة الإلكترونية **التونسي**، الجريدة الرسمية ، عدد 64، صادرة في 11 أوت 2000.
7. قانون عدد 63 لسنة 2004، مؤرخ في27 جويلية 2004 ، المتعلق بحماية المعطيات الشخصية، الجريدة الرسمية**التونسية** ، صادرة 30 جويلية 2004.
8. القانون **الإتحادي** رقم 1 لسنة 2006، بشأن المعاملات والتجارة الإلكترونية، جريدة رسمية رقم 442، يناير 2006.
9. مرسوم سلطاني رقم 2008–69 ، مؤرخ في 17 ماي 2008، المتعلق بإصدار قانون المعاملات الإلكترونية، جريدة رسمية، رقم 864.
10. قانون المعاملات الإلكترونية **الأردني** رقم 85 ، الصادر بتاريخ 11ديسمبر2001.

ثانيا– مراجـــع باللغة العربيـــة

أ– الكتـــــب

❖ المؤلفات العامة

1. د. **إبراهيم حامد طنطاوي**، التلبس بالجريمة وأثره على الحرية الشخصية، الطبعة الأولى، المكتبة القانونية، 1995.
2. **د.أحمد أبو القاسم**، الدليل الجنائي المادي ودوره في إثبات جرائم الحدود والقصاص، الجزء الأول، دار النشر بالمركز العربي للدراسات الأمنية والتدريب ، الرياض، 1993.
3. **د. أحمد شوقي الشلقاني**, مبادئ الإجراءات الإجرائية في التشريع الجزائري، الجزء الثاني، ديوان المطبوعات الجامعية، الجزائر، 1999.
4. **د.أحمد عوض بلال**، الجرائم المادية، المسؤولية الجنائية بدون خطأ، دراسة مقارنة، دار النهضة العربية، القاهرة، 1993.
5. **أحمد غاي**، ضمانات المشتبه فيه أثناء التحريات الأولية، الطبعة الثانية، دار هومة، الجزائر،2011.
6. **د. أحمـــد فتحي سرور:**
   - ✓ الوسيط في قانون العقوبات, القسم الخاص، دار النهضة العربية، القاهرة، 1979.
   - ✓ الوسيط في قانون العقوبات، القسم العام، دار النهضة العربية، القاهرة، 1989.
   - ✓ الوسيط في قانون الإجراءات الإجراءات الجنائية، الطبعة الثانية، دار النهضة العربية، القاهرة، 1981.
7. **د. إدوارد عيد**، موسوعة أصول المحاكمات والإثبات والتنفيذ، الجزء السادس عشر، الإثبات(اليمين–والشهادة)، دون دار نشر، لبنان، 1991.
8. **د.بن شيـــخ لحسين**، مذكرات في القانون الجزائي الخاص–جرائم ضد الأشخاص، جرائم ضد الأموال، الطبعـــة الخامسة، دار هومة، الجزائر، 2006.
9. **د. توفيق محمد الشاوي**، حرمة الحياة الخاصة ونظرية التفتيش، منشاة المعارف بالإسكندرية، 2006.
10. **د. جلال ثروت**، نظم القسم الخاص–جرائم الإعتداء على المال المنقول، الجزء الثاني، دار المطبوعات الجامعية، الإسكندرية، 1995.
11. **د.باسم شهاب**، مباديء القسم العام لقانون العقوبات، ديوان المطبوعات الجامعية، وهران،2007.
12. **د. حسن الجوخدار**، أصول المحاكمات الجزائية، الجزء الثاني، الطبعة الخامسة، منشورات جامعة دمشق، دمشق، 1991.
13. **د. حسنين المحمدي بوادي**، الوسائل العلمية الحديثة في الإثبات الجزائي، منشاة المعارف، الإسكندرية، 2005.
14. **د. رؤوف عبيد**، مباديء الإجراءات الجزائية في القانون المصري، دار الفكر العربي، القاهرة، 2006.
15. **د. رمسيس بهنـــــام:**

- ✓ قانون العقوبات جرائم القسم الخاص، منشاة المعارف، الإسكنـــــدرية، 2005.
- ✓ الإجراءات الجنائية تأصـــيلا وتحليـــلا، منشأة المعارف، الإسكندرية، 1984.

16. **د.عبد الله أوهابيه**, شرح قانون الإجراءات الجزائية الجزائري–التحري والتحقيق–, دار هومه للنشر والتوزيع، الجـــزائر، 2008.
17. **د. سامي حسني الحسيني**، النظرية العامة للتفتيش في القانون المصري والمقارن، دار النهضة العربية، القاهرة، 1972.
18. **د. شوقي عمر أبو خطوة**، شرح الأحكام العامة لقانون العقوبات، دار النهضة العربية، القاهرة، 2003.
19. **د.صوفي أبـــو طالب**، تاريخ النظم القانونية والإجتماعية، دار النهضة العربية، القاهرة، 1977.
20. **د. عبد الوهاب حومد**، أصول المحاكمات الجزائية، الطبعة الرابعة، المطبعة الجديدة، دمشق، 1987.
21. **د.العربي شحط عبد القادر**، الإثبات في المواد الجزائية، دار الهدى، الجزائـــر، 2006.
22. **د. علـــى عبد القـــادر القهوجي:**

- ✓ شرح قانون العقوبات، القسم العام، المسؤولية الجزائية والجزاء الجزائي، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2009.
- ✓ شرحقانون العقوبات القسم الخاص، منشورات الحلـــبي الحقوقية، بيروت، لبنان، 2002.

23. **د.عمار بوضياف**، النظام القضائي الجزائري، دار الريحانة، الجزائر، 2003.
24. **د.عوض محمد عوض:**

- ✓ التفتيش في ضوء محكمة النقض، دراسة نقدية، الإسكندرية، 2006.
- ✓ شرح قانون العقوبات –القسم العام–دار المطبوعات الجامعية، الإسكندرية، 1991.
- ✓ دراسات في الفقه الجنائي الإسلامي، در المطبوعات الجامعية ، الإسكندرية، 1977.

25. **د. فاضل زيدان محمد**، سلطة القاضي الجنائي في تقدري الأدلة، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن،2006.
26. **د.فتوح عبد الله الشاذلي:** شرح قانون العقوبات القسم الخاص، دار المطبوعات الجامعية، الإسكندرية، 2001.
27. **د. فوزية عبد الستـــــــار:**

- ✓ شرح قانون العقوبات، القسم الخاص، دار النهضة العربية، القاهرة، 1990.
- ✓ شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، 1986.

28. **د.مأمون سلامة:**

✓ قانون الإجراءات الجنائية معلقا عليه بالفقه وأحكام النقض، الجزء الأول، الطبعة الثانية، مكتبة رجال القضاء، القاهرة، 2005.
✓ شرح قانون العقوبات، القسم العام، دار النهضة العربية، القاهرة، 1991.

29. **د.محمد حزيط**، مذكرات في قانون الإجراءات الجزائية الجزائري، الطبعة الثالثة، دار هومة،الجزائر، 2008.

30. **د. محمد زكي أبو عامر**، الإجراءات الجنائية، الطبعة السابعة، دار الجامعة الجديدة، الإسكندرية، 2002.

31. **د.محمد صبحي نجم**، قانون العقوبات القسم العام، دار الثقافة للنشر والتوزيع، عمان، 2000.

32. **د. محمود محمود مصطفى:**

✓ الإثبات في المواد الجنائية في القانون المقارن،الجزء الأول، الطبعة الأولى، مطبعة جامعة القاهرة والكتاب الجامعي، 1977.
✓ شرح قانون العقوبات، القسم الخاص، الطبعة الثامنة، مطبعة جامعة القاهرة، 1984.

33. **د. محمود نجيب حسني:**

✓ النظرية العامة للقصد الجنائي، دراسة تأصيلية مقارنة للركن المعنوي في الجرائم العمدية، دار النهضة العربية، القاهرة، 1988.
✓ شرح قانون العقوبات القسم الخاص، دار النهضة العربية، القاهرة، 1992
✓ شرح قانون العقوبات القسم الخاص، الجرائم المضرة بالمصلحة العامة،دار النهضة العربية، القاهرة، 1988.
✓ شرح قانون الإجراءات الجزائية، دار النهضة العربية، القاهرة، 1988.
✓ شرح قانون العقوبات اللبناني، القسم العام، الطبعة الثالثة، منشورات الحلبي الحقوقية، بيروت، 1998.
✓ شرح قانون العقوبات، القسم العام، النظرية العامة للجريمة والنظرية العامة للعقوبة والتدبير الإحترازي، الطبعة الخامسة، دار النهضة العربية، القاهرة،1982.

34. **د.معجب بن معدي الحويقل**، المرشد للتحقيق والبحث الجنائي، الطبعة الأولى، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2003.

35. **نجمي جمال**، جرائم التزوير في قانون العقوبات الجزائري ، دار هومة، الجزائر، 2013.

❖ المؤلفـــات الخاصة

1. د.إبراهيم الدوسقي أبو الليل، الجوانب القانونية للتعاملات الإلكترونية، دراسة للجوانب القانونية للتعامل عبر أجهزة الاتصال الحديثة (التراسل الإلكتروني)، مطبوعات جامعة الكويت، 2003.

2. **د.أحمد إبراهيم مصطفى سليمان،** الإرهاب والجريمة المنظمة، دار الطلائع للنشر والتوزيع والتصدير،القاهرة، 2006.
3. **د.أحمد زيادات وابرهيم العموش،** الوجيز في تشريعات التجارة الأردنية، الطبعة الأولى، دار وائل للنشر، عمان، 1996.
4. **د.أحمد محمود سعد،** نحو إرساء نظام قانوني لعقد المشورة المعلوماتية_المعالجة الآليّة للبيانات بواسطة الحاسب الآلي، الطبعة الأولى، دار النهضة العربية، القاهرة، 1995.
5. **د.أحمد يوسف السولية،** الحماية الجنائية والأمنية للشاهد، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2007.
6. **أسامة أحمد المناعسة, جلال الزعبي, صايل فاضل الهواوشة،** جرائم الحاسب الآلي والانترنت، دار وائل للنشر، عمان، دون تاريخ.
7. **د.أسامة عبد الله قايد،** الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دون دار نشر، 1988.
8. **د.أشرف توفيق شمس الدين** ، الحماية الجنائية للمستند الإلكتروني دراسة مقارنة،الطبعة الأولى، دار النهضة العربية، القاهرة، 2006.
9. **د.أشرف جابر السيد،** مسؤولية مقدمي خدمات الأنترنت عن المضمون الإلكتروني غير المشروع، دراسة خاصة لمسؤولية متعهدي الإيواء، دار النهضة العربية، القاهرة، 2010.
10. **آمال قارة،** الحماية الجزائية للمعلوماتية في التشريع الجزائري، الطبعة الأولى، دار هومه للطباعة والنشر والتوزيع ، الجزائر، 2006.
11. **د.أنور سلطان،** قواعد الإثبات في المواد المدنية والتجارية، دار الجامعة الجديدة للنشر، الإسكندرية، 2005.
12. **د.أودين سلوم الحايك،** مسؤولية مزودي خدمات الأنترنت التقنية،المؤسسة الحديثة للكتاب، طرابلس، لبنان،2009.
13. **د.أيمن عبد الله فكري،**جرائم نظم المعلومات–دراسة مقارنة، دار الجامعة الجديدة للنشر، الإسكندرية، 2007.
14. **د.إيهاب السنباطي،** موسوعة الإطار القانوني للتجارة الإلكترونية، دار النهضة العربية، القاهرة، 2007.
15. **بلال أمين زين الدين،** جرائم نظم المعالجة الآلية للبيانات في التشريع المقارن والشريعة الإسلامية، دار الفكر الجامعي، الإسكندرية، 2008.
16. **بوكـــر رشيدة،** جرائم الإعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، منشورات الحلبي الحقوقية، بيروت، 2011.
17. **بيل جيتس،** المعلوماتية بعد الانترنت، طريق المستقبل، ترجمة عبد السلام رضوان، المجلس الوطني للثقافة والفنون والآداب، العدد 231، الكويت، 1998.

18. **د.تامر محمد سليمان الدمياطي**، إثبات التعاقد الإلكتروني عبر الأنترنت،دراسة مقارنة، دار الكتب المصرية،2009.
19. **د.ثروت عبد الحميد**، التوقيع الإلكتروني، ماهيته، مخاطره وكيفية مواجهته ومدى حجيته في الإثبات، دار النيل للطباعة والنشر، القاهرة، 2001.
20. **د.جميل عبد الباقي الصغير**:
- ✓ الجوانب الإجرائية للجرائم المتعلقة بالانترنت، دار الفكر العربي، القاهرة، 2001.
- ✓ أدلة الإثبات الجزائي والتكنولوجيا الحديثة، (أجهزة الرادار – الحاسبات الآلية – البصمة الوراثية)دراسة مقارنة ، دار النهضة العربية، القاهرة، 2001.

21. **د.حسن سعيد عبد اللطيف**، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الأنترنت، الطبعة الأولى، دار النهضة العربية، القاهرة، 1999.
22. **د.حسن طاهر داود**، جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2000.
23. **د.حسن عبد الباسط جميعي**، إثبات التصرفات القانونية التي يتم إبرامها عن طريق الانترنت، دار النهضة العربية، القاهرة، 2000.
24. **د.حسين محمد عبد الظاهر**، المسؤولية القانونية في مجال شبكات الأنترنت، دار النهضة العربية ، القاهرة،2003.
25. **حمو وأخرون**، الأدلة الإلكترونية من الناحيتين القانونية والتقنية_دراسة تحليلية مقارنة– دون دار النشر، فلطسين، 2015.
26. **د.خالد محمد كدفور المهيري**، جرائم الكمبيوتر والأنترنت والتجارة الإلكترونية، الطبعة الثانية، دار الغريب للطباعة والنشر، دبي، دون تاريخ.
27. **د.خالد ممدوح إبراهيم**:
- ✓ إبرام العقد الإلكتروني، دار الفكر الجامعي، الإسكندرية، 2008.
- ✓ التقاضي الإلكتروني–الدعوى الإلكترونية وإجراءاتها أمام المحاكم، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2008,
- ✓ فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2009

28. **د.رياض فتح الله بصلة**، جرائم بطاقات الإئتمان، الطبعة الأولى، دار الشروق، 1995.
29. **د.عفيفي كمال عفيفي, فتوح الشاذلي**، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون–دراسة مقارنة–، منشورات الحلبي الحقوقية، بيروت، 2003.
30. **د. رشدي محمد علي محمد عيد**، الحماية الجنائية الموضوعية للمعلومات عبرشبكة الأنترنت، دار النهضة العربية، القاهرة، 2013.

31. **د. رياض فتح الله بصلة،** جرائمالإحتيال بالبطاقات الإئتمانية وأساليبمكافحتها، جامعة نيف العربية للعلوم الأمنية،الرياض، 2002.
32. **د.سامح عبد الواحد التهامي،** التعاقد عبر الأنترنت–دراسة مقارنة– دار الكتب القانونية ، القاهرة، 2008.
33. **سامي جلال فقي حسين،** التفتيش في الجرائم المعلوماتية–دراسة تحليلية– دار الكتب القانونية، القاهرة، 2011.
34. **سامي علي حامد عياد,** الجريمة المعلوماتية وإجرام الانترنت، دار الفكر الجامعي، الإسكندرية، 2007.
35. **د. سليمان أحمد فضل،** المواجهة التشريعية والأمنية للجرائم الناشئة عن إستخدام شبكة المعلومات الدولية، دار النهضة العربية، القاهرة، 2013.
36. **د.السيد عتيق،** جرائم الانترنت، دار النهضة العربية، القاهرة، 2000.
37. **د.شمس الدين إبراهيم أحمد،** وسائل مواجهة الاعتداءات على الحياة الشخصية في مجال تقنية المعلومات في القانون السوداني والمصري_دراسة مقارنة_ الطبعة الأولى، دار النهضة العربية، القاهرة، 2005.
38. **د.شيماء عبد الغني،** الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، الإسكندرية،2007.
39. **د.صالح المنـــزلاوي،** القانون الواجب التطبيق على عقود التجارة الإلكترونية، دار الجامعة الجديدة للنشر، الإسكندرية، 2006,
40. **د.صفوت النحاس،** مراجعة د.عبد المنعم يوسف بلال، الحاسبات الشخصية و فيروسات الكمبيوتر، دار النشر هاتيه،دون تاريخ.
41. **عائشة بن قارة مصطفى،** حجية الدليل الإلكتروني في مجال الإثبات الجنائي–دراسة مقارنة بين التشريع الجزائري والقانون المقارن–، دار الجامعة الجديدة، الإسكندرية، 2010.
42. **د. عايد رجا الخلايلة،** المسؤولية التقصيرية الإلكترونية، دار الثقافة للنشر والتوزيع، عمان، 2009.
43. **عبد الرحمن عبد الله السند،** الأحكام الفقهية للتعاملات الإلكترونية، الطبعة الثالثة، دار الوراق، الرياض، 2006.
44. **د.عبد الفتاح بيومي حجازي**
   - ✓ التجارة عبر الأنترنت، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2008.
   - ✓ النظام القانوني لحماية التجارة الإلكترونية، الكتاب الثاني، الحماية الجنائية لنظام التجارة الإلكترونية، دار الفكر الجامعي، الإسكندرية،2002.

- ✓ الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، الإسكندرية، 2008.
- ✓ جرائم الكمبيوتر والانترنت في القانون العربي النموذجي_دراسة متعمقة في القانون المعلوماتي_الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2006.
- ✓ الجرائم المستحدثة في نطاق تكنولوجيا الإتصالات الحديثة، المركز القومي للإصدارات القانونية، القاهرة، 2011.
- ✓ النظام القانوني للتوقيع الإلكتروني، –دراسة تأصيلية مقارنة، دار الكتب القانونية، القاهرة، 2007.
- ✓ مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2006.
- ✓ التوقيع الإلكتروني في النظم القانونية المقارنة، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية،2005.
- ✓ الجوانب الإجرائية لأعمال التحقيق الإبتدائي في الجرائم المعلوماتية، دراسة مقارنة في ضوء القواعد العامة للإجراءات الجنائية، الطبعة الأولى، دار النهضة العربية، القاهرة ، 2009.

45. **عبد القادر المومني**، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2008.

46. د.**عبد الله بن عبد العزيز موسى**، مقدمة في الحاسب والانترنت، الطبعة الثالثة, دون دار النشر, الرياض, 2005.

47. **د.عبد المحسن المقاطع**، حماية الحياة الخاصة للأفراد وضماناتها في مواجهة الحاسب الآلي،مطبوعات جامعة الكويت، 1992.

48. **عبيدات محمد لورانس**، إثبات المحرر الإلكتروني، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2009.

49. **د. علي حسن محمد الطوالبة**، التفتيش الجنائي على نظم الحاسوب والإنترنت، دراسة مقارنة، الطبعة الأولى، عالم الكتب الحديث، أربد، 2004

50. **د.علي عبد القادر القهوجي**، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للنشر والتوزيع، الإسكندرية، 1999.

51. **د.عمر أبـــو الفتوح عبد العظيم الحمامي**، الحماية الجنائية للمعلومات المسجلة الكترونيا،دار النهضة العربية، القاهرة، 2010.

52. **د.عمر محمد أبو بكر بن يونـــس:**

- ✓ الإجراءات الجنائية عبر الانترنت في القانون الأمريكي، المرشد الفدرالي الأمريكي لتفتيش وضبط الحواسيب وصولا إلى الدليل الإلكتروني في التحقيقات الجنائية،دود دار نشر، 2008.

✓ أشهر المبادئ المتعلقة بالانترنت في القضاء الأمريكي، الطبعة الأولى، دار أكاكوس، 2004.
✓ الدليل الرقمي، الطبعة الأولى، دون دار النشر، 2007.

53. **عيسى غسان ربضي**، القواعد الخاصة بالتوقيع الإلكتروني، دار الثقافة للنشر والتوزيع، الأردن، 2012.
54. **فاروق علي الحفناوي**، موسوعة قانون الكمبيوتر ونظم المعلومات، قانون البرمجيات_دراسة متعمقة في الأحكام القانونية برمجيات الكمبيوتر، الكتاب الأول، دار الكتاب الحديث، القاهرة، 2003.
55. **د.فاروق محمد الأباصيري**، عقد الإشتراك في قواعد المعلومات عبر شبكة الأنترنت، دراسة تطبيقية لعقود التجارة الإلكترونية الدولية، دار النهضة العربية ، القاهرة، 2003.
56. **د.فتحي محمد أنور عزت**، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية للمجتمع المعلوماتي،الطبعة الثانية، دار الكتب، 2010.
57. **كميت طالب البغدلدي**، الإستخدام غير المشروع لبطاقة الإئتمان المسؤولية الجزائية و المدنية، دار الثقافة للنشر والتوزيع، الأردن، 2009.
58. **د.محمد أبـــو العلاء عقيدة**، مراقبة المحادثات التلفونية دراسة مقارنة، الطبعة الثانية، دار النهضة العربية، القاهرة، 2008.
59. **د. محمد الأمين البشري**، التحقيق في الجرائم المستحدثة، الطبعة الأولى، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004.
60. **د.محمد أمين الرومي**، المستند الإلكتروني، دار الفكر الجامعي، الإسكندرية، 2007.
61. **د.محمد أمين الشوابكة** ,جرائم الحاسوب والأنترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع،عمان، 2004.
62. **د. محمد حسين منصور**،المسؤولية الإلكترونية، دار الجامعة الجديدة، الأزاريطة، 2007,
63. **د.محمد حماد مرهج الهيتي**، جرائم الحاسوب، ماهيتها، موضوعها، أهم صورها، والصعوبات التي تواجهها–دراسة تحليلية لواقع الاعتداءات التي يتعرض لها الحاسوب وموقف التشريعات الجنائية منها–، الطبعة الأولى، دار المناهج للنشر والتوزيع، عمان، 2006.
64. **محمد خليفة**، الحماية الجنائية لمعطيات الحاسب الآلي دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، 2007.
65. **د.محمد سامي الشوا** ، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، 1994.
66. **د.محمد طارق عبد الرؤوف الخن**، جريمة الاحتيال عبر الانترنت، منشورات الحلبي الحقوقية،بيروت، 2011,

67. **د. محمـــد عبيد الكعبي**، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة، 2010.
68. **د.محمد علي العريان**، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، الإسكندرية، 2004.
69. **د.محمد فهمي طلبـــــة وآخرون**، الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني، موسوعة دلتا كمبيوتر، القاهرة، مطابع المكتب المصري الحديث، 1991.
70. **محمود الزهر ومحمد عثمان**, مقدمة الحاسب الآلي، معهد الإدارة العامة، السعودية،دون تايخ.
71. **د.محمود الكيلاني**، التشريعات التجارية والمعاملات الإلكترونية، الطبعة الأولى، دار وائل للنشر، عمان، 2004.
72. **مدحت عبد الحليم رمضان:**
   - ✓ الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة، 2012.
   - ✓ جرائم الإعتداء على الأشخاص والأنترنت، دار النهضة العربية، القاهرة، 2000.
73. **معادي أسعد محمد صوالحة**، بطاقات الإئتمان النظام القانوني وآليات الحماية الجنائية والأمنية، دار الأفاق المغربية للنشر والتوزيع، الربـــاط، 2008.
74. **د.ممدوح على مبروك**، مدى حجية التوقيع الإلكتروني في الإثبات، دار النهضة العربية، القاهرة، 2005.
75. **منير محمد الجنبيهي, ممدوح محمد الجنبيهي**, جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2004.
76. **ميسرة خالد الحمد**، الدليل الرقمي ومعايير جودته في الإثبات الجنائي، الطبعة الأولى، مركز الكتاب الأكاديمي، عمان، 2014
77. **د.ميشال عيسى طوني**، التنظيم القانوني لشبكة الأنترنت، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2001.
78. **د.نـــاهد فتحي الحموري**، الأوراق التجارية الإلكترونية، الطبعة الأولى، دار الثقافة، عمان، 2009.
79. **نبيلة هبة مولاي علي هروال**، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الإستدلالات، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2007.
80. **د.نعيم مغبغب**، مخاطر المعلوماتية والأنترنت، المخاطر على الحياة الخاصة وحمايتها، دراسة في القانون المقارن، منشورات الحلبي الحقوقية، بيروت، 1998
81. **نهلا عبد القادر المومني**، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2008.

82. **د.هدى حامـــد قشقوش،** الحماية الجنائية للتجارة الإلكترونية،دار النهضة العربية، القاهرة، 2000.

83. **د.هشام رستم،** قانون العقوبات ومخاطر تقنية المعلومات، الطبعة الأولى، مكتبة الآلات الحديثة، أسيوط، 1992.

84. **هلالي عبد الله أحمـــد:**

- ✓ تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة، 2006.
- ✓ إلتـــزام الشاهد بالإعلام في الجرائم المعلوماتية–دراسة مقارنة–الطبعة الثانية، دارالنهضة العربية، القاهرة، 2008.
- ✓ حجية المخرجات الكمبيوترية في المواد الجنائية، الطبعة الثانية، دار النهضة العربية، 2008.
- ✓ الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001، دار النهضة العربية، القاهرة، 2003.

85. **وضاح محمود الوضاح، نشأت مفضي المجالي،** جرائم الأنترنت –التعرض للأخلاق و الآداب العامة، الحض على الفجور ، جرائم الإستغلال الجنسي للأطفال، دار المنار، عمان، 2005

86. **د.وليد السيد سليم،** ضمانات الخصوصية في الأنترنت،دار الجامعة الجديدة، الإسكندرية ، 2012.

87. **د.ياسر الأمير فاروق،** مراقبة الأحاديث الخاصة في الإجراءات الجنائية،دارالمطبوعات الجامعية، الإسكندرية،2009.

88. **يونس عرب،** قانون الكمبيوتر،موسوعة القانون وتقنية المعلومات، الطبعة الأولى، منشورات إتحاد المصارف العربية، 2001.

ب– الرسائل العلميـــة

1. **أحمد حسام طه تمام،** الجرائم الناشئة عن إستخدام الحاسب الآلي، دراسة مقارنة، رسالة دكتوراه، دار النهضة العربية، القاهرة، 2000.
2. **أسامة فرج الله محمود الصباغ،** الحماية الجنائية للمصنفات الإلكترونية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 2011.
3. **أسماء حسن سيد محمد رويعي،** الحق في حرمة الحياة الخاصة في مواجهة الجرائم المعلوماتية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 2013.
4. **آمال عبد الرحيم عثمان،** الخبرة في المسائل الجنائية، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 1964.
5. **أمين عزان،** الحماية الجنائية للتجارة الإلكترونية،دراسة مقارنة، رسالة دكتوراه،كلية الحقوق، جامعة عين شمس.

6. **أيمن رمضان محمد احمد،** الحماية الجنائية للتوقيع الإلكتروني، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 2010.
7. **براهمي حنان،** جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، 2014.
8. **براهيمي صالح،** الإثبت بشهادة الشهود في القانون الجزائري، رسالة دكتوراه، كلية الحقوق، جامعة مولود معمري، تيزي وزو، 2012.
9. **حسين بن سعيد بن سيف الغافري،** السياسة الجنائية في مواجهة جرائم الأنترنت، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 2007.
10. **عمر محمد أبو بكر بن يونس،** الجرائم الناشئة عن إستخدام الانترنت، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 2004.
11. **سامح أحمد بلتاجي موسى،** الجوانب الإجرائية للحماية الجنائية لشبكة الأنترنت، رسالة دكتوراه، كلية الحقوق، جامعة الإسكندرية، 2010.
12. **سعيد بن محمد الغافري،** التعويض في التعامل الإلكتروني–دراسة في النظام السعودي مع التأصيل و المقارنة–رسالة دكتوراه الفلسفة في العلوم الأمنية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2012.
13. **صالح شنين،** الحماية الجنائية للتجارة الإلكترونية–دراسة مقارنة–، رسالة دكتوراه، كلية الحقوق، جامعة أبو بكر بلقايد ، تلمسان، 2013.
14. **عبد الناصر محمد محمود فرغلي،** الإثبات العلمي لجرائم تزييف وتزوير المحررات التقليدية والإلكترونية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 2010.
15. **عمر عبيد محمد الغول،** نطاق تطبيق القانون الجنائي من حيث المكان وفقا للمعطيات التكنولوجية المعاصرة، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 2009.
16. **فايز محمد راجح غلاب،**الجرائم المعلوماتية فيالقانون الجزائري واليمني، رسالة دكتوراه، كلية الحقوق، جامعة الجزائر 1، 2009.
17. **فتحي محمد أنــور عزت،** دور الخبرة في الإثبات الجنائي، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 2007.
18. **ماشاء الله عثمان محمد الزوي،** الحماية الجنائية لحرمة الحياة الخاصة في التشريع الليبي بالمقارنة مع التشريعين الفرنسي والمصري، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 2012.
19. **محمد نور الدين سيد،** المسؤولية الجنائية عن الإستعمال غير المشروع لبطاقات الوفاء، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة.
20. **محمود محمد محمود عبد الله،** الأسس العلمية والتطبيقية للبصمات–دراسة تحليلة مقارنة–، رسالة دكتوراه، كلية الدراسات العليا، أكاديمية الشرطة، مصر،1991.

21. **نائلة عادل محمد فريد قورة**, جرائم الحاسب الآلي الاقتصادية–دراسة نظرية وتطبيقية– الطبعة الأولى، رسالة دكتوراه، منشورات الحلبي الحقوقية، بيروت، 2005.
22. **نسرين هاني علم الدين**، دراسة الحل الأمثل لبناء نظام مركز لتوليد الشهادات الرقمية المستخدمة في أمن المعلومات، رسالة دكتوراه، كلية العلوم، جامعة دمشق، دون تاريخ.
23. –**نور خالد عبد المحسن العبد الرزاق** ، حجية المحررات والتوقيع الإلكتروني في الإثبات عبر شبكة الأنترنت، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 2009.

ت– المقالات العلمية و البحـــوث

1. **إبـــراهيم أبو الليل الدوسقي**، توثيق التعاملات الإلكترونية ومسؤولية جهة التوثيق إتجاه الغير المتضرر، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، الجزء الخامس،كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ماي2003.
2. **أبـــو الوفا محمد أبو الوفاء إبراهيم**، المسؤولية الجنائية عن الإستخدام غير المشروع لبطاقة الإئتمان، مؤتمر الأعمال المصرفية الإلكترونية، الجزء الخامس، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ماي 2003.
3. **أحمد قاسم فرح**، النظام القانوني لمقدمي خدمات الأنترنت –دراسة تحليلية مقارنة، –،مجلة المنارة، المجلد 13 ، العدد 09، 2007.
4. **أسامة بن غانم العبيدي**، التصديق الإلكتروني وتطبيقاته في النظام السعودي، مجلة القضائية، العدد الرابع، وزارة العدل، المملكة العربية السعودية، 1433.
5. **أكمـــل يوسف السعيد يوسف**، المسؤولية الجنائية لمقدمي المواد الإباحية للأطفال عبر الأنترنت، مجلة البحوث القانونية والإقتصادية، كلية الحقوق، جامعة المنصورة، 2011.
6. **آلاء يعقوب النعيـــمي:**
   - ✓ التصديق على التوقيع الرقمي مفهومه والعلاقات القانونية الناشئة عنه، مجلة الحقوق للبحوث القانونية والإقتصداية، العدد الأول، كلية الحقوق، جامعة الإسكندرية، 2011.
   - ✓ الوكيل الإلكتروني مفهومه وطبيعته القانونية، مجلة جامعة الشارقة للعلوم الشرعية و القانونية، المجلد 7، العدد2، ، يونيو 2010.
7. **أمـــجد حمدان الجهني**، جرائم بطاقة الدفع الإلكتروني عبر شبكة الأنترنت، مؤتمرالمعاملات الإلكترونية(التجارة الإلكترونية– الحكومة الإلكترونية)، مركز الإمارات للدراسات والبحوث الإتستراتيجة، 19–20 مايو، 2009.
8. **أورين كير ترجمة:** د/ عمر بن يونس، نطاق الجريمة الافتراضية، تفسير الدخول والتصريح به في إطار تشريعات الإساءة إلى الحاسوب، بحث منشور في مجلة القانون، العدد 78، جامعة نيويورك، نوفمبر 2003, سنة النشر 2004.

9. **د.أيمن عبد الحفيظ،** حدود مشروعية أجهزة الشرطة في مواجهة الجرائم المعلوماتية، مجلة مركز بحوث الشرطة، العدد 25، يناير 2004.
10. **د.بحبح عبد القادر،** إشكالية التحكم في وسائل الدفع البنكية وأثرها على الخدمات المصرفية –حالة الجزائر 1962–2010، مجلة الباحث، عدد 9، 2011.
11. **د.بطرس أنطوان،** حضارة الحاسوب والأنترنت، مجلة العربي، الكويت، 2000.
12. **د.توفيق شمس الدين،** الحماية الجنائية للمستند الإلكتروني، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، الجزء الثاني، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ماي 2003.
13. **د. ثناء أحمد محمد المغربي،** الوجهة القانونية لبطاقات الإئتمان، مؤتمرالأعمال المصرفية الإلكترونية، الجزء الثاني، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ماي 2003.
14. **حسين بن سعيد بن سيف الغافري،** الحماية القانونية للخصوصية المعلوماتية في ظل مشروع قانون المعاملات الإلكترونية العماني،ورقة مقدمة لمؤتمر أمن المعلومات والخصوصية في ظل قانون الإنترنت، القاهرة 2–4 يونيو2008.
15. **د.رايس محمد،** الحماية الجنائية للسند الإلكتروني في القانون الجزائري،مجلة الدراسات القانونية، العدد الأول، ، كلية الحقوق بيروت، 2006–2008.
16. **د.سامح عبد الواحد التهامي،** ضوابط معالجة البيانات الشخصية –دراسة مقارنة بين القانون الفرنسي والقانون الكويتي، المؤتمرالعلميالقانونيالثانيلكليةالقانونالكويتيةالعالمية – 15/16 فبراير 2015.
17. **د.سعد محمد سعد،** البطاقات البلاستيكية كوسيلة وفاء بالإلتزام، بحث مقدم في مؤتمر تشريعات عمليات البنوك بين النظرية و التطبيق، جامعة اليرموك، 2002.
18. **د.سليمان المقداد،** ضوابط الإعتراف بالمحررات الإلكترونية في الإثبات، الندوة العلمية حول المعاملات الإلكترونية : التطبيق المخاطر والحماية ، مركز الدراسات والبحوث الإنسانية والإجتماعية، وجدة، 14–05–2015.
19. **صالح الماوري،** تعزيز قدرات الموارد البشرية في عمليات التحقيق والإدعاء و المحاكمة في الجرائم المتصلة بالكمبيوتر، أعمال الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية، 19–20 نيسان، يونيو 2007.
20. **صالح فايز الشراري،** الحماية التشريعية للأشخاص المتعاملين في التجارة الإلكترونية ، دراسة مقارنة، مجلة الفكر الشرطي، المجلد الثامن عشر ، العدد 71، 2009.
21. **د.الصديق محمد الأمين الضرير،** بطاقات الإئتمان، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، الجزء الثاني، كلية الشريعة والقانون، جامعة الإمارات العربية، 2003.

22. **طارق محمد الجملي**، الدليل الرقمي في مجال الإثبات الجنائي، ورقة عمل مقدمة للمؤتمر المغاربي الأول حول المعلوماتية والقانون المنعقد في الفترة من 28-29 /2009/10 م, أكاديمية الدراسات العليا – طرابلس.

23. **د.عبد الإله محمد النوايسة**، مدى توفير حماية جزائية للتوقيع الإلكتروني ومعطياته في القانون الأردني،المجلة الأردنية في القانون والعلوم السياسية، المجلد 2، العدد 2، ربيع الثاني 1431، نيسان، 2010،

24. **د.عبد العالي برزحو**، مدى إمكانية تطبيق القانون الجنائي المغربي على جرائم المعلومات، مجلة الأبحاث والدراسات القانونية, العدد 4، 2014.

25. **د.عبد الله بن سليمان**، الأثر الإقتصادي لتطبيق الأعمال الحكومية الإلكترونية، منتدى الأعمال الحكومية الثالث، السعودية، 18-20 سبتمبر 2006.

26. **د.عبد المهدي كاظم ناصر**، حسين عبيد شعواط، عقد الإيواء المعلوماتي، مجلة الكوفة للعلوم القانونية والسياسية، العدد 21، جامعة الكوفة، 2014.

27. **د.عبد الناصر محمد محمود فرغلي و د. عبيد سيف سعيد المسماري**، ورقة بحث مقدمة للمؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، دراسة تطبيقية مقارنة، الرياض, المنعقد في الفترة:2-1148/11/04 ه الموافق ل 12-2007/11/14.

28. **عرابة رابح**، دور تكنولوجيا الخدمات المصرفية الإلكترونية في عصرنة الجهاز المصرفي الجزائري، الأكاديمية للدراسات الإجتماعية والإنسانية، العدد 8، 2012.

29. **د.عصام حنفي محمود موسى**، الطبيعة القانونية لبطاقات الإئتمان، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، الجزء الثاني، كلية الشريعة والقانون، جامعة الإمارات العربية، 2003.

30. **د.عصام حنفي محمود موسى**،الطبيعة القانونية لبطاقات الإئتمان، مؤتمر الأعمال المصرفية الإلكترونية، الجزء الثاني، كلية الشريعة والقانون، جامعةالإمارات العربية المتحدة، ماي ، 2003.

31. **د.عطا الله وراد خليل**،آليات أمن المعلومات في ظل الإنفتاح المعلوماتي، مجلة كلية الحقوق، العدد 6، جامعة بنها، 2011.

32. **د.على عبد القادر القهوجي**، الحماية الجنائية للبيانات المعالجة الكترونيا، دراسة مقدمة إلى مؤتمر كلية الشريعة والقانون،القانون والكمبيوتر والأنترنت، جامعة الإمارات العربية المتحدة، 1 مايو 2000.

33. **عـــلي كريمي**، تأثير التطور التكنولوجي على حقوق الإنسان،"الحياة الخصوصية و حماية البيانات الشخصية نموذجا"، مجلة أبحاث الفعل الإحتجاجي بالمغرب،مقاربة الإنسان و السلوكات والقيم، العدد 62،61 ، 2015.

34. **د.علي محمد الحسين موسى،** البطاقات المصرفية تعريفها أنواعها وطبيعتها، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، مجلد 5، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ماي 2003.

35. **د.علي محمود علي حمودة،** الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، بحث مقدم ضمن أعمال المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية، أكاديمية شرطة دبي، الفترة من 26 إلى 48-4-2003.

36. **غزال عادل،** الحكومة الإلكترونية في الجزائر والنفاذ على مجتمع المعلومات، الملتقى الوطني الثامن حول مستقبل ثقافة المعلومات والإتصال لدى الشباب في الجزائر بين صناعة المجتمع الجماهيري ومجتمع المعرفة والمعلومات، جامعة باتنة، 9-8 نوفمبر 2014.

37. **د.غنام محمد غنام،** ذاتية الإجراءات الجنائية في مجال جرائم تقنية المعلومات، بحث مقدم لمؤتمر "مكافحة جرائم تقنية المعلومات "، الإمارات العربية المتحدة ، 26- 30 / 11/ 2006.

38. **فوزي عمارة،** إعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور والتسرب كإجراء تحقيق قضائي في المواد الجزائية،مجلة العلوم الإنسانية، عدد33، جامعة منتوري، قسنطينة، جوان 2010.

39. **اللومي عبد الرؤوف،** المسؤولية التقصيرية على شبكة الأنترنات، المجلة القانونية التونسية ، مركز النشرالجامعي، تونس، 2007.

40. **ماء العينين السعداني،** الإطار القانوني للمصادقة على التعاملات الإلكترونية، مجلة قانون وأعمال، العدد الثاني، دجنبر، 2011.

41. **د.مبارك جزاء الحربي،** بطاقات الإئتمان، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، الجزء 5، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ماي 2003.

42. **د. محمد الأمين البشري،** الأدلة الجنائية الرقمية، مفهومها ودورها في الإثبات، المجلة العربية للدراسات الأمنية والتدريب، المجلد 17، العدد33، 2000.

43. **د. ممدوح عبد الحميد عبد المطلب، زبيدة محمد قاسم، عبد الله عبد العزيز**،نموذج مقترح لقواعد إعتماد الدليل الرقمي للإثبات في جرائم الكمبيوتر، مؤتمر الأعمال المصرفية والالكترونية، الجزء الخامس، كلية الشريعة والقانون،جامعة الإمارات العربية المتحدة،ماي 2003 .

44. **د.ممدوح عبد الحميد عبد المطلب**, إستخدام بروتوكول (tcp/ip) في بحث وتحقيق الجرائم على الكمبيوتر، ورقة عمل مقدمة إلى المؤتمر العلمي الأول حول الجوانب القانونية و الأمنية للعمليات الإلكترونية، الإمارات العربية المتحدة، في 26-28 نيسان 2003.

45. **د.محمد أبو العلا عقيدة،** التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، بحث مقدم للمؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية الشرطة، مركز البحوث والدراسات، دبي خلال الفترة 28/26 أبريل 2003.

46. **محمد أحمد المنشاوي**، سلطة القاضي الجنائي في تقدير الدليل الإلكتروني، مجلة الحقوق، المجلد 36، العدد 2، جامعة الكويت، 2012.

47. **د.محمد السيد عرفة**، التجارة الدولية الإلكترونية عبر الأنترنت، مفهومها والقواعد القانونية التي تحكمها ومدى حجية المخرجات في الإثبات، بحث مقدم إلى مؤتمر القانون و الكمبيوتر والأنترنت، الطبعة الثالثة، المجلد الأول، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة, 1-3 مايو 2000.

48. **محمد أمين الخرشة، نايف عبد الجليل الحمايدة**، الحماية الجنائية للتوقيع الإلكتروني في التشريع الإماراتي والبحريني، مجلة جامعة الأزهر، المجلد 16، سلسلة العلوم الإنسانية، غزة، 2014.

49. **محمد بكرارشوش**، الإختصاص الإقليمي الموسع في المادة الجزائية في التشريع الجزائري، مجلة دفاتر السياسة والقانون، العدد 14،جامعة قاصدي مرباح، جانفي 2016.

50. **. د. محمد حماد مرهج الهيتي**، البحث عن حماية جنائية للبيانات والمعلومات الشخصية المخزنة في الحاسب الآلي، مجلة الشريعة والقانون، العدد 27، جامعة الإمارات العربية المتحدة، جمادى الثانية، يوليو 2006.

51. **د.محمد رأفت عثمان**، ماهية بطاقات الإئتمان وأنواعها، وطبيعتها القانونية، وتمييزها عن غيرها، بحث مقدم لمؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، الجزء الثاني، كلية الشريعة والقانون، جامعة الإمارات العربية، 2003.

52. **د.محمد سليم العوا**، التحكيم في المعاملات المصرفية والإلكترونية، دراسة مقدمة إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة و القانون،الجزء الخامس، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ماي 2003.

53. **د.محمد صبحي نجم**، المسؤولية الجزائية عن الإستخدام غير المشروع لبطاقة الإئتمان، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون،الجزء الثالث، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة،ماي 2003.

54. **د.محمد عبد الحليم عمر**، بطاقات الإئتمان ماهيتها والعلاقات الناشئة عن إستخدامها بين الشريعة والقانون، مؤتمر الأعمال المصرفية والإلكترونية بين الشريعة والقانون، الجزء الثاني، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ماي 2003.

55. **د.محمد عرسان أبو الهيجا، علاء الدين فواز الخصاونة**، المسؤولية التقصيرية لمزوي خدمات الأنترنت عن المحتوى غير المشروع، دراسة في التوجيه الأروبي الخاص بالتجارة الإلكترونية، مجلة الشريعة والقانون، العدد 42، جامعة الإمارات العربية المتحدة، أبريل 2010.

56. **د.محمد عقاد**، جريمة التزوير في المحررات للحاسب الآلي، دراسة مقارنة، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون، القاهرة، 1993.

57. **د.محمد مرسي زهرة**، الدليل الكتابي وحجية مخرجات الكمبيوتر في الإثبات في المواد المدنية والتجارية، مؤتمر القانون والكمبيوتر والأنترنت، الجزء الثالث،الطبعة الثالثة، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ماي 2000.

58. **مفيد تـــركي**, إشكالية المحل في جريمة التزوير المعلوماتي ، مجلة كلية الحقوق، العدد 16، كلية الحقوق والشريعة، جامعة النهرين، أيار 2006.

59. **ممدوح البحر وعدنان احمد العزاوي**، بطاقات الاتمان والآثار القانونية المترتبة بموجبها، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، الجزء الثالث، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ماي 2003.

60. **ممدوح خليل البحر**، عدنان احمد ولي العزاوي، بطاقات الإئتمان والأثار القانونية المترتبة بموجبها، دراسة قانونية مقارنة، مؤتمر الأعمال المصرفية الإلكترونية، الجزء الثالث، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ماي 2003.

61. **د.موسى مسعود ارحومة**، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، بحث مقدم إلى المؤتمر المغاربي الأول حول: المعلوماتية والقانون، أكاديمية الدراسات العليا–طرابلس، المنعقد –خلال الفترة 28–2009/10/29.

62. **د. نادية محمد معوض**، أثرالمعلومـــاتية على الحق في سرية الأعمال، مجلة كلية الحقوق،الجزء الأول، جامعة ببنها، مصر.

63. **نزيه محمد الصادق المهدي**، نحو نظرية عامة لنظام بطاقات الإئتمان من الوجهة القانونية، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، الجزء الثاني، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ماي 2003.

64. **د.نهاد فاروق عباس**، الحماية الجنائية الموضوعية للحياة الخاصة من جرائم الأنترنت في التشريع المصري، دورية الإدارة العامة، العدد الأول، المجلس السادس والأربعون، فبراير 2006.

65. **د.هدى حامد قشقوش**، الحماية الجنائية للتوقيع الإلكتروني، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، الجزء الثاني، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ماي، 2003.

66. **يوسف بوهدون**، الحماية الجنائية للمستهلك في إطار عقود التجارة الإلكترونية، مجلة الملف، العدد 18، المغرب، أكتوبر 2011.

67. **يونس عرب**، دور حماية الخصوصية في تشجيع الاندماج بالمجتمع الرقمي– ورقة عمل مقدمة إلـــى ندوة أخلاق المعلومات، نادي المعلومات العربي، عمان، الأردن، 16–17 أكتوبـــر 2002.

ت_ مصادر الأنترنت

1. **أمجد حسان**, الفيروسات تهدد أنظمة المعلومات، مقال مقدم إلى ملتقى "الإرهاب في العصر الرقمي" المنعقد بجامعة الحسن بن طلال–عمان_, منشور على الموقع التـــالي:
http://www.google.com/search?
2. **د.حسين بن سعيد بن سيف الغافري:** الجرائم الواقعة على التجارة الإلكترونية، مقال متاح على الموقع الإلكتروني التالي:
http://www.mohamoon.com/montada/Default.aspx?Action=Display&ID=106198&Type=3
3. **خالد خالص**، المحاكـــم الإلكترونـــية، مقـــــال متاح على المـــوقع التالي:
http://www.ahewar.org/debat/show.art.asp?aid=29607
4. **د.خالد ممدوح إبراهيم**، التعاقد عبر الوكيل الإلكتروني، مقال متاح على الموقع الإلكتروني التالي:.http://kenanaonline.com/users/basune1/posts/804329
5. **زيـــاد ســـويدان**، انتحال الهوية الرقمية، مقـــــال منـــشور على:
http://www.urdri.fdspt.rnu.tn/articles/colloque-internet-identite-numerique/zied-souiden-usurpation-identite.ppt
6. **د.شيماء عبد الغني**, محمد عطا الله, مكافحة جرائم المعلوماتية في المملكة العربية السعودية, متاح على الموقع الإلكتروني التـــالي:
7. http://www.shaimaaatalla.com/vb/archive/index.php/t-3955.htm
8. **صالح أحمد البربري**، دور الشرطة في مكافحة جرائم الإنترنت في إطار الاتفاقيةالأوروبية الموقعة في بودابست في 2001/11/23، بحث منشور بموقع الدليل الإلكتروني للقانون العربي على شبكة الأنترنت: www.arablaw.info.com
9. **عـــــلي إبراهيم**, ذاكرة الحاسوب *Ram & Rom*, سوريا، مقال منشور على الموقع التالي:
http://www.kutub.info/library/book/5064
10. **لواء فهد إبراهيم الدوسري**، ضبط الآثار والأدلة المادية والجرمية الآبعاد القانونية ، ورقة مقدمة لجامعة نايف العربية للعلوم الأمنية، متاحـــــة على الموقع الإلكتروني التالي:
http://repository.nauss.edu.sa/bitstream/handle/123456789/58291/%D8%A7%D9%84%D8%A3%D8%AF%D9%84%D8%A9%20%D8%A7%D9%84%D9%85%D8%A7%D8%AF%D9%8A%D8%A9.pdf?sequence=1
11. **محمد جابر خلف الله**، التعليم بالمنتديات الإلكترونية، مقال منشور على الموقع التالي:
http://kenanaonline.com/users/azhar-gaper/posts/511728
12. **محمد عبد الله المنشاوي**, جرائم الانترنت من منظور شرعي و قانوني, مكة المكرمة , 1423 هـــ , بحث منشور على الموقع التالي:
http//www.minshawi.com/ginternety.aagstract.htm
13. **مصطفى دالع**، واقع التجارة الإلكترونية في الجزائر، مقالة منشور على الموقـــع الـــتالي:
www.ialamtic.com

14. **نـــداء كاظـــم المـــولى**، الطبيعة القانونية لنظام البطاقة المصرفية، مقال منشور على الموقع التالي:www.arablawinfo.com

15. **يونـــس عـــرب:**

- ✓ التجارة الإلكترونية, مقال متاح على الموقع الإلكتروني التالي:

http://www.arablaw.org/Download/E-commerce_General.doc

- ✓ جرائم الكمبيوتر والانترنت، المعنى والخصائص والصور وإستراتجية المواجهة القانونية، بحث منشور على الموقع التالي:

Http://www. Arablaw. org.

16.**يوسف قجاج**، إشكالية الإختصاص في الجريمة الإلكترونية: مقال متاح على الموقع الإلكتروني التالـــي:

http://www.hespress.com/opinions/256777.htm

ثالثا: المراجع باللغـــة الأجنبـــية

A. Ouvrages

❖ Ouvrages généraux

1. **Dominique Mougenot**, droit des obligations" la preuve" .3 edition. larcier, s,abruxelles, 2002.
2. **Françoise SIBAUD**, DU DROIT PENAL DES AFFAIRES DU FAUX , Sources Editions Jurisclasseur, 2002.
3. **Franklin Kuty**. Principes généraux du droit pénal belge. Tome II – l'infraction pénale. edition larcier , bruxelles . 2010 .
4. **Garron**, "L'incrimination du faux et du Mensonge en droit Pénal" 20 juin 2011, (irc – gov – mu),
5. **Gaston Stefani, georges Levasseur**, **Bernard bouloc**, droit pénal général, 16 eme édition, dalloz, paris, 1997.
6. **Jacques Marie Boileux**, Commentaire sur le code civil. imprimeurs de luniversite royale de france, paris.1843
7. **R. legros**, la preuve légale en droit pénal, in la preuve en droit,bruylant, bruxelles, 1981.
8. **Michel Véron**, droit pénal spécial ,2 éme édition, masson, paris, 1982.
9. **Michel Véron**, droit pénal spécial ,6 éme édition Armand Colin,paris, 1998.
10. **Michéle-laure rassat**, droit pénal général, 2éme édition, presse universitaires de france, paris, 1999.
11. **Patrice gattegno** ,droit pénal spécial,4 éme édition,dalloz,paris,2001.
12. **philippe conte, Patrick Maistre du Chambon**, droit pénal général, 7 eme édition, Armand Collin, paris, 2004.

❖ Ouvrages spéciaux

1. **Alain Bensoussan et Charles Copin**, le livre blanc de la signature electronique . le groupe de travail du Club CSA; *ANALYSES et SYNTHESES. 1999.
2. **Christian Gavalda † Jean Stoufflet**; INSTRUMENTS DE PAIEMENT ET DE CRÉDIT; Effets de commerce, carte de paiement, transfert de fonds; 7e ÉDITION. LexisNexis SA. Paris. **2009.**
3. **Christiane Féral-Schul**, Cyberdroit, le droit à l'épreuve de l'internet, 6ème éd, Dalloz, Paris 2010.
4. **Emmanuel Cauvin**; Vers une nouvelle Cité électronique**.** impr. en Allemagne **.**paris**.**2006**.**
5. **Emmanuel Cauvin;**Vers une nouvelle Cité électronique.Books on Demand, paris.2016 ,
6. **Eoghan Casey,**Digital Evidence and Computer Crime: Forensic Science, Computers and the internet, second edition, a cadimic press,2004.
7. **Ephraim Nissan**, Computer Applications for Handling Legal Evidence, Police Investigation and case argumentation , volume 1, springer, new York ,2012.
8. **Eric A. Caprioli** Vade-mecum juridique de la dématérialisation des documents juridiques ,7ÈME ÉDITION .Fédération des Tiers de Confiance, Paris, 2013.
9. -**Eric Filiol**, Les virus informatiques: théorie, pratique et applications, 2 edition , collection iris, springer, france 2009.
10. **Frédéric , jérôme pausier et emanual jez**. La criminalité sur l'internet , collection que sais- je ? 1ere édition ,paris**.**
11. **Isabelle poitier,** le commerce electronique sur internet, gazette du palais, 4 avril 1996.
12. **john r vacca**,Computer Forensics, Computer Crime Scene Investigation (Networking Series) (Charles River Media Networking/Security), 2002.
13. **John Rittinghouse and William M. Hancock PhD CISSP CISM**, Cybersecurity Operations Handbook, digital press, 2003.
14. **Myriam Quéméner & Yves charpenel** , cybercriminalité – droit pénal appliqué- Economica paris. France,2010.
15. *Olivier Ertzscheid,*QU'EST-CE QUE L'IDENTITÉ NUMÉRIQUE ?Collection : Encyclopédie numérique **,**OpenEdition Press, Marseille,2013.
16. **Pierre BreeseK Gautier Kaufman**, Guide juridique de l'Internet et du commerce électronique . vuibert. paris,2000,
17. **Rosenoer**, Jonathan, CyberLaw, The Law of the Internet, Springer, 1997.
18. **Valérie Sédallian**.Droit de l'Internet: réglementation, responsabilités, contrats, Collection Association des utilisateurs d'Internet, Éd. Net Press, 1997.
19. **Vivant et autres**, :informatique et droit pénal. les biens informatiques; objets d'une fraude.Lamy informatique 1991.
20. **Vincent Gautrais**, Le contrat électronique international, 2 edition, Bruylant Academia , Bruylant, Bruxelles, 2002.

21.-**Yves Charpenel, Myriam Quéméner** , Cybercriminalité)Droit pénal appliqué, Collection : Pratique du droit, 2010.

B . REVUES , ARTICLES ET AUTRE

1. .**ERMAN (sahir),** les crimes informatique et d'autres crimes dans le domaine de la techonologie informatique en TurquieRevue internationale de droit pénal. 1993.
2. **Badinter (Robert**), "La protection de la vie privée contre l'écoute électronique clandestine*", Semaine juridique* 1971, chronique 2435**.**
3. **Bensoussan (A**), Le droit des affaires du XXIe siècle - La signature électronique. Colloque Deauville, n°1. ReV. jur. Com , 27 et 28 juin 2000, 2001.
4. **Cachard** , droit du commerce electronique , RDAI, N 3,2004**.**
5. **Charlène WANPOUILLE**, Le faux, l'usage de faux et le faux en écriture publique Comparaison de l'état du droit et de la jurisprudence en France et à Maurice,Document rédigé en Mars; 'ecole Nationale de la Magistrature, 2015.
6. **Chilstein David**. Législation sur la cybercriminalité en France. In: Revue internationale de droit comparé. Vol. 62 N°2,2010.
7. **Cordier François**, « L'atteinte à l'intimité de la vie privée en droit pénal et les médias », *LEGICOM 4/*1999 (N° 20)**.**
8. .**Eric CAPRIOLI**, Le juge et la preuve électronique, colloque de Strasbourg, "Le commerce électronique : vers un nouveau droit", 8-9 octobre 1999. Revue de droit des technologies de linformation , n10 , 2000.
9. **Francillon (gaques),** Les crimes informatiques ET d' autres crimes dans domaine de la technologie informatique en France,Revue internationale de droit pénal, 1993.
10. **Frédéric LEPLAT**, la reforme des cartes bancaires par la loi du 15 novembre 2001, Revue générale du droit. numéro 840, 2012.
11. **Géraldine DANJAUME***,* La responsabilité du fait de l'information, Revues La Semaine Juridique - Edition Générale - n° 1,3895. 3 Janvier 1996.
12. **H. Croze**, L`apport du droit pénal à la théorie générale du droit de l`informatique (à propos de la loi No 88 - 19 du 5 Janvier 1988 relative à la fraude informatique), Juris-Classeur périodique. 1988**.**
13. **J. Frayssinet,** A propos du droit d'accès des personnes morales, n° 80, D. 21 mai 1992, ,
14. **Jean-Pierre Gridel**,Le droit des preuves au défi de la modernité , actes du colloque du 24 mars 2000.
15. **John R. Vacca,** Computer Forensics: Computer Crime Scene Investigation, Charles River Media, 2002, ISBN,1584500182.
16. **kaspersen**, computer crimes and other crimes against information technology in netherland, RIDP.

17. **Lamberterie Isabelle**, « La valeur juridique de la signature, perspective de longue durée », revue; *Hypothèsets* ; Publications de la Sorbonne 1/2006 (9)
.
18. **Luc GRYNBAUM**, "LCEN. Une immunité relative des prestataires de services Internet", Communication- Commerce électronique, nº 28, Études, Septembre 2004, ,..
19. **M. Michel MERCIER,**Rapport n° 491 (2015-2016) de, fait au nom de la commission des lois, déposé le 23 mars 2016**.**
20. **Maxime Wack, Nathanael Cottin, Bernard Mignot, Abdellah ElMoudni**, CERTIFICATION ET ARCHIVAGE LÉGAL DE DOSSIERS NUMÉRIQUES.revue *Document numérique*. Vol. 6,Lavoisier. 1/2002 .
21. **Michael G. Solomon** and others, computer forensics jump start, published by wiley- default,2005,ISBN:9780782143751.
22. **Michaud (Jean**). Le juge d'instruction et l'expert, Revue de science criminelle et de droit pénal comparé, , n° 3 , 1975.
23. **Michel Masse**. L'utilisation abusive de distributeur automatique de billets, Expertises des systemes dinformation, Nov. 1981
24. **Mohrenschloager (Manfred),** Computer Crime and Other Crimes Against Information Technology in germany ridp,1993.
25. **Myriam Quéméner**, Concilier la lutte contre la cybercriminalité et l'éthique de liberté rev Sécurité et stratégie 1 ,Club des Directeurs de Sécurité des Entreprises,2011,
26. **N adine adine L.C thwaites**; eurojust, autre brique dans l'édifice de 1 coopération judiciaire en matiere pénale ou solide mortier?, R.S.C.C, n 1 , janvier –mars 2003.
27. **Olivier cachard** , droit du commerce electronique , RDAI, N 3,2004-
28. **Padova (Yann).** Un aperçu de la lutte contre la cybercriminalité en France, Revue de science criminelle et de droit pénal comparé, 2002.
29. **Patrick Mennucci** , Rapport d'enquête de la commissiond'enquête sur la surveillance des filières et des individus djihadistes: "Face à la menace djihadiste, la République mobilisée"Assemblée nationale, 2 juin 2015.
30. **Pierre. TRUDEL**, La responsabilité sur Internet, texte préparé pour le séminaire *Droit et Toile*, Bamako, organisé par l'UNITAR (Institut des Nations unies pour la formation et la recherche), en association avec OSIRIS (Observatoire sur les Systèmes d'Information, les Réseaux et les Inforoutes au Sénégal) et l'INTIF (Institut francophone des nouvelles technologies de l'information et de la formation) de l'Agence intergouvernementale de la Francophonie Bamako, 27 mai 2002,
31. -**Stéphanie Faber et Marion Le cardonnel,** Confidentialité des emails; REVUE SQUIRE PATTON BOGGS; 18 Juin 2015
32. **T. Verbiest et E. Wery**, *Le droit de l'Internet et de la société de l'information, Droits européen, ; belge et français*; Revue internationale de droit comparé; n 1, 2002.
.

C– Thèses

1. **1Ibrahim Coulibaly**, La protection des données à caractère personnel dans le domaine de la recherche scientifique,Thèse de doctorat,Droit privé,Université DE GRENOBLE, france, 2011.
2. **Zahi Younes**, L' incidence des nouvelles technologies sur le droit traditionnel des actes juridiques Thèse de doctorat Droit privé , Université Panthéon-Sorbonne . Paris 1 , 2002.

D-Sites internet

❖ *Articles et rapports juridiques sur internet*

1. .**Alain-bensoussan**
   - ✓ Fraude informatique, La protéction d'un système informatique par un dispositif de sécurité n'est pas une condition d'application de la loi Godfrain, art. disponible en lingne á l'adresse suivantehttp://www.alain-bensoussan.com/pages/2903/
   - ✓ Fraude informatique-cybercriminalite -disponible en lingne á l'adresse suivante : http://www.alain-bensoussan.com/pages/2644/.

2. **Anne MOREAUX;** Infiltration et enquête sous pseudonyme: le numérique comme arme judiciaire,disponible en ligne á l'adresse suivante: http://www.affiches-parisiennes.com/infiltration-et-enquete-sous-pseudonyme-le-numerique-comme-arme-judiciaire-6073.html#ixzz42iWuMgmJ
3. **ANTHONY BEM,**
   - ✓ Laprotection des données à caractère personnel par les droits français et européen, articledisponible en ligne a l'adresse suivante: http://www.legavox.fr/blog/maitre-anthony-bem/protection-donnees-caractere-personnel-droits-16105.htm#.VvfUjNKLQSk
   - ✓ Le droit au respect de la vie privée : définition, conditions et sanctions; http://www.legavox.fr/blog/maitre-anthony-bem/droit-respect-privee-definition-conditions-16644.htm#.V_Y0qtSLQSm
   - ✓ L'INTRUSION ET LES ATTEINTES AUX SYSTEMES INFORMATIQUES SANCTIONNEES PAR LE DROIT PENAL, , disponible en lingne á l'adresse suivantehttp://www.legavox.fr/blog/maitre-anthony-bem/intrusion-atteintes-systemes-informatiques-sanctionnees-3158.pdf
4. **Bérengère Peyrat**, LA RÉFORME DU DROIT DES OBLIGATIONS. Article disponible:http://www.village-justice.com/articles/JeSuis1382-reforme-droit-des,21553.html
5. **Bernard COUSIN**, Les protocoles de base d'Internet, disponible en lingne á l'adresse suivante http://www.irisa.fr/prive/bcousin/Cours/I1.pdf
6. **Blandine Poidevin,**La responsabilité des intermédiaires de l'Internet au vu du rapport Lescure, article disponible en lingne á l'adresse suivante http://www.jurisexpert.net/la-responsabilite-des-intermediaires-de-linternet-au-vu-du-rapport-lescure/

7. **Charlène WANPOUILLE**, Le faux, l'usage de faux et le faux en écriture publique Comparaison de l'état du droit et de la jurisprudence en France et à Maurice,2015 articledisponible en lingne á l'adresse suivante: www.ijls.mu/index.php/lecture-notes?download=94:expose-sur-**le-faux**
8. **D. MELISON**, "Responsabilité des hébergeurs: une unité de régime en trompe l'œil", juriscom.net 25 avril 2005, *disponible en lingne á l'adresse suivante*www.juriscom.net
9. **Daniel A. Morris**, Tracking a Computer Hacker, USA Bulletin (May 2001), available at http://www.leetupload.com/database/Misc/Papers/Asta%20la%20Vista/Web%20Papers/tracking_a_computer_hacker.doc
10. **Didier frochot**; vers la notion juridique de vol de donnees; http://www.les-infostrateges.com/actu/14121921/vers-la-notion-juridique-de-vol-de-donnees
11. **Emilie Bailly & Emmanuel DAOUD** , WIFI et conservation des données : Les obligations du fournisseur de services disponible en ligne á l'adresse suivante*;*https://www.cdse.fr/wifi-et-conservation-des-donnees
12. **Emily M.Weitzenboeck**, Electronic Agents and the Formation of Contracts, Available at: http://128.176.101.170/eclip/documentsII/elecagents/contract_formation.pdf
13. **Eric A. CAPRIOLI**, « De l'authentification à la signature électronique : quel cadre juridique pour la confiance dans les communications électroniques internationales ? » https://www.uncitral.org/pdf/english/colloquia/EC/Caprioli_Article.pdf
14. **GUILLAUME CHAMPEAU** L'enquête policière sous pseudonyme sur Internet se généralise disponible en ligne á l'adresse suivantehttp://www.numerama.com/politique/128642-lenquete-policiere-sous-pseudonyme-sur-internet-se-generalise.html
15. **Haja Rakotozafy**, Nguyen Trinh Thiet, les atteintes aux systèmes informatisés de données,realise le 1 mars, 2005, disponible en lingne á l'adresse suivante:. http:\Documents and Settings\user\Desktop\Les atteintes aux systèmes informatisés de données e-juristes_org.mht.
16. **Henry, J.F**, "Testimony before permanent Subcommittee On Governmental Affairs, The United States Senate, Ninety, Ninth Congress, 1984. available at :http://www.igc.apc.org/nemesis/aclu/nudishallof shame/henry.html
17. **Jean Devèze**, Instruments de paiement et de credit, disponible en lingne á l'adresse suivante*:* http://197.14.51.10:81/pmb/COURS%20ET%20TUTORIAL/DROIT/Droit%20Prive/Instruments%20de%20paiement%20et%20de%20credit.pdfqrticle
18. **Jean-Wilfrid Noël** : Internet et enquête judiciaire,disponible en lingne á l'adresse suivante www.droit-internet.com.
19. **Jules Yossa**. Fraude à la carte bancaire : la victime est-elle remboursée ?http://www.village-justice.com/articles/Fraude-carte-bancaire-victime-est,17425.html#uXpf5xiCbqcGhoXi.99
20. Karima MOUSTAID

- ✓ Solutions pour prévenir les modifications non autorisées ,disponible en lingne á l'adresse suivante**http://karimamoustaid.over-blog.com/article-solutions-pour-prevenir-les-modifications-non-autorisees-84767396.html**
- ✓ La falsification de la preuve électronique,. *disponible en lingne á l'adresse suivante:* http://karimamoustaid.over-blog.com/article-la-falsification-de-la-preuve-electronique-84767971.html

21. **Leader, Kathryn**, Closed-Circuit Television Testimony: Liveness and Truth-telling, Law Text Culture, 14, 2010,. Available at:http://ro.uow.edu.au/ltc/vol14/iss1/18
22. **M. Robert DEL PICCHIA,;** Rapp. fait *au nom de la commission des Affaires étrangères, de la défense et des forces armées (1) sur le projet de loi,* ADOPTÉ PAR L'ASSEMBLÉE NATIONALE*, autorisant l'approbationde la* ***c*onvention** *sur la* **cybercriminalité** *et du* **protocole additionnel** *à cette convention, relatif à l'incrimination d'****actes*** *de nature* ***raciste*** *et* ***xénophobe****commis par le biaisde* **systèmes informatiques**, disponible en ligne á l'adresse suivante: http;//www.senat.fr/rap/104-321/104-3210.html
23. **-M. Jean-Marc Nesme**, rapp. fait au nom de la commission des affaires étrangéres sur le projet de loi **(n° 905)**.**autorisant l'approbation de la convention sur la cybercriminalité** disponible en ligne á l'adresse suivante;http://www.assemblee-nationale.fr/12/cr-cafe/04-05/c0405018.asp
24. **Marc SCHAEFER**, Protocole IPv6, 20 janvier 2011 disponible en lingne á l'adresse suivante: https://wiki.alphanet.ch/foswiki/pub/Ateliers/ProchainsDefisInternet/protocole-ipv6.pdf
25. Marc-Antoine Bindler, Le top 4 des fraudes à la carte bancaire; disponible en lingne á l'adresse suivante:http://www.europe1.fr/france/le-top-4-des-fraudes-a-la-carte-bancaire-1374767
26. **Mathias Kuhn,** L'accessibilité du site Internet comme fondement de la compétence du juge dans le cas d'atteinte au droit d'auteur par le biais d'Internet.disponible en lingne á l'adresse suivante: https://www.lepetitjuriste.fr/propriete-intellectuelle/laccessibilite-du-site-internet-comme-fondement-de-la-competence-du-juge-dans-le-cas-datteinte-au-droit-dauteur-par-le-biais-dinternet/
27. **Michel VILLARD**, La cybercriminalité et l'expertise judiciaire; disponible en ligne á l'adresse suivantehttp://www.lajauneetlarouge.com/article/la-cybercriminalite-et-lexpertise-judiciaire#.WCMyQNThASk
28. **Murielle Cahen**,
    - ✓ intrusion dans un systeme informatique, disponible en lingne á l'adresse suivante: http://www.murielle-cahen.com/p_references.asp, voir aussi; du même auteur " Actualités Intrusion dans un système de traitement automatique de données (STAD) : Les réponses du droit", disponible en ligne a l'adresse suivante: http://www.legipme.com/actualite/droit-ntic/intrusion-dans-systeme-traitement-automatique-donnees-stad-reponses-droit.html

- ✓ L'ADRESSE IP EST ELLE UNE DONNEE PERSONELLE, article disponible en lingne á l'adresse suivante: http://www.murielle cahen.com/publications/p_donnees3.asp?
- ✓ PROTECTION DES ECHANGES, article *disponible* en ligne á l'adresse suivante http://www.murielle-cahen.com/publications/page2310.asp

29. **Myriam Quéméne**, Nouvelles techniques d'enquêtes numériquesdisponible en lingne á l'adresse suivante http://www.adij.fr/wp-content/uploads/2015/01/Nouvelles-techniques-d%E2%80%99enqu%C3%AAtes-num%C3%A9riques-MQ.pdf; p6
30. **Noé MARMONIER**, Le vol de données informatiques article disponible en lingne á l'adresse suivante , http://www.legavox.fr/blog/noe-marmonier/donnees-informatiques-20088.pdf
31. **Nicolas Courtheoux** ,Les sanctions pénales dans la loi 78-17 relative à l'informatique, aux fichiers et aux libertés, article disponible en lingne á l'adresse suivante : http://www.e-juristes.org/les-sanctions-penales-dans-la-loi/
32. **Nicolás MelchiorLucie Robin** l'usurpation d'identité numérique : en droit français et en droit espagnol, http://www.eurojuris.fr/fr/particuliers-informatique-et-internet-usurpation-d-identite-numerique#.VwcQ8JyLQSk
33. **Philippe Andrieu**, stad; Accès et maintien frauduleux, disponible en lingne á l'adresse suivante: http://encyclo.erid.net/document.php?id=203 .
34. **Pierrat Emmanuel**, « Les infractions de presse sur l'internet », *LEGICOM, 1*/2000 (N° 21-22), URL : http://www.cairn.info/revue-legicom-2000-1-page-71.htm DOI : 10.3917/legi.021.0071
35. **Pierre Emmanuel OMBOLO MENOGAINSTRUMENT DE CREDIT ET DE PAIEMENT;** disponible en lingne á l'adresse suivante*:* http://lumiairedudroit.centerblog.net/36-instruments-de-credit-et-de-paiement:
36. **Pierre. TRUDEL**, La responsabilité sur Internet, texte préparé pour le séminaire *Droit et Toile*, Bamako, organisé par l'UNITAR (Institut des Nations unies pour la formation et la recherche), en association avec OSIRIS (Observatoire sur les Systèmes d'Information, les Réseaux et les Inforoutes au Sénégal) et l'INTIF (Institut francophone des nouvelles technologies de l'information et de la formation) de l'Agence intergouvernementale de la Francophonie Bamako, 27 mai 2002, p17. *disponible en lingne á l'adresse suivante*:http://pierretrudel.chairelrwilson.ca/cours/drt6929f/Resp.internet-trudel.pdf
37. **René PÉPIN**, Le statut juridique du courriel au Canada et aux États-Unis, Lex Electronica, vol. 6, n°2, Hiver / Winter 2001, disponible en lingne á l'adresse suivante http://www.lex-electronica.org/files/sites/103/6-2_pepin.pdf
38. **Sébastien FONTAINE** , Entête IP disponible en lingne á l'adresse suivante http://www.frameip.com/entete-ip/
39. **Simson L. Garfinkel** , Digital Forensics, available at http://www.americanscientist.org/authors/detail/simson-l-garfinkel

40. **Stéphane babonneau** La protection des témoins en France disponible en ligne á l'adresse suivante; http://www.sba-avocats.com/avocat-droit-penal-la-protection-des-temoins.html
41. **STROWEL (A.) et IDE (N.)** Responsabilité des intermediaries: actualités, législatives ET jurisprudantielles,Droit et Nouvelles Technologie. P. 10. disponible en lingne á l'adresse suivante; http://www.droittechnologie.org 28/12/2010
42. **Thibault Verbiest,Patrick Cuignet**, La création d'un délit d'usurpation d'identité numérique, http://www.droit-technologie.org/actuality-1316/la-creation-d-un-delit-d-usurpation-d-identite-numerique.html
43. **Thiébaut Devergranne**
    - ✓ Le droit à l'oubli sur Internet : petit guide juridique pour faire valoir ses droits, article disonible: https://www.donneespersonnelles.fr/droit-a-l-oubli
    - ✓ Donnees personnelles, articledisponible en ligne a l'adresse suivante:https://www.donneespersonnelles.fr/donnees-personnelles,
    - ✓ Le droit d'opposition institué par la loi informatique et libertés, article disponible en lingne á l'adresse suivante:https://www.donneespersonnelles.fr/droit-opposition
    - ✓ Le principe de loyauté et de licéité de la collecte des données. Article disponible en ligne á l'adresse suivante: https://www.donneespersonnelles.fr/le-principe-de-loyaute-et-de-liceite-de-la-collecte-des-donnees
    - ✓ , Le principe de temporalité, disponible en ligne á l'adresse suivante:https://www.donneespersonnelles.fr/le-principe-de-temporalite
44. **Thierry Vallat**,Surveillance informatique: captation des données s'affichant à l'écran en temps réel avec le décret du 18 décembre 2015, disponible en lingne á l'adresse suivante https://translate.google.dz/?hl=fr#fr/ar/bref%20y%20
45. **Xavier LEMARTELEUR**, Le scan de ports : une intrusion dans un STAD ?, p3, disponible en ligne a l'adresse suivante: http://www.juriscom.net/documents/priv20080613.pdf

❖ ***Sites internet divers***

1. Le site du sénat : http://www.senat.fr/.
2. L'Assemblée Nationale virtuelle. :www.assemblee-nat.fr
3. Les textes législatifs et réglementaires en France , disponible en lingne á l'adresse suivante: http://www.legifrance.gouv.fr
4. Le Journal Officiel de la République Française.:www.journal-officiel.gouv.fr
5. Le site de la Cour de Cassation : www.courdecassation.fr
6. Le site du Conseil d'Etatwww.conseil-etat.fr
7. Le Droit de l'Union Européenne : J.O., traité, législation,jurisprudence, documents d'intérêt public :europa.eu.int/eur-lex/fr
8. Textes de laCommission des Nations Unies pour le droit commercial international: http://www.uncitral.org/uncitral/fr/uncitral_texts.html

9. La Convention sur la cybercriminalité, signée par la France le 23 novembre 2001, est entrée en vigueur avec l'adoption du décret du 23 mai 2006, revue de web, realize le 5/11/2009, disponible en ligne á l'adresse suivante: http://www.foruminternet.org/specialistes/veille-juridique/actualites/publication-de-la-convention-sur-la-cybercriminalite-au-journal-officiel.html
10. Le site officiel de la **Commission Nationale Informatique et Libertés**.:www.cnil.fr

الفهرس

الفهرس