جامعة جيلالي ليابس
سيدي بلعباس
UDL
Université
DJILLALI LIABES
Sidi Bel-Abbès

كلية الحقوق والعلوم السياسية 19 مارس 1962

قسم: الحقوق

الحماية الجزائية للمستند الإلكتروني

أطروحة مقدمة لنيل شهادة الدكتوراه في العلوم.

تخصص: علوم قانونية – فرع: قانون البنوك

تقدم وتناقش علنا من طرف الطالب:

– بلحسيني حمزة

تحت إشراف الأستاذ:

– أ.د بوسندة عباس

أمام لجنة المناقشة

الأستاذ	الرتبة	جامعة الانتماء	الصفة
السيد: معوان مصطفى	أستاذ التعليم العالي	جامعة سيدي بلعباس	رئيسا
السيد: بوسندة عباس	أستاذ التعليم العالي	جامعة سيدي بلعباس	مشرفا ومقررا
السيد: باسم شهاب	أستاذ التعليم العالي	جامعة مستغانم	عضوا
السيد: لريد محمد أحمد	أستاذ التعليم العالي	جامعة سعيدة	عضوا

السنة الجامعية: 2019–2020م/ 1440–1441هـ

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

﴿ يَا أَيُّهَا الَّذِينَ آَمَنُوا إِذَا قِيلَ لَكُمْ تَفَسَّحُوا فِي الْمَجَالِسِ فَافْسَحُوا يَفْسَحِ اللَّهُ لَكُمْ وَإِذَا قِيلَ انْشُزُوا فَانْشُزُوا يَرْفَعِ اللَّهُ الَّذِينَ آَمَنُوا مِنْكُمْ وَالَّذِينَ أُوتُوا الْعِلْمَ دَرَجَاتٍ وَاللَّهُ بِمَا تَعْمَلُونَ خَبِيرٌ ﴾

[سورة المجادلة، الآية 11].

شكـــر وعـــرفان

أول من يشكر ويحمد أناء الليل وأطراف النهار، هو العلي القهار الأول والآخر، الظاهر والباطن الذي أغرقنا بنعمه التي لا تحصى، وأغدق علينا برزقه الذي لا يفنى، وأنار دروبنا فله جزيل الحمد والثناء العظيم، هو الذي أنعم علينا إذ أرسل فينا عبده ورسوله محمد بن عبد الله عليه أزكى الصلوات وأطهر التسليم، أرسله بقرآنه المبين، فعلمنا ما لم نعلم، وحثنا على طلب العلم أينما وجد.

لله الحمد كله أن ألهمنا الصبر على المشاق التي واجهتنا لإنجاز هذا العمل المتواضع.

انطلاقا من حديث المصطفى "من لا يشكر الناس لا يشكر الله" يشرفني أن أتقدم بخالص شكري وتقديري وامتناني إلى أستاذي المشرف، الأستاذ الدكتور "بوسندة عباس"، لما أغدقه علي من علمه الغزير، وتوجيهاته القيمة وآراءه السديدة، والتي كان لها الأثر البالغ في إثراء هذه الدراسة وتقويمها، فقد كان لي ومازال بمثابة أب وأستاذ موجه، ناصح ومرشد فنسأل الله عز وجل أن يجعله ذخراً للكلية و نبراسا للعلم وأن يجازيه عنا خير جزاء وأن يجعل عمله هذا في ميزان حسناته.

كما وأتقدم بوافر الشكر إلى أعضاء لجنة المناقشة، الذين تحملوا عناء قراءة هذا البحث وتقييمه لمناقشته رغم انشغالاتهم العديدة ورغم بعد المسافة وأخص بالذكر أستاذي الأستاذ الدكتور "معوان مصطفى" من جامعة سيدي بلعباس، الأستاذ الدكتور "باسم شهاب" من جامعة مستغانم، وكذا الأستاذ الدكتور "لريد محمد أحمد" من جامعة سعيدة.

ويستمر شكري ليصل كل أساتذتي، وعلى رأسهم عميد كلية الحقوق الأستاذ الدكتور "كراجي مصطفى" لما يبذله من مجهودات من أجل الرقي بكليتنا لما هو أحسن وأفضل وإلى كل الطاقم الإداري للكلية، وأخيراً وليس آخرا إلى كل من ساعدني على إعداد هذا البحث ولو بكلمة طيبة.

إهـــداء

إلى سكان قلبي....

- من علمني أن الدنيا كفلح وسلاحها العلم والمعرفة، إلى من أفنى زهرة شبابه في تربية أبنائه، فزرع فيهم القيم والمبادئ السامية، ولم يبخل عليهم بأي شيء ، إلى أعظم وأعز رجل في الكون، سندي في هذه الحياة والدي الحبيب.

- من تسكن الجنة تحت أقدامها، إلى التي لا يمكن أن أتصور الحياة بدونها، إلى من ساندتني في صلاتها ودعائها، إلى التي سهرت الليالي لتنير دربي، إلى زهرة البيت ونبع العواطف والحنان، إلى المتفائلة التي ترى الدنيا دائما جميلة رغم صعوبات الحياة ومشاقها، إلى أروع إمرأة في الوجود أمي الغالية أطال الله في عمرها.

- من جسدت الحب بكل معانيه فقدمت لي الكثير في صور صبر، أمل ومحبة، إلى من ساندتني ويسرت لي الصعاب، إلى من ضحت وجاهدت ليتم هذا العمل في أحسن صورة، إلى من تقاسمني حياتي بحلوها ومرها، إلى شريكة العمر ورفيقة الدرب، نصفي الثاني ....زوجتي الغالية متمنيا لها المزيد من التألق والنجاح.

- إلى جدتي أطال الله في عمرها وإلى روح جدي و جدتي رحمهما الله.

- إلى المحبة التي لا تنضب والخير بلا حدود، إلى من شاركتهم كل حياتي، إلى كنزي الغالي إخوتي الأعزاء توفيق ، محمد ، بلال.

- إلى قرة عيني وزهرة حياتي، إلى الوحيد الذي أتمنى له أن يكون أفضل مني إلى إبني الغالي إسلام.

- إلى كل أفراد عائلة بلحسيني، عائلة بعوز، وعائلة شرقي.

- إلى كل من هم في قلبي و لم يتذكرهم قلمي.

- إلى كل هؤلاء وبأسمى عبارات الحب و الوفاء أهدي هذا العمل.

قائمة المختصرات

أولا: باللغة العربية.

ج.ر: الجريدة الرسمية.

ج: جزء.

د. س.ن: دون سنة النشر.

د.ب.ن: دون ذكر بلد النشر.

د.ط: دون طبعة.

س: سنة.

ص: صفحة.

ط : طبعة.

ع: عدد.

ق.أ.ج. ج: قانون الإجراءات الجزائية الجزائري.

ق.إ.ج.م: قانون إجراءات جنائية مصري.

ق.ع.ج: قانون العقوبات الجزائري.

ق.م.ج: القانون المدني الجزائري.

مج: المجلد.

ثانيا: باللغة الفرنسية.

A.F.N.O.R :	Association Française du Nord.
AJ Pénal :	Actualité Juridique Pénal.
Al :	Alinéa.
Art :	Article.
C.A :	Cour D'appel.
c.civ.fr :	Code civil français.
C.P.FR :	Code pénal français.
c.p.fr :	Code pénal français.
c.p.p.f :	Code de procédure pénal français.
CE :	Communauté européenne.
Cf :	se conformer.
D :	Dalloz.
Ed :	Edition.
J.O.C.E :	Journal Officiel des Communautés européennes.
J.O.FR :	Journal Officiel Français.
J.O.U.E :	Journal officiel de l'Union européenne.
L.C.R magnétique:	La lettre de change relevé magnétique.
L.C.R papier :	La lettre de change relevé papier.
LGDJ :	Librairie Général de Droit et de Jurisprudence.
N° :	Numéro.
Op.cit :	Operecitato (ouvrage précédemment cité).
P :	Page.
PA :	Petites affiches.

PSC :	Prestataire de Service de Certification.
puf :	Presses Universitaires de France.
T :	Tome.
V :	Voir.
Vol :	Volume.
www :	World wide web.

مقدمة

مقدمة

عالم اليوم معقّد جداً، ومتداخل مع بعضه بعض، بلغ فيه التقدم العلمي والتقني مبلغاً لم يبلغه من قبل، أزالت فيه تكنولوجيا[1] المعلومات والاتصالات الحدود بين الدول، بحيث صار العالم كله بمثابة قرية صغيرة يعرف أقصاها أدناها، وتبوأت فيه المعرفة مكان الصدارة، بحيث لم يعد الصراع في العالم مقتصرا فقط على من يملك ومن لا يملك، بقدر ما صار محتدماً بين من يعرف ومن لا يعرف، وسادت مفاهيم العولمة في مجالات شتى، لعل أبرزها المجالات الاقتصادية والمالية، ووجدت بيئة جديدة أتاحت للمتعاملين وسائل متطورة لإبرام المعاملات المختلفة بما فيها القانونية[2].

وفي ظل هذه التحولات لم يبق القانون بمنأى عن أي تطور، إذ هبت رياح التغيير لتشمله، فتأثر هو الآخر بزخم ووهج التكنولوجيا، وقد كان من نتاج ذلك تحول وصف القاعدة القانونية من قاعدة آمرة وأخرى مكملة إلى قاعدة قانونية تقنية، كما وتراجعت تقسيمات القانون الكلاسيكية، وظهرت تقسيمات جديدة تستلهم تسميتها من المجال الذي تعالج في ضوئه، فظهر قانون المنافسة، قانون النقد والقرض، قانون الاستثمار، قانون حماية البيئة، القانون البنكي، قانون الأعمال...، كما وظهر مؤخراً القانون الإلكتروني[3]، والذي غير مفهوم القانون من معناه التقليدي إلى معنى آخر إلكتروني حتى ذاعت تسمية تكنولوجيا القانون، أو ما يسمى تقننة أو مكننة القانون[4].

---

[1]- تعرف التكنولوجيا بأنها علم يعني بدراسة مجموعة من الصناعة والفنون والحرف، وكل ما يمت لها بصلة من وسائل ومواد، وكلمة (Technology) أصلها إغريقي، وتقسم إلى قسمين Techno ومعناها فن ومهارة اكتساب الأشياء، أما (Logi) فهي تعني طريقة التعبير، وبذلك كلمة تكنولوجيا مجتمعة معناها التعبير عن طريقة اكتساب الأشياء، كما يمكن تعريفها بأنها إيجاد الطرق لتحويل المعلومات والموارد للحصول على قيم محددة.
www.woloo3.com. Date de consultation le site le 25-06-2017 à 14 :30.

[2]- محمد عبيد الكعبي، الحماية الجنائية للتجارة الإلكترونية، أطروحة لنيل شهادة دكتوراه في الحقوق، كلية الحقوق، جامعة القاهرة، 2009، ص.10.

[3]- عجة الجيلالي، مدخل للعلوم القانونية، نظرية القانون بين التقليد والحداثة، دار الخلدونية، الجزائر، د.س.ن.، ص، ص. 349- 350.

[4]- كريم كريمة، تأثير استعمال التقنيات الحديثة في تحقيق الأمن القانوني، ملتقى وطني حول الأمن القانوني، يومي 05 و06 ديسمبر 2012، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، الجزائر، ص. 2.

لقد ظهر هذا المصطلح كنتيجة حتمية للمرونة التي تتميز بها خاصية السلوك الاجتماعي، باعتبارها إحدى خصائص القاعدة القانونية، إذ طالما أن هذه الأخيرة قاعدة سلوك إجتماعي، فهذا يعني أنها قاعدة مرنة تتطور بتطور الجماعة وتسعى إلى مسايرة حاجاتها، ومواكبة مقتضيات العصر المتجددة، بحيث يتحكم في مضمونها عاملا المكان والزمان، إذ تتغير بتغير الأمكنة وبمرور الأزمنة[1]، وهو ما حدث حقاً بعد ولوج الوسائل التكنولوجية مختلف مجالات القانون، بحيث تغيرت المصطلحات التي ظلت راسخة منذ زمن فتحولت الكتابة التقليدية الخطية إلى كتابة إلكترونية، والتوقيع التقليدي إلى توقيع إلكتروني، كما ظهرت المستندات الإلكترونية كبديل للمستندات الورقية التقليدية، وتحول مفهوم الهجوم المسلح في القانون الدولي العام إلى الهجوم الإلكتروني[2]، وتغير مصطلح الجريمة ليبرز ما يسمى بالجريمة المعلوماتية، وتحول معنى الإدارة في القانون الإداري ليظهر ما يعرف بالإدارة الرقمية، وامتد ذلك ليشمل مختلف أشكالها القانونية فوجد العقد الإداري الإلكتروني، القرار الإداري الإلكتروني، كما وشهد القانون الدستوري ميلاد الحكومة الإلكترونية، وإمتد ذلك التحول ليشمل الشريعة العامة بحيث طغت المصطلحات التقنية على فروع القانون المدني لتبرز فكرة العقد الإلكتروني والإثبات الإلكتروني، كما وشمل الأمر القانون التجاري فظهرت وسائل الوفاء الإلكترونية، وعقود التجارة الإلكترونية[3].

ومن ثم فقد استبدلت فكرة التعاملات التقليدية بفكرة التعاملات الإلكترونية والتي تشمل في مفهومها العام كل تعامل يتم إبرامه أو تنفيذه أو إنهاءه بوسيلة إلكترونية أيا كان أطرافه، سواء أكان هذا التعامل بين أفراد أو بين جهات حكومية أو غير حكومية، أو بين دول أو مؤسسات دولية أو بين الجهات المذكورة وبعض آخر، كتعامل الفرد مع الشركات

[1]- محمد سعيد جعفور، مدخل إلى العلوم القانونية، ج1، الوجيز في نظرية القانون، ط 19، دار هومة، الجزائر، 2012، ص.20.

[2]- مصطفى نعوس، حق الدولة في استخدام القوة في الفضاء الإلكتروني للدفاع عن النفس، مجلة الحقوق، مجلة علمية محكمة ربع سنوية تعنى بنشر الدراسات القانونية والشرعية، تصدر عن مجلس النشر العلمي، جامعة الكويت، ع1، س الثامنة والثلاثون، جمادى الأولى 1435هـ- مارس 2014، ص.579.

[3]- جندولي فاطمة زهرة، عقود التجارة الإلكترونية في العلاقات الخاصة الدولية، رسالة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية ، جامعة أبي بكر بلقايد، تلمسان، الجزائر، السنة الجامعية 2017- 2018، ص.2.

التجارية، أو التعامل مع البنوك سواءً فيما بينها أو مع عملائها، عن طريق مستندات إلكترونية[1].

وللإشارة فإن المستندات الإلكترونية تعد ثمرة من ثمرات التزاوج الحاصل بين تكنولوجيا الاتصال وتكنولوجيا المعلومات، بل هي إحدى نتائج الثورة المعلوماتية التي غيرت وجه التاريخ، فقدمت للبشرية إنجازات أعظم من تلك التي قدمتها لها الثورات الزراعية والصناعية.

ولعل هذا التطور التقني في التعامل يرجع فضله إلى ظهور الحاسب الآلي وتزايد إستخدامه حيث لم يعد ثمة مجال اقتصادي أو اجتماعي أو صناعي أو إداري إلا وتساهم الحاسبات وتقنية المعلومات في أدائه وتطويره[2]، وللإشارة فقد ساهم في هذا التطور في ظهور شبكة الإنترنت، هذه الشبكة التي تعني لغوياً الترابط بين الشبكات والتي تتكون من عدد كبير من شبكات الحاسب الآلي المترابطة فيما بينها والمتناثرة في أنحاء العالم كله، فهي وسيلة تواصلية لا تعير للحدود الدولية اهتماما بالرغم من جذورها العسكرية والجامعية[3]، حيث أن بدايتها ترجع إلى سنة 1964 حين صمم العالم الأمريكي (بول باران) شبكة إنترنت لا تعتمد على أية إدارة مركزية[4]، لينتقل سنة 1968 ما بدأه لوزارة الدفاع الأمريكي، حيث أنشأت هذه الأخيرة وكالة مشاريع الأبحاث المتقدمة، وحفزت من خلالها علماء الحاسب الآلي والاتصالات لتصميم شبكة تصل بين عدد من الشبكات تضمن الوصول لأمن البيانات والرسائل التي تنتقل بين أجهزة الكمبيوتر في مرحلة الحرب، وقد كان من ثمار اللجنة ما أطلق عليه (Arpanet).

---

[1]- إبراهيم الدسوقي أبو الليل، توثيق التعاملات الإلكترونية ومسؤولية جهة التوثيق اتجاه الغير المتضرر، بحوث مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، مج الخامس، كلية الشريعة والقانون وغرفة تجارة وصناعة دبي، جامعة الإمارات العربية المتحدة، 9-11 ربيع الأول 1424ه- الموافق 10-12 ماي 2003، ص.1847.

[2]- آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، ط2، دار هومة، الجزائر، 2007، ص.05.

[3]- حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت، دار النهضة العربية، القاهرة، 2009، ص.15.

[4]- ناجي الزهراء، التجربة التشريعية الجزائرية في تنظيم المعاملات الإلكترونية المدنية والتجارية، المؤتمر العلمي المغاربي الأول حول المعلوماتية والقانون المنعقد في الفترة من 28 إلى 29 أكتوبر 2009، أكاديمية الدراسات العليا، طرابلس، ليبيا،2009- 2010، ص.4.

وفي سنة 1983 استخدمت شبكة وكالة مشاريع الأبحاث المتقدمة في المجال العلمي، وبصفة خاصة من قبل الجامعات، وظهر إلى جانب تلك الشبكة دخول شبكة أخرى إليها عظمت من قدراتها في الإمكانيات وزودتها بالصوت والصورة وأدوات الإعلام المتقدمة وهي شبكة (web)[1] والتي عممت للجمهور، ومن ثم فقد أحدثت الإنترنت ثورة في حياة الملايين عبر العالم، فأزالت الحدود واختزلت المسافات، وغيرت المفاهيم التي كانت سائدة من قبل فخلقت الزمن الافتراضي والمكان الافتراضي، وأتاحت للمتعاملين إمكانيات هائلة فسمحت بالولوج إلى عالم رقمي وإبرام مختلف التصرفات والاستفادة من الكثير من الخدمات عن بعد دون تكبد عناء ومشقة الانتقال.

وفي خضم هذا الواقع التقني الذي تتم فيه التعاملات الإلكترونية عن بعد في صورة معطيات معالجة آلياً تنتقل من نظام لآخر عبر شبكة الإنترنت دون دعامات ورقية ملموسة تظهر أهمية المستند الإلكتروني، إذ سيكون غالبا هو السند القانوني المعتمد بين أطراف التعامل الإلكتروني سواءً عند إتمام التعاملات الإلكترونية في شكل عقود إلكترونية، أو عن طريق تنفيذها عن طريق وسائل الوفاء الإلكترونية المختلفة[2]، حيث أصبح هذا المستند الوسيلة الأساسية التي تتم بموجبها وتحفظ فيها التعاملات الإلكترونية المختلفة.

وإذا كانت المعلوماتية قد ارتقت بمستوى الإنسان إلى الأحسن والأفضل ويسّرت له سبل الحياة، فإن كل تطور جديد يحمل في طياته جانباً مظلماً يتجسد في مجال القانون الجنائي بظهور المجرم المعلوماتي التي أصبح يستغل هذا التطور التقني في التعامل من أجل

[1]- يقصد بلفظ شبكة الويب (web) المعلومات الدولية (World Wide Web) وهي تتكون من عدد كبير من الوثائق المخزنة في حواسيب مختلفة بالعالم، وهذه الصورة من التعاقد تتم عن طريق زيارة العميل للموقع الإلكتروني للبائع، أو مقدم الخدمة، لإتمام التعاقد، حيث يتم إنشاء هذا الموقع (site) عن طريق الاشتراك في خدمة إنشاء صفحة خاصة بالعميل (home page) ليضع فيه البائع أو مقدم الخدمة كل ما يرغب فيه من بيانات مكتوبة أو مصورة، أو أفلام داخل هذا الموقع، وذلك للترويج لتلك البضاعة والخدمات ليكون لكل من يرغب في زيارة الموقع الدخول إليه، ودون استخدام لكلمة السر. مشار إليه من طرف، لزهر بن سعيد، النظام القانوني لعقود التجارة الإلكترونية، د.ط، دار هومه، الجزائر، 2012، ص.66.

[2]- ثروت عبد الحميد، التوقيع الإلكتروني، ماهيته، مخاطره وكيفية مواجهته ومدى حجيته في الإثبات، دار النيل للطباعة والنشر، القاهرة، 2001، ص.43.

غايات غير نبيلة، وتحقيق مآرب دنيئة من خلال استغلال الثغرات التقنية والتشريعية المحيطة بهذه النظم الحديثة بغية تحقيق أرباح غير مشروعة[1].

وليس المستند الإلكتروني بمنأى عن هذه الجرائم الجديدة التي اصطلح عليها الجرائم الإلكترونية التي تتميز بسمات خاصة منها أنها عالمية، وأن مخاطرها أمنية مادية وفكرية، وأنها سهلة الارتكاب، وأن إخفاء معالم الجريمة أمر يسير، وأنه يوجد صعوبات بالغة لتتبع مرتكبيها، وتحديد حجم الجريمة وحجم الضرر[2]، لا سيما وأن هذه المستندات قد تتضمن معلومات وبيانات مسجلة إلكترونيا، ويستوي أن تكون مخزنة داخل النظام المعلوماتي أو خارجه على وسيط من وسائط التخزين "كأسطوانة أو شريط ممغنط" قد تكون على قدر كبير من الأهمية والقيمة، خاصة بعد أن أصبحت تمثل نوعاً جديداً من الأموال يعرف بالأموال المعلوماتية، وقد تكون هذه المعلومات ذات طبيعة مالية واقتصادية أو ذات صيغة عسكرية، وقد تكون شخصية وهنا يبرز شبح المساس بحرمة الحياة الخاصة، ويكفي للتدليل على أهمية المعلومات أنها أصبحت الآن بمثابة سلعة تباع وتشترى وتقوم وفقاً لسعر السوق وعلى حسب ظروف العرض والطلب، الأمر الذي أدى إلى ظهور ما يعرف بالسوق السوداء للمعلومات بجانب السوق الشرعية لها[3].

ومن ثم فإنه من الوارد جدا أن يتعرض مستعملو هذه النظم المعلوماتية الحديثة للنصب أو السرقة أو الاحتيال أو الابتزاز أو لإساءة استخدام أسمائهم وتوقيعاتهم في أنشطة غير مشروعة عبر الإنترنت، بل إن الإحصائيات الرسمية تشير إلى التزايد الكبير للجرائم الواقعة على المعاملات الإلكترونية خاصة على شبكة الإنترنت، حيث أشارت دراسة أجرتها الشركة العالمية المتخصصة في تطوير الحلول البرمجية الأمنية (نورتن) أن الجريمة الالكترونية عبر العالم بلغت مستويات مقلقة موضحة أن ثلثي مستخدمي الإنترنت (65%) وقعوا ضحية للجريمة الإلكترونية مرة واحدة على أقل تقدير، وتمثل ذلك في الهجمات

[1]- آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص.1.
[2]- ليلى الزوين، عرض حول الجرائم الإلكترونية المالية، سلسلة ندوات محكمة الاستئناف بالرباط، تأثير الجريمة الإلكترونية على الائتمان المالي، ع السابع، مطبعة الأمنية، الرباط ،المغرب،2014، ص.188.
[3]- علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعية الجديدة للطباعة والنشر والتوزيع، الإسكندرية، مصر، 1997، ص.04.

الفيروسية أو التجسسية أو الاحتيالية لسرقة بيانات البطاقة الائتمانية، أو سرقة الهوية والبيانات المصرفية والشخصية لاستغلالها في أغراض غير مشروعة (إجرامية)[1].

كما أكدت تقارير صادرة عن مركز الدراسات الإستراتيجية والدولية (سي إس آي آس) أن جرائم الإنترنت تكلف الاقتصاد العالمي نحو 445 مليار دولار سنوياً، وأن أكبر الاقتصادات في العالم قد تحملت وطأة هذه الخسائر، حيث بلغ إجمالي الخسائر في الولايات المتحدة والصين واليابان وألمانيا مائتي مليار سنوياً، كما بلغت الخسائر المرتبطة بالبيانات الشخصية مثل البيانات المصرفية 150 مليار دولار، ووفق ما جاء في هذه التقارير فقد تعرض نحو أربعين مليون شخص في الولايات المتحدة لسرقة بياناتهم الشخصية من قبل المتسللين، بينما أثرت الثغرات رفيعة المستوى على 54 مليون شخص في تركيا و16 مليون في ألمانيا وأكثر من 20 مليون في الصين[2].

كما تضرر من هذه الجرائم سنة 2013 حوالي 12 مليون فرنسي، لذلك فوسائل الإعلام لا تخلو أسبوعيا من الأخبار المتعلقة بأمن الشبكات الحاسوبية، مما يؤكد أن الحرب مستمرة بين مدمني الحاسبات الآلية والمختصين بأمن الأنظمة المعلوماتية[3].

وحتى الدول العربية بما فيها الجزائر ليست بمنأى عن هذه الخسائر والاعتداءات سواءً الماسة بالأفراد أو المؤسسات وحتى بالأجهزة الحساسة بالدولة ، حيث ثبت مؤخراً خبر عن تسلل للموقع الإلكتروني لرئاسة الجمهورية بالجزائر، كما تم الولوج إلى الموقع الإلكتروني لوزارة العدل الجزائرية، هذا وسجلت مصالح الدرك الوطني والشرطة الجزائريين حوالي 25000 جريمة إلكترونية خلال2017 بما فيها جرائم القرصنة والابتزاز والتشهير والتحرش الإلكتروني والاحتيال، كما أشارت أرقام المصالح الأمنية المكلفة

[1] -www.emarataloyoun.com date de consultation le site 06-06-2019 à 14 :00.
[2] -www.aljazeera.net. date de consultation le site 06-05-2018 à 12 :30.
[3]- آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص.7.

بمكافحة الجرائم الإلكترونية إلى أن 80% من الجرائم المرتكبة تمت عن طريق مواقع التواصل الاجتماعي[1].

كل هذه المعطيات دعت المجتمع الدولي بأسره أن يفكر في توفير آليات حماية التعاملات الإلكترونية بدءاً بالحماية الفنية، وانتهاءً بالحماية القانونية، المدنية منها والجزائية، لا سيما وأن هذه الجرائم ليست وليدة بيئة معينة، ولا هي محصورة في نطاق محدود بل أصبحت جرائم منظمة عابرة للحدود.

وفي سبيل ذلك تضافرت الجهود لتنظيم المعاملات الإلكترونية عبر الإنترنت من الناحية القانونية، فعلى الصعيد الدولي كانت أبرزها تلك التي بذلتها لجنة قانون التجارة الدولية في الأمم المتحدة الأونيسترال (UNICITRAL)، اعتباراً من منتصف الثمانينات في مجال البحث في مسائل التبادل الإلكتروني للرسائل والمستندات، ليتوج الجهد عام 1995 بإقرار القانون النموذجي للتجارة الإلكترونية والمعروف بقانون الأونيسترال لسنة 1996، الذي يمثل الإطار التشريعي الأساس للتشريعات الوطنية في مجال التجارة الإلكترونية[2]، وإن كان هذا القانون قد اهتم بنوع واحد من مجالات التعامل الإلكتروني وهو التجارة الإلكترونية إلا أنه لم ينف إمكانية تطبيق أحكامه على أي نوع من المعلومات والتي تكون في شكل مستند إلكتروني، هذا وصدر كذلك قانون الأونيسترال بشأن التوقيعات الإلكترونية في سنة 2001[3].

كما عمدت العديد من الدول إلى إبرام المعاهدات، وعقد المؤتمرات الدولية، ومحاولة التنسيق بين القوانين المختلفة للدول بغية مجابهة الجرائم الواقعة على البيانات الإلكترونية،

---

[1]- www.DW.com date de consultation le site 23/04/2018 à 17 :00.

[2]- يهدف القانون النموذجي بشأن التجارة الإلكترونية إلى التمكين من مزاولة التجارة باستخدام وسائل إلكترونية وتعزيز القدرة على التنبؤ بالتطورات القانونية في مجال التجارة الإلكترونية.

Loi Type de la commission des Nations Unies pour le droit commercial international sur le commerce électronique (1996).

[3]- يهدف القانون النموذجي بشأن التوقيعات الإلكترونية إلى وضع إطار تشريعي حديث ومنسق وعادل يعالج موضوع المعاملة القانونية للتوقيعات الإلكترونية معالجة فعالة ويضفي اليقين على وضعيتها القانونية، كما يسعى إلى تيسير استخدام التوقيعات الإلكترونية عن طريق وضع معايير بشأن الموثوقية التقنية اللازمة لتحقيق التكافؤ بين التوقيعات الإلكترونية والخطية.

Loi Type de la Commission des Nations Unies pour le droit commercial international sur les signatures électroniques (2001).

ونسجل في هذا الصدد إبرام معاهدة بودابست لمكافحة جرائم الإنترنت في أواخر سنة 2001[1]، التي تهدف إلى توحيد الجهود الدولية لمكافحة الجرائم الإلكترونية، والتي تضمنت العديد من هذه الجرائم وبينت سبل التحقيق فيها، أما على الصعيد الأوروبي فقد صدرت جملة من التوجيهات التي تهدف إلى حماية البيانات الإلكترونية، كالتوجيه الصادر في 8 يونيو 2000 بشأن التجارة الإلكترونية[2]، التوجيه رقم 1999/93 الخاص بالتوقيعات الإلكترونية[3]، وكذا التوجيه رقم 910-2014 المتعلق بتحديد الهوية الإلكترونية وبث الثقة في التعاملات الإلكترونية في السوق الداخلية[4].

على صعيد التعاون العربي، وبعد أن أدركت الدول العربية ضرورة مواكبة الركب وعدم البقاء في عزلة عن العالم، بادرت بإبرام الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بالقاهرة في 2010/12/21، والتي صادقت عليها الجزائر بالمرسوم الرئاسي رقم 14-252 المؤرخ في 08-09-2014[5]، بالإضافة إلى القانون العربي الاسترشادي بشأن المعاملات والتجارة الإلكترونية، المعتمد بقرار من وزارة العدل العرب رقم 250/812 بتاريخ 2009/11/19، والقانون العربي الاسترشادي للإثبات بالتقنيات الحديثة الذي اعتمده مجلس وزارة العدل العرب بقرار 771/د.24 في 2008/11/27.

---

[1]- La convention sur la Cybercriminalité et son Rapport explicatif ont été adopté par le Comité des Ministres du conseil de l'Europe à l'occasion de sa 109e session, le 8 novembre 2001. La Convention a été ouvert à la signature à Budapest, le 23 novembre 2001, à l'occasion de la Conférence Internationale sur la Cybercriminalité, et elle est entrée en vigueur le 1er juillet 2004.

[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), J.O.C.E , L.178 du 17/07/2000.

[3]- Directive 1999/93/CE du Parlement Européen et du Conseil du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques, JOUE L. 13 du 19-01-2000.

[4]- Règlement (UE) N°910/2014 du Parlement Européen et du Conseil du 23 juillet2014 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]- المرسوم الرئاسي رقم 14-252 مؤرخ 13 ذي القعدة عام 1435 الموافق 8 سبتمبر سنة 2014 ، يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر سنة 2010، ج.ر، ع.57 س. 2014.

على صعيد التشريعات الوطنية الأجنبية كانت السويد على رأس الدول التي سارعت إلى سن تشريعات خاصة بالجرائم الإلكترونية، فأصدرت أول قانون سنة 1973 وهو قانون البيانات الذي جرّم الاحتيال الإلكتروني، وكذا الدخول غير المشروع إلى البيانات الإلكترونية أو تحويلها، أو الحصول غير المشروع عليها، وتلتها بعد ذلك بعض الدول الأخرى كالولايات المتحدة الأمريكية بإصدارها لقانون خاص بحماية أنظمة الحاسب الآلي عام 1985، ودعمته بآخر عام 1986، وكذا بريطانيا وكندا[1].

أما فرنسا فقد طورت قوانينها الخاصة لتتلاءم مع جرائم الحاسب الآلي والإنترنت، فأصدر المشرع الفرنسي أول قانون عام 1988، الذي أضاف إلى قانون العقوبات جرائم الحاسب الآلي، كما أضاف المشرع قواعد قانونية أخرى خاصة بجرائم الاعتداء على البيانات الإلكترونية، سواء من حيث الموضوع أو الإجراءات بموجب تعديل 1994، بعدها بدأت تدخلات سريعة للمشرع في مجال المعلوماتية والإنترنت وخاصة القانون رقم 2000-230 الصادر في 13 مارس 2000 المتعلق بتطويع قانون الإثبات لتكنولوجيا المعلومات والتوقيع الإلكتروني والذي بموجبه أدخل تعديلات على نصوص القانون المدني الفرنسي، وكذا القانون رقم 204-575 الصادر في 2004/06/21 المتعلق بالثقة في الاقتصاد الرقمي[2] لتتوالى القوانين والتعديلات بعد ذلك إلى غاية سنة 2016.

أما على صعيد التشريعات الداخلية للدول العربية فنجد أن بعض الدول كانت سباقة لتعديل قوانينها وإصدار قوانين جديدة منظمة للمعاملات الإلكترونية، وكان أولها تونس التي أصدرت قانون التجارة الإلكترونية لسنة 2000[3]، وقانون عدد 5 لسنة 2004 المتعلق بالسلامة المعلوماتية، ومن الدول العربية الرائدة في مجال المعاملات الإلكترونية نجد دولة الإمارات العربية التي أصدرت القانون الاتحادي رقم 06 لسنة 2006 المتعلق بمكافحة

[1]- طارق فوزي الفقي، الجوانب الإجرائية في الجرائم المعلوماتية - دراسة مقارنة-، رسالة للحصول على درجة دكتوراه في الحقوق، كلية الحقوق، جامعة المنوفية، مصر، 1432هـ- 2011 م ، ص. 258.

[2]- Cf. Jacques Larrieu, Droit de l'internet, 2ème éd. , Ellipses édition, paris, 2010.

[3]- قانون رقم 83 لسنة 2000 مؤرخ في 09 أوت 2000، المتعلق بالمبادلات والتجارة الإلكترونية، ج.ر. ع.64 الصادر في 11 أوت 2000.

جرائم المعلومات، كما أصدر المشرع المصري القانون رقم 15 لسنة 2004 المتعلق بالتوقيع الإلكتروني.

أما المشرع الجزائري، فقد حاول هو الآخر الالتحاق بالركب وبدأ يهتم بتنظيم المعاملات الإلكترونية عامة، وظهر ذلك من خلال بعض النصوص القانونية منها المرسوم التنفيذي رقم 98-257 المؤرخ في 25 غشت 1998 والذي يضبط شروط وكيفيات إقامة خدمات أنترنات واستغلالها[1]، والقانون رقم 2000-03 المؤرخ في 05 غشت 2000، الذي يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية[2].

أما التدخل الفعلي للمشرع الجزائري في الجانب الجزائي الخاص بالمعاملات الإلكترونية، فكان من خلال القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون العقوبات[3]، والذي أضاف بموجبه القسم السابع مكرر بعنوان المساس بأنظمة المعالة الآلية للمعطيات، والذي ضم المواد من 397 مكرر إلى 397 مكرر07، ووفر حماية جزائية موضوعية لمنظومة المعالجة الآلية، كما قام بتعديل قانون الإجراءات الجزائية بموجب القانون رقم 06-22 الصادر في 2006/09/20 والذي أدخل تغييرات إجرائية مهمة تتعلق بجرائم الاعتداء على البيانات الإلكترونية.

كما أصدر المشرع الجزائري أيضاً القانون رقم 09-04 المؤرخ في 05 غشت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[4]، لكن تبقى أبرز طفرة تشريعية عرفها التشريع الجزائري تلك التي عرفتها نصوص القانون رقم 15-04 المؤرخ في 01 فبراير 2015 المتعلقة بالتوقيع والتصديق

---

[1]- مرسوم تنفيذي رقم 98-257 مؤرخ في 3جمادى الأولى عام 1419 الموافق 25 غشت س 1998، يضبط شروط وكيفيات إقامة خدمات 'انترنات' واستغلالها، ج.ر، ع. 63، الصادرة بتاريخ 04 جمادى الأولى عام 1419 هجري.

[2]- القانون رقم 2000-03 مؤرخ في 5 جمادى الأولى عام 1421 الموافق 5 غشت س2000، يحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، ج.ر، ع. 48 الصادرة بتاريخ 06 أوت س 2000.

[3]- قانون رقم 04-15 المؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر س 2044، يعدل ويتمم الأمر رقم 66- 156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو س 1966 والمتضمن قانون العقوبات، ج.ر، ع. 71 الصادرة بتاريخ 10 نوفمبر 2004

[4]- قانون رقم 09-04 مؤرخ في 14 شعبان عام 1430 الموافق 5 غشت س 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر، ع. 47 الصادرة في 16 غشت 2009.

الإلكترونيين[1]، الذي أحدث جوا من الثقة لتعميم التعاملات الإلكترونية وكذا القانون 15-03 المتعلق بعصرنة العدالة، لينتهي الأمر في سنة 2018 بإصدار القانون 18-05 المتعلق بالتجارة الإلكترونية الصادر بتاريخ 2018/05/10[2] في انتظار قوانين أخرى تتعلق بمكافحة الجرائم الإلكترونية سواء بصورة مباشرة أو غير مباشرة.

انطلاقا من كل ما تقدم، تتضح أهمية موضوع الحماية الجزائية للمستند الإلكتروني، وهي في الحقيقة أهمية تبرز من ناحيتين إحداهما نظرية، والأخرى عملية، فأما النظرية فتكمن في تحديد صلاحية القواعد القانونية التقليدية في تنظيم التعامل بالمستندات الإلكترونية سواء من حيث تحديد قوتها الثبوتية من الناحية الجزائية، أو من حيث تنظيمها لوسائل حماية هذه المستندات، وكذا صلاحية النصوص العقابية في فرض حماية جزائية فعالة من جرائم الاعتداء على المستند الإلكترونية سواء من الناحية الموضوعية أو من الناحية الإجرائية وعن مدى ضرورة استحداث نصوص قانونية جديدة لمجابهة هذا الإجرام المستحدث، سواء على المستوى الداخلي أو على المستوى الدولي، هذا عن الأهمية النظرية.

أما الأهمية العملية فتكمن في رصد الحلول التي ينبغي إتباعها لمواجهة الصعوبات التي تطرحها حماية هذه المستندات من الناحية الجزائية باعتبارها كيانات معنوية غير ملموسة، سيما بعد انتشارها المذهل وذلك كله لتمكين رجل القانون، وبصفة خاصة القاضي الجزائري من التعامل معها، خاصة في ظل اتساع معدل جرائم الاعتداء عليها وعلى ما تتضمنه من بيانات.

من هنا يتضح أن اختيار هذا الموضوع لم يكن وليد الصدفة، بل تضافرت فيه عدة اعتبارات وعوامل، ولعل أهمها:

[1]- قانون رقم 15-04 مؤرخ في 11 ربيع الثاني عام 1436 الموافق أول فبراير س 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج.ر، ع. 06 الصادرة في 10 فبراير 2015.

[2]- قانون رقم 18-05 مؤرخ في 24 شعبان عام 1439 الموافق 10 مايو س2018، يتعلق بالتجارة الإلكترونية، ج.ر، ع.28 الصادرة في 16 مايو 2018.

- الإقبال المتزايد للأشخاص على شبكة الإنترنت لإبرام معاملاتهم المختلفة سواء كانت مدنية أو تجارية أو إدارية.
- قصور المنظومة القانونية الوطنية عن ضبط وتنظيم أحكام المعاملات الإلكترونية، مقارنة بتشريعات أخرى عربية وغربية.
- الصعوبات التي يطرحها هذا الموضوع من الناحية الإجرائية لمتابعة مرتكبي الفعل كإجراء التفتيش وغيرها من الإجراءات سواء على المستوى الداخلي أو الدولي.

ومن منطلق أن كل بحث تكتنفه صعوبات، فإن الصعوبات التي اعترضت هذه الدراسة تكمن في:

- قلة المراجع العلمية المتخصصة في هذا الموضوع، ولا يقصد بها الندرة العددية، بل الندرة المعرفية، إذ أن أغلب الكتب، والأطروحات، والرسائل، بل وحتى المقالات قد تعرضت للجريمة المعلوماتية بوجه عام دون أن تتطرق إلى المستندات الإلكترونية بشكل متخصص، ولاسيما من الناحية الجزائية.
- دقة المصطلحات الواردة بالموضوع، فهي مصطلحات تقنية تستلزم الإلمام بأسس وقواعد المعلوماتية، والاتصال الدائم بأصحاب الفن والتخصص.
- عدم وجود قانون في الجزائر يضبط كافة الجوانب المتعلقة بحماية المعاملات الإلكترونية من الناحية الجزائية، ناهيك عن عدم إمكانية حصر القوانين المنظمة لهذا الموضوع لارتباطه بفروع متعددة، منها القانون المدني، القانون التجاري...، إلى جانب المعاهدات والاتفاقيات وكذا القوانين النموذجية المنظمة للمعاملات الإلكترونية بصفة عامة والإجرام المعلوماتي بصفة خاصة.
- قلة الاجتهادات القضائية الجزائرية الواردة بشأن هذا الموضوع، رغم انتشار الوسيلة الإلكترونية في الميدان التجاري، والمدني، واستخدامها كوسيلة لإبرام المعاملات العقدية، أو لإبرامها وتنفيذها.

بناءً على ما تقدم، تبين أن موضوع الحماية الجزائية للمستند الإلكتروني يعد من أكثر المواضيع التي هي بحاجة إلى دراسة ومناقشة وتحليل، لارتباطه بمشاكل عديدة نظرية وقانونية، تجعل من الواجب بل ومن اللازم التطرق إليه وبحثه لتحديد معالمه، خاصة وأنه لن يكون بحثاً فكرياً معزولاً عن الواقع، وعليه تهدف هذه الدراسة إلى رسم تصور شامل لظاهرة من أشد الظواهر تعقيداً، ينظمها قانون أشد تعقداً لم تكتمل حلقاته بعد حتى في الدول المتقدمة، وذلك كله سعياً لرسم وبيان نطاقه الشامل في التشريع الجزائري في ظل نظرية واضحة المعالم.

من خلال ما سبق، يتضح أن تعدد زوايا البحث وتشعبها يستلزم الإجابة على الإشكالية التالية: **ما مدى كفاية الآليات القانونية المقررة لحماية المستند الإلكتروني من الناحية الجزائية؟**

إذا كانت هذه هي الإشكالية المحورية، فإن هناك إشكاليات أخرى تنبري على بساط البحث ولعل أهمها:

- ما مدى نجاعة الأساليب الفنية لحماية المستند الإلكتروني؟
- ما مدى حجية عناصر المستند الإلكتروني في الإثبات الجزائي؟
- هل تمكنت النصوص العقابية التقليدية من مجابهة كل الجرائم الواقعة على المستند الإلكتروني؟
- ما هي العقبات التي تواجه القائم بالتحقيق في الجرائم الواقعة على المستندات الإلكترونية؟
- هل النصوص الإجرائية التقليدية كافية لمتابعة الجرائم الماسة بالمستند الإلكتروني أم لا بد من تدعيمها بنصوص جديدة؟

- هل استطاعت التعديلات القانونية المستحدثة من طرف التشريعات من تحقيق التوازن بين حق الأطراف في الخصوصية ومصلحة المجتمع في متابعة مرتكب الفعل؟

- إلى أي مدى يساهم التعاون الدولي في محاربة الجرائم الواقعة على المستند الإلكترونية؟ وما هي سبل تعزيزه؟ ما هي المعوقات التي تعترضه؟ وكيف يمكن التغلب عليها؟

إن الإجابة على الإشكاليات السابقة، تستلزم تبني مناهج متعددة، وبما أن البحث العلمي يتميز بالتكامل المنهجي لا الأحادية المنهجية، فقد تم الاعتماد على كل من المنهج الوصفي، المنهج التحليلي، والمنهج المقارن، ولتكامل المنهجين الوصفي والتحليلي، فقد تم الاستناد عليهما معاً من خلال الوقوف على المعلومات والحقائق الواردة في هذا الموضوع، وتحليل مختلف جزئياته، انطلاقا من الآراء الفقهية مروراً بالنصوص القانونية، تعريجاً على الأحكام القضائية إن وجدت وصولاً للرأي الأنسب الواجب الإتباع من قبل رجال القانون. ولارتباط الدراسة بالقواعد التقليدية فقد تم اعتماد المنهج التأصيلي، القائم على رد الفروع إلى أصولها بالرجوع إلى نصوص قانون العقوبات.

وبسبب القصور الذي يشهده التنظيم القانوني للمستندات الإلكترونية في الجزائر لا سيما من الناحية الجزائية، فقد تم توسل المنهج المقارن بالاعتماد على النصوص القانونية المنظمة للمعاملات الإلكترونية، ولم يقف الأمر عند هذا الحد، بل تم التطرق لأحدث أوراق العمل الصادرة عن الكيانات المعنية بالقانون، وبخاصة منها الاتفاقيات والتنظيمات وكذا التوجيهات الصادرة عن البرلمان الأوروبي، والقوانين النموذجية الصادرة عن لجنة الأمم المتحدة سواء تلك المتعلقة بالتجارة أو التوقيع الإلكترونيين، وهذا كله قصد تحقيق التراكمية العلمية الكمية منها والنوعية، وإضفاء مزيد من الزخم والتنوع القانوني، لتحديد ما ينبغي على المشرع الجزائري الأخذ به عند سنه لقانون مكافحة الجرائم الواقعة على النظم المعلوماتية بما فيها المستندات الإلكترونية.

ترتيباً على ما تقدم، فإن موجبات بلوغ هذا البحث أهدافه اقتضت تبني الخطة الثنائية، بتقسيمه إلى بابين باب أول سيتم فيه دراسة النظام القانوني للمستند الإلكتروني، ويقسم هذا الباب إلى فصلين، فصل أول سيتم التعرض فيه إلى الضوابط القانونية للمستند الإلكتروني، في حين يتم التطرق في الفصل الثاني إلى الضوابط الفنية لحماية المستند الإلكتروني.

أما الباب الثاني فيعالج الأحكام التنظيمية والإجرائية للمستند الإلكتروني من الناحية الجزائية، وقسم هو الآخر إلى فصلين تطرق الفصل الأول منه إلى جرائم الاعتداء على المستند الإلكتروني سواءً كانت هذه الأفعال ماسة بالمحرر أو بالتوقيع الإلكتروني وورد بعنوان الأحكام التنظيمية للمستند الإلكتروني من الناحية الجزائية، في حين عالج الفصل الثاني الأحكام الإجرائية للمستند الإلكتروني من الناحية الجزائية بين التنظيمين الداخلي والدولي.

الباب الأول

النظام القانوني
للمستند الالكتروني

الباب الأول: النظام القانوني للمستند الالكتروني

لقد فتحت تقنية المعلومات آفاقا رحبة أمام البشرية، دعتها إلى محاولة البحث فيها والتوصل إلى مكوناتها والاستفادة منها في كافة مجالات الحياة، وتعتبر شبكة الانترنت من أهم وسائل المعلوماتية التي أحدثت تطورا هائلا في هذا العصر، بحيث مكنت من اختزال الوقت وتقريب المسافات بين المتعاملين بها، حتى غدا هذا العالم اليوم كأنه قرية كونية صغيرة، يتم الانتقال فيها بكل يسر وسهولة.

ولما كان المستند الإلكتروني أحد مفرزات هذا التطور التكنولوجي، فإن دراسة الحماية الجزائية المقررة له لا تتأتى إلا بالبحث في نظامه القانوني، خاصة أن أهم ما يميزه صفته الإلكترونية التي تجعله يتم بطرق آلية معلوماتية تسمح باختفاء الكتابة التقليدية ذات الوجود المادي الملموس، وكذا التوقيع الخطي التقليدي، ليحل محلهما الكتابة الالكترونية والتوقيع الإلكتروني، فظهور هذه التقنيات مكن المتعاملين من الانتقال من العالم المادي الملموس إلى عالم غير مادي، أي إلى عالم افتراضي.

إن مثل هذا الأمر يثير إشكالات متعددة في شتى المجالات، سواء منها المجال التنظيمي أو القانوني، أو حتى المجال التقني، ولا ريب أن تلك الإشكالات تتمحور حول كيفية حماية هذه المستندات وما تحويه من بيانات ومعلومات، وكذا القوة الثبوتية لها، وهي المسائل التي أدت إلى صدور تشريعات جديدة تتماشى والبيئة الرقمية، وتوفر الحماية اللازمة للمتعاملين بها.

لهذه الأسباب سيتم دراسة النظام القانوني للمستند الإلكتروني، وذلك بالتطرق إلى الضوابط القانونية الخاصة به **(الفصل الأول)**، وكذا الضوابط الفنية المتعلقة به **(الفصل الثاني)**.

الفصل الأول: الضوابط القانونية للمستند الإلكتروني

بفضل التطور التكنولوجي الذي شهدته مختلف مجالات الحياة، بما فيها الجانب القانوني، أصبح التعامل بالنظم المعلوماتية المختلفة واقعا ملموسا، ولما كان المستند الإلكتروني أحد سمات التطور التكنولوجي الحديث وأحد مفرزات البيئة الرقمية، فقد كان لزاما وضع جملة من الضوابط القانونية والفنية لضمان أمن وخصوصية المستند الإلكتروني، سرية البيانات والمعلومات التي يحويها، ناهيك عن ترسيخ الثقة والأمان في هذا النوع من التعاملات الإلكترونية، هذه التعاملات التي غالبا ما تتم في وسط مفتوح وعبر بيئة افتراضية، وبين أشخاص لا يجمعهم مكان واحد، وقد لا يعرف بعضهم البعض.

لأهمية هذه المسائل سيتم التعرض لها بالتطرق لضبط مفهوم المستند الإلكتروني **(المبحث الأول)**، والضوابط الموضوعية والشخصية له **(المبحث الثاني)**.

المبحث الأول: ضبط مفاهيم المستند الإلكتروني

مما لا شك فيه أن المستند الإلكتروني أصبح يتصل حاليا بطائفة مهمة من النظم الإدارية والتجارية والمالية التي تمتد لتشمل الدولة والأفراد على حد سواء، ففكرة المستند الإلكتروني باتت اليوم أحد الأدوات المهمة في تنفيذ فكرة الحكومة الإلكترونية التي تقدم خدماتها إلى الأفراد والهيئات العامة والخاصة[1]، كما أنه أصبح يشكل وسيلة من وسائل تنفيذ أهداف التجارة الإلكترونية، هذه الأخيرة التي أصبحت أحد سمات المجتمع الرقمي والمعلوماتي.

من خلال هذا، يتبين أن دراسة النظام القانوني للمستند الإلكتروني يستلزم الوقوف على المفاهيم المختلفة الواردة بشأنه **(المطلب الأول)**، تحديد أنواعه **(المطلب الثاني)**، وبيان صوره **(المطلب الثالث)**.

[1]- أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني – دراسة مقارنة -، بحوث مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، مج الثاني، كلية الشريعة والقانون وغرفة تجارة وصناعة دبي، جامعة الإمارات العربية المتحدة، 9-11 ربيع الأول1424هـ- الموافق لـ10-12 ماي 2003، ص. 484.

المطلب الأول: مفهوم المستند الإلكتروني.

لا يزال مفهوم المستند الإلكتروني مفهوما غامضا وغير محدد بشكل قانوني ثابت وأكيد، فهناك من يرى أنه سند وهناك من يرى أنه محرر، وهناك من يرى أنه بيانات مكتوبة على دعامة إلكترونية، هذا ويعتبره البعض مفهوم طارئ على النظام القانوني النافذ حاليا، إذ يصعب تكييفه كمستند كتابي واعتبار مضمونه كتابة، خاصة وأن مضمونه لا يظهر إلا باستعمال أجهزة إلكترونية تسهل قراءته[1].

أمام هذا الجدل الفقهي، سيتم التطرق إلى تعريف المستند الإلكتروني **(الفرع الأول)**، ثم التعرض لخصائصه **(الفرع الثاني)**.

الفرع الأول: تعريف المستند الإلكتروني.

نظرا للتطورات التكنولوجية الحاصلة في مجال المعرفة العلمية والمعلوماتية، وأمام واقع العولمة وتطور نظم الاتصالات والمعلومات، كان من الضروري إيجاد نظام معلوماتي يسمح بالكشف عن المعطيات الإلكترونية، التي أضحت المحرك الأول لكافة الأنشطة والعمليات، كما وأصبحت الأساس المرجعي الذي يبنى عليه اتخاذ القرارات[2].

ونظرا لأن هذه المعطيات المعلوماتية تدون على مستندات إلكترونية، فإنه ينبغي التعرض لتعريف المستند الإلكتروني من الناحيتين اللغوية والفقهية **(البند الأول)**، وكذا تعريفه من الناحية التشريعية **(البند الثاني)**.

[1]- عثمان الصديق أحمد محمد، المستند الإلكتروني، أهمية وضرورة إصدار تشريع يكفل حجيته ويضع ضوابطه له، ص.02؛

www.lebramy.gov . date de consultation le site02-04-2015 à12 :30.

[2]- معوان مصطفى، التجارة الإلكترونية ومكافحة الجريمة المعلوماتية (قواعد الإثبات المدني والتجاري)، ط1، دار الكتاب الحديث، القاهرة - مصر، 2008، ص. 17.

البند الأول: التعريف اللغوي والفقهي للمستند الإلكتروني.

نظرا لحداثة مصطلح مستند إلكتروني في النطاق العملي والقانوني، فإنه يظهر جليا تحليل مكوناته تحليلا لغويا، والوقوف على معناه القانوني، وهو الأمر الذي لن يتحقق إلا بالتعرض للتعريف اللغوي للمستند الالكتروني **(أولا)**، وبعدها للتعريف الفقهي له **(ثانيا)**.

أولاً: التعريف اللغوي للمستند الإلكتروني.

إن عبارة المستند الإلكتروني يمكن النظر إليها من خلال تقسيم هذا المصطلح إلى مقطعين أو كلمتين؛ كلمة "مستند" وكلمة "إلكتروني".

فبالنسبة لكلمة "المستند" فمن الناحية اللغوية فهي مأخوذ من السند، وهو كل ما ارتفع من الأرض من قبل الجبل أو الوادي ويجمع على إسناد، ويقال ساندته إلى الشيء فهو يتساند إليه، أي استندته إليه وتساندت إليه أي استندت، ويقال سند الشيء أي دعمه ورتقه، وساند الرجل أي عاضده، وسند إلى الشيء أي جعله له متكأ، ومن ثم فالسند هو كل ما يستند إليه ويعتمد عليه من حائط أو غيره، ومنه أطلق على صك الدين وغيره سند، وهو في الاقتصاد ورقة مالية مثبتة لغرض حاصل ذو فائدة ثابتة.

والمسند من الحديث، ما اتصل إسناده حتى يسند إلى النبي صلى الله عليه وسلم، وبناء على ذلك فإن المستند هو كل ما يمكن الاستناد إليه والاعتماد عليه أو الاحتماء به لدرء خطر، أو إثبات حق والمطالبة به ومنه أسندت إليه أمري، وهو سندي ومستندي.

وإذا كان معنى كلمة مستند جاء عاما في اللغة العربية على النحو السابق، فإنه جاء أكثر تحديداً في اللغة الفرنسية، حيث يقتصر إلى حد ما على الوسائل التي تفيد إثبات الحق أو الدين أو المعلومات والبيانات عن أيهما[1]، حيث تعني كلمة مستند (document) كل كتابة تفيد في الإثبات أو الإعلام (Tout écrit qui sert de preuve ou d'information) .

[1]- حمدي أحمد سعد أحمد، القيمة العقدية للمستندات الإعلانية، دراسة مقارنة بين القانون المدني (المصري والفرنسي) والفقه الإسلامي، دار الكتب القانونية، مصر، 2007، ص. 9.

هذا وتتنوع هذه المستندات بتنوع أشكالها ومضمونها، إذ قد تتخذ شكل مطبوعات (imprimés)، كالنشرات الدورية، والأبحاث التقريرية وبيانات المؤتمرات، أو كتب ومراجع تحليلية، أو تسجيلات مصرح بها أو رسومات وتخطيطات بيانية... إلخ، كما قد تتخذ شكل مصغرات (Micro) لمستندات أو وثائق معينة، كالمصغرات الفيلمية (Microfilms) أو المصغرات الوثائقية (Microfiches)، والتي تتميز بذاتية البحث الآلي (Automatisée)، أو مصغرات تصويرية (Microscopie) تحتوي على أكبر قدر من الوثائق.

بناء على ما سبق، فإن كلمة مستند يمكن أن تمتد لتشمل كل وسيلة للإعلام، أو كل مادة تحتوي معلومات أو بيانات سواء كانت ورقية أو غير ورقية[1].

وفي هذا السياق يرى جانب من الفقه[2] أن كلمة مستند تتأرجح بين ثلاث معاني؛ معنى ضيق، ويقتصر على المستندات الكتابية أو المطبوعة وهي المستندات التي تكون مادتها الوثائقية على شكل كتابة سواءً كانت على أوراق أو على مادة أخرى، ومن ذلك المصغرات الفيلمية أو الوثائقية التي تفيد في الإثبات أو الإعلام، ومعنى واسع نسبيا، بحيث يشمل إلى جانب الكتابة أو المطبوعات كل وثيقة تتضمن أموراً أو بيانات أو معلومات تفيد في الإثبات أو البينة، وعليه يشمل هذا المعنى الرسومات (dessins) والرسومات التخطيطية (schémas tracés)، والخرائط (plans) كما ويشمل أيضا الوثائق المعلوماتية (Informatiques)، ومعنى نسبي، وهو المعنى الخاص لكلمة مستند، وهو الذي يتبادر إلى أذهان الناس، ومن ذلك مستندات الشحن والنقل والفواتير وشهادات التأمين....الخ.

هذا عن كلمة مستند، أما كلمة إلكتروني فهي مأخوذة من كلمة إلكترون، ويعرف هذا الأخير لغةعلى أنه:" دقيقة ذات شحنة كهربائية سالبة، وهو أحد العناصر المؤلفة للذرة"[3].

---

[1]- عبر الفقه عن هذه الفكرة بعبارة (tout média ou élément apportant une information) .مشار إليه من طرف، حمدي أحمد سعد أحمد، المرجع السابق، ص. 11.

[2]- نفس المرجع، ص،ص. 11-12.

[3]- صلاح علي حسين، القانون الواجب التطبيق على عقود التجارة الإلكترونية ذات الطابع الدولي، د.ط، دار النهضة العربية، القاهرة، 2012، ص. 24.

أما كلمة إلكتروني فيتجه العلماء إلى تعريفها بأنها: " كل ما يختص بدراسة حركة وسلوك الإلكترونيات المسببة للتيار، سواء كان ذلك باستخدام الصمامات المفرغة، أو المحتوية على غازات، أو الصمامات الضوئية أو أشياء المواصلات وهكذا، أو هو فرع الكهرباء الذي يهتم بتصرفات واستعمال الأنابيب، وشبه المواصلات وسائر الدوائر التي تستعمل فيها"[1].

بهذا يبدو أن كلمة إلكتروني يقصد بها كل ما يتصل بالتكنولوجيا الحديثة، وله قدرات كهربائية أو رقمية أو مغناطيسية أو لاسلكية أو بصرية[2]، أو كهرومغناطيسية أو مؤتمة أو ضوئية أو ما شابه ذلك، بشكل تكون معه المعلومات ذات الخصائص الإلكترونية في شكل نصوص، أو رموز، أو أصوات، أو صور، أو برامج حاسب آلي أو غيرها من قواعد البيانات، وتكون في شكل نظام، إما لإنشاء أو استخراج، أو إرسال، أو استلام أو تخزين، أو عرض، أو معالجة المعلومات، أو الرسائل الكترونيا[3].

كما يرى البعض أن استخدام كلمة إلكتروني في عبارة المستند الإلكتروني نوع من التوصيف والتحديد لمجال ووسيلة أداء النشاط المحدد في كلمة المستند في حد ذاتها، ويقصد بها أداء النشاط الذي قد يكون في المجال التجاري أو الإداري أو المدني...الخ، وإبرام العقود والصفقات باستخدام الوسائط والشبكات الإلكترونية، ومنها شبكة الإنترنت[4].

ثانياً: التعريف الفقهي للمستند الإلكتروني.

لقد إهتم الفقه بإيجاد تعريف للمستند الإلكتروني، بحيث اعتبره جانب منهم الكتابة الواردة على دعامة إلكترونية، والتي تثبت تصرفا قانونيا ويترتب عليها أثر قانوني، وقد

[1]- علي محمد أحمد أبو العز، التجارة الإلكترونية وأحكامها في الفقه الإسلامي، ط1، دار النفائس، الأردن، 2008، ص.38.

[2]- بوعزة هديات، نظام الدفع الإلكتروني بين المزايا والمخاطر، مجلة دراسات قانونية، مجلة علمية محكمة تصدر دوريا عن مخبر القانون الخاص الأساسي، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، ع11، س2014، ص.297.

[3]- رضا متولي وهدان، النظام القانوني للعقد الإلكتروني، مجلة البحوث القانونية والإقتصادية، مجلة فصلية محكمة يصدرها أساتذة كلية الحقوق جامعة المنصورة، ع الثاني والأربعون، أكتوبر 2007، ص.28.

[4]- خالد ممدوح إبراهيم، إبرام العقد الإلكتروني، دراسة مقارنة، ط1، الدار الجامعية، الإسكندرية، 2007، ص. 58.

استند جانب آخر إلى التعريف السابق، مع استلزام شرط تحرير المستند من طرف موظف عام مختص، وذلك حتى تثبت الصفة الرسمية لذلك المستند[1].

هذا ولقد اتجه جانب من الفقه[2] إلى تعريف المستند الإلكتروني على أنه: "كل دعامة مادية أو غير مادية، تصلح لأن تدون عليها المعلومات أو الآراء"، أو هو: "الشيء المادي الذي يمكن أن يدون عليه شيء معنوي"، و يرى جانب آخر أن المقصود بالمستند في مجال المعلوماتية:" كل شيء مادي متميز (قرص أو شريط ممغنط أو خلافه) يصلح لأن يكون دعامة أو محلا لتسجيل المعلومات المعالجة بواسطة نظام المعالجة الآلية".

هذا وقد أطلق جانب من الفقه[3] على المستند الإلكتروني مصطلح المستند المعالج آلياً، وعرفه بأنه :" كل دعامة مادية مهيأة لاستقبال المعلومات وتسجيل المعطيات عليها من خلال تطبيق إجراءات المعالجة الآلية المعلوماتية[4]." وبعبارة أخرى فهو يقصد بالمستند المعالج آليا:" الدعامة المادية التي تم تحويل المعطيات المسجلة عليها إلى لغة الآلة[5]".

---

[1]- حمدي أحمد سعد أحمد، المرجع السابق، ص.14.

[2]- عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، تقديم فتوح الشاذلي، دار الثقافة للطباعة والنشر، عمان- الأردن، 1999، ص.150.

[3]- محمد عقاد، جريمة التزوير في محررات الحاسب الآلي، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون، دار النهضة العربية، القاهرة ، 1995.، ص.36.

[4]- لقد أطلق المشرع الجزائري على نظام المعالجة الآلية للمعلومات مصطلح نظام المعالجة الآلية للمعلومات والمعطيات للإشارة فلقد عرفت الاتفاقية الدولية للإجرام المعلوماتي أي اتفاقية بودابست الموقعة في 8 نوفمبر 2001" النظام المعلوماتي في مادتها الثانية بحيث جاء في نصها ما يلي: " نظام معلوماتي (système informatique) يعني كل آلة بمفردها أو مع غيرها من الآلات المتصلة أو المرتبطة، والتي يمكن أن تقوم سواء بمفردها أو مع مجموعة عناصر أخرى تنفيذاً لبرنامج معين، بأداء معالجة آلية للبيانات".

أما الفقه الفرنسي فلقد عرف نظام المعالجة الآلية للمعطيات على أنه كل مركب يتكون من وحدة أو مجموعة وحدات معالجة، والتي تتكون كل منها من الذاكرة والبرنامج والمعطيات وأجهزة الإدخال والإخراج وأجهزة الربط، والتي يربط بينها مجموعة من العلاقات التي عن طريقها تتحقق نتيجة معينة وهي معالجة المعطيات على أن يكون هذا المركب خاضع لنظام الحماية الفنية. وحسب رأي الفقه الفرنسي فإن نظام المعالجة الآلية للمعطيات يعتمد على عنصرين:

العنصر الأول: مركب يتكون من عناصر مادية ومعنوية مختلفة تربط بينها نتيجة علاقات توحدها نحو تحقيق هدف محدد.

العنصر الثاني: ضرورة خضوع النظام لحماية فنية.

لتفاصيل أكثر يراجع، آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص. 100؛ هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها، ط1، دار النهضة العربية، القاهرة، 2007، ص.16.

[5]- آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص،ص. 134- 135.

هذا ولقد ذهب فريق آخر من الفقه إلى تعريف المستند الإلكتروني على أنه: " كل محرر يحتوي على معلومات معالجة آليا"، كما عرفه جانب آخر[1] بأنه: " كل محرر معالج بطريقة آلية يكون معدا للإثبات، أو يصلح للإثبات طبقا للمبادئ العامة للإثبات".

من خلال عرض بعض التعاريف الفقهية للمستند الإلكتروني، يتضح أن الفقه قد تبنى اتجاهين اتجاه مضيق واتجاه موسع، فأما الاتجاه المضيق فيرى أن المستند الإلكتروني هو محرر معد للإثبات، في حين يعتبره الإتجاه الثاني كل دعامة مهيأة لاستقبال المعلومات.

بالرجوع لهذين الإتجاهين، يمكن القول أن التعريف الأمثل للمستند الإلكتروني يتحقق من خلال تبني موقف وسطي واعتباره: " كل وثيقة أو ورقة أو محرر أو مجموع محررات إلكترونية تتضمن معلومات وبيانات مكتوبة ومسجلة بطريقة إلكترونية آلية، موضوعة على دعامة إلكترونية، وبشرط أن تكون هذه الوثيقة أو المحررات تتضمن معلومات وبيانات متعلقة بواقعة لها أهمية قانونية، ويستوي أن تكون هذه الوثيقة أو المحررات موقعة توقيعا إلكترونيا، أو غير موقعة، كما ويستوي أن تكون هذه المحررات والوثائق قد خرجت من الآلة، وتم تصنيفها وتخزينها، أم أنها ما تزال بداخلها في انتظار تعديلها واستخراجها".

بعد أن تم تحديد التعريف اللغوي والفقهي للمستند الإلكتروني، يتوجب التطرق للتعريف التشريعي له، وبيان تطابقه مع التعاريف السابقة.

البند الثاني: التعريف التشريعي للمستند الإلكتروني.

لقد ترتب على ذيوع المستند الإلكتروني، وانتشار العمل به سعي الهيئات الداخلية والدولية إلى محاولة وضع تعريف له، بحيث عبر عنه قانون الأونيسترال النموذجي بشأن التجارة الإلكترونية بمصطلح رسالة البيانات، وعرفه في المادة الأولى بأنه: " المعلومات التي يتم إنشاؤها أو إرسالها أو استلامها أو تخزينها بوسائل إلكترونية أو ضوئية أو بوسائل متشابهة بما في ذلك، على سبيل المثال لا الحصر، تبادل البيانات الإلكترونية أو البريد الإلكتروني أو البرق أو التلكس أو النسخ البرقي".

[1]- خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر، أساليب وثغرات، دار الهدى للنشر، عين مليلة- الجزائر، 2010، ص.135.

وللإشارة فإن هذا التعريف هو نفسه الذي أوردته المادة الأولى من قانون الأونيسترال النموذجي بشأن التوقيعات الإلكترونية[1].

إلى جانب هذا التعريف، عرفت القواعد النموذجية والإرشادات حول التجارة الدولية (URGETS) الصادر عن غرفة التجارة اللبنانية المستند الإلكتروني في البند الثالث الفقرة الثالثة واعتبرته: " محتوى أي اتصال يفترض عملية نقل إلكترونية ممكن الوصول إليها، أي قابلة للاستعمال في مراجعات لاحقة"[2].

لئن كانت هذه التعاريف صادرة عن المنظمات الدولية وكذا الهيئات المهنية الداخلية، فإن التشريعات الوطنية هي الأخرى تعرضت لتعريفه، ومن ذلك ما تعرضت له تشريعات دول الخليج والمشرق العربي، بحيث عبر عنه القانون الاتحادي رقم 1 لسنة 2006 في شأن المعاملات والتجارة الإلكترونية بمصطلح السجل أو المستند الالكتروني، وعرفه في المادة9/1 بأنه: "سجل أو مستند يتم إنشاؤه أو تخزينه أو استخراجه أو نسخه أو إرساله أو إبلاغه أو استلامه بوسيلة إلكترونية، على وسيط ملموس أو على أي وسيط إلكتروني آخر، ويكون قابلا للاسترجاع بشكل يمكن فهمه."[3]

وهو ذات التعريف الوارد في المادة 7/2 من القانون الإماراتي الخاص بالمعاملات الإلكترونية والتجارة الإلكترونية[4].

أما قانون المعاملات الإلكترونية الأردني[5] فقد استخدم للتعبير عنه مصطلح السجل الإلكتروني، وعرفه في المادة (7/2) منه بأنه: "القيد أو العقد أو رسالة المعلومات التي يتم إنشاؤها أو إرسالها أو تسلمها، أو تخزينها بوسائل إلكترونية"، وقد عرفت المادة ذاتها في

---

[1]- وائل أنور بندق، قانون التوقيع الإلكتروني (قواعد الأونيسترال ودليلها الإرشادي)، دراسات تشريعية، ط1، مكتبة الوفاء القانونية، الإسكندرية، 2009، ص. 9.

[2]- عثمان الصديق أحمد محمد، المرجع السابق، ص، ص .04- 05.

[3]- قانون اتحادي رقم (1) لسنة 2006 في شأن المعاملات والتجارة الإلكترونية، ج. ر، ع442، س. السادسة والثلاثون بتاريخ 2006/1/31.

[4]- قانون رقم (2) لسنة 2002 بشأن المعاملات والتجارة الإلكترونية في الإمارات العربية الصادر بتاريخ 30 ذي القعدة 1422 الموافق 12 فبراير 2002.

[5]- التنظيم القانوني رقم 85 لسنة 2001 المؤرخ في31 ديسمبر 2001 المتعلق بالمعاملات الإلكترونية الأردني، ع.4524، والذي أصبح ساري المفعول بتاريخ 31 مارس 2002.

الفقرة 06 منها رسالة المعلومات واعتبرتها: "المعلومات التي يتم إنشاؤها أو إرسالها أو تسلمها أو تخزينها بوسائل إلكترونية، أو بوسائل مشابهة بما في ذلك تبادل البيانات الإلكترونية، أو البريد الإلكتروني أو البرق أو التلكس أو النسخ البرقي."

للإشارة، فإن هذا القانون ألغي سنة 2015 ليحل محله قانون المعاملات الإلكترونية رقم15 لسنة 2015[1]، وبالرجوع لهذا الأخير يلاحظ أن المشرع الأردني عرف السجل الإلكتروني في المادة 7/2 بأنه: "رسالة المعلومات التي تحتوي على قيد أو عقد أو أي مستند أو وثيقة من نوع آخر يتم إنشاء أي منها أو تخزينها أو استخدامها أو نسخها أو ارسالها أو تبليغها أو تسلمها باستخدام الوسيط الإلكتروني."

هذا وقد استخدم القانون البحريني الخاص بالمعاملات الإلكترونية[2] نفس المصطلح السابق وعرفه في المادة (3/1) منه بأنه: " ذلك السجل الذي يتم إنشاؤه أو إرساله أو تسلمه أو بثه أو حفظه بوسيلة إلكترونية."

ما ينبغي الإشارة إليه أن هذا القانون ألغي[3]، وحل محله القانون رقم 54 لسنة 2018، وفيه عرفت المادة 3/1 السجل الإلكتروني بأنه: " معلومات يتم إنشاؤها أو ارسالها أو تسلمها أو تخزينها بوسيلة إلكترونية، وتشمل بحسب الأحوال، كافة المعلومات التي تقترن أو ترتبط منطقيا بالسجل على نحو يجعلها جزءا منه سواء انشئت في وقت متزامن أم لا."

أما المشرع المصري فقد استخدم في قانون تنظيم التوقيع الإلكتروني، وإنشاء هيئة تنمية وصناعة تكنولوجيا المعلومات[4]، مصطلح محرر إلكتروني للدلالة على المستند الإلكتروني، وعرفه في المادة (1/ب) بأنه: "رسالة تتضمن معلومات تنشأ أو تدمج أو تخزن، أو ترسل أو تستقبل كلياً أو جزئياً بوسيلة إلكترونية أو ضوئية، أو بأية وسيلة أخرى مشابهة".

---

[1]- قانون رقم 15 لسنة 2015 المتعلق بالمبادلات الالكترونية الأردني.

[2]- مرسوم بقانون رقم (28) لسنة 2002 بشأن المعاملات الالكترونية البحريني، الصادر بتاريخ 7 رجب 1423هـ الموافق 14 سبتمبر 2002 ، ج.ر، ع. 2548 الأربعاء 18 ديسمبر 2002، المعدل والمتمم..

[3]- تنص المادة 3 من مرسوم بقانون رقم (54) لسنة 2018 بإصدار قانون الخطابات والمعاملات الالكترونية الصادر بتاريخ 20 ربيع الأول 1440هـ الموافق 28 نوفمبر 2018 ج.ر 3395 : "يلغى المرسوم بقانون 28 لسنة 2002 بشأن المعاملات الالكترونية كما يلغى كل نص يتعارض مع أحكام هذا القانون."

[4]- القانون رقم 15 لسنة 2004 بشأن تنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات.

من خلال هذا التعريف يبدو أن المشرع المصري انتهج نهج قانون الأونيسترال النموذجي للتجارة الإلكترونية 1996.

للإشارة، فإن هذا التوجه قد انتقد لقصور فكرة رسالة البيانات عن الإلمام بكل صور المستند الإلكتروني، إذ قد يكون هذا الأخير حسب جانب من الفقه[1] محرر إلكتروني أو مجموع محررات إلكترونية تتعدى رسالة البيانات، كون أن هذه الأخيرة وفقا له تنطوي على إيجاب من جهة، وقبول من جهة أخرى، في حين أن نطاق المستند الإلكتروني يكون أكثر اتساعا، إذ يشمل إلى جانب ذلك المحررات المخزنة في السجلات الإلكترونية، الوثائق الإلكترونية كشهادة الميلاد، الوفاة، الزواج...، وهذه المحررات لا تعد رسالة موجهة لأحد.

لئن كان هذا موقف تشريعات دول المشرق العربي، فإن دول المغرب العربي هي الأخرى تبنت الإتجاه ذاته، بحيث عبر المشرع التونسي في القواعد المدنية الخاصة بالإثبات الإلكتروني عن المستند الإلكتروني بمصطلح الوثيقة الإلكترونية، وعرفها عند تنقيحه وتتميمه لبعض فصول مجلة الالتزامات والعقود[2]، وتحديدا الفصل 453 مكرر بأنها: "الوثيقة المتكونة من مجموعة أحرف أو أرقام وأي إشارات رقمية أخرى، بما في ذلك تلك المتبادلة عبر وسائل الاتصال تكون ذات محتوى يمكن فهمه ومحفوظة على حامل إلكتروني يؤمن قراءتها والرجوع إليها عند الحاجة"، كما نصت في الفقرة الثانية من نفس الفصل على أنه: "تعد الوثيقة الإلكترونية كتبا غير رسمي إذا كانت محفوظة في شكلها النهائي بطريقة موثوق بها، ومدعمة بإمضاء إلكتروني"[3].

هذا عن المشرع التونسي، أما المشرع الجزائري فلم يتطرق إلى تعريف المستند الإلكتروني، بل ترك مهمة تعريفه إلى الفقهاء، مكتفيا بتعريف الكتابة الإلكترونية[4]، التي

---

[1]- رايس محمد، الحماية الجنائية للسند الإلكتروني في القانون الجزائري، مجلة الدراسات القانونية، ع، 1، 2006-2008، ط1، منشورات الحلبي الحقوقية، بيروت- لبنان-، 2009، ص،ص.79-80.

[2]- القانون عدد 57 لسنة 2000 المؤرخ في 13 جوان 2000 يتعلق بتنقيح وإتمام بعض فصول من مجلة الالتزامات والعقود.

[3]- معوان مصطفى، المرجع السابق، ص. 713.

[4] - يرى الأستاذ (لزهر بن سعيد) أن اعتراف المشرع الجزائري بالكتابة الإلكترونية من شأنه أن يضع حداً للغموض والجدل الذي كان يكتنف هذا النوع من الكتابة، كما يرى أنه باعترافه هذا يكون قد واكب التطور التقني الهائل في مجال التجارة الإلكترونية...الخ. مأخودة من، لزهر بن سعيد، المرجع السابق، ص. 144.

تعرض لها بموجب المادة 323 مكرر من القانون المدني التي تنص:" ينتج الإثبات بالكتابة من تسلسل حروف أوصاف أو أية رموز ذات معنى مفهوم، مهما كانت الوسيلة التي تتضمنها، وكذا طرق إرسالها"[1].

من خلال عرض التعاريف الواردة بخصوص المستند الإلكتروني، يتبين اختلاف التشريعات فيما بينها في المصطلح المستخدم للدلالة عليه من جهة، وفي مضمون التعريف من جهة أخرى، بحيث لم تتمكن تلك التعاريف من إبراز كل مميزات وخصائص المستند الإلكتروني، وبهذا يمكن القول أن المشرع الجزائري حسنا ما فعل حين لم يتطرق إلى وضع تعريف محدد للمستند الإلكتروني، متفاديا بذلك ما وقعت فيه باقي التشريعات المقارنة، ومن خلط في المفاهيم المتعلقة بهذا المجال.

إستنادا لما تقدم، يمكن القول أن المستند الإلكتروني: " كل وثيقة أو ورقة أو محرر أو مجموعة محررات إلكترونية تتضمن معلومات وبيانات مكتوبة ومسجلة بطريقة إلكترونية آلية، والموضوعة على دعامة إلكترونية على أن تكون هذه الوثيقة، أو هذه المحررات تتضمن معلومات وبيانات متعلقة بواقعة لها أهمية قانونية، ويستوي أن تكون هذه الوثيقة أو المحررات متضمنة لتوقيع إلكتروني يبين محررها أو صاحبها، أو تكون غير موقعة".

الفرع الثاني: خصائص المستند الإلكتروني.

بما أن المستند الإلكتروني يتصل بطائفة مهمة من الأنظمة الإدارية والتجارية والمالية المتنوعة، فإنه يتميز بمجموعة من الخصائص والمميزات التي جعلت منه يتماشى والتطور التقني والتكنولوجي، كما جعلت منه أداة تتناسب والثورة المعلوماتية التي يشهدها العالم المعاصر، هذه الخصائص منها ما هو مرتبط بشكله الإلكتروني ويقصد بذلك الخاصية الإلكترونية للمستند، ومنها ما هو مرتبط ببعض الوظائف والمهام التي يلعبها في بعض المجالات، كما هو الحال بالنسبة لمجال التجارة الإلكترونية والحكومة الإلكترونية.

[1]- قانون رقم 05-10 المؤرخ في13 جمادى الأولى عام 1426هـ الموافق 20 يونيو 2005 المعدل والمـتمم للأمر رقم 75-58 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر س1975 المتضمن القانون المدني الجزائري، ج.ر، ع.44، س.2005.

لأهمية هذه المسألة، سيتم التطرق لها من خلال تحديد الخاصية الإلكترونية للمستند **(البند الأول)**، والخاصية الوظيفية له **(البند الثاني)**.

البند الأول: الخاصية الإلكترونية للمستند.

يعد الشكل الآلي للمستند الإلكتروني من أبرز ما يميزه عن المستندات الورقية التقليدية، وتتجلى الخاصية الإلكترونية له من خلال أمرين؛ أولهما الصفة الإلكترونية الآلية للمستند وما يتضمنه من بيانات ومعلومات، وثانيهما الدعامة الإلكترونية أو الوسيط الإلكتروني الموضوع فيه هذا المستند، بحيث لا يمكن قراءة بياناته إلا بواسطة الآلة أو ما يعرف بجهاز الحاسوب أو الكمبيوتر.

فأما الصفة الإلكترونية للمستند فيقصد بها إجراء العمليات التي تتصل بالمستند ككتابته، حفظه، استرجاعه، نقله، وكذا نسخه بطريقة آلية رقمية، تتصل بتقنية تحتوي على ما هو كهربائي أو رقمي أو مغناطيسي أو لاسلكي أو بصري أو كهرومغناطيسي أو غيرها من العناصر المتشابهة[1]، إذ وعلى عكس المستندات الورقية التي تدون فيها البيانات والمعلومات بطريقة يدوية تقليدية، وتستخدم فيها وسائل بسيطة كالحبر والورق، ويتم حفظها ونسخها بوسائل تقليدية، فإن بيانات المستند الإلكتروني تدون وتحفظ وتستخرج بطريقة آلية إلكترونية، بحيث يكون كل تدوين، ضغط، تخزين، نقل، نسخ أو استرجاع للبيانات متصلا بتقنية تكنولوجية إلكترونية، ولا يمكن استخدامه خارج هذا المجال الإلكتروني[2].

هذا عن الصفة الإلكترونية للمستند، أنا بشأن الدعامة الإلكترونية للمستند أو ما يمكن التعبير عنه بالوسيط الإلكتروني، فيقصد به وضع البيانات الواردة في المستند على دعامة إلكترونية أو وسيط إلكتروني، بحيث لا يمكن الرجوع إليها عند الحاجة إلا بواسطة جهاز الحاسوب، فالكتابة في المستند الإلكتروني لا تظهر لعين الناظر إلا بواسطة جهاز الكمبيوتر، ومرد ذلك كتابة المستند الإلكتروني بلغة الآلة، هذه الأخيرة التي تقوم بمعالجته وتحويله إلى

[1]- أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني- دراسة مقارنة-، المرجع السابق، ص. 504.
[2]- إيهاب فوزي السقا، جريمة التزوير في المحررات الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2008، ص. 17.

كتابة بإحدى لغات الإنسان، ليظهر في نهاية المطاف على شاشة الكمبيوتر كمستند إلكتروني واضح المعالم[1].

وبما أن هذا المستند موجود على دعامة إلكترونية، ويتطلب وسيطا إلكترونيا لقراءته وفحص محتواه، فإنه بناءً على ذلك لا يمكن تحميله ونقله من جهاز إلكتروني لآخر إلا عن طريق الدعامة الإلكترونية، كما أن هذه الأخيرة تسمح بإرسال المستند الإلكتروني عبر شبكات وأجهزة الحاسب الآلي، وذلك عن طريق تحويله إلى رموز أو نبضات، ثم تحويله إلى كلمات مفهومة عن طريق بروتوكولات التعامل عبر الأجهزة الإلكترونية[2].

البند الثاني: الخاصية الوظيفية للمستند الإلكتروني.

يتمتع المستند الإلكتروني بمجموعة من المميزات والتي يمكن اكتشافها من خلال بعض الأدوار المهمة التي يلعبها في بعض المجالات، كما هو الحال بالنسبة للحكومة الإلكترونية والتجارة الإلكترونية، ويتضح ذلك فيما يلي:

أولاً: المستند الإلكتروني أداة لتنفيذ أهداف الحكومة الإلكترونية.

يعد المستند الإلكتروني الأداة الرئيسية لتنفيذ فكرة الإدارة الإلكترونية، والتي أطلق عليها حاليا مصطلح الحكومة الإلكترونية، هذه الأخيرة التي تقضي باستخدام نظم المعلومات الرقمية في إنجاز المعاملات الإدارية وتقديم الخدمات المرفقية، والتواصل مع المواطنين بمزيد من الإفصاح والشفافية[3].

لا شك في أن استخدام المستند الإلكتروني في نظام الحكومة الإلكترونية يجعل التعامل مع الأجهزة الحكومية سهلاً وميسوراً، وذلك من خلال الاتصال الإلكتروني بمواقع

---

[1]- سعد شيخو مراد السعدي، المسؤولية المدنية الناتجة من استخدام الكمبيوتر، رسالة ماجستير مقدمة إلى كلية الحقوق في جامعة بغداد، 1990، ص. 305. مشار اليه من طرف، نبيل مهدي زوين، المحررات الإلكترونية، دراسة قانونية، ص.13.
http://www.lawjo.net/vb/attachent.p...1&d=1282599206. Date de consultation le site 21-4-2017 à17 :00.

[2]- إيهاب فوزي السقا، المرجع السابق، ص .17.

[3]- عمار كريم كاظم، ناريمان جميل نعمة، القوة القانونية للمستند الإلكتروني، مجلة مركز دراسات الكوفة، مج 5، ع السابع، الكوفة، 2003، ص.178.

مختلفة، كما أنه يجعل إنجاز التعاملات سهلاً وسريعاً من خلال هذا الاتصال، ناهيك عن أنه يمكن المتعامل سواء كان فرداً أو شخصا معنويا عاما أو خاصا أن يتعامل مع الحكومة بوزاراتها وأجهزتها المختلفة، فيستطيع مثلا أن يتعامل مع إدارة الضرائب، الصحة، الهيئات التعليمية، البنوك، وما إلى غير ذلك من القطاعات[1].

ولعل خير مثال على ذلك ما ظهر حديثا من أنظمة مالية جديدة تسمح بالوفاء بالالتزامات عن طريق الوسائل الإلكترونية، وهو ما يعرف بنظام الدفع الإلكتروني.

إلى جانب ما سبق، تبرز خاصية المستند الإلكتروني في مجال الحكومة الإلكترونية من خلال تمكينه الأشخاص من الدخول إلى قاعدة البيانات المخزنة على شكل ملفات لدى الدولة والمصالح المعنية بشؤون العاملين والعملاء للحصول على المعلومات بسهولة ويسر.

وعلى ضوء هذا، أضحى بإمكان المتعامل الاطلاع على الوثائق أو الشهادات التي تكون مخزنة على شكل مستند إلكتروني، ما عدا المعلومات التي يترتب على الاطلاع عليها اعتداء على المصالح الأساسية كالمساس بسرية الحسابات البنكية، سرية الحياة الخاصة للأشخاص، سرية معاملاتهم.

إستنادا لما تقدم، يتضح أن إستخدام المستند الإلكتروني في مجال الحكومة الإلكترونية يؤدي إلى ضمان السرعة وربح الوقت في إنجاز المعاملات، فإنجاز المستند قد لا يتجاوز دقائق معدودة، وهو ما يوفر عناء الانتقال إلى مقر الإدارة وإنجاز المعاملة يدويا فضلا عن ذلك، فقد نجم عنى إستخدام المستند الإلكتروني في مجال الحكومة الإلكترونية الاستغناء عن خدمات بعض المرافق كخدمة مرفق البريد العادي، والذي أستبدل بخدمة البريد الإلكتروني (الإيميل)، وذلك لما يتميز به من سرعة الإرسال والاستقبال، فالرسالة تصل إلى موقع المرسل إليه في لحظات، كما يمكن أن يصل رد المرسل إليه إلى المرسل خلال لحظات أيضا إذا كان المرسل إليه مستعداً للرد، وذلك كله بسبب تخصيص بعض شركات

[1]- أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني- دراسة مقارنة-، المرجع السابق، ص. 525.

المعلومات الخاصة بالبريد بعض المواقع لهذا الغرض، ومن ذلك مثلا مثل شركة (هوتميل)[1].

لهذا كله، يرى البعض – وهو على حق- أن الحكومة الإلكترونية هي وسيلة مهمة لتعزيز الديمقراطية، والأخذ بها يحقق التواصل بين أفراد المجتمع وسلطة الدولة، ناهيك عن أنها وسيلة فعالة لنفاذ القانون[2]، وعليه فهي تمثل الجانب السياسي للثورة الرقمية، هذه الأخيرة التي حققت التواصل بين الأفراد والإدارة، من خلال ما لعبه المستند الإلكتروني من دور بارز باعتباره أحد أهم أدوات الحكومة الإلكترونية في تنفيذ أهدافها.

ثانياً: المستند الإلكتروني وسيلة لتحقيق أهداف التجارة الإلكترونية.

تعتبر التجارة الإلكترونية وليدة الثورة الرقمية التي يشهدها العالم المعاصر[3]، حيث أنها تقوم على تبادل البيانات الإلكترونية التي ترتكز على المعرفة المعلوماتية عن بعد، ويقصد بالتجارة الإلكترونية: "كل معاملة تجارية تتم عن بعد باستخدام وسيلة إلكترونية كشبكة الإنترنت"[4].

في هذا السياق، يبدو أن المستند الإلكتروني يلعب دوراً مهما في تحقيق أهداف هذه التجارة، إذ عن طريقه يمكن إنجاز المعاملات، وإبرام الصفقات والتصرفات القانونية بسهولة ويسر مما يؤدي إلى توفير النفقات، خاصة وأن هذه المعاملات يتم إبرامها بوسيلة

---

[1]- عمار كريم كاظم، ناريمان جميل نعمة، المرجع السابق، ص. 179.

[2]- أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني- دراسة مقارنة-، المرجع السابق، ص. 526.

[3]- يذهب جانب من الفقه الفرنسي (Allain Rallet) إلى القول أن تعبير "التجارة الإلكترونية" تعبير غير دقيق، وذلك لأن التجارة الإلكترونية لا تختلف عن التجارة التقليدية إلا أنها تأثرت بظاهرة تكنولوجيا الاتصالات الحديثة، ولذا يفضل استخدام مصطلح إلكترونية التجارة، بدلا من مصطلح التجارة الإلكترونية، في حين ينادي اتجاه آخر ومنهم (فيصل زكي عبد الواحد) ضرورة استخدام مصطلح التجارة عبر الوسائل الإلكترونية بدلا من اصطلاح التجارة الإلكترونية.
مشار إليه من طرف، محمد فريد الشافعي، التجارة الإلكترونية وإشكالية تسليم المنتجات عبر شبكة الاتصالات الدولية الإنترنت (دراسة مقارنة بين الفقه الإسلامي والقانون الوضعي)، دار الكتاب الحديث، القاهرة، مصر، 2009، ص. 07؛ ياسين محمد المدهون، النظام القانوني لحماية التجارة الإلكترونية، رسالة لنيل درجة الدكتوراه في الحقوق، كلية الحقوق، جامعة عين شمس، 1428هـ- 2007م، ص.9.

[4]- محمد فريد الشافعي، المرجع السابق، ص. 37.

إلكترونية دون حاجة إلى وسيط سواءً كان هذا الوسيط فرداً أو شركة، الأمر الذي يترتب عليه تخطي العقبات والحواجز الجغرافية بين دول العالم[1].

لقد ترتب على استخدام المستند الإلكتروني في مجال التجارة الإلكترونية تحول من استعمال الدعامات الورقية، والأوراق التجارية الورقية لإبرام المعاملات التجارية التقليدية، إلى استخدام الدعامة الإلكترونية في إتمام المعاملات التجارية، وهو ما أدى إلى ظهور بعض المصطلحات الجديدة أو التقنيات الجديدة في البيئة التجارية الرقمية، كالعقود التجارية الإلكترونية، النقود الإلكترونية، الأوراق التجارية الإلكترونية والتي من بينها الاعتماد المستندي الإلكتروني والشيك الإلكتروني.

بهذا يبدو أن هناك صلة وثيقة بين المستند الإلكتروني والتجارة الإلكترونية، وتفسير ذلك يظهر بوضوح في أنه إذا كانت هذه التجارة تعتمد على تبادل السلع والخدمات، فإن هذا التبادل لا يعدو أن يكون في حقيقة الأمر عقد يستجمع كافة شروطه القانونية من إيجاب وقبول، ويقترن بتوقيع ينسب إلى صاحبه ويرتب آثاره القانونية، وهذا العقد في مجال التجارة الإلكترونية ما هو إلا عبارة عن مستند إلكتروني توافرت فيه كل أركان وشروط العقد المكتوب، ويذيل بتوقيع إلكتروني يتناسب مع طبيعته[2].

إضافة إلى ما سبق، فإن المستند الإلكتروني يلعب دورا كبيرا في توفير الحماية لحقوق المتعاقد والمستهلك، هذه الخاصية التي تعتبر أيضا من بين أهداف التجارة الإلكترونية، بحيث يعمل المستند الإلكتروني على تمكين المتعاقدين من التعرف على ما هو معروض من سلع وخدمات، وكذا بيان نوعيتها وأوصافها وشروط تسليمها وأثمانها، وهو الأمر الذي يعزز الشفاهية، كما يجعل المتعاقد يبرم التصرف وهو على بينة وبصيرة على كل شروط التعاقد وظروفه[3].

---

[1]- عمار كريم كاظم، ناريمان جميل نعمة، المرجع السابق، ص،ص. 179- 180.

[2]- أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني- دراسة مقارنة -، المرجع السابق، ص. 527.

[3]- أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني- دراسة مقارنة -، المرجع السابق، ص. 527؛ عمار كريم كاظم، ناريمان جميل نعمة، المرجع السابق، ص. 180.

أما بخصوص دوره في مجال حماية المستهلك فيتضح في أن المستند الإلكترونية يعد المرجع الأساسي لمعرفة ما اتفق عليه طرفا العقد الإلكتروني، وكذلك تحديد التزاماتهم، فهو ببساطة المرجع الذي يبين حقوق وحدود التزامات طرفي العقد، لا سيما وأن عقد الاستهلاك يعد من العقود النمطية التي تكونت بواسطة ثورات التكنولوجيا وتقدم نوعية الحياة، خاصة وأنها ترد على أموال وخدمات يكون أحد طرفيها ضعيفا يحتاج إلى حماية، وهو الأمر الذي يؤدي إلى اختلال التوازن بين أطراف العلاقة القانونية، نتيجة لعدم توافر المساواة الفنية والاقتصادية بين الطرفين، وهو ما جعل التشريعات بما فيها التشريع الجزائري يتدخل لحماية الطرف الضعيف (المستهلك) في العقد، وذلك من خلال وضع نماذج معينة للعقد سلفاً، ويستوي في ذلك كون المستهلك شخصاً عادياً يرمي إلى إشباع حاجة شخصية، أو مهني يدخل في تصرفات قانونية يرجع فيها الميل إلى غياب التوازن العقدي بينه وبين الطرف الآخر[1]، ومن ثم فإن الحماية المقررة قانوناً للمستند الإلكتروني تضمن في الوقت ذاته حماية المستهلك[2]، وحماية هذا الأخير تعد من بين أهداف التجارة الإلكترونية، وسبب من أسباب بقاءها ودوامها.

من خلال ما سبق ذكره، يتبين أن المستند الإلكتروني وسيلة فعالة لتحقيق أهداف ومبتغيات التجارة الإلكترونية.

[1]- عمار كريم كاظم، ناريمان جميل نعمة، المرجع السابق، ص. 181.

[2]- في إطار حماية المستهلك هناك الكثير من التشريعات والجهود الدولية والمنظمات غير الحكومية قد نظمت حماية المستند الإلكتروني لضمان حقوق المستهلك، ومن هذه التشريعات تقنين الاستهلاك الفرنسي الصادر في عام 1995 وكذلك الإعلان الذي أصدرته منظمة التعاون الاقتصادي والتنمية عام 1998 في مدينة أوتاوا الكندية، والذي يتضمن خطة عمل للتجارة الإلكترونية وما يتعلق بها من وثائق، وكذلك التقرير الذي أعدته الغرفة الدولية للتجارة عام 1999 حول إرشادات حماية المستهلك في مجال التجارة الإلكترونية، واتبعته بتقريرين آخرين:
- الأول: حدد نطاق قوانين وسياسات حماية المستهلك المطبقة في مجال التجارة الإلكترونية.
- والثاني: شمل التقرير الخاص عن مبادرات تشجيع وتنفيذ حماية المستهلك في مجال التجارة الإلكترونية في أيار 2001.
مأخوذة من، عمار كريم كاظم، ناريمان جميل نعمة، المرجع السابق، ص. 181؛ محمد سعيد أحمد إسماعيل، أساليب الحماية القانونية لمعاملات التجارة الإلكترونية، دراسة مقارنة، ط1، منشورات الحلبي الحقوقية، بيروت، لبنان، 2009، ص.100.

المطلب الثاني: أنواع المستند الإلكتروني.

لقد أحدثت الثورة المعلوماتية أثرا كبيرا في طريقة إبرام التصرفات والمعاملات المختلفة، بحيث انتقل المتعاملون من استعمال المستندات الورقية التقليدية إلى استخدام المستندات الإلكترونية، وذلك لما تتمتع به هذه الأخيرة من خصائص ومميزات سبق بيانها.

ولئن كان التطور العلمي والتكنولوجي أثر بشكل جلي وواضح على طرق إبرام التصرفات القانونية، فهل امتد ذلك التأثير ليشمل أنواع المستندات المعروفة في مجال البيئة الرقمية؟

الإجابة على هذا، يتم من خلال التعرض لكل المستند الإلكتروني الرسمي **(الفرع الأول)**، والمستند الإلكتروني العرفي **(الفرع الثاني)**.

الفرع الأول: المستند الإلكتروني الرسمي.

يعرف جانب من الفقه[1]المستند الرسمي العادي الورقي، بأنه المستند الذي يحرره موظف في حدود اختصاصاته المقررة قانونا، هذا وقد عرفت المادة 1317 من القانون المدني الفرنسي[2] المحرر الرسمي بأنه المحرر الذي يتلقاه موظف عام له حق التوثيق في المكان الذي كتب فيه المحرر، وفقاً للشكليات المطلوبة.

كما عرف المشرع الجزائري العقد الرسمي في المادة 324 من القانون المدني[3]التي تنص: "عقد يثبت فيه موظف أو ضابط عمومي أو شخص مكلف بخدمة عامة، ما تم لديه أو ما تلقاه من ذوي الشأن، وذلك طبقا للأشكال القانونية وفي حدود سلطته واختصاصه".

---

[1]- أحمد عزمي الحروب، السندات الرسمية الإلكترونية، دراسة مقارنة، ط1، دار الثقافة، عمان- الأردن، 2010، ص. 76.

[2]- Art 1317 Al 1 c.civ.fr modifier par loi n°2000-230 du 13 mars 2000 – art .1 JORF 14 mars 2000 dispose que: « L'acte authentique est celui qui a été reçu par officiers ayant le droit d'instruments dans le lieu ou l'acte a été rédigé , et avec les solennités requises ».

[3]- الأمر رقم 75-58 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر س1975 المتضمن القانون المدني الجزائري، المعدل والمتمم، ج.ر، ع.78، السنة الثانية عشرة، صادرة بتاريخ 24 رمضان عام 1395هـ- الموافق 30 سبتمبر س.1975.

ولئن كان هذا تعريف المستند الرسمي الورقي، فإن جانبا من الفقه[1] يعرف المستند الإلكتروني الرسمي بأنه:" كتابة إلكترونية مثبتة لواقعة هي تصرف قانوني تترتب عليها آثار معينة، بشرط أن يكون قد تدخل في تحريرها موظف عام مختص".

كما يعرفه جانب آخر[2] بأنه:" المستند الذي ينظمه أصحابه بطريقة إلكترونية ويصادق عليه الموظف العام، أو موظف التصديقات الذي من اختصاصه المصادقة عليه بطريقة إلكترونية طبقا للقانون".

بهذا يلاحظ أن المستند الإلكتروني الرسمي هو ذلك الذي يتولى تحريره شخص مختص ومكلف بهذه الوظيفة كالموثق في الجزائر ومصر، أو شخص مكلف بخدمة عامة ككاتب العدل في فرنسا ولبنان، وذلك وفقا للأوضاع التي تقررها القوانين المختلفة[3].

هذا ويرى البعض من الفقه أن المستند الإلكتروني حتى يكون رسميا لا بد أن يتضمن بيانات أو كتابة إلكترونية، وأن تكون هذه الأخيرة مذيلة بتوقيع إلكتروني من مصدرها، وأن يصدّق على هذا التوقيع جهة ثالثة مختصة به، مهمتها التأكد من هوية صاحب التوقيع، وللإشارة فإنه يمكن أن تكون الجهة الثالثة شخصاً معنوياً أو طبيعياً يملك رخصة محلية حكومية مسبقة بالتصديق على الإمضاءات الإلكترونية، كما قد تخضع جهة التصديق لرقابة لاحقة من ناحية مدى توفيرها الأمان اللازم للمعاملات الإلكترونية وعلى مدى حياديتها واستقلالها، ومدى توافر الشروط والضوابط الفنية والتقنية في إعمالها[4].

من خلال التعريفات السابقة للمستند الإلكتروني الرسمي يتضح جليا أن هذا الأخير يتطلب مجموعة من الشروط حتى يتخذ الصفة الرسمية وتتمثل هذه الشروط في:

---

[1]- خالد مصطفى فهمي، النظام القانوني للتوقيع الإلكتروني في ضوء التشريعات العربية والاتفاقيات الدولية، دار الجامعة الجديدة، الإسكندرية، 2007، ص. 70؛ أحمد عزمي الحروب، المرجع السابق، ص. 76.

[2]- أحمد عزمي الحروب، المرجع السابق، ص. 77.

[3]- باسم رمزي معروف دياب، جريمة تزوير المحرر الرسمي، الأمن والحياة، إعلامية-أمنية- ثقافية، جامعة نايف العربية للعلوم الأمنية، ع (340)، س التاسعة والعشرون، رمضان 1431هـ، أغسطس/سبتمبر 2010، ص.54.

[4]- أحمد سفر، أنظمة الدفع الإلكترونية، ط1، منشورات الحلبي الحقوقية، لبنان، 2008، ص. 15.

1- أن يكون هذا المستند صادر من موظف عام، أو من شخص مكلف بخدمة عامة[1].

2- أن يصدر هذا المستند في حدود اختصاص الموظف العام، وفي حدود صلاحياته الوظيفية.

3- ضرورة مراعاة الأوضاع القانونية المقررة في تدوين المستند الإلكتروني.

فبالنسبة للشرط الأول، يمكن القول أن المستند الإلكتروني حتى يتخذ صفة الرسمية لا بد أن يصدر عن موظف عام مختص، والموظف العام هو كل شخص تعينه الدولة للقيام بعمل من أعمالها سواء كان ذلك بمقابل أو بدون مقابل، هذا ويختلف الموظفون باختلاف نوع المستندات والمحررات التي يختصون بكتابتها، فالقاضي مثلا يعتبر موظفا عاما بالنسبة للأحكام التي يقوم بتحريرها، وكاتب الجلسة يعتبر موظفا عاما بالنسبة لمحاضر الجلسات التي يقوم بكتابتها، وضابط الحالة المدنية يعتبر موظفا عام بالنسبة لعقود الزواج وشهادات الميلاد التي يقوم بتحريرها، والموثق يعتبر موظفا عاما بالنسبة للأوراق الرسمية المدنية التي يقوم بتحريرها[2].

وللإشارة فإنه في مجال البيئة الرقمية قد اختلفت التشريعات الخاصة بالمعاملات الإلكترونية في تسمية هذا الموظف، فمنها من أطلق عليه اسم الموثق، ومنها من أطلق عليه اسم مزود الخدمة ومنها من أسمته بالمعول، ومنها من أطلقت عليه اسم كاتب العدل باعتباره الموظف العام المكلف بالمصادقة على المعاملات التي تتم بين الأطراف، كما هو الحال بالنسبة للتشريع الفرنسي.

هذا وقد عرف جانب من الفقه هذا الموظف بأنه: "كل شخص طبيعي أو معنوي يحدث ويسلم ويتصرف في شهادات المصادقة، ويسدي خدمات أخرى ذات علاقة بالتوقيع الإلكتروني، بحيث يعتبر تدوين المستند بمعرفته بمثابة إدخال للصفة الرسمية لأنه قد حرر بمعرفته[3]".

---

[1] - Cf.J.M. oliver, l'authenticité en droit positif français , PA, 28 juin1993, p.12.

[2]- الأنصاري حسن النيداني، القاضي والوسائل الإلكترونية الحديثة، دار الجامعة الجديدة، الإسكندرية، 2009، ص. 183.

[3]- أحمد عزمي الحروب، المرجع السابق، ص، ص. 78- 79.

مما سبق ذكره، يتضح أنه إذا انتفت صفة الرسمية بالنسبة للقائم بالعمل، فلا يعتبر ذلك المستند رسميا.

هذا عن الشرط الأول، أما بالنسبة للشرط الثاني، والذي ينبغي توفره في المستند الإلكتروني حتى يكتسي الصفة الرسمية فيتمثل في ضرورة أو وجوب صدور هذا المستند في حدود اختصاص هذا الموظف، وفي حدود كل صلاحياته الوظيفية، إذ لا يكفي صدور المستند الإلكتروني من موظف، بل يشترط أن يكون هذا الموظف قد قام بتحرير هذا المستند في حدود سلطته واختصاصه، ويقصد بالسلطة والاختصاص في هذا السياق أن يكون للموظف الولاية في تحرير المستند من حيث الموضوع والزمان والمكان[1].

فمن حيث الاختصاص الموضوعي، يختص كل موظف عام بتحرير نوع معين من المستندات الرسمية، فالقاضي مثلاً يختص بتحرير الأحكام ولكنه ليس مختصا بتحرير محاضر الجلسة، لأن هذا من اختصاص كاتب الضبط أو كاتب الجلسة... وهكذا، أما من حيث الاختصاص الزماني فإنه من المتعارف عليه أن الموظف تنقضي ولايته بالعزل أو النقل أو الوقف عن العمل، ومن ثم فإنه إذا قام بتحرير مستند بعد انقضاء ولايته عدّ ذلك المستند باطلاً، وذلك لصدوره من غير ذي مختص، أما من حيث الاختصاص المكاني فإن القانون حدد لكل موظف اختصاصاً إقليميا، ولا يجوز له أن يباشر عمله خارج دائرة اختصاصه، وعليه فإنه حتى يكون المستند الإلكتروني رسميا وصحيحا، فلابد أن يكون صادرا عن موظف مختص من حيث الموضوع، ومن حيث الزمان، وكذا من حيث المكان.[2]

ولئن كان هذا هو مضمون الشرط الثاني، فإنه بالنسبة للشرط الثالث الواجب توافره في المستند الإلكتروني حتى يتخذ الصفة الرسمية فيتمثل في ضرورة مراعاة الأوضاع القانونية المقررة في تدوين هذا المستند، ذلك أن الموظف يجب عليه أن يراعي في تدوين المستند الإلكتروني بعض الأوضاع القانونية وبعض الإجراءات التي فرضها القانون، والتي

[1]- خالد مصطفى فهمي، المرجع السابق، ص. 72.
[2]- الأنصاري حسن النيداني، القاضي والوسائل الإلكترونية الحديثة، المرجع السابق، ص. 184.

من بينها أن يتحقق من موافقة الأطراف على مضمون المستند الإلكتروني[1]، وأن يتحقق من أن المستند الإلكتروني مكتوب بشكل واضح ومقروء، بما يكفل له الثبات والاستمرارية، وأن يتأكد من أن المستند محفوظ بالشكل القانوني المطلوب، وأنه موقع عليه من قبل الأطراف بالتوقيع الإلكتروني، وبأنه مؤمن ومحفوظ بطريقة تمكن من كشف أي تعديل أو تغيير فيه[2].

وللإشارة فإن هذه الأوضاع المقررة في تدوين المستند منها ما هو جوهري كالتأكد من شخصية أصحاب الشأن وأهليتهم القانونية، والتوقيع الإلكتروني على المستند، وذكر تاريخ التوثيق واسم الموظف، وأسماء أصحاب الشأن والشهود وتوقيعاتهم...الخ، ومنها ما هو غير جوهري كدفع الرسوم الواجبة أو ترقيم صفحات المستند الإلكتروني[3].

وفي هذا يرى بعض الفقه – وبحق- أن اختلال الأوضاع القانونية لا يؤدي إلى بطلان المستند الإلكتروني، ولا ينفي صفة الرسمية عنه، إلا إذا كان الإخلال متعلقا بأوضاع جوهرية كعدم ذكر البيانات العامة في المستند، أو عدم ذكر تاريخ التوثيق أو اسم الموثق أو عدم توقيع أصحاب الشأن، أما الإخلال بأوضاع غير جوهرية مثل عدم استيفاء الرسم المستحق لتحرير المستند الإلكتروني الرسمي أو عدم ترقيم صفحاته، فإنه لا يؤدي إلى بطلان المستند الإلكتروني ولا ينفي صفة الرسمية عنه[4].

هذا ويرى جانب من الفقه أن شروط صحة المستند الإلكتروني الرسمي مسألة قانونية، يخضع فيها القاضي لرقابة أعلى جهة قضائية، وعليه لا يجوز له الانتقاص من هذه الشروط أو الإضافة إليها، كما لا يجوز له الاعتداد بمستند إلكتروني واعتباره مستندا رسميا رغم عدم توافر شروطه، ومن ثم يبدو أن دور القاضي بالنسبة لشروط صحة المستند الإلكتروني يقتصر على التحقق من توافر هذه الشروط من عدمه[5].

---

[1]- للإشارة فإن الموظف يتأكد ويتحقق من أهلية المتعاقدين وشخصيتهم من خلال شهادة المصادقة الإلكترونية أو شهادة التصديق الإلكتروني التي تكون بحوزة كل واحد منهم، هذه الشهادة يكون المتعاقدين قد حصلوا عليها مسبقا من الوكالة العامة للتصديقات الإلكترونية، أو من مزود الخدمة الذي يمنح شهادات المصادقة الإلكترونية للأطراف، وهذه الشهادة تكون بمثابة هوية للتعرف على شخصية وأهلية المتعاقد.مأخوذة من، أحمد عزمي الحروب، المرجع السابق، ص، ص.80- 81.

[2]- أحمد عزمي الحروب، المرجع السابق، ص. 81.

[3]- الأنصاري حسن النيداني، القاضي والوسائل الإلكترونية الحديثة، المرجع السابق، ص،ص. 192- 193.

[4]- خالد مصطفى فهمي، المرجع السابق، ص، ص. 73- 74.

[5]- الأنصاري حسن النيداني، القاضي والوسائل الإلكترونية الحديثة، المرجع السابق، ص،ص. 193- 194.

وعليه فإن المستند الإلكتروني الرسمي يفقد رسميته إذا صدر من غير موظف أو من موظف عام غير مختص، أو من موظف عام مختص إلا أنه لم يراعي الأوضاع القانونية في تدوينه.

الفرع الثاني: المستند الإلكتروني العرفي.

يعرف جانب من الفقه[1]المستند العرفي الورقي بأنه: "مستند غير رسمي يصدر من الأفراد دون أن يتدخل في تحريره موظف عام، أو شخص مكلف بخدمة عامة"، كما يعرفه جانب آخر[2] بأنه:"مستند مكتوب يشتمل على توقيع من صدر عنه أو على خاتمه أو بصمة إصبعه، دون أن تتوافر فيه شروط المستند الرسمي"، هذا ويعرفه جانب آخر من الفقه[3] بأنه: "أوراق لا تتوافر لها المقومات الرسمية، كما أنها لا تصدر عن موظف عام أو شخص مكلف بخدمة عامة، ذلك أنها تتضمن كتابة يوقعها شخص، قاصدا إعداد دليل على واقعة معينة".

هذا من الناحية الفقهية، أما من الناحية التشريعية فيلاحظ أن المشرع الفرنسي لم يعرّف المستند العرفي أو المحرر العرفي كما سماه بل ترك مسألة تعريفه للفقه، وقد حذا المشرع الجزائري حذو المشرع الفرنسي، ولم يتطرق إلى تعريف المحرر العرفي على خلاف المحرر الرسمي الذي تطرق إليه في المادة 324 من القانون المدني والتي سبق بيانها.

عليه فإنه وبمفهوم المخالفة يعرف المستند العرفي حسب التشريع الجزائري بأنه: "كل ما يُحرر من غير الأشخاص المذكورين في نص المادة 324 من القانون المدني، بمعنى يحرر من غير موظف أو ضابط عمومي، أو شخص مكلف بخدمة عامة"، وأبعد من ذلك يلاحظ أن التشريع الجزائري قد اعتبر أن المستند يكون عرفيا ولو حُرِّر من طرف الأشخاص المحددين بالمادة السالفة الذكر أو من طرفهم، متى كان ذلك خارج نطاق

[1]- أحمد سفر، المرجع السابق، ص. 18؛خالد مصطفى فهمي، المرجع السابق، ص. 79.
[2] - عامر محمود الكسواني، التجارة عبر الحاسوب، ماهيتها، إثباتها، وسائل حمايتها والقانون الواجب التطبيق عليها في كل من الأردن ومصر وإمارة دبي، دراسة مقارنة، ط1، دار الثقافة، الأردن، 2009، ص. 136.
[3]- خالد مصطفى فهمي، المرجع السابق، ص. 79.

اختصاصهم، وهذا ما أكدت عليه المادة 326 مكرر من القانون المدني والتي نصت على أنه: " يعتبر العقد غير رسمي بسبب عدم كفاءة أو أهلية الضابط العمومي ،أو انعدام الشكل كمحرر عرفي إذا كان موقعا من قبل الأطراف"[1].

هذا بشأن المستند العرفي الورقي، أما بشأن المستند الإلكتروني العرفي فيعرف على أنه: "كل كتابة إلكترونية متفق عليها ومحررة بين طرفين أو أكثر بوسيلة إلكترونية، وموقع عليها بين أطرافها، ودون أن يتوافر فيها مقومات وشروط الكتابة الرسمية الإلكترونية"، كما يمكن تعريفه بأنه: " كتابة إلكترونية مثبتة لواقعة هي تصرف قانوني تترتب عليها آثار معينة بشرط أن تكون موقعة بالتوقيع الإلكتروني، وألا يكون قد تدخل في تحريرها موظف عام مختص".

بهذا يبدو أن المستند الإلكتروني العرفي هو كل مستند غير مصادق عليه من طرف الجهة التي تملك المصادقة على التوقيعات الإلكترونية كما وضحنا سابقا، كما ويعتبر مستندا إلكترونيا عرفيا، كل مستند تدخل في تحريره موظف عام مختص، ولكن بشرط أن يتم ذلك خارج مهامه واختصاصاته الوظيفية، أو أن يقوم بتحريره خارج الأوضاع المقررة قانونا.

من خلال تعريف المستند الإلكتروني العرفي يتضح جلياً أن هذا الأخير يتمتع بخصائص تجعله يتميز عن المستند الإلكتروني الرسمي، كما أنه يتطلب كذلك توافر مجموعة من الشروط حتى يقوم بأداء وظيفته على الوجه الصحيح.

فمن بين الخصائص المميزة للمستند الإلكتروني العرفي خاصية انعدام الرسمية، حيث أن هذه الخاصية تعتبر أهم ما يميز هذا النوع من المستندات، ومفاد هذه الخاصية أنه على خلاف المستند الرسمي الإلكتروني الذي يشترط الرسمية لإنشائه، فإن الأمر ليس كذلك بالنسبة للمستند الإلكتروني العرفي الذي لا يتطلب الشكل الرسمي، بمعنى أن الأفراد العاديين

[1]- الأمر رقم 75-58 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر س1975 المتضمن القانون المدني الجزائري المعدل والمتمم، سابق الإشارة إليه.

هم الذين يتولون تحرير وصياغة وإعداد المستند العرفي، ولا دخل لأي موظف رسمي في ذلك.

بسبب هذه الخاصية لا يتوفر في هذا النوع من المستندات الضمانات الكافية، ولا تكون له ذات القوة الثبوتية التي تتميز بها المستندات الإلكترونية الرسمية[1]، ولكن بالرغم من هذا إلا أن الأفراد كثيرا ما يلجؤون في معاملاتهم إلى تحرير مستندات عرفية للمحافظة على حقوقهم، ولعل ما يدفعهم لذلك هو ما تتميز به هذه المستندات من سرعة التحرير، وسهولة الإعداد وما توفره من نقص في التكاليف.

إن من بين الخصائص المميزة للمستند الإلكتروني العرفي كذلك خاصية عدم اشتراطه لإجراءات وشكليات معينة إلا استثناءاً، ومفاد هذه الخاصية أنه طبقا لمبدأ التراضي فإنه لا يشترط لصحة المستند الإلكتروني العرفي افتراض مراعاة أوضاع وإجراءات وشكليات معينة ومحددة، بمعنى أن صحة مضمونه وما ورد فيه يتوقف على تراضي الأطراف، ودون التقيد بأي شكلية وهذا كقاعدة عامة، أما الاستثناء الوارد على هذه القاعدة فيتمثل في أنه في بعض الحالات قد يتطلب لصحة المستند الإلكتروني العرفي ضرورة مراعاة بعض الأوضاع وبعض البيانات الشكلية، وذلك كما هو الحال بالنسبة للأوراق التجارية الإلكترونية، هذه الأخيرة التي تعتبر إحدى صور المستند الإلكتروني والتي يشترط لقيامها صحيحة وجوب ذكر تاريخ، ومكان تحرير هذه الأوراق بالإضافة إلى بعض البيانات الإلزامية الأخرى[2].

هذا عن خصائص المستند العرفي الإلكتروني، أما عن الشروط الواجب توافرها في هذا النوع من المستندات، فيمكن القول من خلال تعريفه أن هذا الأخير يستلزم ضرورة توافر شرطين أساسيين وهما: شرط الكتابة، وشرط التوقيع.

فأما بخصوص شرط الكتابة، فينبغي أن يكون المستند الإلكتروني العرفي مكتوبا، ويُشترط في هذه الكتابة أن تكون دالة على الغرض الذي أعدت من أجله، أي أن تكون واردة

[1]- أحمد سفر، المرجع السابق، ص. 15.
[2]- يراجع في ذلك، ص 57 وما يليها من هذه الأطروحة.

على الواقعة التي عد المستند دليلا عليها، وبما أن هذا المستند يتمتع بالخاصية الإلكترونية فالكتابة المقصودة هنا هي الكتابة الإلكترونية التي تكون على دعائم إلكترونية.

وللإشارة اعترف المشرع الجزائري بهذا النوع من الكتابة بموجب القانـــون رقم 05-10 المعدل والمتمم للقانون المدني، بحيث نصت المادة 323 مكرر منه على أنه: " ينتج الإثبات بالكتابة من تسلسل الحروف أو أوصاف أو أرقام أو أية علامات أو رموز ذات معنى مفهوم، مهما كانت الوسيلة التي تتضمنها، وكذا طرق إرسالها"[1].

هذا ويضيف الفقه شرطا آخر في الكتابة حتي يكون للمستند الإلكتروني العرفي القيمة والحجية ويقوم بأداء وظيفته على الوجه الصحيح، ويتمثل هذا الشرط في إمكانية قراءة هذه الكتابة بمعنى أن تكون هذه الكتابة مقروءة، خاصة وأن شرط القراءة هو شرط بديهي لإمكانية الاعتداد بأي مستند ومنحه الحجية القانونية، ومن ثم يرى الفقه أنه إذا كانت الكتابة عبارة عن رموز تعبر عن واقعة قانونية، فإن قراءتها تسمح بالتعبير عن وجودها الفعلي، خاصة وأنه يتم قراءة المستندات الإلكترونية العرفية من خلال الحاسب الآلي، والذي يتدخل مباشرة لتحويل لغة الآلة والرموز المستخدمة إلى لغة مقروءة وفقا لقواعد التباديل والتوافق[2]، ومن ثم يشترط في الكتابة الإلكترونية أن تكون مقروءة ومفهومة، لاسيما وأنها موجودة على دعامة إلكترونية وفي وسط افتراضي.

زيادة على ذلك يشترط الفقه في الكتابة الإلكترونية التي يتضمنها المستند الإلكتروني العرفي شرط الاستمرار، بمعنى ضرورة أن تدون هذه الكتابة على وسائط ودعامات تسمح بثبوت هذه الكتابة واستمرارها، وذلك نظرا لما تتمتع به الوسائط الإلكترونية من حساسية بالغة مما يجعلها عرضة للتلف السريع، ناهيك عن التكوين المادي المتميز للكتابة الإلكترونية والذي يتمتع بقدر عال من الحساسية مما يجعلها عرضة للمخاطر منذ تدوينها وتسجيلها في نظام معلوماتي، وقد تصل الخطورة إلى غاية المعلومات عند نقلها من دعامة لأخرى بالإضافة إلى إمكانية تبديلها وتحريفها[3].

---

[1]- قانون رقم 05-10 المؤرخ في 20 يونيو 2005 المعدل والمتمم للقانون المدني الجزائري، سابق الإشارة إليه.
[2]- خالد مصطفى فهمي، المرجع السابق، ص.82.
[3]- المرجع نفسه، ص. 84.

ومن ثم وجب تدوين الكتابة على نحو يجعلها محمية من كل التلاعبات، وعلى نحو يجعلها ثابتة ومستمرة الوجود، وبطريقة تُمكن من الرجوع إليها كلما اقتضت الحاجة والضرورة.

هذا عن الكتابة الإلكترونية، أما عن التوقيع الإلكتروني والذي يعتبر الشرط الثاني الواجب توافره في المستند الإلكتروني العرفي، فينبغي الذكر أنه شرط أساسي وجوهري لوجود هذا النوع من المستندات، ذلك أنه يدل على هوية موقعه وصدوره منه ما لم يطعن فيه بالإنكار، ذلك أن التوقيع يتميز بالطابع الشخصي، ولا يمكن إعطاء أي قيمة للمحرر إلا إذا كان صادرا ممن ينسب إليه.

بهذا يعتبر التوقيع على المستند إحدى الوسائل التي يعبر فيها الشخص عن نفسه وذاتيته، وهو بهذا المفهوم لا يشترط فيه سوى أن يكون دالاً دلالة نافية للجهالة على صاحبه، كما يعد أيضا الأساس الأول الذي يعتمد عليه لنسبة مستند معين لمصدره، فتوقيع الشخص على المستند يعني بالتأكيد نسبة هذا المستند لذلك الشخص، والتزامه بما جاء فيه[1].

وبما أن الخاصية الإلكترونية هي أهم ما يميز المستند الإلكتروني، فالمقصود بالتوقيع هنا ليس التوقيع اليدوي التقليدي، بل التوقيع الإلكتروني الرقمي، هذا الأخير الذي اعترف به المشرع الجزائري بموجب القانون رقم 05-10 من القانون المدني حيث نصت المادة 327 الفقرة 02 منه على أنه:" ويعتد بالتوقيع الإلكتروني وفقا للشروط المذكورة في المادة 323 مكرر أعلاه"[2].

وبالرجوع إلى أحكام المادة 323 مكرر يتبين أن هذه الشروط تتمثل في إمكانية تحديد الشخص الذي أصدر المستند، وحفظ التوقيع الإلكتروني بصفة تضمن سلامته، وعليه فإن وجود التوقيع يعتبر شرطا جوهريا ولازما لصحة المحرر الإلكتروني العرفي.

[1]- عامر محمود الكسواني، المرجع السابق، ص. 139.
[2]- قانون 05- 10 المؤرخ في 20 يونيو2005 المعدل والمتمم للقانون المدني الجزائري، سابق الإشارة إليه.

مما سبق ذكره، فإن المستند الإلكتروني العرفي لا يكون صحيحا، ولا يؤدي دوره على الوجه التام، إلا إذا كان مكتوبا بطريقة تمكن من قراءته وحفظه واستمرار دوامه، ناهيك عن وجود توقيع الأطراف عليه.

المطلب الثالث: صور المستند الإلكتروني.

لقد ترتب على التطور التكنولوجي الذي شهدته كافة مجالات الحياة الاقتصادية، الاجتماعية، الإدارية والسياسية تغير جذري في سير حياة المجتمعات، إذ أصبحت هذه الأخيرة تشهد نمطاً جديدا ومميزا من المعاملات يختلف عن ذلك النمط الذي شهدته البشرية في القرون السابقة، إذ أضحت الحياة الجديدة تقوم على استغلال الحاسبات الآلية وشبكات الإنترنت في إبرام التصرفات وقضاء الحاجات[1]، وهو ما أدى إلى ظهور مصطلحات لم تكن معهودة من قبل، ومن بين هذه المصطلحات مصطلح التجارة الإلكترونية[2]، الإدارة الإلكترونية، والحكومة الإلكترونية.

لقد أدى التطور السابق الذكر إلى الانتقال من تقديم الخدمات العامة والمعاملات من شكلها الروتيني إلى الشكل الإلكتروني عبر الإنترنت، حتى ظهرت صور جديدة للمستند الإلكتروني، هذه الصور تتعدد بتعدد المجالات وبتعدد التصرفات القانونية المختلفة.

إذ ظهر في مجال المعاملات المدنية ما يسمى بالمستند الإلكتروني ذو الطابع المدني، فكان وسيلة مهمة لإبرام المعاملات والتصرفات القانونية المدنية، كما ظهر في مجال المعاملات الإدارية ما يسمى بالمستند الإلكتروني ذو الطابع الإداري، وقد اعتبر هذا الأخير إحدى سمات الإدارة الإلكترونية والحكومة الإلكترونية بوجه عام، كما وبرز في مجال البيئة التجارية ما يعرف بالمستند الإلكتروني ذو الطابع التجاري، وكان هذا الأخير إحدى أهم السمات المميزة للتجارة الإلكترونية، وأداة لتنفيذ معاملاتها.

[1]- محمد فواز المطالقة، النظام القانوني لعقود إعداد برامج الحاسب الآلي، دار الثقافة، عمان- الأردن، 2004، ص. 36.
[2]- حوالف عبد الصمد، نظام الدفع الإلكتروني، الحجة، مجلة دورية تصدر عن منظمة المحامين لناحية تلمسان، الإتحاد الوطني لمنظمات المحامين الجزائريين، ع2، أكتوبر 2011، ص.139.

نظرا لأن هذه المستندات أهم ما ولدته البيئة الرقمية الجديدة، فماذا يقصد بكل منها؟، وما هي الأحكام المنظمة لها؟

هذا ما سيتم تحديده بالتطرق للمستند الإلكتروني ذو الطبيعة المدنية والإدارية **(الفرع الأول)**، والمستند الإلكتروني ذو الطبيعة التجارية **(الفرع الثاني)**.

الفرع الأول: المستند الإلكترونية ذو الطبيعة المدنية والإدارية.

تعتبر المستندات الإلكترونية ذات الطبيعة المدنية والإدارية إحدى الأدوات الحديثة التي أصبحت تتم بموجبها التصرفات والمعاملات سواء بين الأفراد، أو بينهم وبين الإدارات أو الجهات الحكومية.

لقد ظهرت هذه النقلة النوعية نتيجة لتطور التقنيات المستخدمة في الحاسب الآلي، وظهور شبكة المعلومات العالمية، فقد أدى التطور غير مسبوق في مجال التكنولوجيا إلى إنشاء شبكة افتراضية تحاكي الواقع في أغلب مظاهره، شبكة أقل ما يمكن القول عنها أنها صالحة لاستيعاب معظم الأنشطة الممارسة عن بعد.

لقد كان للتطور السابق ذكره، دور فعال في ميلاد صور جديدة للمستندات الإلكترونية، حيث أصبح الأفراد يتجهون إلى إبرام تصرفاتهم وتنظيم معاملاتهم وإثبات حقوقهم وإبرام عقودهم المختلفة عن طريق مستندات إلكترونية آلية، كما وأصبحت المستندات وسيلة لإثبات الحق، ومرجعا لبيان ما لكل طرف من حق وما عليه من إلتزام، حتى أضحى بإمكان المدين الوفاء بالتزاماته العقدية وغير عقدية بطريقة إلكترونية جد حديثة، وعن طريق مستندات ذات طابع مدني، من خلال استخدام حوالة الوفاء الإلكترونية باعتبارها وسيلة حديثة للوفاء بالديون الناتجة عن المعاملة المدنية.

هذا بالنسبة للمستند الإلكتروني ذو الطابع المدني، أما بالنسبة للمستند الإلكتروني ذو الطابع الإداري، والذي يعتبر وليد التقنية الرقمية وسمة من سمات الإدارة الإلكترونية والحكومة الإلكترونية التي تهدف إلى تسهيل المعاملات بين الدولة ومواطنيها، وتقريب

الإدارة من المواطن إلى أقصى حد ممكن، حتى يتمكن هذا الأخير من ممارسة أنشطته الإدارية بسهولة ويسر.

للإشارة فإنه إلى جانب المستند الإلكتروني ذو الطبيعة المدنية، والمستند ذو الطبيعة الإدارية، هناك مستندا إلكترونيا ذو طبيعة مزدوجة حيث يكتسي أحيانا الطبيعة المدنية المحضة، وأحيانا أخرى الطبيعة الإدارية.

لأهمية هذه المسألة سيتم بيان المستندات الإلكترونية ذات الطبيعة المدنية المحضة، وفيها سيتم التركيز على حوالة الوفاء الإلكترونية باعتبارها طريقة جديدة للوفاء بالالتزامات ذات الطابع المدني **(البند الأول)**، كما سيتم بعدها التطرق إلى المستندات الإلكترونية الإدارية، والمستندات ذات الطبيعة المزدوجة **(البند الثاني)**.

البند الأول: المستند الإلكتروني ذو الطبيعة المدنية.

يعتبر الوفاء بالالتزامات العقدية وغير العقدية أحد المسائل الهامة التي تميز المعاملات المدنية بين الأفراد، ولأهميته فإنه يعد واحدا من مفاهيم نظرية الالتزام، وعلى وجه الخصوص أحكام الالتزام أو آثار الحق الشخصي، كما يعد من أهم طرق تنفيذ الالتزام، وفي الوقت ذاته سببا من أسباب انقضائه[1]، لذلك تختلف القواعد التي تنظمه تبعا لنوع الالتزام الموفى به.

تبرز أهمية الوفاء في جوانب قانونية مختلفة فهو يرتبط بمسائل الإثبات، وبالقواعد الخاصة المنظمة للعقود المسماة، كما أنه يرتبط بالقوانين المالية التي تحكم شؤون الرسوم والضرائب[2].

[1]- لقد عالج المشرع الجزائري أحكام الوفاء في الباب الخامس من التقنين المدني الجزائري، تحت عنوان "انقضاء الالتزام" واعتبر الوفاء أحد أسباب انقضاء الالتزام، كما نظم أحكامه في الفصل الأول من الباب الخامس، في المادة 258 وما يليها، بحيث نصت المادة 258 ق.م. ج على أنه: "يصح الوفاء من المدين أو من نائبه أو من أي شخص له مصلحة في الوفاء، وذلك مع مراعاة ما جاء في المادة 170 من نفس القانون".

[2]- عدنان إبراهيم سرحان، الوفاء الإلكتروني، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، دبي، 2003، ص. 267.

للإشارة فقد شهدت وسائل الوفاء تطورا ملحوظا مع ظهور التقنية الرقمية ووسائل الاتصال الحديثة، بحيث تم الانتقال من الوفاء التقليدي اليدوي إلى ما يسمى بالوفاء الإلكتروني، الذي مكن المدين من الوفاء بالتزاماته بواسطة الوسائل الإلكترونية كحوالة الوفاء الإلكترونية، والتي تعد مستندات إلكترونية غرضها الوفاء، وفيها يتم إستخدام التقنية الالكترونية للوفاء بالإلتزامات، وقد يتم توجيه أمر من المدين إلى بنكه أو مؤسسته المالية، للوفاء بالتزام في ذمته بوسيلة إلكترونية إلى دائنه، وهو ما يُعرف بالتحويل الدائن، كما ويمكن أن يتم الوفاء عن طريق توجيه أمر من المدين إلى بنكه لتحصيل مبلغ من حساب دائنه بناء على تفويض مسبق بواسطة إلكترونية، وهو ما يُعرف بالتحويل المدين.

إذ وبالنسبة للطريقة الأولى أي التحويل الدائن ففيها يقوم الدائن باتخاذ الإجراءات المصرفية اللازمة لتحويل مبلغ معين إلى المستفيد، سواء تم ذلك في نفس البنك أو في بنك آخر، وسواء تم دفع المبلغ مقدما إلى البنك المحول أو تم تفويضه بقيد المبلغ على حسابه لدى البنك، كما يمكن للدائن أن يوجه تعليمات بذلك إلى بنكه من خلال رسالة إلكترونية، وعند وصولها يقوم البنك بالتأكد من صحتها، ومن باقي شروط التحويل، مثل كفاية الرصيد ليقوم بعدها بتنفيذ العملية.

أما الصورة الثانية والتي يطلق عليها التحويل المدين، فإنها تتم بتفويض بنك المستفيد في تحصيل قيمة التحويل من الدائن أو بنكه، وفي هذا التحويل يقوم المستفيد بإصدار تعليمات إلى بنكه بتحصيل مبلغ محدد من النقود من الدائن أو من بنكه أو مؤسسته المالية، وللإشارة فإنه في هذه الصورة يجب أن يرفق المستفيد مع طلب التحويل تفويضا من المحول (المدين) يفوضه فيه بتحويل المبلغ إلى حساب المستفيد، وبقية القيمة على حسابه، وللتنبيه فإن أمر التحويل هذا يعد هو الآخر مستندا إلكترونيا[1].

[1]- أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني –دراسة مقارنة–، المرجع السابق، ص. 524.

البند الثاني: المستند الإلكتروني ذو الطبيعة المزدوجة.

إن التطورات المالية في مجال تكنولوجيا المعلومات قد جعلت من المستند الإلكتروني أداة فعالة في مجال المعاملات المدنية والإدارية، وعليه سيتم التطرق في هذا البند إلى السجلات الطبية الإلكترونية باعتبارها صورة جديدة للمستند الإلكتروني ذو الطابع الإداري **(أولا)**، ثم بعد ذلك سوف يتم التطرق إلى العقد الإلكتروني كصورة للمستند الإلكتروني ذو الطابع المزدوج، إذ قد يأخذ العقد الإلكتروني الصبغة المدنية، كما قد يأخذ الصبغة الإدارية **(ثانيا)**.

أولاً: السجلات الطبية الإلكترونية.

تعد السجلات الطبية أو ما يطلق عليها تسمية ملف المريض أو الملف الطبي أحد النقاط المحورية التي تعتمد عليها عملية تقديم الرعاية الصحية داخل المستشفيات، وبين مختلف أنواع المؤسسات الطبية، هذا ويعرف الملف الطبي على أنه مجموع الوثائق، التقارير، صور الراديو التي يؤشر عليها الطبيب أو المشرف على العلاج، سواء أكان هذا الطبيب اختصاصي أم عام ويُدَوِن فيها ملاحظاته بخصوص نتائج التحاليل، ومختلف التطورات التي طرأت على المريض خلال فترة العلاج، وكذا مجمل الاستشارات الطبية المتحصل عليها خلال الفترة السالفة الذكر[1]، وذلك بهدف ضمان جودة الخدمات واستمراريتها من جهة، وسلامة العلاجات المقدمة وتنظيمها من جهة أخرى.

بهذا يبدو أن أهمية السجلات الطبية تنبع من دورها الفعال في حفظ كافة معلومات المريض من بيانات رئيسية وطبية شاملة لكل ما تم إجراؤه من فحوصات وتشخيصات وعلاج وتقارير متابعة وقرارات طبية هامة[2].

[1]- Cf.Angelo Castelletta, Responsabilité médicale, droits des malades, Ed. D. Paris, 2002, p. 32 ; Marc Dupont, Claudine Esper, Christian Paire, Droit hospitalier, 3ème éd., De Paris, 2001, p.301.

[2]- Cf.Cécile Manaouil, Marie Graser, Olivier Jarde, Le dossier médical du patient majeur, droit, déontologie et soin, vol. 3, N°4, décembre 2003, p. 464.

ولقد ظلت ولعقود طويلة من الزمن هذه السجلات الطبية ثابتة في شكل ملف أو مجموعة من الأوراق التي كتبت عليها المعلومات بخط اليد، غير أنه مؤخرا وبفضل التطورات التكنولوجية والعلمية، فقد عمد المتخصصين في مجال الرعاية الصحية وتكنولوجيا المعلومات إلى تصميم واختراع سجلات طبية إلكترونية تعتمد على الكمبيوتر بكل إمكانياته المتطورة من تخزين المعلومات، ونقل البيانات عن طريق ما يعرف اليوم بشبكة المعلومات ووسائل الاتصال الحديثة.

ومن تم فإن السجلات الطبية الإلكترونية -والتي تعتبر في أغلب الأحوال مستندات إلكترونية ذات طابع إداري- لا تختلف كثيرا عن السجلات الورقية التقليدية في وظيفتها والهدف منها، لكنها تختلف كليا في طبيعتها وخواصها وإمكانيات استخدامها وفوائدها، فهي تمثل نقطة مركزية تصب فيها وتنشق عنها قنوات عديدة من المعلومات المرتبطة بتقديم الرعاية الصحية للمريض، كما أنها تمتاز بدقة محتواها وسهولة الوصول إليها من خلال تكاملها مع مصادر المعلومات المختلفة عن طريق نظم شبكات المعلومات، والتي أدى استخدامها بالتبعية إلى تطور فكرة اللامركزية، وتواصل المعلومات بين أكثر من مستشفى ومؤسسة طبية، فضلا عن أنها أضحت وسيلة لعلاج المرضى عبر مختلف أقطـــار العـــالم، وذلك بسبب ما وفرته شبكة الإنترنت الدولية[1] من إمكانية التواصل بين الأطباء والمرضى[2].

[1]- للإضافة فإن المعلومات التي يتضمنها السجل الطبي الإلكتروني لا تستعمل فقط داخل الوطن، وإنما خارج الوطن بحيث يتم تبادل المعلومات الطبية بين الدول، وهناك بعض السجلات يسمح بالاطلاع عليها من خارج الحدود، ففي فرنسا هناك سجلات إلكترونية تعطي معلومات عن الأدوية المستعملة، كما أن هناك أنواع متعددة من بنوك المعلومات ومنها ما يمكن أي طبيب من أخذ المعلومات منه بمجرد أن يجري اتصالا هاتفيا، كما أن هناك بنك معلومات خاص بالأمراض السرطانية، وهناك بنك معلومات أمريكي يمكن استشارته من فرنسا وبإمكانه أن يعطي معلومات من مراجع لا تقل عن 3 آلاف مجلة دورية منشورة في العالم. مأخوذة من، بولين أنطونيوس أيوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، دراسة مقارنة، ط 1، منشورات الحلبي الحقوقية، بيروت- لبنان، 2009، ص. 118.

[2]- مقالة مفصلة تحت عنوان "السجل الطبي الإلكتروني" مأخوذة من الموقع الإلكتروني ويكيبيديا الموسوعة الحرة، العنوان الإلكتروني سجل-طبي-إلكتروني

ar-wikipedia-org/wiki/ . Date de consultation le site 30-01-20114à 11 :00.

ثانياً: العقود الإلكترونية.

لقد أدى استخدام المعلوماتية في كافة مناحي الحياة إلى ظهور العقود الإلكترونية، التي تعد من العقود الحديثة في عصرنا هذا[1]، بل هي إحدى صور المستندات الإلكترونية التي تتميز بخصائص متعددة مقارنة بالعقود التقليدية الأخرى[2].

لاشك أن التنوع الشديد للعقود الإلكترونية كان له تأثير بارز على وجهات نظر الفقه، الذي اختلف في تعريفها، بحيث عرفها جانب من الفقه[3] بأنها: "التفاوض الذي انتهى بالاتفاق التام بين إرادتين صحيحتين باستخدام وسيلة اتصال حديثة، غالبا ما تكون هذه الوسيلة شبكة المعلومات الدولية الإنترنت"، في حين عرفها جانب آخر بأنها: ''إتفاق بين طرفي العقد من خلال تبادل الإيجاب والقبول، عن طريق استخدام شبكة المعلومات خلال مرحلة المفاوضات العقدية أو خلال التوقيع أو في أية مرحلة من مراحل إبرام العقد، وسواء تم ذلك التصرف في حضور طرفي العقد في مجلس العقد أو من خلال التلاقي عبر شاشات الحاسب الآلي، أو أية وسيلة إلكترونية سمعية أو بصرية''[4].

هذا ويرى جانب ثالث من الفقه أن العقد الإلكتروني بصفة عامة، ما هو إلا ذلك: "العقد الذي تتلاقى فيه عروض السلع والخدمات التي يعبر عنها بالوسائط التكنولوجية المتعددة (Multimédias)، خصوصا شبكة المعلومات الدولية (الإنترنت)، من جانب أشخاص متواجدين في دولة أو دول مختلفة بقبول يمكن التعبير عنه من خلال ذات الوسائط لإتمام العقد"[5].

هذا من الناحية الفقهية، أما من الناحية التشريعية فقد حظيت العقود الإلكترونية باهتمام تشريعي خاص، وذلك نظرا لأهميتها العملية من جانب، ولكونها أحد الأساليب الحديثة لممارسة الأنشطة الإدارية والمدنية من جانب آخر، فبالرجوع إلى نصوص القانون

---

[1]- فادي محمد عماد الدين توكل، عقد التجارة الإلكترونية، ط 1، دار الثقافة، الأردن، 2008، ص. 25.
[2]- عصام عبد الفتاح مطر، التجارة الإلكترونية في التشريعات العربية والأجنبية، دار الجامعة الجديدة، الأزاريطة- الإسكندرية، 2009، ص. 148.
[3]- لزهر بن سعيد، المرجع السابق، ص. 42.
[4]- فادي محمد عماد الدين توكل، المرجع السابق، ص. 28.
[5]- رحيمة الصغير ساعد نمديلي، العقد الإداري الإلكتروني، دراسة تحليلية مقارنة، ط1، دار الجامعة الجديدة، الإسكندرية، مصر، 2007،، ص، ص. 44- 45.

النموذجي الصادر عن الأمم المتحدة بشأن التجارة الإلكترونية (UNICITRAL) يلاحظ أنه قد عرف العقد الإلكتروني من خلال تعريفه لرسالة البيانات، وذلك في نص المادة الثانية منه، كما أورد في نفس المادة تعريفا لتبادل البيانات الإلكترونية (L'échange de données informatisées) والتي جاء فيها أنه:" يراد بمصطلح "تبادل البيانات الإلكترونية" نقل المعلومات من حاسوب إلى آخر باستخدام معيار متفق عليه لتكوين المعلومات"[1].

أما بالنسبة للتشريعات العربية، فيلاحظ أن المشرع الأردني عرفه في المادة 2 من قانون المعاملات التي نصت:" العقد الإلكتروني هو الاتفاق الذي يتم انعقاده بوسائط إلكترونية كليا أو جزئيا"[2]، وأضافت نفس المادة إلى ذلك تعريفا خاصا للوسائل الإلكترونية التي يبرم بواسطتها العقد واعتبرتها: "أي تقنية لاستخدام وسائل كهربائية أو مغناطيسية أو ضوئية، أو أية وسائل مشابهة في تبادل المعلومات وتخزينها".

أما بخصوص المشرع الجزائري، فيلاحظ أنه لم يعرف العقد الإلكتروني، بل عرف عقد التجارة الإلكترونية في المادة 6 من قانون 18-05 المتعلق بالتجارة الإلكترونية التي نصت:"العقد بمفهوم القانون رقم 04-02 المؤرخ في05 جمادى الأولى عام 1425 الموافق23 يونيو سنة 2004 الذي يحدد القواعد المطبقة على الممارسات التجارية، ويتم إبرامه عن بعد، دون الحضور الفعلي والمتزامن لأطرافه باللجوء حصريا لتقنية الإتصال الإلكترونية."

إستنادا للمادة سالفة الذكر، يلاحظ أن المشرع الجزائري منح تعريفا قاصرا على مجال التجارة الإلكترونية، في حين أن العقود الإلكترونية متعددة، ولا تقتصر على المجال التجاري، إذ قد تكون عقودا مدنية، كما قد تكون عقودا إدارية.

[1]- المادة 2/2 من قانون الأونيسترال النموذجي بشأن التجارة الإلكترونية لسنة 1996، سابق الإشارة إليه.
[2]- التنظيم القانوني رقم 85 لسنة 2001 المتعلق بالمعاملات الإلكترونية الأردني، سابق الإشارة إليه.

لاشك في أن أغلب التعاريف الواردة في مجال العقد الإلكتروني قد عملت على تحديد مفهوم عقد التجارة الإلكترونية الذي يعرفه جانب من الفقه[1] بأنه: " تقابل لعرض مبيعات أو خدمات يعبر عنها بوسيلة اتصال سمعية مرئية، من خلال شبكة دولية للاتصالات عن بعد، مع قبول والذي يكون قابلا لأن يظهر باستعمال النشاط الحواري بين الإنسان والمعلومة التي تقدمها الآلة".

بهذا يتضح أن عقد التجارة الإلكترونية اتفاق يتم من خلاله تنفيذ بعض أو كل المعاملات التجارية، من خلال تبادل السلع والخدمات بين مشروع تجاري وآخر أو بين تاجر ومستهلك، وذلك باستخدام تكنولوجيا المعلومات والاتصالات.

ولقد شهد هذا النوع من العقود نمواً متصاعداً حيث بات يشكل نسبة كبيرة من حجم التجارة الدولية والداخلية، وذلك بسبب سهولة وسرعة إبرام هذه العقود وتنفيذها، حيث يمكن للشخص الوصول إلى ما يرغب فيه من خلال العروض المتسعة الخيار، وذلك بالضغط على لوحة المفاتيح الموجودة بجهازه الخاص المتصل بالإنترنت دون حاجة إلى الانتقال، هذا بالإضافة إلى سهولة الاتصال والتفاعل الدائم بين طرفي العقد، مما يكفل لهما التفاوض ومناقشة بنود العقد بحرية تامة[2].

الفرع الثاني: المستند الإلكتروني التجاري.

تعتبر المستندات الإلكترونية التجارية وليدة التجارة الإلكترونية، ظهرت بظهورها كوسيلة لإبرام المعاملات التجارية التي أصبحت تتم داخل البيئة الرقمية، هذه التجارة التي اتسع نطاقها شيئا فشيئا وتشعبت أنواعها ومجالاتها، وتعددت التشريعات الدولية المنظمة لها، وذلك نظرا لمزاياها وتماشيها مع مقتضيات العصر، ويظهر ذلك جليا في إلغائها الحدود والقيود أمام دخول الأسواق التجارية، حيث بفضلها تحول العالم إلى سوق مفتوح أمام المستهلك بغض النظر عن الحدود الجغرافية للبائع والمشتري[3].

---

[1]- لزهر بن سعيد، المرجع السابق، ص. 41؛ إيمان مأمون أحمد سليمان، إبرام العقد الإلكتروني وإثباته، الجوانب القانونية لعقد التجارة الإلكتروني، د.ط، دار الجامعة الجديدة، الأزاريطة، الإسكندرية، 2008، ص.56.

[2]- محمد حسين منصور، المسؤولية الإلكترونية، ج1، ط1، منشأة المعارف، الإسكندرية، مصر، 2006، ص. 17.

[3]- محمد فريد الشافعي، المرجع السابق، ص.20.

فمثلا بالنسبة لرجال الأعمال أصبح من الممكن لهم تجنب مشقة السفر للقاء شركائهم وعملائهم، إذ أصبح بمقدورهم الحد من الوقت والمال للترويج لبضائعهم وعرضها في الأسواق، أما بالنسبة للزبائن فليس عليهم التنقل كثيرا للحصول على ما يريدون، أو بذل الوقت أو حتى الاستخدام الفعلي للنقود التقليدية، إذ يكفي اقتناء جهاز حاسوب وبرنامج متصفح الإنترنت واشتراك بالإنترنت[1].

ومن ثم فقد أصبحت صناعة المعلومات وترويج السلع عبر الشبكة العنكبوتية المجال الخصب لجذب الاستثمارات، خصوصا مع تحقيق التزاوج بين المعلوماتية وأدوات الاتصال اللاسلكية، وبما أن المتعارف عليه في البيئة التجارية، أن الأموال هي الوسيلة الرئيسية لتسوية المعاملات المالية، وعادة ما كان يتم دفع هذه الأموال نقداً وبصورة فورية (monnaie liquide)،أو بوسيلة بديلة كالأوراق التجارية التقليدية[2].

غير أنه مع ظهور الثورة الإلكترونية التي تعتمد بشكل رئيسي على الفكر البشري وعلى القدرة على الإبداع والتطوير، والاستجابة إلى المتغيرات الحديثة التي لا تعيقها حدود سياسية أو جغرافية[3]، أصبحت تلك الوسائل المادية لا تصلح لتسهيل التعامل الذي يتم عن بعد في بيئة غير مادية، كالعقود الإلكترونية التي تبرم عبر شبكة الإنترنت حيث تتوارى المعاملات الورقية.

من هنا كانت أهمية ابتكار أسلوب سداد يتفق مع طبيعة التجارة الإلكترونية[4]، بحيث ظهرت المستندات الإلكترونية التجارية كوسيلة لضمان الحقوق وتسوية المعاملات، كما ظهرت الأوراق التجارية الإلكترونية كبديل للأوراق التجارية الورقية[5].

---

[1]- فادي محمد عماد الدين توكل، المرجع السابق، ص.12.

[2]- محمد حسين منصور،المسؤولية الإلكترونية، المرجع السابق، ص. 101.

[3]- محمد فريد الشافعي، المرجع السابق، ص. 07.

[4]- محمد حسين منصور، المسؤولية الإلكترونية، المرجع السابق، ص. 101.

[5]- تعرف الأوراق التجارية على أنها محررات شكلية تتطلب لصحتها عدة بيانات حددها القانون،وتمثل مبلغا من النقود واجب دفعها في تاريخ معين أو قابل للتعيين، وهي قابلة للتداول بالطرق التجارية كما يمكن تحويلها فوراً إلى نقود يتم خصمها لدى البنوك واستخدامها كأداة لتسوية الديون. مأخوذة من فادي محمد عماد الدين توكل، المرجع السابق، ص. 89 وما يليها

بهذا يلاحظ أن البيئة الرقمية مكنت من خلق أنماط مستحدثة من وسائل إدارة النشاط التجاري، على نحو تتوافق فيه الأنماط التجارية المعمول بها، وسمات هذا العصر وسلوكياته[1].

لأهمية هذه المسألة، سيتم التطرق إلى بعض من الأوراق التجارية الإلكترونية باعتبارها صور للمستندات الإلكترونية التجارية، إذ سيتم التعرض للسفتجة الإلكترونية **(البند الأول)**، ثم الشيك الإلكتروني **(البند الثاني)**، وبعده اللاعتماد المستندي الإلكتروني **(البند الثالث)** باعتباره إحدى التقنيات الحديثة التي أصبحت تستخدم في عالم التجارة.

البند الأول: السفتجة الإلكترونية.

تعتبر السفتجة الإلكترونية إحدى صور المستند الإلكتروني التجاري، وهي تندرج تحت إطار الأوراق التجارية الإلكترونية، هذه الأخيرة التي عرفها الفقه على أنها: "محررات معالجة إلكترونيا، بصورة كلية أو جزئية، تمثل حقا موضوعه مبلغاً من النقود، وقابلة للتداول بالطرق التجارية ومستحقة الدفع لدى الإطلاع أو بعد أجل قصير، وتقوم مقام النقود في الوفاء".

أما عن تعريف السفتجة الإلكترونية فإن تعريفها لا يختلف عن مثيلتها الورقية التقليدية، ومن ثم يمكن القول بأنها محرر شكلي ثلاثي الأطراف معالج إلكترونيا بصورة كلية أو جزئية، يتضمن أمرا من شخص يسمى الساحب إلى شخص آخر يسمى المسحوب عليه، بأن يدفع مبلغاً من النقود لشخص ثالث يسمى المستفيد لدى الاطلاع أو في تاريخ معين.

ترتبط نشأة السفتجة الإلكترونية بالتجربة الفرنسية لوجود الحاسب الآلي للمقاصة بالبنك المركزي بفرنسا، وقد ظهرت السفتجة الإلكترونية كنتيجة لجهود اللجان التي اضطلعت بمحاولة حل المشاكل المالية والإدارية الناشئة عن التعامل بالسفاتج، خاصة التي تكون البنوك أحد أطرافها[2].

[1]- محمد فريد الشافعي، المرجع السابق، ص. 20.

[2]- مصطفى كمال طه، وائل أنور بندق، الأوراق التجارية ووسائل الدفع الإلكترونية الحديثة، دار الفكر الجامعي، الإسكندرية، 2006، ص، ص.343- 345.

هذا ويرجع تاريخ بدء العمل بالسفتجة الإلكترونية إلى 2 يوليو لسنة 1977، وذلك استجابة لتوحيد لجنة تطوير الائتمان قصير الأجل والمعروفة بلجنة جيليت (Gilet)[1]، ولعل نشأة السفتجة الإلكترونية في رحاب البنوك بهذه الصورة هي التي جعلت من التجربة الفرنسية نبراسا لدى الفقهاء الذين تعرضوا للأوراق التجارية الإلكترونية، حيث تعرضوا لها في إطار هذه التجربة مستبعدين من تصورهم إمكانية وجود الأوراق الإلكترونية في غير مجالات العمليات المصرفية، والواقع أنه ليس هنالك ما يمنع من الناحية القانونية أن توجد السفتجة الإلكترونية فيما بين الأفراد والشركات مع بعضها البعض من خلال الشبكات الخاصة، بل ومن خلال شبكة الإنترنت، خاصة مع ظهور التجارة الإلكترونية، أين أصبحت تتم المعاملات عن بعد وفي عالم افتراضي رقمي.

للإشارة فإن السفتجة الإلكترونية تنقسم إلى نوعين؛ سفتجة إلكترونية ورقية، وسفتجة إلكترونية ممغنطة[2]، فأما السفتجة الإلكترونية الورقية والتي يرمز لها اختصاراً (L.C.R. papier) فهي تلك التي تصدر من البداية في شكل ورقة كأي سفتجة تقليدية، ثم يتم معالجتها إلكترونيا عند تقديمها لدى البنك لتحصيلها أو بمناسبة تظهيرها[3] لأي طرف آخر، أما بالنسبة للنوع الثاني أي السفتجة الإلكترونية الممغنطة والتي يرمز لها اختصارا بـ(L.C.R. magnétique) فيختفي دور الورق فيها، لتصدر من البداية على دعامة ممغنطة، والواقع أن هذا النوع هو الذي يمثل قمة الاستفادة من التقنيات الإلكترونية الحديثة[4].

---

[1]- خالد ممدوح إبراهيم، حجية البريد الإلكتروني في الإثبات، دراسة مقارنة، ط1، دار الفكر الجامعي، الإسكندرية، 2008، ص.103.

[2]- مصطفى كمال طه، وائل أنور بندق، المرجع السابق، ص. 345.

[3]- التظهير هو طريقة تجارية لتداول الأوراق التجارية، حيث يوضع بيان مختصر على ظهر الورقة التجارية قصد نقل الحقوق الثابتة فيها بشكل يسير وسريع يستجيب لمقتضيات التجارة التي تقوم على دعامتي السرعة والائتمان هذا من جهة، ومن جهة أخرى فإن التظهير يسمح لحامل الورقة التجارية من الحصول على المال السائل قبل تاريخ الاستحقاق وذلك عن طريق التنازل عنها لشخص من الغير يسمى (L'endossataire) أي المظهر عليه أو الحامل الجديد، الذي يحول له الحق الثابت في السفتجة من قبل الحامل الأصلي للورقة التجارية، والذي يسمى بالمظهر.
لتفاصيل أكثر، نادية فوضيل، الأوراق التجارية في القانون الجزائري، دار هومة، الجزائر، 2006، ص. 38 وما يليها.

[4]- محمد أمين الرومي، المستند الإلكتروني، ط1، دار الفكر الجامعي، الإسكندرية، مصر،2007، ص. 66؛ خالد ممدوح إبراهيم، حجية البريد الإلكتروني في الإثبات، المرجع السابق، ص.103؛ مصطفى كمال طه، وائل أنور بندق، المرجع السابق، ص. 346.

هذا ويُشير بعض الفقه أن السفتجة الإلكترونية حتى تكون صحيحة ومعمول بها لابد أن تكون ملمة بالإضافة إلى الشروط الشكلية المنصوص عليها قانونا، شروطا ثلاثة وتتمثل هذه الأخيرة في صدورها على نموذج مطبوع يسمح بمعالجتها، والإطلاع عليها بوسائل الإطلاع الآلية والبصرية، شمولها لإسم البنك المسحوب عليه، ورقم حساب المسحوب عليه في هذا البنك، ضرورة توفر الاتفاق المبدئي بين سائر الأطراف المتدخلة لإستخدامها[1].

البند الثاني: الشيك الإلكتروني.

يعتبر الشيك الإلكتروني إحدى صور المستند الإلكتروني التجاري، وبالأخص الأوراق التجارية الإلكترونية، كما أنه يعتبر أحد مفردات نظام الوفاء الإلكتروني، حيث تقوم فكرة الشيكات الإلكترونية على استخدام الوسائل الإلكترونية لتحويل الشيكات الورقية إلى شيكات رقمية[2].

هذا ولقد عرف جانب من الفقه[3] الشيك الإلكتروني بأنه: "محرر ثلاثي الأطراف معالج إلكترونيا بشكل كلي أو جزئي، يتضمن أمراً من شخص يسمى الساحب إلى البنك المسحوب عليه بأن يدفع مبلغاً من النقود لإذن شخص ثالث يسمى المستفيد".

كما عرفه جانب آخر[4] بأنه رسالة إلكترونية موثقة ومؤمنة يرسلها مصدر الشيك إلى مستلمه (حامله)، ليعتمده ويقدمه للبنك الذي يعمل عبر الإنترنت، ليقوم هذا الأخير بتحويل قيمة الشيك المالية إلى حساب حامل الشيك، وبعدها يقوم بإلغاء الشيك وإعادته إلكترونياً إلى مستلمه (حامله) حتى يكون دليلا على أنه قد صرفه فعلاً، هذا ويمكن لمستلم الشيك أن يتأكد إلكترونياً من أنه قد تم بالفعل تحويل المبلغ لحسابه[5].

---

[1]- محمد أمين الرومي، المستند الإلكتروني، المرجع السابق، ص. 66.
[2]- محمد سعيد أحمد إسماعيل، المرجع السابق، ص. 320.
[3]- ناهد فتحي الحموري، الأوراق التجارية الإلكترونية، دراسة تحليلية مقارنة، ط1، دار الثقافة، عمان- الأردن، 2009، ص. 183؛ مصطفى كمال طه، وائل أنور بندق، المرجع السابق، ص. 350.
[4]- عبد الصبور عبد القوي علي مصري، التنظيم القانوني للتجارة الإلكترونية، ط1، مكتبة القانون والإقتصاد، الرياض، 1433هـ- 2012م، ص. 83؛ خالد ممدوح إبراهيم، حجية البريد الإلكتروني في الإثبات، المرجع السابق، ص.105.
[5]- حوالف عبد الصمد، المرجع السابق، ص.149.

بهذا يتبين أن آلية عمل الشيكات الإلكترونية تعتمد على وجود وسيط يقوم بعملية التحقق والدفع الإلكتروني لها، وغالبا ما يكون هذا الوسيط أحد البنوك الإلكترونية التي تعمل على شبكة الإنترنت[1].

الملاحظ أن تلك الآليات تم تصميمها بشكل خاص كأنظمة تشغيل للشيك الإلكتروني، على نحو يمكن معه الاستفادة من البنية التحتية الرقمية للبنوك الإلكترونية التي تقدم خدماتها مباشرة عبر شبكة الإنترنت، ورغم تمام العملية عبر شبكة الإنترنت، إلا أنها تمتاز بالأمن وذلك بسبب إعتماد البنوك على خدمات شركات وسيطة تضمن أمن وسلامة هذه المستندات، ولعل من بين الشركات التي قامت بتطوير أنظمة آمنة للتعامل بالشيكات الإلكترونية شركة (TELECKECK) الأمريكية التي تقدم خدماتها لأكثر من 27000 من المؤسسات المالية، كما انخرطت الحكومة الأمريكية ومجلس الخزانة الأمريكية سنة 1998 في نظام (FSTC)[2].

من خلال ما سبق، يتبين أن استخدام الشيك الإلكتروني في المعاملات يوفر العديد من المزايا، ولعل أهمها تقليل النفقات مقارنة باستخدام الشيكات الورقية، كما أنه يوفر الجهد والوقت وهو الأمر الذي تقتضيه وتتطلبه التجارة الإلكترونية، خاصة وأن البنوك الإلكترونية تهدف من خلال المعاملات المالية التي تجريها مع الأفراد التجار، وغير التجار والمؤسسات الحكومية وغير الحكومية إلى زيادة الأرباح، وذلك من خلال السيطرة على التكاليف وخفض المصروفات التشغيلية متخذة من التكنولوجيا أدوات لتحقيق ذلك[3]، وفعلا فقد كان لها ذلك من خلال استحداثها لنظام الشيكات الإلكترونية، وإدخالها حيز التطبيق في المعاملات المختلفة، ويظهر ذلك جلياً في انه قد أثبتت الدراسات التي تمت في الولايات المتحدة بأن البنوك تستخدم سنوياً أكثر من 500 مليون شيك ورقي، وتتكلف إجراءات تشغيلها حوالي 79 سنتا لكل شيك، وإن إعداد الشيكات الورقية يزداد بنسبة 3% سنويا، وبإجراء المقارنة بين

[1]- محمد سعيد أحمد إسماعيل، المرجع السابق، ص. 323.

[2]- في هذا المجال تبنت البنوك الكبرى فكرة بناء مواصفات قياسية للشيكات الإلكترونية، وذلك نظرا لأهمية هذا النوع من وسائل الدفع، وبالخصوص في إجراء الدفعات التي تتضمن مبالغ كبيرة نسبيا، فمثلا تم في الربع الثالث من عام 2002 معالجة 1,46 مليار صفقة تجارية في الولايات المتحدة بواسطة الشيكات بقيمة إجمالية تقدر بحوالي 3,95 مليون دولار.
مأخوذة من، محمود محمد أبو فروة، الخدمات البنكية الإلكترونية عبر الانترنت، ط1، دار الثقافة، عمان -الأردن، 2009، ص. 51.

[3]- محمود محمد أبو فروة، المرجع السابق، ص. 49.

استخدام الشيكات الإلكترونية، وغيرها من الشيكات الورقية تبيّن أن تكلفة التشغيل للشيك الإلكتروني يمكن أن تنخفض إلى 25 سنتا بدلا من 79 سنتا، وبذلك تحقق الشيكات الإلكترونية وفرا يزيد عن 250 مليون دولار سنويا في الولايات المتحدة فقط[1].

فضلا عن ذلك، فإن من بين المزايا أيضا التي يوفرها استخدام الشيكات الإلكترونية في التعامل عدم استلزامها وجود حسابات مصرفية لطرفي المعاملة بنفس البنك الذي يقوم بعملية المقاصة، وهو الأمر الذي ييسر إجراء التعاملات بهذه التقنية، خاصة مع ظهور نظام المقاصة الآلية، هذا النظام الذي أصبح يسمح بإمكانية إجراء المقاصة بين البنوك بعيداً عن الإجراءات اليدوية[2]، ومن ثم فإن الشيكات الإلكترونية تلاءم الأفراد الذين لا يملكون إئتمان، وهذا ما أشارت له الإحصائيات، إذ قد أكدت هذه الأخيرة أن 12% من جميع المشتريات عبر الإنترنت سددت بواسطة هذه الشيكات، بحيث تم في الربع الثالث من عام 2002 معالجة 1,46 مليار صفقة تجارية في الولايات المتحدة بواسطة الشيكات الإلكترونية، وذلك بقيمة إجمالية تقدر بـ 3,91 ترليون دولار[3].

بالإضافة إلى الشيك الورقي والشيك الإلكتروني، يوجد نظام وسط وهو ما يعرف بالشيك الذكي، والذي هو عبارة عن شيك ورقي يماثل الشيك التقليدي غير أنه مزود بشريط أو خلايا ممغنطة مسجل عليها بيانات مشفرة، وعند إدخال الشيك في جهاز خاص يقوم بقراءة هذه البيانات، والاتصال بحساب الشخص في المصرف المسحوب عليه الشيك والتأكد من صحة بياناته، ومدى وجود الرصيد وكفايته وقابليته للسحب، ثم يقوم بحجز قيمة الشيك لحساب المستفيد[4]، وبخصوص الشيك الذكي يرى جانب من الفقه أن هذا الأخير لا يعد مستنداً إلكترونيا، لأن الطبيعة الورقية ما زالت هي الغالبة عليه، ولا يغير من هذه الطبيعة وجود مجرد خلايا إلكترونية عليه.

---

[1]- محمد سعيد أحمد إسماعيل، المرجع السابق، ص. 321.

[2]- محمود محمد أبو فروة، المرجع السابق، ص .50.

[3]- مصطفى كمال طه، وائل أنور بندق، المرجع السابق، ص. 351.

[4]- علاء حسين مطلق التميمي، الأرشيف الإلكتروني وكيفية المحافظة على المستند الإلكتروني عبر الزمن، دراسة مقارنة، ط1، دار النهضة العربية، مصر، 2010، ص. 147.

البند الثالث: الاعتماد المستندي الإلكتروني.

تتعدد الخدمات التي تقدمها المؤسسات المالية لعملائها كما تتعدد الأنشطة التي تمارسها في إطار معاملاتها المصرفية، ومن المعروف أن قبول الودائع لا يشكل في حد ذاته النشاط الرئيسي لمؤسسات الائتمان، وإنما يعتبر فقط جزء من النشاط الأساسي المتمثل في منح الائتمان، وتوزيعه على مختلف القطاعات التجارية والصناعية المحتاجة له، باستعمال الودائع النقدية في إجراء العمليات التي لا تستطيع القيام بها بالاعتماد على أموالها الذاتية فقط، فالعمليات الائتمانية التي يقوم بها البنك كثيرة ومتنوعة منها القرض، الخصم الوارد على الأوراق التجارية ، عمليات فتح الاعتماد[1]، هذا الأخير الذي هو عبارة عن عقد يلتزم البنك بمقتضاه بوضع مبلغ نقدي تحت تصرف العميل خلال مدة معينة، ويكون للعميل الخيار في استخدام هذا المبلغ كله أو بعضه، أو عدم استخدامه أو سحب سفاتج عليه مقابل أجر يتقاضاه البنك من العميل[2].

وللإشارة فإن الائتمان عن طريق فتح الاعتماد يتخذ صورتين رئيسيتين في أغلب الحالات، ويتعلق الأمر بالاعتماد البسيط والاعتماد المستندي، والذي يمكن تعريفه بأنه تعهد صادر من البنك بناء على طلب عميله الذي يسمى الآمر بفتح الاعتماد، لصالح الغير الذي يسمى المستفيد، مضمون بحيازة مستندات ممثلة لبضاعة منقولة أو معدة للنقل[3].

والإعتماد المستندي عملية يقبل بموجبها بنك المستورد الحلول محل المستورد في الالتزام بتسديد وارداته لصالح المصدر الأجنبي عن طريق البنك الذي يمثله مقابل استلام الوثائق أو المستندات التي تدل على أن المصدر قد قام فعلا بإرسال البضاعة المتعاقد عليها،

---

[1]- محمود محمد أبو فروة، المرجع السابق، ص،ص. 52- 53.

[2]- يرى بعض الفقه أن فتح الاعتماد هو فعل ثقة يضم تبادل خدمتين متباعدتين في الوقت، فهو تقديم أموال مقابل وعد بالتسديد مع فائدة معينة تغطي عمليتين أساسيتين وهما: الفارق الزمني والخطر، فهم يرون أن هذه العملية ترتكز على عوامل ثلاثة رئيسية هي: الثقة والوقت والوعد . ومن ثم فقد توصلوا إلى وضع المعادلة التالية: الاعتماد = الثقة + الوقت + الوعد.

لتفاصيل أكثر يراجع، بخراز يعدل فريدة، تقنيات وسياسات التسيير المصرفي، ط 4، ديوان المطبوعات الجامعية، الجزائر، 2008، ص. 109 وما يليها؛

Tahar Hadj Sadok, Les risques de l’entreprise et de la banque, édition Dahleb, Algérie, 2007, p .11.

[3]- محمود محمد أبو فروة، المرجع السابق، ص. 53.

وعليه فإن العلاقة التي تنجم عن فتح الاعتماد المستندي لصالح المستورد تربط بين أربعة أطراف وهم: المستورد، المصدر، بنك المستورد، وبنك المصدر.

للإشارة، فإن هذا النظام أنشأه العرف المصرفي لتمويل التجارة الدولية التي تتم بين أطراف لا يعرف أي منهم حقيقة المركز المالي للآخر، وذلك بخلاف البنوك التي تعرف إلى حد كبير مراكز عملائها فتستفيد من ذلك بفتحها بناء على طلبهم إعتمادا للطرف الآخر، وعليه يعتبر الاعتماد المستندي من أشهر الوسائل المستعملة في تمويل الواردات، وذلك نظرا لما يقدمه من ضمانات للمصدرين والمستوردين على حد سواء[1].

هذا عن تعريف الإعتماد المستندي، أما عن طريقة وإجراءات التعامل به، فتتمثل في إتفاق المشتري المستورد للبضاعة بإبرام عقد مع البائع على دفع الثمن عن طريق هذه التقنية (أي عن طريق الاعتماد المستندي)، ليقوم بعدها المشتري بالتوجه إلى بنكه طالبا فتح الإعتماد المستندي لصالح البائع محددا فيه كافة تفاصيل عملية البيع، ويقوم بعد ذلك البنك بإبلاغ البائع بالاعتماد المفتوح لصالحه، إما بشكل مباشر وإما عن طريق بنك مراسل له في بلد المصدر، على أنه يمكن لهذا الأخير –أي البنك المراسل له– تعزيز الاعتماد، ومتى تحقق ذلك أصبح ملتزما بالدفع للمستفيد، بالإضافة إلى البنك مصدر الاعتماد، فإن اقتنع البنك مصدر الاعتماد بأن مستندات البضاعة مطابقة لشروط الاعتماد دفع للبنك المراسل قيمة ما دفعه هذا الأخير إلى المستفيد، أما إذا وجد مستندات البضاعة مخالفة لشروط الاعتماد قام بإرسال إخطار إلى البنك المراسل برفض المستندات في مدة معقولة[2].

ولقد كانت الاعتمادات المستندية تتم بصورة يدوية، إلا أن التطور التكنولوجي أدى إلى الاستغناء عن هذه الطريقة، واستبدالها بطريقة أخرى تعتمد على استخدام الكمبيوتر وشبكة الإنترنت، فظهر ما يسمى بالاعتماد المستندي الإلكتروني، والذي يقوم فيه المستورد بإرسال طلبه لإصدار اعتماد مستندي عن طريق الإنترنت، فإذا ما وافق البنك على طلب

[1]- الطاهر لطرش، تقنيات البنوك، ط2، ديوان المطبوعات الجامعية، الجزائر، 2003، ص. 117.
[2]- أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني –دراسة مقارنة–، ط1، دار النهضة العربية، 2006، ص، ص. 72- 73.

عميله، فإنه يقوم بإرسال نص الاعتماد وبنفس الطريقة، وقبل انتهاء الأجل المحدد في الاعتماد يقوم المستفيد بإرسال كافة المستندات المتعلقة بالشحن، واللازمة للحصول على قيمة الاعتماد، بحيث يرسلها بطريقة إلكترونية، ويطلب من كافة الأطراف المشاركة في العملية كالشاحن والمؤمن أن يقوموا بإرسال مستنداتهم للبنك مصدر الاعتماد عن طريق الإنترنت[1].

أما إذا تدخل أكثر من بنك في العملية، فإن كل واحد من البنوك يقوم بإرسال الرسائل الإلكترونية الواردة إليه للبنك المبلغ (أي البنك الذي يتعامل معه المستفيد)، وإذا ما كانت المستندات موافقة لما ورد في الاعتماد، فإنه يقوم بتحويل المبلغ بصورة إلكترونية[2].

للإشارة فإن استخدام الاعتماد المستندي الإلكتروني في المعاملات يوفر جملة من المزايا، أهمها إتمام الصفقات في سهولة ويسر وبسرعة كبيرة، وهو الأمر الذي يخول المتعاملين به قدرة تنافسية تفوق غيرهم من المتعاملين بالطرق التقليدية، ناهيك عن أنه يؤدي إلى التقليص من تكلفة إرسال المستندات، والاستفادة من ميزة التبادل الإلكتروني في حل المشكلات الناتجة عن وصول البضائع قبل وصول المستندات[3].

[1]- علاء حسين مطلق التميمي، الأرشيف الإلكتروني وكيفية المحافظة على المستند الإلكتروني عبر الزمن، دراسة مقارنة، المرجع السابق، ص، ص. 144- 145؛ محمود محمد أبو فروة، المرجع السابق، ص. 54؛ أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني –دراسة مقارنة–، ط1، المرجع السابق، ص. 73.

[2]- محمود محمد أبو فروة، المرجع السابق، ص، ص. 54- 55.

[3]- علاء حسين مطلق التميمي، الأرشيف الإلكتروني وكيفية المحافظة على المستند الإلكتروني عبر الزمن، دراسة مقارنة، المرجع السابق، ص. 145؛ أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني –دراسة مقارنة–، ط1، المرجع السابق، ص، ص. 73- 74.

المبحث الثاني: الأطراف الفاعلة في المستند الإلكتروني وضوابطه القانونية

لقد سبق الذكر، أن إستخدام الوسائل الإلكترونية في شتى مجالات الحياة أدى إلى ظهور ما يعرف بالمستندات الإلكترونية، هذه الأخيرة تمتاز بتعدد أطرافها، ويستلزم لقيامها صحيحة إحترامها لضوابط القانونية موضوعية وشخصية.

وعليه ماهي الضوابط الواجب توافرها لصحة المستندات الإلكترونية؟ ومن هي الأطراف الفاعلة في تحريرها؟

لأهمية هذه المسألة سيتم التعرض للأطراف الفاعلة في تحرير المستند الإلكتروني **(المطلب الأول)**، ولضوابط المستند الإلكتروني الموضوعية **(المطلب الثاني)**، وبعدها لضوابطه الشخصية **(المطلب الثالث)**.

المطلب الأول: الأطراف الفاعلة في تحرير المستند الإلكتروني.

إن أهم ما يميز المستند الإلكتروني عن المستند التقليدي هو غياب العلاقة المباشرة بين أطرافه، كما أنه يتميز أيضا بوجود الوسيط الإلكتروني بين طرفيه، وعليه فإن الأطراف الفاعلة أو المساهمة في تحرير المستند الإلكتروني تكمن في طرفيه وهما المرسل (أو منشأ المستند)، والمرسل إليه، ويوجد إلى جانب هذين الطرفين طرف ثالث موثوق يطلق عليه اسم الوسيط الإلكتروني.

فما هو الدور المنوط لكل طرف من الأطراف الفاعلة في المستند الإلكتروني، وما هو موقف التشريعات منها؟.

الفرع الأول: المرسل

يلعب المرسل أو منشأ المستند الإلكتروني دورا كبيرا في تحرير المستند الإلكتروني، ذلك أنه هو الذي يُنْشِأه ويدخله حيز الوجود، ونظرا للدور الكبير الذي يلعبه فقد اعتبرت مسألة تعريفه من بين القواعد القياسية لتأمين المعاملات الإلكترونية التي وضعها الإتحاد العالمي للاتصالات التابع للأمم المتحدة، والتي حُدد فيها طرفي المستند الإلكتروني[1].

[1]- أسامة أبو الحسن مجاهد ،الوسيط في المعاملات الالكترونية وفقا لأحدث التشريعات في فرنسا، مصر، الأردن، دبي ، البحرين، الكتاب الأول، المدخل لقانون المعاملات الإلكترونية- العقد الإلكتروني- الإثبات الإلكتروني، دار النهضة العربية، القاهرة، 2007، ص. 366.

إن أهمية الدور الذي يلعبه المنشأ دفع التشريعات إلى وضع تعريف له، بحيث عرفته المادة 2/ج من قانون الأونيستيرال النموذجي للتجارة الإلكترونية: "يراد بمصطلح "منشئ" رسالة البيانات الشخص الذي يعتبر أن إرسال أو إنشاء رسالة البيانات قبل تخزينها، إن حدث قد تم على يديه أو نيابة عنه، ولكنه لا يشمل الشخص الذي يتصرف كوسيط فيما يتعلق بهذه الرسالة"[1].

كما عرفته المادة 12/2 من قانون المعاملات الإلكترونية الأردني واعتبرته الشخص الذي يقوم، بنفسه أو بواسطة من ينيبه، بإنشاء أو إرسال رسالة المعلومات قبل تسلمها وتخزينها من المرسل إليه[2].

للإشارة فقد ألغي هذا القانون وحل محله قانون 2015[3] الذي عرف المنشئ في المادة 10/2 واعتبره الشخص الذي يقوم بإنشاء رسالة المعلومات أو إرسالها.

أما قانون إمارة دبي فقد عرف المنشأ في المادة 9/2 بأنه: "الشخص الطبيعي أو المعنوي الذي يقوم أو يتم بالنيابة عنه إرسال الرسالة أيا كانت الحالة، ولا يعتبر منشأ الجهة التي تقوم بمهمة مزود خدمات، فيما يتعلق بإنتاج أو معالجة أو إرسال أو حفظ تلك الرسالة الإلكترونية، وغير ذلك من الخدمات المتعلقة بها"[4].

هذا وقد ورد أيضا بقانون المعاملات الإلكترونية البحريني تعريفا لمنشئ المستند، إذ نصت المادة 1/ 5 منه: "المنشئ هو الشخص الذي يرسل، أو يرسل نيابة، عنه السجل الإلكتروني، أو من يظهر من السجل الإلكتروني قيامه بإنشاء أو إرسال السجل الإلكتروني قبل حفظه -إن كان قد تم ذلك- ولا يشمل الشخص الذي يعمل وسيط شبكة بشأن هذا السجل"[5].

[1]- قانون الأونيسترال النموذجي بشأن التجارة الالكترونية ، سابق الإشارة إليه.
[2]- القانون رقم 85 لسنة 2001 المتعلق بالمعاملات الالكترونية الأردني، سابق الإشارة إليه.
[3]- قانون رقم 15 لسنة 2015 المتعلق بالمبادلات الالكترونية الأردني، سابق الإشارة إليه.
[4]- قانون إمارة دبي رقم 2 لسنة 2002 بشأن المعاملات والتجارة الالكترونية، سابق الإشارة إليه.
[5]- مرسوم بقانون رقم (28) لسنة 2002 بشأن المعاملات الالكترونية البحريني، سابق الإشارة إليه.

للإشارة فقد ألغي هذا القانون، وحل محله قانون رقم 54 لسنة 2018[1] وقد أشار هذا القانون للمنشئ بمصطلح المصدر وعرفه في المادة 39/1 منه بـأنه: "شخص يقوم بنفسه أو بالنيابة عنه، بإرسال سجل إلكتروني، أو القيام بإنشاء أو إرسال سجل إلكتروني قبل تخزينه إن كان قد تم ذلك، ولا يشمل ذلك الشخص الذي يكون بمثابة وسيط بشأن هذا السجل."

أما عن مشروع القانون الكويتي للتجارة الإلكترونية فقد ذهب في تعريفه لمنشأ المستند الإلكتروني أنه الشخص الذي يعتبر أن إرسال أو إنشاء مستند إلكتروني قبل تخزينه، إن حدث قد تم منه أو نيابة عنه.

في هذا السياق، ينبغي الذكر أنه قد صدر قانون المعاملات الإلكترونية الكويتي[2]، وفيه عرفت المادة1/ 8 المنشئ بأنه: "الشخص الطبيعي أو المعنوي الذي يقوم أو يتم بالنيابة عنه إرسال المستند أو السجل عن طريق رسالة إلكترونية، أو من يثبت قيامه بإنشاء أو إرسال المستند أو السجل قبل حفظه.

ولا يعتبر –منشأ- الجهة التي تقوم بمهمة مزود خدمات فيما يتعلق بإنتاج أو معالجة أو إرسال أو حفظ ذلك المستند أو السجل الإلكتروني وغير ذلك من الخدمات المتعلقة بها."

كما ورد أيضا في مشروع القانون الفلسطيني للمبادلات والتجارة الإلكترونية أن المرسل هو أي شخص طبيعي أو اعتباري يقوم بإرسال أو إنشاء بيانات قبل تخزينها بنفسه أو يقوم بها شخص آخر نيابة عنه، ولكنه لا يشمل الشخص الذي يتصرف كوسيط فيما يتعلق بهذه الرسالة.

إذا كان هذا التعريف قد ورد في مشروع القانون الفلسطيني للمبادلات والتجارة الإلكترونية، فإنه ينبغي الذكر أن قانون المعاملات الإلكترونية صدر سنة 2017[3] وفيه عرفت المادة 11/1 المرسل بأنه: "الشخص الذي يقوم بنفسه أو بواسطة من ينيبه بإنشاء أو إرسال رسالة البيانات."

---

[1]- مرسوم بقانون رقم (54) لسنة 2018 المتعلق بإصدار قانون الخطابات والمعاملات الإلكترونية، سابق الإشارة إليه.
[2]- قانون رقم 20 لسنة2014 في شأن المعاملات الإلكترونية الكويتي .
[3]- قرار بقانون رقم (15) لسنة2017 بشأن المعاملات الإلكترونية الفلسطيني.

وتنبغي الإشارة، أن قانون التوقيع الإلكتروني المصري جاء خاليا من أي تعريف لمنشئ أو مرسل المحرر أو المستند الإلكتروني.

كما وجاء قانون التجارة الإلكترونية الجزائري خاليا من تعريف المنشأ، وحسنا ما فعل المشرع الجزائري، ذلك أن مهمة التعريف من إختصاص الفقه، وفي هذا يمكن القول أن المنشأ هو الشخص الذي يقوم بإنشاء المحرر أو إرساله سواء قام بذلك بنفسه أو قام به من ينيبه، وقد يكون منشئ الرسالة شخصا طبيعيا أو شخصا معنويا كما في الحاسبات المؤتمتة، إذ من خلال نظام الحسابات المؤتمنة يمكن للمحاسب القيام بإنشاء المحرر الإلكتروني بعد إمداده بالبرنامج المخصص لذلك، والذي يكمن دوره يقوم في إعداد رسائل البيانات، والرد على الرسائل من دون تدخل العنصر البشري.

الفرع الثاني: المرسل إليه.

يعتبر المرسل إليه الطرف الثاني الفاعل في المستند الإلكتروني، وهو الطرف الذي يقصد مرسل الرسالة أو المستند أن يبعثه إليه، أما عن موقف التشريعات من هذا الطرف الثاني فيلاحظ أن المادة2/د من قانون الأونيسترال النموذجي للتجارة الإلكترونية عرفت للمرسل إليه بأنه:" للشخص الذي قصد المنشئ أن يتسلم رسالة البيانات، ولكنه لا يشمل الشخص الذي يتصرف كوسيط فيما يتعلق بهذه الرسالة".

كما عرفته المادة13/2 من قانون العاملات الالكترونية الأردني[1] بأنه: "الشخص الذي قصد المنشئ تسليمه رسالة المعلومات".

الملاحظ أنه بعد إلغاء القانون السالف الذكر وحلول القانون الجديد محله[2]، لم يعرف المشرع الأردني المرسل إليه، وذلك بخلاف ما تبناه بالنسبة للمنشئ في المادة 2 من القانون الساري المفعول.

[1] - القانون رقم 85 لسنة 2001، و المتعلق بالمعاملات الالكترونية الأردني، سابق الإشارة إليه.
[2] - قانون رقم 15 لسنة 2015 المتعلق بالمبادلات الالكترونية الأردني، سابق الإشارة إليه.

نظرا لأهمية الدور المنوط لهذا الطرف يلاحظ أن قانون إمارة دبي بشان المعاملات والتجارة الالكترونية هو الآخر قد تطرف إليه، وعرفه في المادة 10/2على أنه: "الشخص الطبيعي أو المعنوي الذي قصد منشئ الرسالة توجيه رسالته إليه، ولا يعتبر مرسلا إليه الشخص الذي يقوم بتزويد الخدمات فيما يتعلق باستقبال أو معالجة أو حفظ المراسلات الإلكترونية ،وغير ذلك من الخدمات المتعلقة بها".

هذا وقد عرف قانون المعاملات الالكترونية البحريني المرسل إليه في المادة 1/ 6 منه واعتبرته:"الشخص الذي يقصد المنشئ تسليم سجل إلكتروني إليه، ولا يشمل ذلك الشخص الذي يعمل وسيط شبكة بشأن هذا السجل"[1].

وقد أضحت هذا المادة بعد إلغاء قانون 2002، المادة 40/1 واعتبرت المرسل إليه: "شخص يقصد المصدر تسليمه خطابا إلكترونيا من قبل المصدر، ولا يشمل ذلك الشخص الذي يكون بمثابة وسيط بشأن هذا الخطاب."[2]

أما مشروع قانون التجارة الإلكترونية الكويتي فقد ذهب في تعريفه للمرسل إليه المستند الإلكتروني أنه:"الشخص الذي قصد المنشئ أن يستلم المستند الإلكتروني"، ونفس الشأن بالنسبة لمشروع القانون الفلسطيني للمبادلات والتجارة الإلكترونية حيث عرف المرسل إليه أنه هو: "أي شخص طبيعي أو اعتباري أراد المرسل تسليمه رسالة البيانات، ولكنه لا يشمل الشخص الذي يتصرف كوسيط فيما يتعلق بهذه الرسالة"، ويلاحظ أيضا أن القانون المصري قد جاء خاليا من أي تعريف للمرسل إليه أما عن موقف التشريع الجزائري من مفهوم المرسل إليه.

وعليه فإنه مما سبق من تعريف المرسل إليه يتبين أنه الشخص الطبيعي أو المعنوي الذي قصد المنشئ أن يسلمه رسالة البيانات الخاصة به، وكذلك يختلف الشخص المرسل والمرسل إليه عن الوسيط في المحرر الإلكتروني، وهو ما سنوضحه من خلال بيان دور الوسيط الإلكتروني.

[1] - مرسوم بقانون رقم (28) لسنة 2002 بشأن المعاملات الالكترونية البحريني، سابق الإشارة إليه.
[2] - مرسوم بقانون رقم (54) لسنة 2018 المتعلق بإصدار قانون الخطابات والمعاملات الإلكترونية ، سابق الإشارة إليه

الفرع الثالث: الوسيط الإلكتروني.

يعتبر الوسيط الإلكتروني طرفا فاعلا في المستند الإلكتروني، ونظرا لأهمية الدور المنوط به فقد حظي باهتمام التشريعات المنظمة للمعاملات الإلكترونية، أما عن مفهومه فإننا نجد أنه قد جاء القانون النموذجي المتعلق بالتجارة الالكترونية، أنه يراد بمصطلح الوسيط، فيما يتعلق برسالة بيانات معينة، الشخص الذي يقوم نيابة عن شخص آخر بإرسال أو استلام أو تخزين رسالة البيانات أو تقديم خدمات أخرى فيما يتعلق برسالة البيانات هذه .

كما جاء بالقانون الأردني المتعلق بالمعاملات الالكترونية أن الوسيط الإلكتروني ما هو إلا برنامج الحاسوب أو أي وسيلة إلكترونية أخرى تستعمل من أجل تنفيذ إجراء، أو الاستجابة لإجراء بقصد إنشاء أو إرسال أو استلام رسالة بيانات بدون تدخل شخصي[1].

وقد حل محل هذا النص المادة 11/2 من قانون المعاملات الألكترونية الأردني لسنة 2015[2] وعرفت الوسيط الإلكتروني بأنه: "البرنامج الالكتروني الذي يستعمل لتنفيذ إجراء أو الاستجابة لإجراء بشكل تلقائي بقصد إنشاء رسالة معلومات أو إرسالها أو تسلمها."

أما قانون إمارة دبي بشأن المعاملات والتجارة الالكترونية[3]، فقد عرف الوسيط الإلكتروني بأنه:" برنامج أو نظام إلكتروني لحاسب آلي يمكن أن يتصرف أو يستجيب لتصرف بشكل مستقل كليا أو جزئيا دون إشراف أي شخص طبيعي، في الوقت الذي يتم فيه التصرف أو الاستجابة له".

وإلى جانب قانون إمارة دبي فإننا نجد أن القانون البحريني قد أطلق عليه اسم وسيط الشبكة، ونص بأنه" يقصد بوسيط الشبكة بالنسبة للسجل الإلكتروني، الشخص الذي يقوم نيابة عن شخص آخر بإرسال أو تسلم أو بث أو حفظ ذلك السجل الإلكتروني أو تقديم خدمة أخرى بشأن ذلك السجل الإلكتروني"[4]،

[1]- المادة 11/2 من القانون رقم 85 لسنة 2001 المتعلق بالمعاملات الالكترونية الأردني، سابق الإشارة إليه.
[2] - قانون رقم 15 لسنة 2015 المتعلق بالمبادلات الالكترونية الأردني، سابق الإشارة إليه.
[3] - المادة 17/2 من قانون إمارة دبي رقم 2 لسنة 2002 بشأن المعاملات والتجارة الالكترونية، سابق الإشارة إليه.
[4]- المادة 7/1من مرسوم بقانون رقم (28) لسنة 2002 بشأن المعاملات الالكترونية البحريني، سابق الإشارة إليه.

للإشارة حل محل هذا النص المادة 41/1 من قانون الخطابات والمعاملات الإلكترونية البحريني لسنة 2018 وأوردت في تعريف الوسيط ذات التعريف الذي تضمنه القانون الملغى[1] ، هذا وقد تطرق المشرع المصري كذلك إلى الوسيط وعرفه بأنه:" هو أداة أو أدوات أو أنظمة إنشاء التوقيع الإلكتروني"، و ما يمكن ملاحظته عن المشرع المصري أن تعريفه للوسيط الإلكتروني يختلف عن باقي تعريفات للوسيط في البيئة الإلكترونية، حيث لم يبين التشريع المصري دور الوسيط بتلقيه لرسالة البيانات من المنشئ وتخزينها وإرسالها إلى المرسل إليه، وإنما حصر دوره في منظومة التوقيع الإلكتروني فقط.

أما عن موقف المشرع الجزائري فإذا تفحصنا نصوص القانون الجزائري فإننا نجد أنه لم يعطي تعريف للوسيط مثلما فعلت جل التشريعات العربية المذكورة سابقا، وحسن ما فعل لأن مسألة التعريف هي من اختصاص الفقه لا التشريع.

وعليه فأنه يتبين من التعريفات السابقة أن الوسيط هو شخص آخر غير المنشئ والمرسل إليه وهو قد يكون شخصا طبيعيا أو اعتباريا، كما جاء بقانوني دولة الإمارات والمملكة الأردنية أي أن الوسيط قد يكون مؤتمتا أي باستخدام نظام الحاسوب المؤتمت، كما يلاحظ على ما سبق من تعريفات الوسيط بأنه لم يأت على إطلاقه بالمحررات الإلكترونية، وهذا يعني أن نفس الوسيط يمكن أن يكون طرفا في محرر إلكتروني كمنشأ أو مرسل إليه أو وسيط فيما يتعلق بمحرر إلكتروني آخر.

المطلب الثاني: الضوابط الموضوعية للمستند الالكتروني.

لقد كان للتطور الهائل الذي شهدته نظم الاتصالات والمعلومات أثر كبير على وسائل إبرام المعاملات وكذا ضوابطها، وهو الأمر الذي دفع بمختلف دول العالم إلى تحديد الضوابط الموضوعية للمستند الالكتروني، خاصة وأنه أصبح وسيلة مستحدثة لإبرام التصرفات المختلفة[2]، وبالرجوع للمستند يتبين أنه يتكون من جزأين أحدهما عام، والآخر

[1] - مرسوم بقانون رقم (54) لسنة 2018 المتعلق بإصدار قانون الخطابات والمعاملات الإلكترونية ، سابق الإشارة إليه
[2]- محمد أمين الرومي، المستند الإلكتروني، المرجع السابق، ص.06؛ عبد الصبور عبد القوي مصري، الجريمة الالكترونية، ط1، دار العلوم، القاهرة، 2008، ص.84.

خاص، فأما الجزء العام للمستند فيتكون من مجموع البيانات التي يحتويها عن الشخص صاحب المستند، وتشمل هذه البيانات المعلومات الدالة على هوية ذلك الشخص والموجهة له، وللإشارة فإن هذه البيانات قد تكون مجموعة من الحروف أو الأرقام أو أي علامات أخرى ذات مفهوم.

أما بالنسبة للجزء الخاص من هذا المستند فهو الجزء الذي يتألف من مجموع الأرقام أو الحروف الدالة على توقيع الشخص صاحب المستند الإلكتروني، وهي تعبر أساسا عن المفتاح الرئيسي للمستند[1].

فلئن كان المستند الورقي يتخذ من الورق والكتابة التقليدية دعامة له، ويتشكل من كتابة تحدد مضمونه، وتوقيع يفيد نسبته إلى شخص معين هو الموقع، فإن المستند الالكتروني يتشكل من دعامة مختلفة وكتابة متميزة ذات نوع خاص، فهو إذن يختلف عن المستند الورقي من حيث الدعامة والكتابة طريقة وشكلا، فضلا عن اختلاف التوقيع الالكتروني عن التوقيع التقليدي.

ومن تم فإن الضوابط الموضوعية للمستند الالكتروني تتمثل في عنصرين اثنين: أولهما الكتابة الالكترونية وثانيهما التوقيع الالكتروني، فما المقصود بكل منهما؟.

هذا ما سيتم بيانه بالتعرض للكتابة الإلكترونية **(الفرع الأول)**، وبعدها للتوقيع الإلكتروني **(الفرع الثاني)**.

الفرع الأول: الكتابة الالكترونية.

إن الكتابة الالكترونية لفظ متكون من كلمتين كلمة "كتابة" وكلمة "الكترونية"، فبالنسبة لكلمة "كتابة" فهي مشتقة لغة من الفعل الثلاثي كتب بمعنى خط فيقال كتب الشيء أي خطه، والخط رسم يُدرك بحاسة البصر[2].

[1]- علاء حسين مطلق التميمي، حجية المستند الالكتروني في الإثبات المدني، ط1، دار النهضة العربية، القاهرة- مصر، 2009، ص.81.

[2]- علاء حسين مطلق التميمي، المستند الالكتروني، عناصره وتطوره ومدى حجيته في الإثبات المدني، دراسة مقارنة، ط2، دار النهضة العربية، القاهرة- مصر-، 2011 ، ص.32.

أما اصطلاحا فيمكن تعريف الكتابة بصفة عامة على أنها: "مجموعة الرموز المرئية التي تعبر عن القول أو الفكر"، كما أن هناك من يعرفها على أنها: "عبارة عن نقوش أو رموز تعبر عن قصد صاحبها بشكل واضح ومفهوم وبصفة مستمرة، أيا كانت المادة التي تكتب بها أو الدعامة التي تدون عليها"، وليس هناك في اللغة أو القانون ما يتطلب أن تكون الكتابة على الورق، بل يجوز أن تكون على الورق أو الخشب أو الرمل أو الجلد، ونخلص من ذلك إلى عدم وجود ارتباط بين فكرة الكتابة والورق، فلا يشترط أن تكون الكتابة على الورق بمفهومه التقليدي، وهو ما يفتح الباب على مصراعيه أمام قبول كل الدعامات أيا كانت مادة صنعها[1].

هذا عن التعريف العام للكتابة، أما عن كلمة الكترونية فتجدر الإشارة أن هذه الكلمة قد سبق بيان مفهومها اللغوي والاصطلاحي، وبالتالي فلا داعي لإعادة تعريفها مرة أخرى[2].

هذا ولقد شهدت الكتابة في معناها تطورا ملموسا على مر العصور، فبعد أن كانت تتم على جلد الحيوانات أصبحت تتم على الورق، ثم تقدمت فظهرت الوسائل المستحدثة في التعاقد كالفاكس والتلكس عامة، والانترنت خاصة، ولقد كان للتطور العلمي دور كبير في تطور فكرة الكتابة، وذلك بظهور وسائل التعاقد المستحدثة، وبذلك لم تعد تربط الكتابة بالورقة التقليدية، بل أصبح الفكر القانوني يستخدم مصطلح لكتابة الالكترونية المستخرجة من أجهزة الحاسب والانترنيت، طالما أنه يمكن التأكد من مضمونها لإثبات المعاملات بين المتعاقدين[3].

بهذا يمكن القول، أن التطور التكنولوجي أدى إلى إستحداث الكتابة الالكترونية كبديل للكتابة التقليدية، ولئن كانت هذه الأخيرة تعد أحد مفرزات التقنية التكنولوجية، فما المقصود بها؟ وما موقف تشريعات المعاملات الإلكترونية منها؟.

---

[1]- علاء حسين مطلق التميمي، حجية المستند الالكتروني في الإثبات المدني، المرجع السابق، ص، ص. 88-89.

[2]- يراجع في ذلك، ص 21 من هذه الأطروحة.

[3]- إبراهيم الدسوقي أبو الليل، الجوانب القانونية للتعامل عبر وسائل الاتصال الحديثة، دار النهضة العربية، القاهرة، 1999، ص.27.

هذا ما سيتم بيانه بالتطرق للكتابة الالكترونية من الناحية الفقهية **(البند الأول)**، وإلى مفهومها من الناحية التشريعية **(البند الثاني)**.

البند الأول: التعريف الفقهي للكتابة الإلكترونية.

لقد حاول فقهاء القانون تعريف الكتابة الالكترونية، بحيث عرفها جانب من الفقه[1] بأنها: "كل حروف أو أشكال أو أرقام أو رموز أو إشارات، أو أي علامات أخرى ذات دلالة قابلة للإدراك أيا كانت الدعامة المثبتة عليها، إلكترونية أو رقمية، أو ضوئية أو أية وسيلة أخرى مشابهة"، كما عرفها اتجاه آخر[2] بأنها : " الكتابة التي يتم وضعها في صورة رقمية، وتخزينها كبيانات الكترونية على أقراص مدمجة، و قد تتضمن هذه الكتابة حروفا أو أرقاما أو رموزا أو أية علامة أخرى تثبت على دعامة إلكترونية أو رقمية أو ضوئية، أو أية وسيلة أخرى مشابهة ، وتعطي دلالة قابلة للإدراك".

ما يلاحظ على التعاريف التي جاء بها هذا الاتجاه الفقهي أنها متشابهة إلى حد ما، وعليه فقد اتجه فريق ثاني[3] إلى تعريف الكتابة الالكترونية على أنها: "مجموعة من الحروف أو الأرقام أو الرموز أو الأصوات، أو أي علامة أخرى يمكن أن تثبت على دعامة إلكترونية تؤمن قراءتها، وتضمن عدم العبث في محتواها وحفظ المعلومات الخاصة بمصدرها، وتاريخ ومكان إرسالها وتسلمها والاحتفاظ بكافة المعلومات الأخرى على نحو يتيح الرجوع إليها عند الحاجة".

في حين عرفها اتجاه ثالث بأنها: "المعلومات التي يتم إنشاءها أو إرسالها أو تخزينها بوسائل إلكترونية أو ضوئية أو بوسائل مشابهة".

وفقا لهذا الاتجاه يجوز أن تشمل الكتابة الالكترونية المعلومات الواردة على المحررات، والتي تنشأ بقصد إبلاغها للغير، أو بقصد تخزينها والاحتفاظ بها، سواء نشأت

[1]- علاء حسين مطلق التميمي، المستند الالكتروني، عناصره وتطوره وحجيته في الإثبات، المرجع السابق، ص.42.
[2]- علاء مطلق حسين التميمي، حجية المستند الالكتروني في الإثبات المدني، المرجع السابق، ص.101.
[3]- نور خالد عبد المحسن العبد الرزاق، حجية المحررات والتوقيع الالكتروني في الإثبات على شبكة الانترنت، رسالة للحصول على درجة الدكتوراه في الحقوق، كلية الحقوق جامعة عين شمس، مصر، 2009، ص.381؛ الأنصاري حسن النيداني، القاضي والوسائل الإلكترونية الحديثة، المرجع السابق، ص.10 وما يليها.

تلك المعلومات بتدخل العنصر البشري، أو تلقائيا بواسطة أجهزة الكمبيوتر، كما ويستوي أن تبلغ المعلومات الواردة بالمحررات إلكترونيا بواسطة وسائل الاتصال الحديثة، أو يتم تسليمها يدويا على الأقراص المغناطيسية التي تحتوي على المعلومات.

من خلال ما تقدم، يتضح أن التعريف السابق يتسع ليشمل جميع صور الكتابة الالكترونية، والمحررات الالكترونية المعروفة حاليا، أو تلك التي قد تسفر عنها التقنيات الحديثة مستقبلا[1].

وفي هذا الصدد، يمكن القول أن من أهم التعاريف التي خصها الفقه بالكتابة الالكترونية ذلك الذي يعتبرها: "مجموعة من الحروف أو الأرقام أو من الكلمات أو الرموز، التي تعبر عن معنى محدد دقيق، أيا كانت ركيزتها، وأيا كان شكلها ووسيلة نقلها، حتى ولو لم تظهر بصورة مادية محسوسة، أو مجردة للقارئ دون الاستعانة بوسائط أخرى".

بهذا يتضح أن الكتابة الالكترونية لا تخرج عن التعاريف السابقة، فهي تتميز بخاصية أساسية تشمل على دعامة إلكترونية، فالذي يميز الكتابة الالكترونية ليس مضمونها، ذلك أن هذا المضمون لا يختلف عن مضمون الكتابة التقليدية، وعليه يكمن التمييز في نوع الدعامة أو الوسيط الذي ترد عليه.

ترتيبا على ما سبق، فإنه يمكن تعريف الكتابة الالكترونية بأنها: "كل رموز وأرقام تدون آليا على دعامة الكترونية وتدل على معنى مفهوم"[2].

البند الثاني : التعريف التشريعي للكتابة الالكترونية.

بعد أن أدركت التشريعات على المستوى الدولي، الإقليمي، والوطني أن الأمان الممنوح للمعاملات الإلكترونية يتوقف على ثقة المتعاملين بها عمدت إلى مواكبة التطور التقني الهائل، الذي شهده مجال تقنيات الإتصال عن بعد، فأصدرت نصوصا قانونية لإماطة

[1]- نور خالد عبد المحسن العبد الرزاق، المرجع السابق، ص،ص.382-383.
[2]- علاء حسن مطلق التميمي، المستند الالكتروني، عناصره وتطوره وحجيته في الإثبات، المرجع السابق، ص.42؛ نور خالد عبد المحسن العبد الرزاق، المرجع السابق، ص.389.

اللثام عن الغموض والجدل الذي يكتنف المعاملات الإلكترونية، بما فيها الكتابة الإلكترونية التي تعد دعامة تلك المعاملات[1].

وفي هذا الصدد يلاحظ أن قانون الأونسترال النموذجي بشأن التجارة الالكترونية تعرض لمسألة الكتابة في المادة السادسة منه والتي تنص على أنه :

"1- عندما يشترط القانون أن تكون المعلومات مكتوبة تستوفي رسالة البيانات ذلك، الشرط إذا تيسر الاطلاع على البيانات الواردة فيها، على نحو يتيح استخدامها بالرجوع إليها لاحقا.

2- تسري أحكام الفقرة الأولى سواء اتخذ الشرط المنصوص عليه فيها شكل التزام، أو اكتفى في القانون بمجرد النص على العواقب التي تترتب إذا لم تكن المعلومات مكتوبة."[2]

هذا بالنسبة للتشريعات الدولية، أما بالنسبة للتشريعات المقارنة، فيلاحظ أن المشرع الفرنسي قد اعترف بمسألة الكتابة الالكترونية، بحيث وسع من مفهوم الكتابة أثناء تعريفه للدليل الكتابي ليشمل إضافة إلى الكتابة الخطية، الكتابة الالكترونية، وأي شكل آخر يظهر في المستقبل، وهذا ما أورده في نص المادة 1316من تعديل القانون المدني رقم 2000/230 الصادر بتاريخ 13 مارس 2000، والتي نصت على أن: "الإثبات الخطي أو الإثبات بالكتابة ينتج من تدوين للحروف أو العلامات أو الأرقام، أو أي رموز أو إشارات ذات دلالة تعبيرية مفهومة وواضحة، أيا كانت دعامتها أو وسيلة نقلها"[3].

---

[1]- للإشارة فإنه بخصوص وضع تعريف محدد لاصطلاح الكتابة الالكترونية نجد أن غالبية التشريعات الدولية والإقليمية والعربية قد قصدت في البداية عدم وضع تعريف محدد للكتابة الالكترونية، وذلك لغرض استيعاب أي شكل يظهر في المستقبل مع تطور التقنيات، إلا أن هذه التشريعات وجدت نفسها أمام ضرورة تحديد معيار تعريفي للكتابة الالكترونية وذلك باستخدام عبارات، وكلمات مفتاحية في نصوصها القانونية على نحو يجعلها تستوعب التطورات التي قد تطرأ في المستقبل. لتفاصيل أكثر يراجع، علاء حسن مطلق التميمي، المستند الالكتروني، عناصره وتطوره وحجيته في الإثبات، المرجع السابق، ص.37 وما يليها.

[2]- قانون الأنيسترال النموذجي بشأن التجارة الالكترونية لسنة 1996، سابق الإشارة إليه.

[3] -Art 1316 c.civ.fr (loi 2000-230 du 13mars 2000 art.1 JO du 14 mars 2000) dispose que: " La preuve littéral, ou prevue par écrit , résulte d'une suite de lettres, de caractères, de chiffres ou de tous acute signes ou symboles dotés d'une signification intelligible quels que soient leur supports et leur modalités de transmission".

وما يلاحظ على نص هذه المادة أنه جاء عاما بما يسمح ليس فقط بإدخال الكتابة الالكترونية إلى جانب الكتابة التقليدية، بل كذلك باستيعاب مختلف صور الكتابة التي يمكن استحداثها مستقبلا[1].

إلى جانب التشريع الفرنسي، عرف قانون الإثبات الاتحادي للولايات المتحدة الأمريكية والصادر بتاريخ 1 ديسمبر 2006 الكتابة في المادة 1001 منه إذ نص: "الكتابة والتسجيلات التي تتألف من الرسائل أو الكلمات أو الأرقام أو ما يعادلها، أو ما أنزل بكتابة يدوية أو طباعة أو تصوير أو اندماج مغناطيسي أو تسجيل إلكتروني أو ميكانيكي، أو أي شكل آخر من تجميع البيانات"[2].

أما بالنسبة لموقف التشريعات العربية من الكتابة الالكترونية فيلاحظ أن التشريع المصري قد أدرك سلبيات عدم تحديد مفهوم للكتابة الالكترونية فسارع إلى إيراد تعريف لها عندما أصدر قانون تنظيم التوقيع الالكتروني رقم 15 لسنة 2004، بحيث نص في المادة الأولى الفقرة 5 من هذا القانون على أنه يقصد بالكتابة الالكترونية: "كل حروف أو رموز أو أرقام أو علامات أخرى تثبت على دعامة إلكترونية، أو رقمية أو ضوئية أو أية وسيلة أخرى مشابهة، وتعطي دلالة قابلة للإدراك"[3].

حسب هذا التعريف فإن الكتابة الالكترونية تتشكل من تسلسل الأحرف الأبجدية أو الأرقام، أما الرموز والعلامات الأخرى، فالمقصود بها كافة الطرق غير الأبجدية التي تعبر عن الفكر، كالإشارات المستخدمة في ذاكرة الحاسب الآلي، أو الرموز أو القرص الممغنط (CD).

بهذا يتبين أن مفهوم الكتابة يستقل عن طبيعة الإشارات المؤلفة منها، ولذلك اشترط المشرع المصري في الأحرف أو الأرقام أو الرموز أن تعطي دلالة قابلة للإدراك، أي أن

[1]- أسامة أبو الحسن مجاهد، المرجع السابق، ص،ص.341-342.
[2]- نقلا عن علاء حسين مطلق التميمي، الأرشيف الالكتروني وكيفية المحافظة على المستند الإلكتروني عبر الزمن، دراسة مقارنة، المرجع السابق، ص.98.
[3] - القانون رقم 15 لسنة 2004 المتعلق بتنظيم التوقيع الالكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات، سابق الإشارة إليه.

تشكل تلك الأحرف أو الأرقام أو الرموز معنى يفهمه العقل البشري، بحيث تكون الكتابة الالكترونية ذات معنى ومدلول.

بهذا يتبين أن المعيار الذي اتخذه المشرع المصري لتحديد الكتابة الالكترونية غير محدد على سبيل الحصر، حيث اشترط أن تثبت على دعامة إلكترونية أو رقمية أو ضوئية، ثم أضاف بعدها مصطلح وأية وسيلة أخرى مشابهة... بشرط أن تعطي هذه الوسيلة الأخرى المشابهة دلالة قابلة للإدراك[1].

هذا عن المشرع المصري، أما بالنسبة للتشريع الأردني، فيلاحظ أن قانون المعاملات الإلكترونية الأردني[2]، لم يتطرق إلى تعريف الكتابة الالكترونية بشكل مباشر، وإنما تطرق إليها من خلال تعريفه لاصطلاح (المعلومات)، وذلك بحسب نص المادة الثانية منه بحيث يقصد بالمعلومات: "البيانات والنصوص والصور والأشكال، والأصوات والرموز وقواعد البيانات وبرامج الحاسوب، وما شابه ذلك"، فالبيانات والنصوص المذكورة عادة تتكون من الأحرف والأرقام التي تشكل في النهاية كتابة مقروءة، وبما أنها تثبت على وسيط إلكتروني فإنها تعتبر كتابة إلكترونية.

وبعد أن تم تحديد موقف التشريع المصري والأردني من الكتابة الالكترونية فإنه ينبغي التساؤل عن موقف المشرع الجزائري من هذه الكتابة.

للإجابة على هذا السؤال، يمكن القول أن المشرع الجزائري هو الآخر قد ساير ركب التشريعات المقارنة بما فيها الأجنبية أو العربية، واعترف بالكتابة الالكترونية سنة 2005 بحيث كرس ذلك من خلال تعديله لقواعد الإثبات المنصوص عليها في القانون المدني الجزائري، بموجب قانون 05 – 10 المؤرخ في 20 يونيو 2005 المعدل والمتمم للقانون المدني، بحيث أورد في المادة 323 مكرر من القانون المدني تعريفا للكتابة فذكر: "ينتج

[1]- علاء حسن مطلق التميمي، المستند الالكتروني، عناصره وتطوره وحجيته في الإثبات، المرجع السابق، ص،ص.40-41.

[2] - القانون رقم 85 لسنة 2001 المتعلق بالمعاملات الالكترونية الأردني، سابق الإشارة إليه.

الإثبات بالكتابة من تسلسل حروف وأوصاف وأرقام وأية علامات أو رموز ذات معنى مفهوم مهما كانت الوسيلة التي تتضمنها، وكذا طرق إرسالها"[1].

حسب هذا النص، فإن المقصود بالكتابة في الشكل الالكتروني[2] تسلسل الحروف أو الأوصاف أو الأرقام، أو أية علامات أو رموز مكتوبة على دعامة الكترونية، بغض النظر عن طرق إرسالها، المهم أن تكون ذات معنى مفهوم، ومثال ذلك المعلومات والبيانات التي تحتويها الأقراص الصلبة أو المرنة، أو تلك التي يتم كتابتها بواسطة الكمبيوتر وإرسالها ونشرها على شبكة الانترنت.

الملاحظ أن نص المادة 323 مكرر من القانون المدني يعتبر أول نص عرف من خلاله المشرع الجزائري الكتابة التي يمكن استعمالها كوسيلة إثبات للتصرفات القانونية بصفة عامة، والتصرفات الالكترونية بصفة خاصة، وذلك محاولة منه لتفادي الجدل الذي قد يثور حول الاعتراف بالكتابة الالكترونية كدليل إثبات، كون أن المفهوم التقليدي للكتابة كان مرتبطا بشكل وثيق بالدعامة المادية أو الورقية، إلى درجة عدم إمكانية الفصل بينهما. وعليه، فإن القانون الجزائري لم يعترف بالكتابة المدونة على دعامة الكترونية افتراضية، إلا بموجب نص المادة 323 مكرر المستحدثة سنة 2005.

---

[1]- ما يلاحظ على هذا النص أن المشرع الجزائري استعمل في تعريف الكتابة عبارة ، "أيا كانت الوسيلة التي تتضمنها" والصحيح هو عبارة "أيا كانت الدعامة التي تتضمنها" حسب الترجمة الفرنسية للنص.

"Quels que soient leur support"

حيث أن صياغة المادة 323 مكرر من القانون المدني باللغة الفرنسية تكون كالآتي :

Art 323 bis (Loi N° 05 – 10 DU 20 JUIN 2005) : "La preuve par écrit résulte d'une suite de lettres de caractères, ou de chiffres ou de tous autre signe ou symboles doté d'une signification intelligible quels que soient leur supports et leur modalités de transmission".

يراجع في ذلك ، قانون رقم 05-10 المؤرخ في 20 يونيو 2005 المعدل والمتمم للقانون المدني الجزائري، سابق الإشارة إليه.

[2] - استعمل المشرع الجزائري أيضا مصطلح الكتابة في الشكل الالكتروني، وليس الكتابة الالكترونية وحسنا ما فعل لأن شكل الكتابة هو الذي يتغير وليس طبيعتها، ونفس الاتجاه سلكه قبله المشرع الفرنسي وفي هذا الشأن يقـول الأستـاذ (Eric Caprioli):

"Nous préférons également l'expression écrit sous forme électronique a celle d'écrit électronique car ne sont que les formes de l'écrit qui changent et non sa nature, s'il peut exister plusieurs formes de preuve littérale, les écrits à condition qu'ils remplissent les exigences fixées par le législation sont de même nature et d'une force probante équivalente".

Cf . Eric Caprioli, Le juge et la preuve électronique, réflexion sur le projet de loi portant adaptation de la preuve aux technologies de l'information et relatif à la signature électronique, www.caprioli-avocats.com. Date de consultation le site 25-3-2017 à 15 :30.

زيادة على ذلك، فإن مفهوم الكتابة الذي جاءت به المادة 323 مكرر من القانون المدني الجزائري هو مفهوم قابل للتوسع، ذلك أن صياغتها بالنص على أنه: «ينتج الإثبات بالكتابة من تسلسل حروف أو أرقام أو أية علامات أو رموز ذات معنى مفهوم مهما كانت الوسيلة التي تتضمنها » يفهم منه أن المشرع الجزائري يعتد لإثبات التصرفات القانونية بأية دعامة كانت عليها الكتابة سواءا أكانت على الورق، أو على القرص المضغوط أو على القرص المرن.

ويتسع المفهوم إلى كل الدعائم التي يمكن أن تفرضها التطورات التكنولوجية في المستقبل، وهذا ما يدل على أن المشرع الجزائري قد أخذ بالمفهوم الموسع للكتابة شأنه في ذلك شأن باقي التشريعات الأجنبية والعربية المقارنة.

زيادة على ذلك فإن هذا المبدأ الذي أخذ به المشرع الجزائري في عدم التفرقة بين الدعامات الالكترونية سماه الفقه الفرنسي بـــ :

« Principe de neutralité technique et non-discrimination a l'encontre d'un support ou d'un média. »[1].

والمقصود به مبدأ الحياد التقني وعدم التمييز بين أي دعامة ووسيلة إعلام .

هذا ويعتد المشرع الجزائري أيضا في مفهوم الكتابة بأية وسيلة من وسائل نقلها فيشمل بذلك تعريف الكتابة في الشكل الالكتروني التي تكون منقولة عن طريق اليد، والتي تكون منقولة على شبكات الاتصال المختلفة.

زيادة على ذلك فإن اشتراط المشرع أن تكون هذه الكتابة مفهومة (Signification intelligible)[2] معناه يجب أن تكون هذه الأحرف أو الأشكال أو الإشارات أو الرموز أو الأرقام لها دلالة قابلة للإدراك وللقراءة، والمقصود بذلك أنه لو كان المحتوى المعلوماتي للكتابة المعبر عنها في الشكل الالكتروني مشفرا، بحيث لا يمكن إدراك معانيه

[1]- لقد كرس المشرع الفرنسي المبدأ ذاته في نص المادة 1316 من القانون المدني الفرنسي.
[2] - باسم رمزي معروف دياب، المرجع السابق، ص.55.

من قبل الإنسان بل من قبل الحاسوب فقط، فإن هذه الكتابة لا تصلح لتكون دليل إثبات، لأنه لا يمكن للقاضي إدراك محتواها في حالة النزاع[1].

يلاحظ مما سبق ذكره عن موقف التشريعات العربية من الكتابة الالكترونية أن قوانين المعاملات الالكترونية العربية بما فيها موقف المشرع الجزائري في القانون المدني، جاءت كلها متأثرة بقانون الأونيسترال النموذجي للتجارة الالكترونية، الذي بين المراد من رسالة البيانات بأنها: "المعلومات التي يتم إنشائها أو إرسالها أو استلامها أو تخزينها بوسائل الكترونية أو ضوئية أو بوسائل متشابهة، بما في ذلك على سبيل المثال لا الحصر تبادل البيانات الالكترونية أو البريد الالكتروني أو البرق أو التلكس أو النسخ البرقي"[2]. كما ذكر في المادة 6 منه: "وعندما يشترط القانون أن تكون المعلومات مكتوبة تستوفي رسالة البيانات ذلك الشرط إذا تيسر الاطلاع على البيانات الواردة فيها على نحو يتيح استخدامها بالرجوع إليها لاحقا"[3].

الفرع الثاني : التوقيع الالكتروني.

يعتبر التوقيع الالكتروني من ثاني الضوابط الموضوعية الواجب توافرها في المستند الالكتروني، ذلك أن الكتابة لا تعتبر دليلا كاملا في الإثبات إلا إذا كانت مذيلة بالتوقيع سواء كان هذا التوقيع في صورة إمضاء أو ختم أو بصمة، وعليه يعتبر التوقيع بمثابة العنصر الثاني من عناصر الدليل الكتابي المعد أصلا للإثبات، فهو الذي ينسب المستند إلى من وقعه حتى ولو كان مكتوبا بخط غيره[4]، ناهيك عن أنه الشرط الوحيد لصحة الورقة العرفية، وفقا لما تقره الكثير من التشريعات[5].

---

[1]-Cf. Eric Caprioli, op. cit, p.06

[2]- المادة الثانية من قانون الأونيسترال النموذجي بشأن التجارة الالكترونية 1996، سابق الإشارة إليه.

[3]- المادة 1/6 من قانون الأونيسترال النموذجي بشأن التجارة الالكترونية،1996، سابق الإشارة إليه..

[4]- لزهر بن سعيد، المرجع السابق، ص. 152

[5] - للإشارة فإن الكثير من التشريعات قد أقرت هذا المبدأ بما فيها المشرع الجزائري، بحيث نص في المادة 327 فقرة 2 من القانون المدني الجزائري المعدل والمتمم على أنه : "يعتبر العقد العرفي صادرا ممن كتبه أو وقعه أو وضع عليه بصمة إصبعه ما لم يذكر صراحة ما هو منسوب إليه، أما ورثته أو خلفه فلا يطلب منهم الإنكار ويكفي أن يحلفوا يمينا بأنهم لا يعلمون أن الخط أو الإمضاء أو البصمة هو لمن تلقوا منه هذا الحق.
ويعتد بالتوقيع الالكتروني وفق الشروط المذكورة في المادة 323 مكرر1 أعلاه".

هذا ولقد ظهرت الحاجة إلى التوقيع الالكتروني نظرا لانتشار الحاسب الآلي والاعتماد عليه في كافة مناحي الحياة، ويظهر ذلك جليا وبصفة خاصة مع تعميم نظم المعالجة الالكترونية للمعلومات، هذه النظم التي بدأت تغزوا الشركات والإدارات والبنوك، وهو الأمر الذي جعل الواقع العلمي يفرز طرق ووسائل حديثة في التعامل، لاسيما بعد أن أصبح التوقيع اليدوي عقبة من المستحيل تكييفها مع النظم الحديثة، ولهذا تم الاتجاه نحو بديل لذلك التوقيع اليدوي الذي أصبح لا يتماشى وثورة المعلومات، فتم بذلك استحداث نظام بديل ألا وهو نظام التوقيع الالكتروني[1].

هذا النظام الذي بات يحظى بأهمية قصوى في كافة المعاملات القانونية، سواء كانت مدنية أو تجارية أو إدارية، حيث بدأ الاعتماد عليه بشكل كبير في عقود التجارة عبر الانترنيت، وهي ما يطلق عليها بعقود التجارة الالكترونية، وذلك كوسيلة لحماية هذه المعاملات والعقود[2].

وبالإضافة إلى ذلك فقد اتجهت جهات الإدارة إلى التوقيع الالكتروني لحماية معاملاتها التي تتم بطريق الحاسب الآلي والانترنت في إطار تحولها إلى ما يسمى بالحكومة الالكترونية سواء كانت الإدارة في نطاق القطاع الخاص، أو العام[3].

إن أهمية التوقيع الإلكتروني دفعت الفقه والتشريع إلى الإهتمام به، ولكن إلى أي مدى بلغ نطاق هذا الإهتمام؟، ما هي صور هذا التوقيع؟ وماهي الخصائص المميزة له؟

هذا ما سيتم التعرض له من خلال التطرق إلى مفهـــوم التوقيـــع الإلكترونـــي **(البند الأول)**، وصوره **(البند الثاني)**.

---

[1]- عبد الفتاح بيومي حجازي، التوقيع الالكتروني في النظم القانونية المقارنة، دار الفكر الجامعي، الإسكندرية، مصر، د.س.ن، ص.07؛

Isabelle De Lamberterie, les actes authentiques électroniques, la documentation française, paris , 2002, p.163.

[2]- عبد الفتاح بيومي حجازي، التوقيع الالكتروني، المرجع السابق، ص، ص.8 – 9.

[3]- تأتي أهمية التوقيع الالكتروني في نطاق الحكومة الالكترونية في أنه يعتبر الوسيلة لكي تكتسب المستندات والمخرجات الخاصة بمعاملات الأشخاص لدى الحكومة الصفة الرسمية، حين تحمل التوقيع الالكتروني للمسؤول أو لمدير الإدارة في الحكومة الالكترونية....لتفاصيل أكثر يراجع، عبد الفتاح بيومي حجازي، التجارة الالكترونية في القانون العربي النموذجي لمكافحة جرائم الكمبيوتر والأنترنت، ط1، دار الفكر الجامعي، الإسكندرية، 2006، ص،ص.228 – 229.

البند الأول: مفهوم التوقيع الإلكتروني.

لقد عرف الفقه التوقيع بصفة عامة على أنه علامة أو إشارة خاصة ومميزة للشخص الموقع، يضعها على مستند أو وثيقة للتعبير عن إرادته في الالتزام بمضمون المستند، وإقراره لمحتواه وبواقعة صدوره عنه، وهو بذلك وسيلة التعرف على الموقع وتحديد هويته وشخصيته[1].

هذا عن تعريف التوقيع عموما، أما عن تعريف التوقيع الالكتروني فقد حاول الفقه إعطاء تعريفات مختلفة له، بحيث عرفه جانب من الفقه[2] بأنه: "كل إشارات أو رموز أو حروف مرخص بها من الجهة المختصة باعتماد التوقيع، ومرتبطة ارتباطا وثيقا بالتصرف القانوني، تسمح بتمييز شخص صاحبها، وتحديد هويته، وتتم دون غموض عن رضاه بهذا التصرف القانوني".

هذا وقد عرفه جانب آخر على أنه: "التوقيع الناتج عن إتباع إجراءات محددة تؤدي في النهاية إلى نتيجة معروفة مقدما، بحيث يكون مجموع هذه الإجراءات هو البديل الحديث للتوقيع بمفهومه التقليدي، أو ما يسميه البعض بالتوقيع الإجرائي أو الالكتروني"[3].

في حين عرفه جانب آخر بأنه: "مجموعة الإجراءات أو الوسائل التقنية التي يتاح استخدامها عن طريق الرمز أو الأرقام أو الشفرات، بقصد إخراج علامة مميزة لصاحب الرسالة التي نقلت الكترونيا"[4].

استنادا للتعاريف السابقة، يتبين أن التوقيع الإلكتروني يتميز عن غيره من التوقيعات الأخرى ببعض العناصر والخصائص، أهمها:

---

[1]- عبد الفتاح بيومي حجازي، مقدمة في التجارة الالكترونية العربية، الكتاب الأول، (شرح المبادلات والتجارة الالكترونية التونسي)، دار الفكر الجامعي، الإسكندرية، 2002، ص.86.

[2]- Cf. Olivier D'Auzon, les droits des internautes a l'ère de l'économie numérique, éditions du puits fleuri, France, 2009, p,p. 85-86; Isabelle De Lamberterie, op .cit , p. 163.

[3]- عبد الفتاح بيومي حجازي، التوقيع الالكتروني في النظم القانونية المقارنة، المرجع السابق، ص.07.

[4]- عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية، الكتاب الثاني، الحماية الجنائية لنظام التجارة الالكترونية، دار الفكر الجامعي، الإسكندرية، 2002، ص.72.

- أنه لا يتم عبر وسيط مادي أي دعامة ورقية، بل يتم كليا أو جزئيا عبر وسيط الكتروني من خلال أجهزة الكمبيوتر أو عبر الأنترنت،[1] كما أنه يتكون من عناصر منفردة، وسمات ذاتية خاصة بالموقع تتخذ شكل حروف أو أرقام أو رموز أو إشارات أو نبرات صوت أو غيرها، وذلك كله حتى يحدد شخصية الموقع، ويبين هويته ويميزه عن غيره من الأشخاص، وبالتالي يتضح أن وجود التوقيع الإلكتروني يعبر عن رضا الموقع والتزامه بالتصرف القانوني الذي يتضمنه المستند الالكتروني[2].

هذا من الناحية الفقهية، أما من الناحية التشريعية فيلاحظ أن معظم التشريعات التي نظمت مسألة التوقيع الالكتروني جاءت بتعريفات متشابهة إلى حد ما، ولكن مع اختلاف في الألفاظ المستخدمة، وللإشارة فإن هناك بعض التشريعات التي تناولت تنظيم التوقيع الالكتروني في قانون خاص بالتوقيع الالكتروني مثل: القانون النموذجي للأمم المتحدة بشأن التوقيعات الالكترونية لسنة 2001، والتوجيه الأوربي رقم 99– 1993 وقانون التوقيع الالكتروني المصري رقم 15 لسنة 2004، وكذا القانون الجزائري 15-04 المتعلق بالتوقيع والتصديق الالكترونيين، بينما قامت بعض التشريعات الأخرى بتنظيم التوقيع الالكتروني ضمن قانون موحد للمعاملات والتجارة الالكترونية، ومن ذلك مثلا القانون التونسي رقم 83 لسنة 2000 بشأن المبادلات والتجارة الالكترونية، والقانون الأردني رقم 85 لسنة 2001 بشأن المبادلات والتجارة الالكترونية، والقانون الإماراتي رقم 02 لسنة 2002 بشأن المعاملات والتجارة الالكترونية.

فبالنسبة لمفهوم التوقيع الالكتروني في قانون الأونيسترال النموذجي فإنه ينبغي التمييز بين قانون الأونيسترال المتعلق بالتجارة الإلكترونية، وقانون الأونيسترال المتعلق بالتوقيع الإلكتروني، بحيث لم يتطرق قانون الأونيسترال المتعلق بالتجارة الإلكترونية

[1]- بودالي محمد، التوقيع الالكتروني، إدارة ، مجلة المدرسة الوطنية للإدارة، مجلة سداسية تصدر عن مركز التوثيق والبحوث الإدارية، مج 13، ع 02، العدد 26، 2003، ص.57.

[2]- خالد علي العراقي علي إسماعيل، مكافحة جرائم التوقيع الالكتروني بدولة الإمارات العربية المتحدة، مجلة الفكر الشرطي، دورية ربع سنوية علمية محكمة ومفهرسة تعني بالأبحاث الشرطية تصدر عن مركز بحوث الشرطة للإمارات العربية المتحدة، مج الثاني والعشرون، ع 85، أبريل سنة 2003، ص،ص.121 – 122.

لتعريف التوقيع الالكتروني، بل اكتفى بتحديد الشروط الواجب توافرها فيه[1]، وذلك بخلاف القانون الأونسترال النموذجي المتعلق التوقيعات الالكترونية الصادر سنة 2001، بحيث عرف هذا الأخير التوقيع الالكتروني في المادة الثانية منه، والتي جاء فيها: "التوقيع الالكتروني يعني 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 رسالة البيانات"، كما عرف هذا القانون الموقع في الفقرة (د) من نفس المادة واعتبره: "شخص حائز على بيانات إنشاء توقيع ويتصرف إما أصالة عن نفسه، وإما نيابة عن الشخص الذي يمثله"[2].

وما يظهر عن التعريفين السابقين أن القانون النموذجي قد اهتم بمسألتين وهما تعيين هوية الشخص الموقع، وبيان موافقته على المعلومات الواردة في المستند، وهو بذلك انسجم مع الأصل العام للتوقيع في الدلالة على شخص الموقع، وللتأكيد على أن إرادته قد اتجهت للالتزام بما وقع عليه[3].

هذا عن تعريف قانون الأونسترال للتوقيع الإلكتروني، أما عن التعريف الوارد في التوجيه الأوربي رقم 93 – 1999 بشأن التوقيع الالكتروني[4]، فيلاحظ أن المادة الثانية الفقرة 01 منه، عرفت التوقيع الإلكتروني بأنه : " بيان أو معلومة معالجة الكترونيا ترتبط منطقيا بمعلومات أو بيانات الكترونية أخرى (كالرسالة أو محرر)، والتي تصلح كوسيلة لتمييز الشخص وتحديد هويته".

---

[1]- تنص المادة 07 من قانون الأونيسترال النموذجي بشأن التجارة الالكترونية لسنة 1996 ، سابق الإشارة إليه على أنه :
"عندما يشترط القانون وجود توقيع من شخص يستوفي ذلك الشرط بالنسبة إلى رسالة البيانات إذا :
أ-استخدمت طريقة لتعيين هوية ذلك الشخص والتدليل على موافقة ذلك الشخص على المعلومات الواردة في رسالة البيانات.
ب-كانت تلك الطريقة جديرة بالتعويل عليها بالقدر المناسب للغرض الذي أنشأت أو بلغت من أجله رسالة البيانات في ضوء كل الظروف بما في ذلك أي اتفاق متصل بالأمر....."
لتفاصيل أكثر يراجع، محمد خالد جمال رستم، التنظيم القانوني للتجارة والإثبات الالكتروني في العالم، منشورات الحلبي الحقوقية، لبنان، 2006، ص 302 .

[2]- قانون الأونيسترال النموذجي بشأن التوقيع الإلكتروني الصادر سنة 2001، سابق الإشارة إليه.

[3]- لزهر بن سعيد، المرجع السابق، ص،ص. 153 – 154.

[4]- التوجيه الأوربي رقم 99/93 الصادر سنة 1999 الصادر عن المجلس الأوربي و المتعلق بالتوقيعات الالكترونية.

من خلال هذا التعريف يتبين أن التوجيه الأوربي قد وضع تعريفا وصفيا للتوقيع يسمح بالاعتراف به بمجرد أداءه لوظائفه، وهي تمييز وتحديد هوية موقعه والتعبير بوضوح عن الرضا، والقبول بمضمون المستند الذي تم إصدار التوقيع بشأنه[1].

ولقد طبق المشرع الفرنسي التعليمات، والأحكام الواردة بالتوجيه الأوربي رقم 93– 1999 بشأن التوقيع الالكتروني، وتطبيقا لذلك صدر القانون الفرنسي رقم 2000 – 230[2]، والذي عدل من نصوص القانون المدني الفرنسي، حيث عرف التوقيع الالكتروني في المادة 1316 الفقرة 04 منه بأنه: "التوقيع الضروري لاكتمال التصرف القانوني، والذي يحدد هوية من يحتج به عليه، ويعبر عن رضاء الأطراف بالنسبة للالتزامات الناشئة عن هذا التصرف، عندما يتم التوقيع بمعرفة موظف عام يكون التصرف رسمي، وعندما يكون التوقيع الكترونيا ينبغي استخدام وسيلة آمنة لتحديد الشخص، بحيث تضمن صلته بالتصرف الذي وقع عليه ويفترض أمان هذه الوسيلة، ما لم يوجد دليل مخالف.

بمجرد وضع التوقيع الالكتروني الذي يتحدد بموجبه الشخص الموقع ويضمن سلامة التصرف، وذلك بالشروط التي يحددها مرسوم يصدر من مجلس الدولة"[3].

من خلال هذا النص يتضح أن المشرع الفرنسي قد وضع مفهوما موسعا للتوقيع، ولم يفرق بين التوقيع التقليدي والتوقيع الالكتروني[4].

---

[1]- سمير حامد عبد العزيز الجمال، التعاقد عبر تقنيات الاتصال الحديثة (دراسة مقارنة)، دار النهضة العربية، القاهرة، 2006، ص.208.

[2]- صدر هذا القانون في 13 مارس سنة 2000 مشار إليه من طرف.

- Olivier D'Auzon ,op .cit ,p. 96-97 .

[3]- Art 1316-4 c.civ.fr crée par loi n°2000-230 du 13 mars 2000-art .4 JORF 14 mars 2000 dispose que: "La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'oppose, elle manifeste le consentement des parties aux obligation 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 procède fiable identification garantissant sou lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est crée, l'identité du signature assurée et intégrité de l'acte garantie dans des conditions fixées par décret en conseil d'état".

[4]- للإشارة فإن هناك من يرى أيضا أن هذا التعريف قد ركز على وظائف التوقيع ولم يبين الوسائل الفنية التي تضمن فعاليته في اثبات شخصية المتعاقد. لتفاصيل أكثر يراجع، باطلي غنية، حجية المستند الالكتروني، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية، كلية الحقوق، جامعة الجزائر، ع3، سبتمبر ، س2011، ص.175.

هذا بالنسبة للتشريعات الأجنبية، أما بالنسبة للتشريعات العربية، فيلاحظ أن أغلبيتها نصت على التوقيع الالكتروني، حيث أشار إليه بداية القانون التونسي سنة 2000[1]، كما تطرق له قانون المعاملات الإلكترونية الأردني وعرفه في المادة9/2 بأنه : "البيانات التي تتخذ هيئة حروف أو أرقام أو رموز أو إشارات أو غيرها، وتكون مدرجة بشكل إلكتروني أو رقمي أو ضوئي أو أي وسيلة أخرى مماثلة في رسالة معلومات أو مضافة عليها أو مرتبطة بها، ولها طابع يسمح بتحديد هوية الشخص الذي وقعها ويميزه عن غيره من أجل توقيعه وبغرض الموافقة على مضمونه"[2].

للإشارة فقد أضحى مضمون هذا الفقرة بعد إدخال قانون رقم 15 لسنة 2015 حيز التنفيذ كالآتي .التوقيع الإلكتروني: "البيانات التي تتخذ شكل حروف أو أرقام أو إشارات أو غيرها وتكون مدرجة في سجل إلكتروني أو أي وسيلة أخرى مماثلة في السجل الإلكتروني، أو تكون مضافة عليه أو مرتبطة به بهدف تحديد هوية صاحب التوقيع وانفراده باستخدامه وتمييزه عن غيره."[3]

هذا وقد عرف قانون المعاملات والتجارة الالكترونية الإماراتي التوقيع الالكتروني في المادة الثانية[4] ، والتي جاء فيها بأنه: "توقيع مكون من حروف وأرقام ورموز وأصوات أو نظام معالجة ذي شكل الكتروني، وملحق، أو مرتبط منطقيا برسالة الكترونية، وممهور بنية توثيق أو اعتماد تلك الرسالة".

---

[1]- إذا رجعنا إلى القانون التونسي رقم 83 لسنة 2000 والمتعلق بالمبادلات والتجارة الالكترونية، سابق الإشارة إليه. فإننا نجد أن المشرع التونسي قد أشار إلى مسألة التوقيع الالكتروني في هذا القانون، بالرغم من أنه لم يعرف هذا التوقيع بنص صريح، بل تناول في هذا القانون تعريف العناصر المؤدية إلى هذا التوقيع معرفا بذلك مسألة إحداث الإمضاء بأنها : "مجموعة وحيدة من عناصر التشفير الشخصية أو مجموعة من المعدات المهيأة خصيصا لإحداث إمضاء إلكتروني"، وحتى قبل هذا التاريخ بموجب القانون عدد 57 لسنة 2000 المؤرخ في 13 جوان 2000 المتعلق بتنقيح بعض الفصول من مجلة الالتزامات والعقود نجد أنه نص في الفصل 453 الفقرة الثانية على أنه : " يتمثل الإمضاء في وضع اسم أو علامة خاصة بخط يد العاقد نفسه مدمجة بالكتب المرسوم بها أو إذا كان إلكترونيا في استعمال منوال تعريف موثوق به يتضمن صلة الإمضاء المذكور بالوثيقة الالكترونية المرتبطة به".
مشار إليه من طرف، عبد الفتاح بيومي حجازي، التوقيع الالكتروني في النظم القانونية المقارنة، المرجع السابق، ص.96؛ معوان مصطفى، المرجع السابق، ص.713 وما يليها.

[2]- القانون رقم 85 لسنة 2001، و المتعلق بالمعاملات الالكترونية الأردني، سابق الإشارة إليه.

[3]- قانون رقم 15 لسنة 2015 المتعلق بالمبادلات الالكترونية الأردني، سابق الإشارة إليه.

[4] - قانون إمارة دبي رقم 2 لسنة 2002 بشأن المعاملات والتجارة الالكترونية، سابق الإشارة إليه.

وبالمثل اعترف المشرع المصري بالتوقيع الالكتروني سنة 2004، وعرفه في نص المادة الأولى من القانون المتعلق بتنظيم التوقيع الالكتروني وإنشاء هيئة صناعة تكنولوجيا المعلومات بأنه: "ما يوضع على المحرر الالكتروني ويتخذ شكل حروف أو أرقام أو إشارات أو غيرها، ويكون له طابع منفرد يسمح بتحديد شخص الموقع ويميزه عن غيره"[1].

بعد استعراض موقف التشريعات الأجنبية والعربية من مفهوم التوقيع الالكتروني، فما هو موقف المشرع الجزائري حول هده المسألة؟

للإجابة على هذا التساؤل فانه يمكن القول أن التشريع الجزائري هو الآخر قد اعتد بالتوقيع الالكتروني وعرفه، وذلك على الرغم من أن الجزائر كانت متأخرة نوعا ما في هذا المجال مقارنة بالتشريعات العربية كتونس والإمارات مثلا، إذ وبعدما اعترف المشرع الجزائري بموجب المادة 323 مكرر من القانون المدني الجزائري بالكتابة الالكترونية وبالبصمة الالكترونية سنة 2005، تدخل بموجب المرسوم التنفيذي رقم 07 – 162[2] وعرفه في نص المادة 03 مكرر على النحو التالي : "التوقيع الالكتروني : هو معطى ينجم عن استخدام أسلوب عمل يستجيب للشروط المحددة في المادتين 323 مكرر و323 مكرر1 من الأمر رقم 75 – 58 المؤرخ في 16 سبتمبر 1975 والمذكور أعلاه".

من خلال هذا التعريف يتبين أن المشرع الجزائري أحال إلى نصوص المادتين 323 مكرر و323 مكرر1 من القانون المدني[3]، كما أدرج المشرع الجزائري في نفس المرسوم التنفيذي تعريفا للموقع، بحيث عرفه في الفقرة الثالثة من نفس المادة بأنه : "شخص طبيعي يتصرف لحسابه الخاص أو لحساب الشخص الطبيعي أو المعنوي الذي يمثله، ويضع موضوع التنفيذ جهاز إنشاء التوقيع الالكتروني".

---

[1]- المادة الأولى الفقرة ج من القانون المصري رقم 15 لسنة 2004 المتعلق بتنظيم التوقيع الالكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات، سابق الإشارة إليه.

[2]- المرسوم التنفيذي رقم 07-162 المؤرخ في 13 جمادى الأولى عام 1428 الموافق 30 ماي 2007 المعدل والمتمم للمرسوم التنفيذي رقم 01 – 132 المؤرخ في15 صفر عام 1422 الموافق 09 ماي 2001، والمتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية، وعلى مختلف خدمات المواصلات السلكية واللاسلكية، ج.ر، ع37، س2007..

[3]- معوان مصطفى، المرجع السابق، ص.682.

خلاصة لما تقدم، يلاحظ من خلال التعريفات الواردة بشأن التوقيع الالكتروني يمكن اقتراح تعريف بسيط له واعتباره: "مجموعة حروف أو أرقام أو رموز أو أصوات الكترونية، أو تشفير رقمي أو أي نظام معالجة الكتروني آخر، بحيث يمكن أن يعبر عن رضاء أطراف التصرف القانوني، وأن يميز ويحدد هوية شخص موقعه، بحيث يمكن ارتباطه بمضمون المحرر الثابت على أية دعامة الكترونية".

البند الثاني: صور التوقيع الإلكتروني.

نظرا للتطور التقني المذهل في مجال نظم المعلومات والاتصالات، ظهرت العديد من الصور التي يتخذها التوقيع الالكتروني، والتي تختلف تبعا لاختلاف الطريقة التي يتم بها، وتبعا لاختلاف وسائل الثقة والأمان التي يقوم عليها، ولعل من أهم صور التوقيع الالكتروني:

- التوقيع الرقمي أو الكودي (digital signature):

يتركب هذا النوع من التوقيع من عدة أرقام تكون في النهاية شفرة يتم التوقيع بها، ويستخدم هذا النظام في المراسلات الإلكترونية التي تتم بين التجار أو بين الشركات وبعضها كما يستخدم في التعاملات البنكية[1]، وأفضل مثال لذلك بطاقة الائتمان[2] التي تحتوي على رقم سري لا يعرفه سوى الوحيد الذي يدخل البطاقة في ماكينة السحب، حين يطلب الاستعلام على حسابه أو حين يبدي رغبة في صرف جزء من رصيده[3].

[1] - باطلي غنية، المرجع السابق، ص.176.

[2]- للإشارة فإن المشرع الجزائري قد اعترف ببطاقة الائتمان في سنة 2005، وعرفها بموجب القانون رقم 05-02 المؤرخ في27 ذي الحجة عام 1425 الموافق 06 فبراير 2005 المعدل والمتمم للأمر 75-59 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975 والمتضمن القانون التجاري، ج.ر، ع.11 س 2005. شملها لكل من بطاقات الدفع والسحب وعرفها في نصوص المواد 543 مكرر 23 و543 مكرر 24 من القانون التجاري ، بحيث تنص المادة 543 مكرر 23 على أنه:"تعتبر بطاقة الدفع كل بطاقة صادرة من البنوك والهيئات المالية المؤهلة قانونا، وتسمح لصاحبها بسحب أو تحويل أموال"، كما نص في المادة 543 مكرر24 من القانون التجاري على أنه: "الأمر أو الالتزام بالدفع المعطى بموجب بطاقة الدفع غير قابل للرجوع فيه ولا يمكن الاعتراض على الدفع إلا في حالة ضياع أو سرقة البطاقة المصرح بها قانونا أو تسوية قضائية أو إفلاس المستفيد."

[3]-Cf.Alain Buquet, manuel de criminalistique moderne et de police scientifique, 5ème édition augmentée et mise a jour ,puf,2011, p.p. 316-317.

للإشارة، فإن هذه البطاقة تعمل بنظام) (off-line)، ونظام (on-line)، فحسب نظام (off-line) فإنه يتم تسجيل العملية المالية على شريط مغناطيسي، ولا يتغير موقف العميل المالي في حسابه إلا في آخر اليوم، وبعد انتهاء مواعيد العمل .

أما في نظام (on- line) فإنه يتم قيد موقف العميل وتحديثه فور إجراء المعاملة المالية، وهو الغالب في التعامل بنظام البطاقات الذكية التي تحتفظ بداخلها بذاكرة تسجيل كل عمليات العميل[1].

على هذا الأساس يعتبر التوقيع الرقمي وسيلة آمنة لتحديد هوية الشخص الذي قام بالتوقيع من خلال الحاسب الآلي، بل يعد من أكثر الطرق التي يلجأ إليها البنك الالكتروني للتعرف على شخصية العميل، وذلك نظرا لما يقوم به هذا التوقيع من قوة الربط بين الموقع والتصرف الصادر عنه، هذا بالإضافة إلى سهولة استخدام هذا التوقيع[2].

فمثلا في بطاقات الائتمان يتم التوقيع الالكتروني الرقمي عندما يقوم العميل بعملية السحب، حيث أن هناك إجراءات معينة يتم إتباعها، ومتفق عليها بين حامل البطاقة والجهة المصدرة للبطاقة، وتبدأ هذه الإجراءات عن طريق وضع البطاقة داخل الصراف الآلي، ثم إدخال الرقم السري الذي لا يعلمه سوى صاحب البطاقة، عند إدخال هذا الرقم تظهر عدة خيارات منها هل المطلوب (سحب أم إيداع)، ثم خيارات المبالغ المطلوبة حسب الحد الأقصى المسموح به، والحد الأدنى الذي لا يجوز النزول عنه، ثم يتم إشعاره بالرصيد المتبقي بعد السحب إن طلب هو ذلك، فإذا تمت هذه الإجراءات بطريقة صحيحة حسب الاتفاق بين البنك والعميل تتم عملية السحب على المبلغ الذي حدده لنفسه، والخلاصة من هذا كله أن هذه الإجراءات قد حلت محل التوقيع المكتوب والذي يعد شرطا لإتمام عملية السحب اليدوي، ذلك لأن السحب الآلي تم من خلال الرقم السري للعميل، دون توقيع مكتوب منه[3].

---

[1]- هدى حامد قشقوش، الحماية الجنائية للتجارة الالكترونية عبر الانترنت، دار النهضة العربية، القاهرة، 2000، ص،ص.75-76؛ عبد الفتاح بيومي حجازي، التوقيع الالكتروني في النظم القانونية المقارنة، المرجع السابق، ص،ص.23-24؛ باطلي غنية، المرجع السابق، ص.176.

[2]- علاء التميمي، التنظيم القانوني للبنك الالكتروني على شبكة الانترنت، دار الجامعة الجديدة، الإسكندرية، 2012، ص،ص. 656-657.

[3]- عبد الفتاح بيومي حجازي، التجارة الالكترونية في القانون العربي النموذجي في مكافحة جرائم الكمبيوتر والانترنت المرجع السابق، هامش ص. 239.

بالرغم من نجاعة هذه الصورة في التعامل، إلا أنها تتمتع بمزايا ويكتنفها عيوب ونقائص، ولعل من مزايا التوقيع الرقمي أنه يساعد ويسمح بإبرام الصفقات عن بعد دون حضور المتعاقدين جسديا، وهو الأمر الذي يساعد على تنمية وضمان التجارة الالكترونية[1]، ناهيك عن أنه يحقق سرية المعلومات التي تتخذها المستندات الالكترونية، بحيث لا يتمكن من الإطلاع على مضمون هذه المستندات إلا الطرف الذي يكون بحوزته الرقم السري[2]، زيادة على ذلك فإن التوقيع الرقمي يعد وسيلة آمنة لتحديد هوية الشخص الذي قام بالتوقيع، خاصة أنه وبسبب إجراءات المتبعة يمكن للحاسب الآلي التأكد من أن من قام بالتوقيع هو صاحب بطاقة السحب مثلا [3].

في مقابل هذه المزايا هناك عيوب تنقص من قيمة التوقيع الرقمي ولعل أهمها إمكانية سرقة الرقم السري أو تعرضه للضياع، قدرة تقليد الشريط الممغنط الموجود على بطاقة الائتمان، ولهذا فقد اتجه جانب من الفقه إلى التأكيد على عدم قدرة التوقيع الرقمي على التعبير عن شخصية صاحبه شأنه شأن التوقيع التقليدي بالكتابة .

رغم انتقاد الفقه للتوقيع الرقمي، إلا أن من الفقه من اعتبر تلك الانتقادات واهية، فإمكانية سرقة الرقم السري لا تنقص من قيمته، خاصة وأن التوقيع التقليدي هو الآخر قد يكون عرضة للعديد من الأخطار، أهمها التقليد والتزوير، ناهيك عن قدرة التوقيع الرقمي على تحديد الموقع، فسرية الرقم السري كافية لتحديد صاحب التوقيع، سيما وأن العميل ملزم بالحفاظ على رقم البطاقة وذلك بموجب اتفاقه مع البنك، وإساءة استخدامه للرقم يجعله تحت طائلة المسائلة القانونية.

إلى جانب هذا كله، فإن إمكانية تقليد الشريط الممغنط الموجود على البطاقة الائتمانية أمر مردود عليه، إذ لا يؤثر هذا الأمر على التوقيع الرقمي، ذلك أنه لا يمكن استعمال البطاقة دون رقمها السري، خاصة وأن هذا الأخير معلوم من قبل العميل وحده.

---

[1]- عبد الفتاح بيومي حجازي، التوقيع الالكتروني في النظم القانونية المقارنة، المرجع السابق، ص.26.

[2]- علاء التميمي، التنظيم القانوني للبنك الالكتروني على شبكة الانترنت، المرجع السابق، ص.660.

[3] - عبد الفتاح بيومي حجازي، التجارة الالكترونية في القانون العربي النموذجي في مكافحة جرائم الكمبيوتر والانترنت، المرجع السابق، هامش ص،ص .240-241 .

إلى جانب التوقيع الرقمي، يوجد توقيع إلكتروني آخر يطلق عليه تسمية التوقيع البيومتري[1]، ويعتبر هذا الأخير أحد أساليب التحقق من شخصية المتعامل، كون أنه يعتمد على الخواص الفيزيائية والطبيعة والسلوكية للأفراد، ويتمتع بدرجة عالية من الثقة، ويعود هذا إلى اعتماده على حقيقة عملية ثابتة مفادها أن لكل فرد صفاته الجسدية الخاصة التي تختلف من شخص إلى آخر، والتي تتميز بالثبات النسبي الذي يجعل لها قدرا كبيرا من الحجية في التوثيق والإثبات [2].

للإشارة فإن الصفات الجسدية أو البيومترية التي يعتمد عليها التوقيع البيومتري كثيرة ومتعددة ومن أهمها البصمة الشخصية، مسح العين البشرية، ملامح الوجه البشري، نبرة الصوت، التوقيع الشخصي، البطاقة الذكية، وغير ذلك من الطرق الأخرى التي تعتمد على تعاقب نظم الحماية وتعددها في أي نظام واحد[3].

وفقا لهذا النوع من التوقيع يتم التأكد من شخصية المتعامل أو المستخدم من هذه الطرق البيومترية عن طريق إدخال المعلومات المتعلقة بالصفات البيومترية في الحاسوب، إذ وبعد التقاط صورة دقيقة لعين المستخدم أو بصمته الشخصية أو نبرة الصوت، يتم تخزينها في ذاكرة الحاسوب، بإتباع نظام التشفير وفك التشفير، ليتم بعدها التحقق من صحة التوقيع البيومتري من خلال مطابقة الصفات والخواص الطبيعية لمستخدم التوقيع مع الصفات والخواص التي تم تخزينها على جهاز الحاسوب[4].

إن من أهم النواحي الإيجابية لاستخدام التوقيع البيومتري عدم إعتماده على المفاتيح السرية وما يتعلق بها من مشاكل، خاصة التي تتعلق بنسيان أو تزوير أو سرقة أرقام وكلمة

---

[1]- تعني كلمة بيومتري (biometrique) القياسات الحيوية وهي تطلق على الوسائل المرتبطة مباشرة بالصفات المميزة والصفات الفيزيائية والطبيعة والسلوكية للإنسان، والتي تختلف من شخص لآخر وللإشارة فقد شهدت الأنظمة البيومترية هذه تطورا عام 1998، وذلك عندما بدأت شركة (oki) اليابانية للصناعات الكهربائية، ومؤسسة (city bank) الأمريكية في نيويورك باختيار بعض الأنظمة التي تعتمد على قزحية العين لاستعمالها في جهاز الصرف الآلي للنقود حيث تقوم هذه التجربة على تثبيت كاميرا رقمية تعمل على مطابقة الخواص البشرية التي تقوم بالتقاطها مع تلك الخواص المخزنة فيها، وذلك للتأكد من شخصية العميل. يراجع في ذلك، علاء التميمي، التنظيم القانوني للبنك الالكتروني على شبكة الانترنت، المرجع السابق، ص.652؛ منير محمد الجنبيهي، ممدوح محمد الجنبيهي، تزوير التوقيع الالكتروني، دار الفكر الجامعي، الإسكندرية، 2006، ص. 46.

[2] -إبراهيم الدسوقي أبو الليل، التوقيع الالكتروني ومدى حجيته في الإثبات "دراسة مقارنة"، مجلة الحقوق، فصلية علمية محكمة تعنى بنشر الدراسات القانونية والشرعية، تصدر عن مجلس النشر العلمي بجامعة الكويت ع الثالث، السنة التاسعة والعشرون، س 2005،ص.110؛

Alain Buquet ,op. cit,p.320.

[3]- خالد علي العراقي علي إسماعيل، مكافحة جرائم التوقيع الالكتروني بدولة الإمارات العربية المتحدة، المرجع السابق، ص.125.

[4]-منير محمد الجنبيهي، ممدوح محمد الجنبيهي، المرجع السابق، ص.46؛ سمير حامد عبد العزيز الجمال، المرجع السابق، ص.220؛ إبراهيم الدسوقي أبو الليل، التوقيع الالكتروني ومدى حجيته في الإثبات "دراسة مقارنة"، المرجع السابق، ص.110.

السر، كما أنه يعتمد على خواص طبيعة خاصة تختلف من عميل لآخر، ولا يمكن القول بوجود فردين متماثلين في هذه الخواص[1].

في مقابل هذه المزايا يرى بعض الفقهاء أن هذا النظام يثير الكثير من المشاكل، وتعتريه العديد من العيوب والتي منها إمكانية مهاجمة أو نسخ هذا النوع من التواقيع بواسطة التقنيات التي يستخدمها قراصنة الحاسوب، أو عن طريق نظم فك التشفير، وذلك بسبب الاحتفاظ بصورة التوقيع على القرص الصلب لجهاز الحاسوب، بحيث يتم مثلا تقليد بصمات الأصابع باستخدام بصمات بلاستيكية مقلدة، كما يمكن لقراصنة الحاسوب استخدام أنواع معينة من العدسات اللاصقة بنفس اللون والشكل والخصائص التي تم تخزينها على الحاسوب، خاصة إذا تمت برمجة الحاسوب على حصول التوقيع بواسطة مسح العين البشرية، زيادة على ذلك فإن هذه التقنية الحديثة لا تستطيع أن تتوفر في كل الحاسوبات، وذلك نظرا لاختلاف نظم التشغيل وأساليب التخزين، وخصوصيات حزم البرامج المتنوعة، ولهذا يرى الفقهاء بأن التوقيع الالكتروني في صورته البيومترية لا يزال في مراحله الأولى، وللإستفادة منه ارتأوا ضرورة إحاطته بسياج من أمان، وذلك حتى يطمئن له الأفراد في معاملاتهم[2] .

أما الصورة الثالثة للتوقيع الالكتروني فتتمثل في التوقيع بالقلم الالكتروني (PEN –OP) في هذه الصورة من التوقيع يتم استخدام طريقة (PEN OP)، أو ما يعرف بالقلم الالكتروني، والتي تتمثل في استخدام قلم رقمي حسابي يتم من خلاله الكتابة على شاشة الكمبيوتر عن طريق برنامج معين يكون هو المسيطر والمحرك لكل هذه العملية، حيث يقوم هذا البرنامج بوظيفتين أساسيتين؛ الأولى هي خدمة التقاط التوقيع، والثانية هي خدمة التأكد من صحة هذا التوقيع[3].

---

[1]- علاء التميمي، التنظيم القانوني للبنك الالكتروني على شبكة الانترنت، المرجع السابق، ص.653.

[2]- سمير حامد عبد العزيز الجمال، المرجع السابق، ص.220؛ إبراهيم الدسوقي أبو الليل، التوقيع الالكتروني ومدى حجيته في الإثبات، "دراسة مقارنة"، المرجع السابق، ص. 111.

[3]- خالد ممدوح إبراهيم، أمن المعلومات الالكترونية، الدار الجامعية، الإسكندرية- مصر، 2008، ص.122 ؛ هدى حامد قشقوش، المرجع السابق، ص.77.

في هذا النوع من التواقيع يتلقى البرنامج أولا بيانات المستخدم عن طريق بطاقته الخاصة، والتي هي عبارة عن بطاقة تحقيق هوية إلكترونية خاصة تحتوي على بيانات كاملة عن هذا الشخص، تتم وضعها في الآلة المستخدمة، ليظهر بعدها بعض التعليمات على شاشة الحاسوب، يقوم المستخدم بإتباعها إلى غاية أن تظهر رسالة على الشاشة تطلب منه كتابة توقيعه باستخدام القلم الإلكتروني داخل مربع يعرض على الشاشة[1].

وعندما يقوم المستخدم بتحريك القلم بيده، وكتابة التوقيع على شاشة الحاسوب، يقوم هذا البرنامج بالتقاط حركة اليد، كما يعمل على قياس بعض الخصائص المعينة للتوقيع من حيث الحجم وشكل الحروف والدوائر، بالإضافة إلى السرعة النسبية التي يتم بها وضع الحروف، ثم يظهر للمستخدم أو العميل بعد ذلك ثلاثة أيقونات، الأولى موافقة على شكل التوقيع، والثانية إعادة المحاولة، والثالثة لإلغاء التوقيع.

فإذا وافق المستخدم على شكل التوقيع الذي ظهر أمامه، فإنه يقوم بالضغط على أيقونة موافق، حيث يقوم البرنامج بعد ذلك بتجميع هذه البيانات وتشفيرها وحفظها على نحو يتيح أو يسمح باستخدامها عند الضرورة، ثم بعد ذلك يقوم البرنامج بوظيفته الثانية، والمتمثلة في التحقق من صحة التوقيع، حيث يعمل على فك رموز الشفرة، ثم يقوم بإجراء المطابقة بين البيانات التي تم إدخالها من قبل المستخدم، والبيانات المخزنة لديه حيث يعطي هذا البرنامج إشارة تظهر على جهاز المستخدام بما يفيد مطابقة التوقيع من عدمه[2].

إن هذه الطريقة توفر مزايا لا يمكن إنكارها نظرا لسهولة استخدامها، حيث يتم من خلالها تحويل التوقيع التقليدي إلى شكل إلكتروني ينساب عبر أنظمة معالجة للمعلومات[3]، يضاف إلى ذلك صعوبة تزوير هذا التوقيع، حيث أن البرنامج يعمل على التأكد من صحة هذا التوقيع من خلال إجراء المطابقة بين توقيع المستخدم والتوقيع المحفوظ لديه بدقة كبيرة مما يسهل معها اكتشاف أي تزوير.

---

[1] - عبد الفتاح بيومي حجازي، التوقيع الالكتروني في النظم القانونية المقارنة، المرجع السابق ، ص.33.

[2]- علاء التميمي، التنظيم القانوني للبنك الالكتروني على شبكة الانترنت، المرجع السابق، ص.655 ؛ هدى حامد قشقوش، المرجع السابق، ص،ص.77-78؛ عبد الفتاح بيومي حجازي، التوقيع الالكتروني في النظم القانونية المقارنة، المرجع السابق، ص.34.

[3]- سمير حامد عبد العزيز الجمال، المرجع السابق، ص.226.

في المقابل هذه المزايا، يرى جانب من الفقه أن استعمال هذه الطريقة من الناحية العملية قد يكون محفوف بالعديد من المشكلات التي من بينها مشكلة إثبات العلاقة بين التوقيع والمستند، فقدرة المرسل إليه على الإحتفاظ بنسخة من التوقيع الذي يصله على أحد المستندات، يسمح له بوضعه على مستند آخر ليس صادر من صاحب التوقيع، وهو الأمر الذي من شأنه أن يعدم الصلة بين التوقيع والمحرر الذي يحمله، وهذا كله يؤدي إلى زعزعة الثقة في المعاملات[1].

زيادة على ذلك فإن هذا النوع من التوقيعات يتطلب وجود حاسوب قلمي ذي مواصفات خاصة تمكنه من أداء مهمته في التقاط التوقيع على شاشته، والتحقق من مطابقته للتوقيع المحفوظ بذاكرته [2]، وهو الأمر الذي قد يكلف الدولة مبالغ طائلة.

بالإضافة إلى الصور الثلاثة للتوقيع الالكتروني السالفة الذكر، فإن هناك من الفقه من يضيف صور أخرى منها التوقيع بالضغط على مربع الموافقة (OK BOX) أو ما يسميه البعض بالتوقيع عن طريق الضغط على أحد المفاتيح في لوحة الحاسب الآلي على نحو يفيد الموافقة على التصرف القانوني، حيث كثيرا ما يحدث في العقود الالكترونية أن تتم الموافقة عن طريق النقر على زر الموافقة في المكان المخصص لذلك في لوحة مفاتيح الكمبيوتر، أو بالضغط على الخانة المخصصة للقبول في نموذج العقد المعروض على شاشة الكمبيوتر، وزيادة في التأكيد فإنه يتطلب من العميل أو المستخدم بالضغط مرتين(DOUBLE CLICK) وذلك لضمان الجدية في التعامل، غير أن جانب آخر من الفقه يرى أن هذه الطريقة لا تعتبر في حد ذاتها توقيعا يكتسب به المستند الإلكتروني العناصر اللازمة لاعتباره دليلا كاملا، ويدعمون حجتهم في ذلك بأن أغلب المنشآت التجارية تلجأ في معاملتها إلى إضافة خانة في نموذج التعاقد الموجود على صفحة الويب يضع فيها المتعاقد الرقم السري الخاص ببطاقته الإئتمانية.[3]

---

[1]- علاء التميمي، التنظيم القانوني للبنك الالكتروني على شبكة الانترنت، المرجع السابق، ص،ص.655-656؛ سمير حامد عبد العزيز الجمال، المرجع السابق، ص.227.

[2]- إبراهيم الدسوقي أبو الليل، التوقيع الالكتروني ومدى حجيته في الإثبات، المرجع السابق، ص.111؛ خالد علي العراقي علي إسماعيل، المرجع السابق، ص.127 .

[3]- خالد ممدوح إبراهيم، أمن المعلومات الالكترونية، المرجع السابق، ص.123 .

المطلب الثالث: الضوابط الشخصية للمستند الإلكتروني.

إن المستند الإلكتروني باعتباره سمة من سمات التطور التكنولوجي الحديث، وأحد مفرزات البيئة الرقمية تحكمه جملة من الضوابط الشخصية، ويعطي لصاحبه -صاحب البيانات التي يتضمنها المستند الإلكتروني-، وللغير جملة من الحقوق كما يسمح له بالقيام بجملة من التصرفات.

هذه الضوابط منها ما هو شخصي ويتعلق بصاحب البيانات التي يتضمنها المستند الإلكتروني، ومنها ما هو مقرر للغير المطلع على هذا المستند، وقد وجدت هذه الضوابط لتوفير أكبر حماية للمستند الإلكتروني، وضمان أمنه وخصوصيته، وكذا لحماية البيانات والمعلومات الواردة به، خاصة وأن البيانات التي يتضمنها غالبا ما تكون سرية، ويخشى وصول يد العابثين والمتطفلين إليها بسبب ما قدمته الشبكات الإلكترونية.

لأهمية الضوابط الشخصية سيتم التعرض لتلك الضوابط المتعلقة بصاحب المستند **(الفرع الأول)**، وبعدها للضوابط المقررة للغير المطلع على المستند الإلكتروني **(الفرع الثاني)**.

الفرع الأول: الضوابط الشخصية المتعلقة بصاحب المستند الالكتروني.

مما لا شك فيه أن حرية انتقال الأفكار والمعلومات هي إحدى الحريات الأساسية التي يحرص عليها كل مشرع، كما أنها من المبادئ والقواعد التي يتوقف عليها تقدم الأمم وازدهارها، ناهيك عن أن حرية التعبير بصورها المختلفة تعد إفصاحا عن الشخصية الإنسانية في المجتمع، وهي الضمان الذي يقوم عليه أي مجتمع ديمقراطي [1].

والمعلوم أن حرية انتقال المعلومات، وكذا حرية الاستفسار عنها، والإطلاع عليها ليست حرية مطلقة بل تحكمها مجموعة من القيود، إذ أن هناك بيانات ومعلومات تمس بخصوصية الإنسان وبعض مصالحه الهامة التي يخشى إطلاع الغير عليها، وهو الأمر الذي

[1]- علاء حسين مطلق التميمي، المستند الالكتروني، عناصره، تطوره ومدى حجيته في الإثبات المدني، المرجع السابق، ص.78.

يستوجب معه أن تحاط هذه البيانات بنوع من السرية والأمن، وفي سبيل تحقيق ذلك فإنه في مجال المعاملات الالكترونية أقرت تشريعات المعاملات الإلكترونية[1] لصاحب البيانات التي يتضمنها المستند الالكتروني بعض الضوابط أو بعض الحقوق الخاصة بشخصه، ومن بين أهم هذه الحقوق الحق في الاستعلام والاستفسار.

وحتى لا يمس هذا الحق بخصوصية الأفراد، وببعض المعلومات الهامة منحت التشريعات لصاحب المستند الالكتروني حقا آخر وهو الحق في سرية بعض البيانات والمعطيات المخزنة بطريقة إلكترونية.

ولئن كان حق الإستعلام، وحق السرية من الحقوق التي يتمتع بها صاحب المستند الإلكتروني. فما المقصود بكل منهما؟، وما هي الصلاحيات التي يمنحها كل حق لصاحب البيانات التي يتضمنها المستند الإلكتروني؟

البند الأول: الحق في الاستعلام والحق في السرية.

إن الحق في الاستعلام والاستفسار عن مدى وجود معلومات مخزنة بطريقة الكترونية على مستند الكتروني له علاقة وطيدة بالحق في السرية، حيث يعتبر الحق الثاني قيدا من القيود الواردة على حرية ممارسة الحق الأول، كما يعد من بين الضمانات الموضوعة من طرف المشرعين لتوفير الأمن والخصوصية في مجال المعاملات الإلكترونية.

وعليه سيتم التطرق إلى بيان الحق في الاستعلام والاستفسار، ثم التعرض إلى الحق في السرية.

أولا: الحق في الاستعلام.

يقصد بالحق في الاستعلام حق كل شخص في أن يستفسر ويسأل ويتلقى ويستخلص المعلومات والأنباء والآراء والبيانات على أي صورة وفي أي مجال ما دام أن القانون يسمح له بذلك[2].

[1]- Cf. Cédric Manara, droit du commerce électronique, LGDJ, lextenso édition, France, 2013, p.p.93-94.

[2]- أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني –دراسة مقارنة-، ط1، المرجع السابق، ص.86.

هذا وتتعدد الوسائل التي يستعلم بها الشخص عن المسألة التي يبحث عنها إلى وسائل مسموعة، مرئية، ومكتوبة، كما أن مجالات استعمال هذا الحق متعددة، إذ جرى العمل في المجال المصرفي على تقديم البنوك للمعلومات، والاستشارات كخدمة مصرفية لمساعدة العملاء على اتخاذ قراراتهم حيال الأنشطة التجارية والاقتصادية[1]، وتقوم البنوك بهذه العملية بسبب وظيفتها التي تمكنها من التوصل إلى أكبر عدد ممكن من المعلومات عند الإطلاع على سير الحسابات وتقديم الاعتمادات، وقبول الودائع وخصم ما يقدم إليها من أوراق تجارية.

بهذا يعد البنك الأقدر على الإجابة على الأسئلة التي يطرحها العميل حول ائتمان أحد المشروعات، أو التي يطرحها الغير حول ائتمان أحد العملاء.

ولقد تطور دور البنك بوصفه مصدرا للمعلومات في العصر الحالي، خاصة بعد أن أضحى الجانب الأكبر من الثروات لا يشمل العقارات كما كان الحال سابقا، بل أصبح يتمثل في أوراق مالية (قيم منقولة) يصعب معرفة نوعها وقيمتها الحقيقية، دون الاستعانة بالبنوك التي تقوم بحفظها ومسك حساباتها وإدارة محافظها[2].

ونتيجة لذلك وبغية مسايرة التطورات التكنولوجية وضمان خدمة تقديم المعلومات للعميل -ماعدا ما كان منها يتنافى ومبدأ السر المصرفي-، بدأت البنوك تطور من هذه الخدمات، فعملت على إنشاء أقسام المعلومات، وغرف للمشورة مما أدى إلى التوسع في مجال خدمة المعلومات والاستشارات المصرفية[3] .

ولقد أدى التطور التقني الذي يشهده المجال البنكي إلى استخدام صور جديدة أمكن لنقل المعلومات والاستعلام عنها بسرعة من خلال شبكات المعلومات المفتوحة أو المغلقة، كما

[1]- أحمد بركات مصطفى، مسؤولية البنك عن تقديم المعلومات والاستشارات المصرفية، دار النهضة العربية، مصر، 2009، ص.09.

[2]- عاشور عبد الجواد عبد الحميد، دور البنك في خدمة تقديم المعلومات، دراسة مقارنة في القانونين المصري والفرنسي، دار النهضة العربية، القاهرة 2008، ص.321.

[3]- أحمد بركات مصطفى، المرجع السابق، ص.09.

قامت الهيئات والمؤسسات العامة والخاصة بإنشاء مواقع إلكترونية يسمح الولوج إليها بالوصول إلى المعلومات، وتندرج تلك المواقع ضمن ما يعرف ببنوك المعلومات[1].

إن تطور حق الإستعلام في مجال البيئة الرقمية دفع بعض التشريعات إلى منح صاحب المستند الإلكتروني الحق في الإطلاع على المعلومات التي يحتويها المستند الإلكتروني، وذلك لتمكينه من التأكد من صحة وسلامة المعلومات الواردة به، وكذا لتجنب المشاكل الناجمة عن الأخطاء التي يمكن أن ترد بالمعلومات المدرجة في المستند الالكتروني[2]، فمثلا وفي مجال التجارة الإلكترونية يتم تبادل العديد من المستندات الالكترونية والبيانات والمعلومات الخاصة بالمتعاملين، وإذا تم تبادل بيانات ومعلومات خاطئة أو مغلوطة من بنك أحد المتعاملين على الشبكة إلى البنك الآخر الخاص بالعميل الآخر، فإن هذه المعلومات قد تضر بوضع العميل الائتماني، كما قد تضر كذلك بالصفقات التي يريد أن يبرمها، لذلك نجد أن معظم التشريعات المقارنة تقرر حق صاحب الشأن في أن يقدم طلب استعلام لبنوك المعلومات، أو للجهات التي تقوم بتجميع المعلومات حيث يطلب منها الاستعلام عن وجود معلومات خاصة به لديها أم لا.[3]

والأكثر من ذلك فإن هناك دُوَلًا تلزم بنوك المعلومات بأخطار صاحب الشأن بقيامها بإجراء تجميع المعلومات الخاصة به، ولكن بسبب أن ذلك الأمر يتطلب نفقات باهضة من أوراق وتكاليف بريد وخلافه، فإن هناك التشريعات الأخرى تعفى بنوك المعلومات من تقديم ذلك الإخطار لصاحب الشأن [4].

ثانيا: الحق في السرية.

يرتبط الحق في سرية البيانات والمعطيات المخزنة بالحق في الخصوصية،[5] خاصة وأن السر بمعناه العام يحتل جانب من جوانب الحرية الشخصية، حيث أن لكل فرد أن يحتفظ

---

[1]- علاء حسين مطلق التميمي، المستند الالكتروني، عناصره، تطوره ومدى حجيته في الإثبات المدني، المرجع السابق، ص.78؛ أشرف توفيق شمس الدين، الحماية الجنائية للمستند الالكتروني- دراسة مقارنة-، ط1، المرجع السابق، ص، ص.86-87.

[2]- أشرف توفيق شمس الدين، الحماية الجنائية للمستند الالكتروني- دراسة مقارنة-، ط1، المرجع السابق، ص،ص.86-87.

[3]- محمد أمين الرومي، المستند الإلكتروني، المرجع السابق، ص.140.

[4]- المرجع نفسه، ص،ص.140-141 .

[5]- للإشارة فإن السرية لغة تأتي من السر والسر هو ما يكتم وهو خلاف الإعلان، والجمع أسرار الحديث إسرارا أي أخفيته كما يعرف السر لغويا بأنه ما يكتمه الشخص، أو هو ما يكتمه الإنسان في نفسه فهو كل خبر يقتصر العلم به على عدد=

بأسراره في مكنونات ضميره، كما له إن أراد الإدلاء بها أو ببعضها إلى شخص آخر يثق به.

وبناء على ذلك يتعين على المعهود إليه بالسر أن يكتمه، ذلك أن كتمان السر واجب فرضته بداية قواعد الدين، واقتضته قواعد الأخلاق والشرف والأمانة، ليتحول بعدها إلى التزام قانوني يترتب على مخالفته مسؤولية مدنية وكذا جزائية[1].

ونظرا لأن المعلومات والبيانات أصبحت في مجال البيئة الرقمية تدون وتحفظ على دعامة الكترونية عن طريق الحاسب الآلي، ولقدرة هذا الأخير الهائلة على جمع وترتيب البيانات فإنه أضحى بالإمكان المساس بالحقوق الشخصية للأفراد[2]، خاصة مع ظهور الانترنت، والتي أضحت بموجبها الاتصالات والمعلومات، وكذا البيانات تتدفق عبر الحدود دون أي اعتبار للجغرافيا والسيادة، وهو الأمر الذي قد ينجر عنه منح بعض المعلومات وبعض البيانات لجهات داخلية وخارجية، ولربما إلى جهات ليس لها مكان معروف، وهو ما قد يثير مخاطر إساءة استخدام هذه البيانات، خاصة في الدول التي لا تتوفر فيها مستويات الحماية القانونية للبيانات الشخصية[3].

وبما أن هذه المعلومات والبيانات تكون مدرجة في مستندات الكترونية، فإنه بالنتيجة يجب أن تحاط هذه المستندات بالسرية اللازمة والكافية، وذلك من أجل عدم انتشار وإذاعة ما تحتويه من معلومات قد تكون مهمة وذات شأن، فقد يؤدي مثلا إفشاء المعلومات التي يحتويها المستند الالكتروني إلى تحقيق منافسة غير مشروعة بين المشروعات، كذلك قد

=محدود من الأشخاص ، وهو كل معلومة مقرر لها أن تكون مكتومة ، أو هو ما يفشي به الشخص لآخر مستأمنا إياه عدم إفشائه، بل إنه يشمل واقعة تقترن بها أدلة تدل على أنه يجب أن تكون مكتومة، أو كان العرف يقضي بكتمانها، كما جاء في معنى السر أيضا بأنه الإخفاء أو الكتمان وعدم العلانية خاصة في المفهوم القانوني بما يحفظ بعيدا عن علم وملاحظة الناس الذين يمكن أن يتأثروا بالفعل أو الحدث أو الشيء الذي يكون محله محل الكلام، فهو الشيء الذي يعرفه شخص واحد أو قلة من الناس ويكون بمعزلة عن علم الآخرين. مأخوذ من، محمد عبد الودود عبد الحفيظ أبو عمر، المسؤولية الجزائية عن إفشاء السر المصرفي، ط1، دار وائل للنشر، الأردن، 1999، ص.21.

[1]- القاضي غسان، قانون العقوبات الاقتصادي (دراسة مقارنة حول جرائم رجال الأعمال والمؤسسات التجارية، المخالفات المصرفية والضريبة الجمركية وجميع جرائم التجار) طبعة مزيدة ومنقحة منشورات الحلبي الحقوقية، بيروت- لبنان، 2004، ص.123.

[2]- محمد أمين الرومي، المستند الإلكتروني، المرجع السابق، ص. 129.

[3]- بولين أنطونيوس أيوب، المرجع السابق، ص.21.

تكون هذه المستندات تحتوي على معلومات متعلقة بأمن الدولة وسلامتها، أو بمعلومات شخصية هامة خاصة بصاحب المستند.

لأهمية هذه المسألة عمدت التشريعات المتعلقة بالمعاملات الالكترونية على حضر إفشاء المعلومات التي يتضمنها المستند الالكتروني[1]، خاصة وأنه في بيئة الانترنت قد تستخدم العديد من الوسائل التقنية لتتبع المعلومات الشخصية للمشتركين، ومن أشهرها ما يعرف بوسائل الكوكيز (cookies) التي تنتقل إلى نظام المستخدم بمجرد دخوله للموقع، حيث تتمكن من تسجيل بيانات تخصه وقد لا يرغب في الكشف عنها، كما وأن محركات البحث باعتبارها أهم وسائل الوصول المباشر للمعلومات المطلوبة من قبل المستخدم، تقوم بعمليات جمع وتبويب وتحليل بيانات المستخدمين على نحو واسع، مستخدمة الكوكيز أو غيرها من التقنيات التي تسمح بالتعرف على خصوصية زوار المواقع الالكترونية، ودون أن تطلع المستخدم بذلك[2]، ومن ثم كان لزاما على المستخدم أن يحتاط من سرية بياناته ومعلوماته الشخصية.

وفضلا عن ما سبق فإنه ينبغي الذكر أن السماح للأفراد بتخزين المعلومات الخاصة بهم على دعامة الكترونية خاصة بهيئة معينة، أو ببنك من بنوك المعلومات لا يعني السماح لهم بنشر وافشاء هذه المعلومات للعامة ،إذ يجب على الجهة التي تقوم بجمع وتخزين هذه المعلومات أن تحافظ على سريتها، وألا تستخدمها من أجل تحقيق أغراض غير مشروعة[3].

وعليه فإنه من حق صاحب المستند الالكتروني أن تكون المعلومات والبيانات التي يتضمنها هذا المستند سرية وبمنأى من تدخل العابثين والمتطفلين.

[1]- محمد أمين الرومي، المستند الإلكتروني، المرجع السابق، ص. 122.
[2]- بولين أنطونيوس أيوب، المرجع السابق، ص، ص.21-22.
[3]- محمد أمين الرومي، المستند الإلكتروني، المرجع السابق، ص.138.

البند الثاني: الحقوق اللصيقة بشخصية صاحب البيانات التي يتضمنها المستند الالكتروني.

الحقوق اللصيقة بشخصية صاحب البيانات التي يتضمنها المستند الالكتروني حقوق مقررة لصاحب المستند الالكتروني يمارسها بنفسه، وهي مقررة لضمان سلامة وصحة البيانات والمعلومات المدرجة في هذه المستندات، ومن تم سلامة التعاملات القانونية التي سوف يبرمها الشخص المعني، ذلك أن كل خطأ أو تغيير في صحة هذه المعلومات والبيانات المخزنة قد ينعكس سلبا على مركز صاحب هذه المعلومات، وكذا على جدية التعاملات التي يريد أن يبرمها، ومن بين هذه الحقوق الحق في الاطلاع على مدى وجود بيانات أو معلومات مخزنة بطريقة الكترونية وعلى مستند الكتروني، وكذا الحق في تصحيح هذه المعلومات، إذا ما تم إدراجها بطريقة مغلوطة أو إذا تضمنت خطأ أو حذف أو تغيير أو ما شابه ذلك.

أولا: حق الاطلاع المباشر.

يخول هذا الحق للفرد إمكانية الإطلاع على البيانات والمعلومات الخاصة به والمسجلة على دعامات الكترونية، ويستوي في ذلك أن يكون قد تم تسجيل وتدوين هذه البيانات من طرف بنوك المعاملات الخاصة، أو من قبل هيئات أو مؤسسات حكومية، وسواء تم تدوين هذه البيانات والمعلومات بموافقة صريحة من صاحب الشأن، أو تم تدوينها دون الحصول على إذن منه بذلك، كما يستوي أن تكون هذه المعلومات قد دونت بمعرفة وعلم صاحب الشأن، أو تم تدوينها دون معرفته وعلمه، وسمي هذا الحق بالمباشر لأنه حق يمارسه صاحبه بذاته وبنفسه ويباشره شخصيا دون أن يمارسه عنه وكيل أو نائب، خاصة وأن المعلومات المخزنة على دعامة الكترونية قد تعتبر معلومات شخصية، وأحيانا تكون هذه المعلومات سرية لا يجوز للغير أن يطلع عليها دون إذن من صاحبها.[1]

ومما لاشك فيه أن ممارسة حق الاطلاع يحقق ميزة كبيرة لصاحب الشأن، وذلك في حالة ما إذا احتوت هذه البيانات على معلومات مغلوطة، أو في حالة ما إذا تضمنت حذف أو

[1]- محمد أمين الرومي، المستند الإلكتروني، المرجع السابق، ص.140 .

تغيير أو تبديل وأريد استخدامها في أغراض أخرى، خاصة وأن صاحب البيانات التي يتضمنها المستند الالكتروني قد يبرم صفقات وتعاملات قانونية في مجال البيئة الرقمية، وهو الأمر الذي يتطلب تبادل العديد من المستندات الالكترونية والبيانات والمعلومات بين المتعاملين فيما بينهم، ومن ثم فإنه إذا تم تبادل البيانات مغلوطة أو يكون قد حصل فيها حذف أو تبديل، فإن هذا سوف يضر بوضع صاحب هذه البيانات أي بوضع العميل الائتماني، كما قد ينعكس سلبا على جدية وصحة التعاملات، وكذا الصفقات التي يريد أن يبرمها [1].

وعلى هذا فإنه ينبغي على الجهة التي تقوم بتجميع وتخزين المعلومات ألا تخفي أي بيانات أو معلومات متعلقة بصاحب الشأن إن أراد أن يطلع عليها، فلا يجوز لها أن تقدم له بعض البيانات وتخفي البعض الآخر، وإذا حدث ذلك فإنها تقع تحت المسؤولية القانونية، كما يجب أيضا على الجهة التي تقوم بتجميع وتخزين المعلومات أن تتيح لمن يريد الاطلاع على المعلومات الوقت الكافي للإطلاع، وأن لا تتأخر في الرد على طلبه بدون مبرر مقبول، كما لا يجب أيضا أن تلزم صاحب الشأن بأن يبرر سبب إطلاعه، إن كان هو قد قدم طلب إلى هذه الجهات يسأل فيه ممارسة حق الاطلاع [2].

وللإشارة فإن الاطلاع على المعلومات إما يكون بمقابل مادي، وإما أن يكون بدون مقابل مادي، إلا أنه في حالة ما إذا كان الاطلاع بمقابل مادي فيجب ألا يكون هذا المقابل المادي مبالغا فيه، وذلك حتى لا يعد شرطا تعجيزيا لمن يريد أن يمارس حقه في الاطلاع[3].

أما عن كيفية ممارسة حق الاطلاع فإنها تتم إما عن طريق الدخول إلى مقر بنك المعلومات والاطلاع على المعلومات والبيانات الاسمية على شاشة الحاسب الآلي عن طريق المشاهدة، وهذا في حالة ما إذا سمحت الجهة القائمة بجمع المعلومات بذلك، أما إذا لم تسمح بذلك فإنه يتم ممارسة حق الاطلاع على المعلومات عن طريق الحصول على مستخرج ورقي بهذه البيانات أو المعلومات، كما قد يتم الدمج بين الأسلوبين، بمعنى أن يشاهد الشخص

[1]- محمد أمين الرومي، المستند الإلكتروني، المرجع السابق، ص، ص. 140-141.
[2]- المرجع نفسه، ص.142.
[3]- المرجع نفسه، ص.142.

المعني البيانات، والمعلومات الخاصة على شاشة الحاسب الآلي، ثم يطلب بعد ذلك مستخرج رسمي ورقي بهذه المستندات.

هذا ويرى بعض الفقه أن حق الاطلاع يشمل معرفة مصدر المعلومات المسجلة على دعامة الكترونية والمدرجة على مستندات الكترونية، في حين يرى جانب آخر عكس ذلك بحيث لا ينبغي إلزام بنوك المعلومات أو الجهات القائمة على تخزين المعلومات بالإفصاح عن مصدر هذه المعلومات.[1]

وما يمكن ملاحظته عن حق الاطلاع أنه شبيه نوعا ما بحق الاستعلام من حيث مدى وجود معلومات مخزنة على دعامة الكترونية أو مدرجة في مستند الكتروني، ذلك أن القاسم المشترك بينهما هو التأكد من وجود معلومات من عدمه، إلا أن الفرق بينهما واضح، ذلك أن الحق في الاستعلام هو دائما حق مباشر يمارسه صاحب الشأن بنفسه إن أراد ، أما الحق في الاطلاع فإما يكون مباشر أي بواسطة الشخص المعني بذاته، وإما أن يكون الاطلاع غير مباشر أي أن يقوم شخص آخر بالإطلاع نيابة عن صاحب الشأن، زيادة على ذلك فإن الهدف من ممارسة حق الاطلاع على هذه البيانات والمعلومات هو ممارسة حق آخر يلحق بحق الاطلاع، وهو الحق في تصحيح هذه المعلومات إذا كانت مغلوطة، أو كان قد شابها خطأ أو حدثت فيها تغيرات في حالة أو مركز الشخص المعني.[2]

ثانيا: الحق في تصحيح المعلومات الخاطئة.

يقصد بهذا الحق تصحيح المعلومات والبيانات المدرجة على دعامة الكترونية، والتي قد تتضمن خطأ أو غلط أو إضافة أو حذف أو ما شابه ذلك، وممارسة الحق في التصحيح مرتبط بممارسة حق الاطلاع، خاصة وأنه قد يترتب على تخزين معلومات غير الصحيحة في بنوك المعلومات إلحاق الضرر بالشخص المعني بالمعلومة، وهذا الضرر قد يلحق سمعته أو شرفه أو اعتباره، أو يمس بالثقة الائتمانية له لدى البنوك والمؤسسات المالية، لذا فإن الهدف الأساسي من حق الاطلاع هو تصحيح أي خطأ في المعلومات المدرجة في

[1]- محمد أمين الرومي، المستند الإلكتروني، المرجع السابق، ص.141.
[2]- المرجع نفسه، ص.140.

المستند الالكتروني والمخزنة على الحاسب الآلي، هذا ويستطيع صاحب الشأن أن يطالب بنوك المعلومات أو الجهة التي قامت بتخزين المعلومات الخاطئة بالتعويض، وذلك في حالة ما إذا أثبت أنه لحقه ضرر إلى جانب توافر أركان المسؤولية الموجبة التعويض[1].

ويتضمن الحق في التصحيح كافة المعلومات، وذلك إذا كانت هذه المعلومات تتضمن بيانات خاطئة وبيانات صحيحة، أو تتضمن بيانات مبهمة أو تثير اللبس لدى الغير بحيث تحتمل أكثر من احتمال، ويمكن تأويلها على أكثر من نحو.

ولقد طرح الفقه تساؤلا بخصوص الطرف الذي يقع عليه عبء إثبات عدم صحة المعلومات؟، إذ هل يلتزم بذلك صاحب المعلومة الذي يرى من وجهة نظره أنها خاطئة، أم تلتزم بذلك الجهة التي قامت بجمع وتخزين هذه المعلومات والبيانات[2]؟

وفي هذا يرى الفقيهين الفرنسيين "أنسل، ولوكاس" أن عبء إثبات صحة المعلومات المخزنة في المستند الإلكتروني يقع على الجهة التي تقوم بجمع وتخزين المعلومات، ولا ينتقل هذا الأخير إلى صاحب المعلومة إلا إذا كان هو ذاته المصدر الذي استقت منه الجهة المختصة هذه المعلومات[3].

والحق في تصحيح المعلومات يمكن أن يمارسه صاحب الشأن أي صاحب المعلومات الخاطئة، كما يجوز أن يمارسه كل من له مصلحة [4]، هذا وتتعدد أوجه تصحيح المعلومات المخزنة على دعامة الكترونية، بحيث يجوز لصاحب المعلومة أن يطلب تصحيح المعلومة إذا كانت صحيحة في بادئ الأمر ثم حدث تغيير في الوقائع أدى إلى عدم صحتها، كما يجوز لصاحب الشأن أن يطلب محو وشطب المعلومة، إذا تم الحصول عليها بطريق غير مشروع مع حفظ حقه في التعويض المدني، وإذا أثبت أن المعلومات المجمعة والمخزنة غير صحيحة، فعلى الجهة القائمة بالجمع والتخزين أن تصحح هذه المعلومات، وأن تزود الجهات

[1]- محمد أمين الرومي، المستند الإلكتروني، المرجع السابق، ص.143.
[2]- المرجع نفسه، ص. 143.
[3]- المرجع نفسه، ص، ص. 143-144.
[4]- يقصد بكل من له مصلحة مثلا أن يطلع تصحيح المعلومات ورثة صاحب المعلومة الخاطئة، وذلك إذا كان في تصحيح هذه المعلومة رفع أذى عن سمعتهم أو سمعة مورثهم.

الأخرى بالمعلومات الصحيحة إذا كان قد سبق لها وأن زودتها بمعلومات قديمة أو غير صحيحة، كما يجوز لهذه الجهات القائمة بجمع المعلومات أن تصحح بمفردها هذه المعلومات المخزنة إذا تبين لها عدم صحتها، كما يحق للشخص المعني طلب محو وشطب المعلومات التي يكون قد مر على تخزينها والاحتفاظ بها وقت معين لا يجوز بعده الاحتفاظ بها، وهذا طبقا لمبدأ تأقيت تخزين المعلومات[1].

زيادة على ذلك فإن الحق في التصحيح قد يمتد ليشمل حتى الأسس التي تم على إثرها المعالجة الإلكترونية للبيانات، والتي تم على أساسها الحصول على المعلومات التي تم تخزينها، ويعود ذلك لسببين: أولهما أن الحاسب الآلي لا يدخل في اعتباره الجانب والعنصر البشري واختلاف شخصية صاحب المعلومة من شخص لآخر، وثانيها أن برامج الحاسب الآلي تختلف من برنامج لآخر، فقد يتم مثلا تحميل الحاسب الآلي ببعض البيانات ويتم الحصول على معلومات محددة، ثم بعد ذلك يتم إدخال نفس البيانات لجهاز حاسب آلي آخر، فتكون النتيجة الحصول على معلومات مغايرة عن المعلومات التي تم الحصول عليها من الحاسب الأول، ومرد ذلك اختلاف البرنامج من حاسب إلى آخر، ومن ثم فإنه وحتى لا نجعل الآلة تتحكم في مصير الإنسان وتحدد خطواته، يلاحظ أن الفقه قرر حق الشخص في تصحيح المعلومة يمتد ليشمل الأسس التي تم من خلالها التوصل إلى هذه المعلومات[2].

الفرع الثاني: الحقوق الشخصية للغير المطلع على المستند الالكتروني.

إلى جانب الحقوق المقررة لصاحب البيانات التي يتضمنها المستند الالكتروني من حق اطلاع مباشر وحق في سرية البيانات والمعطيات، أقرت تشريعات المعاملات الالكترونية المقارنة حقوقا للغير المطلع على هذه البيانات والمعطيات أو بالأحرى للمتعاملين في مجال البيئة الرقمية، ومن بين هذه الحقوق حق الاطلاع غير المباشر، وكذا الحق في إبرام التصرفات القانونية، خاصة وأن المعلومات المدرجة على دعامة الكترونية أو التي يتضمنها مستند الكتروني قد تضمن عروضا مختلفة وإيجابا خاصا بمعاملات كثيرة، تفرغ في النهاية في عقود الكترونية متنوعة.

[1]- محمد أمين الرومي، المستند الإلكتروني، المرجع السابق، ص.144.
[2]- المرجع نفسه، ص.ص. 144-145.

ويقصد بحق الإطلاع غير المباشر تمكين غير المتعاقدين من الإطلاع على المعلومات الواردة بالمستند، وللإشارة فإن حق الغير في الإطلاع على البيانات يقتصر على البيانات العامة، التي تساعده على معرفة الطرف الذي يرغب في التعامل معه، ومعرفة المعلومات المتعلقة بالسقف الذي يكون بإمكانه التعامل معه فيه، وهذا كله إستنادا لمبدأ التبصر، وحتى يتمكن الغير من اتخاذ قراره عن بينة ودراية.

ولعل سبب حصر المعلومات التي يمكن للغير الاطلاع عليها في ما هو عام، يرجع إلى ضمان حق الطرف الآخر في السرية، كون أن هناك معلومات لا يمكن لغير صاحبها من الإطلاع عليها.

وإلى جانب حق الاطلاع غير المباشر، يكون للغير حق إبرام التصرفات القانونية المختلفة، وذلك متى لقيت دعوة الموجب قبولا من الطرف الآخر.

إن إقرار مثل هذه الضوابط والحقوق للغير المتعامل على الشبكة راجع بالدرجة الأولى إلى الرغبة في حماية الغير وكذا تفعيل التعاملات في البيئة الرقمية الافتراضية التي أصبحت بديلاً عن البيئة المادية المحسوسة.

الفصل الثاني: الضوابط الفنية للمستند الإلكتروني

بما أن المعاملات الإلكترونية تتم عبر نظم معلوماتية معقدة وفي وسط إفتراضي فإن أكثر ما يهددها هو مسألة التحقق من هوية أطراف المعاملة ومن صحة التوقيعات الإلكترونية ونسبتها لمصدرها، وكذا سلامة البيانات التي تتضمنها المستندات الإلكترونية ومن مدى صحة وسلامة الإرادة التعاقدية وبعدها عن الغش والاحتيال.

كما أنه من بين المشاكل التي تعترض هذه التقنية المستحدثة في التعامل مشكلة تأمين البيانات، وكذا المستندات الإلكترونية من المتطفلين ومن مجرمي المعلوماتية، خاصة وأن هذه المستندات قد تتضمن أسرارا شخصية، كما قد تتضمن معلومات على درجة من الأهمية، هذا وقد تثار كذلك مسألة مدى إمكانية حفظ وتخزين هذه المستندات بطرق آمنة وموثوقة تمكن من الرجوع إليها عند الحاجة، وذلك من أجل إستعمالها كوسيلة لإثبات التصرفات القانونية.

فضلا عن ذلك، فإن ظهور المستند الإلكتروني المتضمن الكتابة والتوقيع الالكترونيين قد أدى في بدايته إلى إيجاد فراغ قانوني في التشريعات المختلفة، وذلك بسبب عدم تكييف المفاهيم القانونية الجديدة مع القواعد التقليدية للإثبات، خاصة عنصر الدليل الإلكتروني سواء من الناحية المدنية أو الجزائية ومدى قبوله كدليل في الإثبات، وهو الأمر الذي جعل التشريعات تعمل جاهدة من أجل سد الفجوة القانونية، وهو ما تقرر من خلال تطوير المفاهيم القانونية التقليدية، وذلك بإعادة صياغتها أو وضعها في تشريع خاص بغية مواكبة التطور التكنولوجي واستغلاله والاستفادة منه حتى لا يكون القانون حائلا أو عقبة في طريق هذا التطور المتسارع، سيما وأن القاضي الجزائي قد يجد نفسه مضطرا لأن يتعامل مع أشكال مستحدثة في مجال الإثبات الجزائي.

استنادا لما تقدم تتجلى أهمية التساؤلات التالية، ما مدى حجية المستندات الإلكترونية؟، وما مدى فعاليتها في توفير قناعة القاضي الجزائي؟

إن الإجابة على هذه الإشكاليات يستوجب التطرق إلى وسائل الحماية الفنية والقانونية لضمان سلامة المستند الإلكتروني **(المبحث الأول)**، ثم القوة الثبوتية للمستند الالكتروني من الناحيتين المدنية والجزائية **(المبحث الثاني)**.

المبحث الأول: وسائل الحماية لضمان سلامة المستند الإلكتروني.

لقد أدى شيوع استخدام الإنترنت وظهور التجارة الإلكترونية إلى ازدياد حجم المعاملات الإلكترونية بين الأفراد، وبعد أن أظهر الواقع العملي نوعا جديدا من الكتابة والتوقيع، وتم استبدالهما بالكتابة الإلكترونية والتوقيع الإلكتروني، والتي تتخذ دعامة لها المستندات الإلكترونية، ظهرت الحاجة إلى إيجاد وسائل حماية لضمان سلامة المعلومات والبيانات، وذلك بغية تعزيز التعامل بهذه التقنيات الحديثة، كما تطلب الأمر إيجاد تقنيات فنية سريعة وآمنة لتبادل تلك المعاملات، سواء في مجال البيع أو الشراء أو في مجال التعاقدات التي تتم عبر الشبكة العنكبوتية، وهو ما تجسد فعلا حيث عملت التشريعات الأجنبية والعربية المقارنة إلى إيجاد تقنيات ووسائل تحمي بها البيانات والمستندات المعالجة آلياً على نحو توثق به هذه المعاملات، وذلك حتى تكون هذه الأخيرة مؤمنة من أي عبث أو تدخل، ومحل تداخل الغير المتعامل بها.

زيادة على ذلك فقد يتطلب القانون في بعض الحالات الاحتفاظ بالمستندات أو السجلات لفترة زمنية معينة، وتطبيق هذه الفكرة على المستند يقتضي مراعاة طبيعة هذا الأخير باستخدام قواعد تراعي ذلك، وتحقق الهدف منه على نحو يمكن معه كشف أي تعديل أو تبديل في بيانات المستند الإلكتروني والتوقيع الإلكتروني مهما طال الزمن، وذلك عن طريق استخدام نظام حفظ البيانات الإلكترونية بصفة مستمرة طوال مدة محددة بما يضمن صحتها ويحافظ على سلامتها.

وبغية توفير حماية فعالة للمستند الإلكتروني من الناحية الفنية، فإنه سيتم التطرق إلى توثيق المستند الإلكتروني **(المطلب الأول)**، كما سيتم بيان مسألة تأمين المستند الإلكتروني

وتقنياته **(المطلب الثاني)**، هذا وسيتم إلقاء الضوء على حفظ المستنـــد الإلكتـــروني **(المطلب الثالث)**.

المطلب الأول: توثيق المستند الإلكتروني.

إن شيوع التعاملات الإلكترونية يتوقف على قدر ما تتمتع به من أمان وثقة لدى مستخدمي وسائل الاتصال الحديثة، ولما كانت المستندات الإلكترونية بما فيها العقود تتم عن بعد بين أطراف قد يجهل بعضهم البعض، فضلاً عن عدم وجود علاقات سابقة بينهم، وهو الأمر الذي يتطلب توفير الضمانات ووسائل تكفل تحديد هوية المتعاقدين، وتضمن التعبير عن إرادتهم على نحو صحيح، وبطريقة يمكن معها نسبة التصرف إلى صاحبه، غير أن توفير هذا كله يتطلب إيجاد حلول تقنية لا سيما في ظل تنامي القرصنة الإلكترونية، وإساءة استخدام أسماء الغير وتوقيعاتهم في أنشطة غير مشروعة عبر الإنترنت[1].

ولهذا ظهرت الحاجة إلى وجود طرف ثالث محايد موثوق به، يتأكد بطرقه الخاصة من سلامة المستند الإلكتروني، وكذا من صحة التواقيع الإلكترونية، وكذا الإرادة التعاقدية الإلكترونية ممن تنسب إليه، كما يتأكد أيضا من جدية هذه التواقيع وبعدها عن الغش والاحتيال، ويتمثل هذا الطرف الثالث المحايد في أفراد أو شركات أو جهات مستقلة تقوم بدور الوسيط بين المتعاملين لتوثيق تعاملاتهم الإلكترونية، يطلق عليها اسم جهات التوثيق أو سلطات التوثيق[2].

وعليه فإن التوثيق[3] أو التصديق **(certification)** في مفهومه العام يعني التصديق والتأكيد، وقد عرّفه الفقه الفرنسي على أنه: "إجراء بمقتضاه يقدم طرف ثالث (شخص من

---

[1]- لزهر بن سعيد، المرجع السابق، ص. 172؛ إيمان مأمون أحمد سليمان، المرجع السابق، ص. 308.

[2]- سليم سعداوي، عقود التجارة الالكترونية - دراسة مقارنة- ط1، دار الخلدونية، الجزائر، 2008، ص.87؛
Isabelle De Lamberterie, op. cit,p.p.166-167.

[3]- للإشارة فإن كلمة توثيق (certification) هي كلمة مستمدة في اللغة الفرنسية من كلمة (certificat) وهذه الكلمة في الأصل لاتينية المصدر ويطلق عليها بهذه اللغة (certus)، ومعناها في اللغة الفرنسية قرر (décide)، صمم (résolu)، حدد (fixé, déterminé)، دقّق (précis)، عين (certain)، وافق (convenu)، أكد (sur) عزم، أمن (sécurité)، أما عن معناها القانوني فيلاحظ أن القواميس اللغوية أعطتها العديد من المعاني وهي في مجملها تدور بين التأمين والإشهاد والترخيص وكذا الضمان. لتفاصيل أكثر يراجع، مصطفى أبو مندور موسى، الجوانب القانونية لخدمات التوثيق الإلكتروني، دراسة مقارنة، دار النهضة العربية، مصر، 2004، ص. 18 وما يليها.

الغير) ضماناً بأن مستند أو منتج أو برنامج معين، أو خدمة أو هيئة معينة يتوافق مع ضوابط ومعايير واشتراطات خاصة"[1].

على ضوء هذا التعريف، يمكن القول أن التوثيق وسيلة أو أداة تقدم مقياسا موضوعيا على مطابقة مستند للقانون، أو على جودة سلعة أو برنامج أو خدمة معينة، وذلك من خلال تبني معايير أو ضوابط معينة يجب توافرها في هذا المستند أو تلك الخدمة أو ذلك البرنامج ، فالتوثيق باختصار شديد هو بمثابة ميزان بيد المتعامل يزن به درجة جودة ما هو معروض عليه من خدمات وبرامج، ليتمكن بالتالي من المفاضلة بينها، واختيار أفضلها[2].

وإذا كان التوثيق بمعناه العام يعني ضمان المطابقة إلى ضوابط ومعايير واشتراطات معينة، فإن التوثيق الإلكتروني أو التصديق في المجال الإلكتروني وتكنولوجيا المعلومات يعني بشكل أخص ضمان سلامة وتأمين "sécurité" التعامل عبر الإنترنت، سواء من حيث أطرافه ومضمونه ومحله وتاريخه، ذلك أنه وسيلة آمنة للتحقق من صحة التوقيع أو المستند حيث يتم نسبته إلى شخص أو كيان معين[3].

بعبارة أخرى يعني التوثيق الإلكتروني خلق بيئة إلكترونية آمنة للتعامل عبر الإنترنت، خاصة وأن هذا التعامل يتم غالبا بين أشخاص لا يربطهم مكان واحد، وعبر وسيط مفتوح وغير آمن، وعن طريق التجول في متجر افتراضي قوامه الأشكال والصور، وبطريقة ينعدم فيها أي دليل مادي على حقيقة ما تم، وهو الأمر الذي يقتضي بالضرورة اللجوء إلى هذه الآلية، وذلك بغية خلق نوع من الثقة والأمان في هذا النوع من التعاملات[4].

---

[1]- "La certification est une procédure par laquelle une tierce partie donne une assurance écrite qu'un document, un produit, un système qualité, un organisme est conforme à des exigences spécifies." Cf. Xavier Liant De Bellfond, le droit du commerce électronique, puf, paris, 2005, p .103.

[2] - مصطفى أبو مندور موسى، المرجع السابق، ص. 19.

[3] - محمد حسين منصور، الإثبات الإلكتروني، دار الفكر الجامعي، الإسكندرية، 2006، ص. 209.

[4]- أيمن أحمد الدلوع، التنظيم القانوني للتوثيق الالكتروني، دار الجامعة الجديدة ، مصر، 2016، ص.27؛ مصطفى أبو مندور موسى، المرجع السابق، ص. 23.

وطالما أن جهات التوثيق أو التصديق هي التي تتولى مهمة التصديق على المستند والتوقيع الإلكتروني، فماذا يقصد بهذه الجهات؟ وما هو دورها؟، ما طبيعة عملها؟ ما هو نوع الشهادات التي تصدرها؟

هذا ما سيتم بيانه بالتطرق إلى جهات التصديق أو توثيق المستند الإلكتروني **(الفرع الأول)**، وبعدها لشهادة التصديق الالكتروني **(الفرع الثاني)**.

الفرع الأول: جهات توثيق المستند الإلكتروني.

تتعدد تسمية هذه الجهات فهناك من أطلق عليها تسمية الغير محل الثقة **(le tiers de confiance)**، وهناك من عبر عنها بمزودي خدمات المصادقة الإلكترونية أو مراقبي خدمات التوثيق، في حين أشار لها البعض الآخر بتسمية موفر الخدمات أو مقدم خدمات التصديق.

هذه التسميات في كل صيغها تعبر بصدق عن حقيقة الدور المنوط بهذا الشخص الذي يتمثل في تأكيد وتوثيق المعاملة، وبالتالي بث الثقة لدى مستعملي الشبكات المفتوحة وذلك من خلال إتباع مجموعة من الوسائل والإجراءات الفنية اللازمة لتأمين ما يجري بينهم من تعاملات، وصونها من العبث طوال فترة حفظها[1].

وعليه فإن جهة التوثيق تعرف على أنها شخص أو جهة أو منظمة عامة، أو خاصة مستقلة ومحايدة تقوم بدور الوسيط بين المتعاملين لتوثيق تعاملاتهم الإلكترونية مصدرة بذلك شهادة إلكترونية، ويرمز لهذه الجهة اختصارا برمز **(PSC)** حيث تتدخل هذه الجهة بناءاً على طلب شخصين أو أكثر بهدف إنشاء وحفظ وإثبات الرسائل الإلكترونية[2].

هذا ولقد تطرق قانون الأونيسترال النموذجي لسنة 2001 المتعلق بالتوقيعات الإلكترونية لهذه الجهة تحت مسمى مقدم خدمات التصديق، وعرفه في نص المادة الثانية

[1] - مصطفى أبو مندور موسى، المرجع السابق، ص.29؛
Xavier Liant De Bellfond,,op. cit, p.103.

[2] - أيمن أحمد الدلوع، المرجع السابق ،ص. 26.؛ لزهر بن سعيد، المرجع السابق، ص. 172؛ إيمان مأمون أحمد سليمان، المرجع السابق، ص. 309.

الفقرة (هـ) بأنه: " شخص يصدر شهادات، ويجوز أن يقدم خدمات أخرى ذات الصلة بالتوقيعات الإلكترونية"[1].

كما عرف التوجيه الأوروبي رقم 93 لسنة 1999 هذه الجهة في المادة الثانية فقرة 11 منه بأنها: " كل شخص طبيعي أو معنوي يصدر شهادات توثيق التوقيع الإلكتروني، أو يتولى خدمات أخرى مرتبطة بالتوقيع الإلكتروني"[2].

كما ألزم هذا التوجيه الدول الأعضاء في الاتحاد الأوروبي بالترخيص بقيام جهات خاصة تتولى مهام اعتماد التوقيعات الإلكترونية، وذلك عن طريق إصدارها لشهادات تثبت استيفاء التوقيع الإلكتروني للشروط اللازمة لكي يعتد به في الإثبات، وتضمن ارتباطه بالمستند المذيل به، مع تأمينه ضد أي تعديل أو تغيير في مضمونه[3].

أما عن موقف التشريعات العربية من جهات التصديق على المعاملات الإلكترونية، فنجد مثلا أن المشرع التونسي كان سبّاقا في تنظيم هذه الجهة، وهذا بموجب القانون رقم 83 لسنة 2000 المتعلق بالمبادلات والتجارة الإلكترونية، حيث سماها بمزودي خدمات المصادقة الإلكترونية، وعرّفها في نص المادة الثانية من القانون المذكور بأنها: "كل شخص طبيعي أو معنوي يحدث أو يسلم أو يتصرف في شهادات المصادقة، ويسدي خدمات أخرى ذات صلة بالإمضاء الإلكتروني"[4].

كما نص في المادة الثامنة من نفس القانون على إنشاء الوكالة الوطنية للمصادقة الإلكترونية، واعتبرها مؤسسة عامة تتمتع بالشخصية المعنوية والاستقلال المالي، حيث

---

[1] - خالد ممدوح إبراهيم، حجية البريد الإلكتروني في الإثبات، المرجع السابق، ص،ص. 208- 209.

[2]- يقصد بالخدمات المرتبطة بالتوقيع الإلكتروني التقنيات التي تسمح بإصدار توقيع مؤرخ، وخدمات النشر والاطلاع والخدمات المعلوماتية الأخرى كالحفظ في الأرشيف،
وللإشارة فإن نفس هذا التعريف أورده المشرع الإماراتي في نص المادة الثانية من قانون المعاملات والتجارة الإلكترونية الإماراتي رقم 2 لسنة 2002. مشار إليه من طرف، علاء حسين مطلق التميمي، الأرشيف الإلكتروني وكيفية المحافظة على المستند الإلكتروني عبر الزمن، دراسة مقارنة، المرجع السابق، ص. 98.

[3] - إيمان مأمون أحمد سليمان، المرجع السابق، ص.312؛ لزهر بن سعيد، المرجع السابق، ص. 174.

[4]- الفصل 2 الفقرة الثالثة من قانون رقم 83 لسنة 2000 المتعلق بالمبادلات والتجارة الإلكترونية، سابق الإشارة إليه.

جعلها تتولى منح تراخيص مزاولة نشاط مقدمي خدمات المصادقة الإلكترونية، وكذا مراقبة تلك الجهات لأحكام القانون[1].

وقد اعترف المشرع الجزائري بهذه الجهة وسماها بمؤدي خدمات التصديق، وعرّفها بداية في نص المادة 3 مكرر من المرسوم التنفيذي 162/07 المتعلق بنظام استغلال الشبكات بما فيها السلكية الكهربائية، وعلى مختلف خدمات المواصلات السلكية واللاسلكية بأنها: "كل شخص في مفهوم المادة 8-8 من القانون رقم 02/2000 المؤرخ في 5 غشت سنة 2000 المذكور أعلاه، يسلم شهادات أو يقدم خدمات أخرى في مجال التوقيع الإلكتروني"[2]. وبالرجوع إلى المادة 08 الفقرة 08 من القانون رقم 2000-03 المحدد للقواعد العامة المتعلق بالبريد والمواصلات السلكية واللاسلكية، نجد أنه يعرف موفر الخدمات على أنه: "كل شخص معنوي أو طبيعي يقدم خدمات مستعملاً وسائل المواصلات السلكية واللاسلكية"[3].

بعد ذلك أصدر المشرع الجزائري القانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين[4]، وفيه خصص المادة الثانية الفقرة 12 لتعريف مؤدي خدمات التصديق، بحيث اعتبره: " كل شخص طبيعي أو معنوي يقوم بمنح شهادات تصديق إلكتروني موصوفة، وقد يقدم خدمات أخرى في مجال التصديق الإلكتروني".

إن جديد المشرع الجزائري في التصديق الإلكتروني إستحداثه بموجب قانون التوقيع والتصديق الإلكترونيين لثلاث سلطات للتصديق الإلكتروني، حيث فصل أحكامها في باب كامل من هذا القانون، وهو الباب الثالث الذي سماه بـسلطات التصديق الإلكتروني، وهذه السلطات تتمثل في السلطة الوطنية والسلطة الحكومية، وكذا السلطة الاقتصادية للتصديق الإلكتروني، كما حدد مهام كل سلطة على نحو تكمل كل منهما عمل الأخرى، وبصورة

[1]- الفصل 8 والفصل 9 من قانون رقم 83 لسنة 2000 المتعلق بالمبادلات والتجارة الإلكترونية، سابق الإشارة إليه.
[2]- المرسوم التنفيذي رقم 07-162 المعدل والمتمم للمرسوم التنفيذي رقم 01-123 والمتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللالسلكية الكهربائية، وعلى مختلف خدمات المواصلات السلكية واللاسلكية، سابق الإشارة إليه.
[3]- القانون رقم 2000-03 المحدد للقواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، سابق الإشارة إليه.
[4]- قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، سابق الإشارة إليه.

تضمن ترقية استعمال التوقيع والتصديق الإلكترونيين وتطورهما وتضمن موثوقية استعمالهما[1]، حيث قرر بداية للسلطة الوطنية للتصديق الإلكتروني عدة مهام من بينها: مهمة إعداد سياسة التصديق الإلكتروني، والسهر على تطبيقها، كما أناط لها مهمة الموافقة على سياسات التصديق الإلكتروني الصادرة من السلطتين الحكومية والاقتصادية للتصديق الإلكتروني، وبموجب نفس القانون أعطى المشرع السلطة الوطنية الحق في أن تقترح على الوزير الأول ما تراه مناسبا من مشاريع تمهيدية للنصوص التشريعية والتنظيمية التي تتعلق بمجال التوقيع أو المصادقة الإلكترونية، كما جعل دور هذه السلطة استشاري عند إعداد مشاريع النصوص التشريعية أو التنظيمية ذات الصلة بهذا المجال[2]، وهذا كله محاولة من المشرع لجعل هذه السلطة طرفا فاعلاً في إعداد النصوص التشريعية المتعلقة بهذه التقنية المستحدثة.

هذا عن السلطة الوطنية، أما بخصوص السلطة الحكومية للتصديق الإلكتروني فيلاحظ أن المشرع الجزائري وبموجب القانون آنف الذكر كلفها بمهمة متابعة ومراقبة التصديق الإلكتروني، وكذا ضمان توفير خدمة التصديق لفائدة المتدخلين في الفرع الحكومي، كما خول لها عدة مهام أخرى من بينها إعداد القواعد والإجراءات التنظيمية والتقنية المتعلقة بالتوقيع والتصديق الإلكترونيين، وكذا السهر على تطبيقهما، وذلك بعد الحصول على موافقة من السلطة الوطنية.

هذا وقد أناط لها كذلك مهمة إرسال كل المعلومات المتعلقة بنشاط التصديق الإلكتروني إلى السلطة دوريا سواءً بمفردها، أو بناءً على طلب من السلطة بذلك[3].

أما السلطة الاقتصادية للتصديق الإلكتروني فقد وسّع المشرع الجزائري من مهامها بموجب القانون المذكور، حيث أعطى لها الحق في منح التراخيص لمؤدي خدمات التصديق الإلكتروني، وكذا الموافقة على سياسات التصديق الصادرة عن هذه الهيئات، وفي حالة عجز

[1]- المادة 16 وما يليها من قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، سابق الإشارة إليه.
[2]- المادة 18 من القانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، سابق الاشارة إليه .
[3]- المادة 28 من القانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، سابق الإشارة إليه.

مؤدي خدمات التصديق عن تقديم خدماته فإن المشرع قد خول للسلطة الاقتصادية الصلاحية في أن تتخذ كل التدابير اللازمة لضمان استمرارية الخدمات، وأكثر من ذلك فقد أعطى المشرع لهذه السلطة صلاحية التحكيم في النزاعات القائمة بين مؤدي خدمات التصديق فيما بينهم أو مع المستعملين، كما أعطاها أيضا الحق في تبليغ النيابة العامة عن كل فعل ذي طابع جزائي تكتشفه وهي تقوم بتأدية مهامها[1].

والجدير بالذكر أن المشرع باستحداثه لهذا النص التشريعي، فإنه يكون قد ساهم بقسط وافر في إزالة الغموض حول عدة نقاط كانت تثار في السابق من طرف الفقه ورجال القانون.

وفضلا عما سبق ذكره، يلاحظ أن المشرع الجزائري قد اعتمد نظام التصديق الإلكتروني حتى في قطاع العدالة، وذلك رغبةً منه في عصرنة هذا القطاع، وتحسين مستوى الخدمات، وهو الأمر الذي جسده عمليا بصدور قانون رقم 15-03 المتعلق بعصرنة العدالة[2]، والذي بموجبه استحدث منظومة معلوماتية مركزية للمعالجة الآلية للمعطيات وجعلها تابعة لوزارة العدل، كما أجاز في نفس القانون أن تمهر الوثائق والمحررات القضائية التي تسلمها مصالح وزارة العدل بتوقيع إلكتروني[3].

الفرع الثاني: شهادة توثيق المستند الإلكتروني.

تعمل جهات التوثيق الإلكتروني على توثيق المستند والتوقيع الإلكتروني مصدرة بذلك شهادة تبين بأن التوقيع الإلكتروني صحيح وصادر ممن نسب إليه، وأنه يستوفي الشروط والضوابط المطلوبة فيه[4].

---

[1]- لتفاصيل أكثر حول مهام السلطة الاقتصادية للتصديق الإلكتروني، يراجع المادة 30 من القانون 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين، سابق الإشارة إليه.

[2]- قانون 15-03 المؤرخ في 11 ربيع الثاني عام 1436 ه الموافق ل 01 فبراير 2015 المتعلق بعصرنة قطاع العدالة، ج.ر، ع06، لسنة 2015.

[3]- المادة 04 من القانون 15-03 المتعلق بعصرنة العدالة، سابق الإشارة إليه.

[4]- خالد ممدوح إبراهيم، أمن المعلومات الإلكترونية، المرجع السابق، ص. 117؛ أيمن أحمد الدلوع، المرجع السابق، ص.26؛ سليم سعداوي، المرجع السابق، ص.92؛

Lionel Bochunrberg, internet et commerce électronique, 2ème éd, Delmas, 2001, p.142.

كما تؤكد هذه الشهادة أيضا أن البيانات الموقع عليها والتي يحتويها المستند الإلكتروني هي بيانات صحيحة، ولم يتم التلاعب فيها سواء بالتعديل أو الحذف أو الإضافة أو التغيير، وهو الأمر الذي من شأنه أن يرسخ الثقة والأمان لدى المتعاملين عبر الإنترنت[1]، وتسمى هذه الشهادة بشهادة التصديق الإلكتروني، وللإشارة فإن هذه الشهادة عرفت تحت تسمية بطاقة إثبات الهوية الإلكترونية[2] وعُرفت بأنها: "شهادة تصدر أثناء عملية التوقيع الإلكتروني، من شأنها إثبات هوية الموقع".

هذا وقد عرّفها البعض بأنها: "عملية إلكترونية تربط بين شخص معين (قد يكون شخص طبيعي أو معنوي) بخصائص معينة تسمح بتمييزه عن غيره"، كما عرفها جانب آخر بأنها: " الشهادات التي تصدرها جهات التوثيق المرخص لها من قبل الجهات المسؤولة في الدولة، لتشهد بأن التوقيع الإلكتروني هو توقيع صحيح ينسب إلى من أصدره، وأنه يستوفي الشروط والضوابط المطلوبة فيه باعتباره دليل إثبات يعول عليه"[3]، وعرفها جانب آخر بأنها: "شهادة في شكل إلكتروني تثبت العلاقة ما بين معطيات مراقبة التوقيع والموقع.[4]

ونظراً لأهمية هذه الشهادة عمدت التشريعات المقارنة والعربية إلى تنظيمها وضبط أحكامها بموجب نصوص قانونية، ومن ذلك ما قرره التوجيه الأوروبي رقم 99/93 بشأن التوقيعات الإلكترونية الصادر في 13 ديسمبر 1999 الذي اعترف بها وميّز بين نوعين منها: وهما الشهادة الإلكترونية البسيطة والشهادة الإلكترونية الموصوفة، وهذا في نص المادة الثانية الفقرة 09 و10، بحيث عرّف النوع الأول (الشهادة البسيطة) بأنها: "الشهادة الإلكترونية التي تربط البيانات الخاصة لفحص التوقيع الإلكتروني وشخص معين، وتؤكد هوية هذا الشخص"، أما الشهادة الثانية (الموصوفة) فقد عرفتها نفس المادة واعتبرتها:

---

[1] - لزهر بن سعيد، المرجع السابق، ص .182.

[2]- Cf. B.Chankire, Problèmes juridique posée par l'internet dans la vente internationale de marchandises, DEES droit des affaires, des université D'abomey- Calavi (République de Bénin), 2004, p.82.

[3]- علاء حسين مطلق التميمي، الأرشيف الإلكتروني وكيفية المحافظة على المستند الإلكتروني عبر الزمن، المرجع السابق، ص. 109.

[4]- Cf.A. Bensoussaan, Informatique Télécoms Internet, 4 ed, éditions Francis Lefebvre, 2008, p.216.

"شهادة تستوفي المتطلبات المنصوص عليها في الملحق الأول، والتي يقدمها المكلف بخدمة التوثيق المستوفي للمتطلبات المنصوص عليها في الملحق الثاني"[1].

أما قانون الأونيسترال النموذجي بشأن التوقيعات الإلكترونية لسنة 2001، فقد عرّف شهادة التصديق الإلكتروني في نص المادة الثانية منه بأنها: " رسالة بيانات أو سجل آخر يؤكدان الارتباط بين الموقع، وبيانات إنشاء التوقيع"[2].

أما بالنسبة للتشريعات العربية، فيلاحظ أن المشرع التونسي قد اعترف بهذه الشهادة بموجب قانون المبادلات والتجارة الإلكترونية[3]، وعرّفها في الفصل الثاني منه بأنها: "الوثيقة الإلكترونية المؤمنة بواسطة الإمضاء الإلكتروني للشخص الذي أصدرها، والذي يشهد من خلالها أثر المعاينة على صحة البيانات التي تتضمنها".

كما عرفها المشرع المصري في المادة الأولى من قانون التوقيع الإلكتروني بأنّها: "الشهادة التي تصدر من الجهة المرخص لها بالتصديق، وتثبت الارتباط بين الموقع وبين إنشاء الشهادة"[4].

أما بخصوص المشرع الجزائري، فيلاحظ أن هذا الأخير قد اعترف بها وأطلق عليها تسمية الشهادة الإلكترونية، وذلك بموجب المرسوم التنفيذي رقم 162/07 والذي عرفها فيه على أنها: "وثيقة في شكل إلكتروني تثبت الصلة بين معطيات فحص التوقيع الإلكتروني والموقع"[5]، ثم جاء المشرع بعد ذلك في القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين وأعطاها تقريبا نفس التعريف[6].

---

[1]- إيمان مأمون أحمد سليمان، المرجع السابق، ص،ص. 320- 321؛ علاء حسين مطلق التميمي، الأرشيف الإلكتروني وكيفية المحافظة على المستند الإلكتروني عبر الزمن، دراسة مقارنة، المرجع السابق، ص. 108.

[2]- قانون الأونيسترال النموذجي بشأن التوقيعات الإلكترونية لسنة 2001، سابق الإشارة إليه.

[3] - القانون رقم 83 لسنة 2000 المتعلق بالمبادلات والتجارة الإلكترونية، سابق الإشارة إليه.

[4] - المادة الأولى الفقرة و من القانون رقم 15 لسنة 2004 المتعلق بتنظيم التوقيع الالكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات سابق الإشارة إليه.

[5]- المادة 03 مكرر من المرسوم التنفيذي رقم 07-162 المعدل والمتمم للمرسوم التنفيذي رقم 01-123 والمتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية، وعلى مختلف خدمات المواصلات السلكية واللاسلكية، سابق الإشارة إليه.

[6]- للإشارة فإن المشرع الجزائري قد أورد نفس التعريف المذكور في نص المادة الثانية الفقرة 07 من القانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، سابق الإشارة إليه.

ولعل الجديد الذي أورده المشرع الجزائري في قانون التوقيع والتصديق الإلكترونيين تمييزه بين نوعين من شهادة التصديق، شهادة التصديق العادية، وشهادة التصديق الإلكترونية الموصوفة، وهو في ذلك يكون قد سار على نهج التوجيه الأوروبي رقم 99/93 المتعلق بالتوقيعات الإلكترونية.

وقد عرف المشرع الجزائري شهادة التصديق بصفة عامة في المادة 02/07 من قانون التوقيع والتصديق الإلكتروني واعتبرها: "وثيقة في شكل إلكتروني تثبت الصلة بين بيانات التحقق من التوقيع الإلكتروني والموقع".

في حين خص شهادة التوقيع الإلكتروني الموصوفة بنص المادة 15 من ذات القانون، واشترط لإضفاء هذا الوصف عليها توفر بعض المتطلبات القانونية وكذا تضمنها بيانات محددة، فأما عن متطلبات هذه الشهادة فتتمثل في ضرورة صدورها من طرف ثالث موثوق[1]، أو من طرف مؤدي خدمات تصديق إلكتروني طبقا لسياسة التصديق الموافق عليه، مع منحها للموقع دون سواه، أما عن بيانات هذه الشهادة، فتشمل ضرورة التأشير عليها لتأكيد أنها شهادة موصوفة، وكذا تحديد هوية الطرف الذي أصدرها سواءً كان طرفا ثالث موثوق أو مؤدي خدمات تصديق إلكتروني، وكذا تحديد البلد الذي يقيم فيه، هذا ويشترط أيضاً إدراج اسم الموقع وصفته عند الاقتضاء، وذلك حسب الغرض من استعمال هذه الشهادة، وللإشارة فإن حصول مقدم الخدمات على هذه المعلومات يتم إما من طرف الموقع شخصيا، أو من طرف أشخاص يخول لهم الموقع التصريح بها[2].

إلى جانب هذه البيانات، يجب أن تتضمن هذه الشهادة بيانات تتعلق بالتوقيع الإلكتروني كتلك التي تتعلق بالتحقق من هذا التوقيع، بداية ونهاية مدة صلاحية شهادة التصديق الإلكتروني، زيادة على بيانات أخرى عددها المشرع الجزائري في هذا القانون[3].

---

[1]- عرف المشرع الجزائري الطرف الثالث الموثوق في المادة الثانية فقرة 11 من القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين، سابق الإشارة إليه بأنه: " شخص معنوي يقوم بمنح شهادات تصديق إلكتروني موصوفة، وقد يقدم خدمات أخرى في مجال التصديق الإلكتروني".

[2]- Cf. Sédallian (V), preuve et signature électronique :www.internet-juridique.net. date de consultation le site 12-12-2014 à17 :00.

[3] - المادة 15 من القانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، سابق الإشارة إليه.

كما نص المشرع على صاحب شهادة التصديق الإلكتروني وعرّفه في ذات القانون المذكور بأنّه: " شخص طبيعي أو معنوي تحصل على شهادة التصديق الإلكتروني من طرف مؤدي خدمات التصديق الإلكتروني أو طرف ثالث موثوق"[1]، هذا وقد نظم أيضا مسؤولية صاحب هذه الشهادة حيث اعتبره المشرع مسئولا عن سرية بيانات إنشاء التوقيع، كما منع صاحب شهادة التصديق الإلكتروني الموصوفة من استعمال هذه الشهادة لأغراض أخرى غير تلك التي منحت من أجلها[2].

أما عن أنواع شهادات التوثيق الإلكتروني، فيمكن القول أنها أصبحت في الوقت الحالي تتعدد وتتنوع، فإلى جانب شهادة توثيق التوقيع الرقمي التي سبق الإشارة إليها، هناك شهادات أخرى تتنوع بحسب الهدف منها ومن أمثلتها، شهادة توثيق تاريخ الإصدار (Digital Time Stamp) التي توثق تاريخ ووقت إصدار التوقيع الرقمي، حيث يقوم صاحب الرسالة بعد التوقيع عليها بإرسالها إلى جهة التوثيق التي تقوم بتسجيل التاريخ عليها وتوقيعها من جهتها لتعيدها بعد ذلك إلى مرسلها، هذا وتوجد أيضاً شهادة الإذن (Authorizing Certificate) والتي بمقتضاها يتم تقديم بيانات ومعلومات إضافية عن صاحبها مثل: عمله ومؤهلاته ومحل إقامته والتراخيص التي يملكها، كما توجد أيضا شهادة البيان (Attesting Certificate) والتي تثبت صحة واقعة معينة، ووقت وقوعها[3].

من خلال ما سبق، تبرز أهمية هذه الشهادات ومدى خطورة المعلومات التي تتضمنها، نظرا لاعتماد الغير عليها لإبرام معاملاته مع صاحبها في حدود معينة.

هذا فيما يخص شهادة التوثيق المحلية الصادرة عن مؤدي خدمات تصديق محلي، أما فيما يخص شهادات التصديق الأجنبية، أي الصادرة من مؤدي خدمات التصديق الموجود في بلد أجنبي، فيثار الإشكال حول مدى قيمة وفعالية هذه الشهادات من الناحية القانونية؟ وهل يمكن اعتبار شهادات التصديق الأجنبية (الصادرة عن مزود خدمة أجنبي) متساوياً من حيث

[1]- المادة الثانية الفقرة 14 من القانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، سابق الإشارة إليه.

[2]- المواد 61- 62 من القانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، سابق الإشارة إليه.

[3]- خالد ممدوح إبراهيم، أمن المعلومات الإلكترونية، المرجع السابق، ص.118؛ إيمان مأمون أحمد سليمان، المرجع السابق، ص. 325؛ سليم سعداوي، المرجع السابق، ص.95.

القيمة مع شهادات التصديق التي يسلمها مزود خدمة التصديق المحلي، خاصة في ظل القانون الجزائري؟.

لقد أجاب المشرع الجزائري عن هذا الإشكال في نص المادة 3 مكرر 1 من المرسوم التنفيذي رقم 07-162، والتي تقضي بـ: "تكون للشهادات التي يسلمها مؤدي خدمات تصديق إلكتروني مقيم في بلد أجنبي نفس قيمة الشهادات المسلمة بموجب أحكام هذا المرسوم، إذا كان هذا المؤدي الأجنبي يتصرف في إطار اتفاقية للاعتراف المتبادل أبرمتها سلطة ضبط البريد والمواصلات السلكية واللاسلكية"[1].

من خلال هذه المادة، يلاحظ أن المشرع الجزائري قد وضع مبدأ المساواة ما بين شهادة التصديق الإلكترونية الصادرة عن مزود خدمة أجنبي، وشهادة التصديق الصادرة عن مؤدي خدمة التصديق خاضع للقانون الجزائري، وقد أكد المشرع هذا المبدأ سنة 2015 من خلال نص المادة 63 من القانون المتعلق بالتوقيع والتصديق الإلكترونيين[2]، حيث تقضي هذه الأخيرة: "تكون لشهادات التصديق الإلكتروني التي يمنحها مؤدي خدمات التصديق الإلكتروني المقيم في بلد أجنبي نفس قيمة الشهادات الممنوحة من طرف مؤدي خدمات التصديق الإلكتروني المقيم في الجزائر، بشرط أن يكون مؤدي الخدمات الأجنبي هذا قد تصرف في إطار اتفاقية للاعتراف المتبادل أبرمتها السلطة".

المطلب الثاني: تأمين المستند الإلكتروني.

إن أكثر ما يهدد المعاملات الإلكترونية بصفة عامة، والتجارة الإلكترونية بصفة خاصة المساس بأمن المعلومات، وعدم تأمين المستندات الإلكترونية وكذا التواقيع الإلكترونية التي تتضمنها هذه المستندات، وهو الأمر الذي يؤدي إلى عدم ضمان سلامة عملية تداول المعلومات الخاصة بإتمام المعاملات والصفقات، ولعل السبب وراء هذا كله

[1]- المرسوم التنفيذي رقم 07-162 المعدل والمتمم للمرسوم التنفيذي رقم 01-123 والمتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية، وعلى مختلف خدمات المواصلات السلكية واللاسلكية سابق الإشارة إليه.

[2] - قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، سابق الاشارة إليه .

يكمن في اتسام المعاملات الإلكترونية، وخاصة تلك المبرمة عبر الإنترنت بوجود طرف ثالث غير المتعاقدين، قد يكون الغير مستخدم الشبكة، كما قد يكون جهة أخرى[1].

بسبب هذا كان من اللازم أن يحاط المستند الإلكتروني بقدر من السرية تكفل له عدم اطلاع الغير عليه وعلى ما يحتويه من معلومات[2]، كما كان لا بد من إيجاد تقنية لحفظ سرية البيانات وحمايتها، حتى لا يستطيع أي شخص باستثناء المتعاقدين أو من يصرح له القانون بذلك الاطلاع عليها[3]، وفي سبيل تحقيق هذا كله تم استحداث نظام التشفير كتقنية فنية لتأمين المعلومات والتواقيع الإلكترونية، وكذا المعاملات الإلكترونية، ذلك أنه إجراء يؤدي إلى توفير الثقة والأمان.

من هنا ينبغي التساؤل ما المقصود بتقنية التشفير؟ وما هو نظام عمله وطرق استعماله؟ وما هي أحدث التقنيات المستعملة لتأمين المعلومات والبيانات التي تحتويها المستندات الإلكترونية؟.

للإجابة على هذه التساؤلات سوف يتم التعرض إلى نظام التشفير ومختلف المفاهيم المتعلقة به، وكذا طرق استخدامه **(الفرع الأول)**، على أن يتم بعدها التطرق لبعض التقنيات الحديثة التي تستخدم كوسيلة لتأمين المستند الإلكتروني **(الفرع الثاني)**.

الفرع الأول: التشفير كوسيلة لتأمين المستند الإلكتروني.

يعد نظام التشفير أحد فروع العلوم الرياضية، وهو يُستخدم كوسيلة فنية لحماية البيانات والمعطيات المعالجة آليا، وللإشارة فإن استخدام التشفير في الزمن الماضي كان مقتصرا على الأغراض الحكومية والعسكرية فقط، ولكن حالياً امتدت استخداماته حتى أصبح يدخل في كثير من نظم المعلومات والشبكات، هذا ولقد مر التشفير بمراحل عديدة من التطور وما زال هذا النظام في تطور مستمر حتى الآن، ذلك أنه عندما يضع المشفرون نظام

[1]- هدى حامد قشقوش، المرجع السابق، ص. 61.
[2]- عبد المحسن بدوي أحمد، حقوق الملكية الفكرية وتكنولوجيا المعلومات، الأمن والحياة، إعلامية- أمنية- ثقافية، ع (325)، س الثامنة والعشرون، جمادى الآخرة 1430هـ- يونيو 2009، ص.44.
[3]- محمد أمين الرومي، المستند الإلكتروني، المرجع السابق، ص. 67؛ هدى حامد قشقوش، المرجع السابق، ص، ص.61-62.

تشفير يأتي آخرون ويحاولون فك هذا النظام ومعرفة سر الشفرة، فيلجأ المشفرون لنظام جديدا وهكذا دواليك[1].

ونظرا لأن نظام التشفير مسألة علمية محضة، سيتم السعي لبيان مفهومها **(البند الأول)**، ثم التعرض لطرقها **(البند الثاني)**.

البند الأول: مفهوم التشفير.

تعددت المفاهيم الفقهية الواردة بشأن التشفير، بحيث عرّفه جانب من الفقه[2] بأنه: "عملية يتم فيها تحويل الرسالة، وكذا التوقيع عليها من صورتها العادية إلى صورة أرقام أو رموز غير مفهومة، وذلك باستخدام مفاتيح سرية وطرق حسابية معقدة "لوغاريتمات"، لا يمكن فهمها إلا بفك تشفيرها ممن يملك مفتاح فك التشفير".

كما عرفه جانب آخر[3] بأنه: "عملية الحفاظ على سرية المعلومات الثابت منها والمتحرك، باستخدام برامج لها القدرة على تحويل وترجمة تلك المعلومات إلى رموز، بحيث إذا ما تم الوصول إليها من قبل أشخاص غير مخول لهم بذلك لا يمكنهم فهم أي شيء، لأن ما يظهر لهم هو خليط من الرموز والأرقام والحروف غير المفهومة".

ولمصطلح التشفير عبر الإنترنت معنى آخر يستخدمه الفقه كناية عنه، وهو مصطلح التخفي أو الإخفاء (cryptage) وهو يفيد إخفاء المعلومة في أساس بياناتها، بحيث إذا ظهرت تلك البيانات فإنها لن تعبر عن فحواها الحقيقي، وهو الأمر الذي يجعلها معلومة غير ذات معنى أو ناقصة.

بهذا يبدو أن التشفير عبارة عن فلسفة معينة يتم بها حصر معلومة في نطاق محدد، وهو أسلوب يتم اللجوء إليه قصد حجب معلومة ما من التداول العام، ومنع الغير بمعنى من

[1] - محمد أمين الرومي، النظام القانوني للتوقيع الإلكتروني، دار الكتب القانونية، مصر، 2008، ص. 32.
[2] - مصطفى أبو مندور موسى، المرجع السابق، ص. 31؛
Céline Castets-Renard, droit de l'internet: droit français et européen, 2éme éd, Montchrestien, lextenso édition, paris, France, 2012, p .29.
[3] - محمد أمين الرومي، النظام القانوني للتوقيع الإلكتروني، المرجع السابق، ص. 32.

ليس لهم الحق في التعامل مع الموقع أو المستند الإلكتروني من الدخول إليه والحصول على خدماته ما لم يصرح له المالك بذلك، ويكون تصريح المالك للغير بالاطلاع على المعلومات المشفرة باستخدام مفتاح فك التشفير، وهذا الأخير هو عبارة عن منتج أو آلة أو مركب تم تصميمه لكي يقوم بفك شفرة الدخول، هذا ويطلق على المعلومة حال تشفيرها عبارة نص مشفر (Cipher Text)، أما المعلومات التي لم يتم تشفيرها فيطلق عليها مصطلح النص الكامل (Plain Text) [1].

ونظرا لأهمية التشفير ودوره الفعال في حماية البيانات، فقد عمدت التشريعات إلى تنظيمه في نصوصها القانونية، غير أن مواقفها تباينت في ذلك، إذ بينما تعرضت له بعض التشريعات بصفة صريحة، وخصته بتعريف دقيق لم تتطرق تشريعات أخرى لتعريفه، ويندرج ضمن الطائفة الأولى قانون المبادلات والتجارة الإلكترونية التونسي[2]، إذ عرفه في المادة الثانية منه بأنه: "استعمال رموز وإشارات غير متداولة تصبح بمقتضاها المعلومات المرغوب تمريرها أو إرسالها غير قابلة للفهم من قبل الغير، أو استعمال رموز وإشارات لا يمكن الوصول إلى معلومة بدونها".

كما عرفه المشرع المصري في المادة 01 الفقرة 09 من اللائحة التنفيذية المتعلقة بالتوقيع الإلكتروني[3] على أنه: "منظومة تقنية حسابية تستخدم مفاتيح خاصة لمعالجة وتحويل البيانات والمعلومات المقروءة إلكترونيا، بحيث تمنع استخلاص هذه البيانات والمعلومات إلا عن طريق استخدام مفتاح أو مفاتيح فك الشفرة".

ولئن كان المشرعين السابقين حددا صراحة المقصود بالتشفير، فإن المشرع الجزائري وقبل صدور قانون التوقيع والتصديق الإلكترونيين، لم يتطرق للتشفير إلا بصفة ضمنية عن طريق إدراج شرط فني ضمن نص المادة 323 مكرر1 من القانون المدني

[1]- عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الإنترنت، رسالة دكتوراه في القانون الجنائي، كلية الحقوق، جامعة عين شمس، 2004، ص . 379 وما يليها..

[2]- قانون رقم 83 لسنة 2000 المتعلق بالمبادلات والتجارة الإلكترونية، سابق الإشارة إليه.

[3]- قرار رقم 109 لسنة 2005 بتاريخ 15-05-2005 المتعلق بإصدار اللائحة التنفيذية للتوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة وتكنولوجيا المعلومات المصري.

الجزائري المعدل والمتمم، والتي اعترف بالكتابة في الشكل الإلكتروني، ومنح لها الحجية في الإثبات بحيث نصت المادة آنفة الذكر: " يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق، بشرط إمكانية التأكد من هوية الشخص الذي أصدرها، وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها"[1].

وعليه كان يستخلص من الشرط الفني السابق والمتمثل في "أن تكون معدة ومحفوظة في ظروف تضمن سلامتها" أن المشرع يستلزم توفر بعض الوسائل لحماية الكتابة الإلكترونية والتوقيع الإلكتروني.

وقد استمر الوضع رغم صدور قانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين، حيث لم يتطرق المشرع الجزائري فيه إلى تعريف التشفير، بل اكتفى بتحديد أنواعه والنص عليه كلما اقتضت ضرورة استخدامه، وهو ما يتضح من نص المادة الثانية في فقرتيها الثامنة والتاسعة[2].

والواقع أن المشرع الجزائري قد أصاب في هذا المجال، ذلك أن عملية التعريف مسألة فقهية محضة لا شأن للنص القانوني بها، وفي هذا يمكن القول أن التشفير عبارة عن مجموعة من الرموز والإشارات غير المتداولة، تجعل من المعلومات المرسلة غير قابلة للفهم من قبل الغير، إلا باستخدام رموز وإشارات أخرى لفك معناها، وهو بذلك وسيلة فنية لحماية البيانات من الآخرين.

البند الثاني: طرق التشفير.

يتم تشفير البيانات والمعلومات المعالجة آليا قصد حمايتها وتأمينها باستخدام مفاتيح سرية خاصة وعامة لتشفير الرسائل والبيانات وفك تشفيرها، هذا وتتم عملية التشفير بإتباع طرق ثلاث، تسمى الطريقة الأولى بالتشفير السيمتري أو المماثل، في حين تسمى الطريقة الثانية التشفير اللامماثل، ويطلق على الطريقة الثالثة التشفير عن طريق المزج بين النظامين

[1]- القانون رقم 05-10 المتضمن القانون المدني الجزائري المعدل والمتمم، سابق الإشارة إليه.
[2]- يحدد المشرع الجزائري في المادة الثانية فقرة 8 و9 من القانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين كل من مفتاح التشفير العام والخاص ويمنح تعريف لكل منهما.

السابقين. فما هو نظام عمل كل طريقة من هذه الطرق؟ وهل أن المشرع الجزائري تطرق إلى هذه التقنيات في نصوصه القانونية؟

أولاً: التشفير المماثل أو السيمتري(La cryptologie symétrique)

في هذا النوع من التشفير يستخدم كل من المرسل والمرسل إليه، أو مستقبل الرسالة نفس المفتاح السري لتشفير الرسالة وفك شفرتها وعليه يكون المفتاح السري معلوماً للطرفين، حيث يتفق الطرفان في البداية على عبارة مرور (un mot de passe) التي سيتم استخدامها، وتتكون عبارة المرور من حروف ورموز متعددة يتم تحويلها بموجب برمجيات التشفير إلى عدد ثنائي، حيث يشكل هذا العدد الثنائي الناتج مفتاح تشفير الرسالة، وبعد استقبال الرسالة المشفرة يستخدم المستقبل عبارة المرور نفسها، من أجل فك شفرة النص المشفر وتحويله إلى شكله الأصلي المفهوم[1]، وبهذا يلاحظ أن نفس المفتاح تختلف وظيفته بالنسبة لكل من المرسل والمستقبل، بحيث يستخدمه الأول في التشفير، في حين يستخدمه الثاني لفك التشفير.

وإذا كانت هذه الطريقة تتميز بالبساطة، إلا أن أهم ما يعيبها أنها تفترض سبق معرفة أطراف المعاملة لبعضهم البعض، وهو ما يتنافى والطبيعة العالمية المفتوحة لشبكة الإنترنت، هذه الشبكة التي لا تظهر فائدتها إلا في التعامل بين أطراف تفصل بينها الحدود والمسافات وقد لا يعرف بعضهما بعضاً[2].

كما أن ما يعيب هذه الطريقة عدم وجود وسيلة آمنة لتبادل المفتاح الوحيد المستخدم بين المرسل والمرسل إليه، وهو ما يعني التأثير سلباً على عامل الثقة الذي هو أساس نجاح المعاملات الإلكترونية بصفة عامة والتجارة الإلكترونية بصفة خاصة، فتبادل المفتاح السري نفسه بين الطرفين من خلال إرساله عبر الشبكة المفتوحة قد يسهل فرص التقاطه من قبل

[1]- سمير حامد عبد العزيز الجمال، المرجع السابق، ص. 219؛ عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، المرجع السابق، ص. 31 وما يليها؛

Xavier Liant De Bellfond, op. cit, p102.

[2]- مصطفى أبو مندور موسى، المرجع السابق، ص. 35.

القراصنة، ومن ثم اقتحام ومهاجمة البيانات التي تم إرسالها لدوافع كثيرة أقلها التلصص والاعتداء على الخصوصية[1].

فضلاً عن ذلك فإن هذه التقنية تفترض وجود مفتاح لكل معاملة بما يعني تعدد المفاتيح بتعدد المعاملات وتعدد المرسل إليهم، وهو الأمر الذي قد يقضي على عامل السرعة الذي تتميز به المعاملات التي تتم عن طريق الوسائل التقنية الحديثة[2]، وعليه فإن كل هذه العيوب أدت إلى تراجع استخدام هذه التقنية في التشفير.

أما بخصوص موقف المشرع الجزائري من هذه الطريقة، فيلاحظ أن القانون المتعلق بالتوقيع والتصديق الإلكترونيين لم يتطرق إليها في نصوصه، فهل تطرق للطريقة الثانية من التشفير؟

ثانياً: التشفير اللاممماثل أو التشفير باستخدام المفتاح العام (La cryptologie asymétrique)

نظراً لنقائص التشفير المماثل عمد العلماء إلى البحث عن بديل آخر يحل محله، ويؤدي الغاية المرجوة منه، بحيث ظهرت تقنية التشفير غير مماثل، وهي تقنية تقوم على وجود مفتاحين أحدها خاص والآخر عام[3]، حيث يتكون المفتاح الخاص (clé privée) من مجموعة من الرموز والأرقام يمكن تخزينها على بطاقة إلكترونية، ويكون هذا المفتاح معروفاً لطرف واحد وهو المرسل والذي يظل محتفظا بسريته، ويستخدم هذا المفتاح لتشفير الرسالة[4]، وهو ما أخذ به المشرع الجزائري في نص المادة الثانية فقرة 08 من القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين[5].

---

[1]- لورانس محمد عبيدات، إثبات المحرر الإلكتروني، دار الثقافة للنشر، الأردن، 2005، ص. 141.

[2]- مصطفى أبو مندور موسى، المرجع السابق، ص. 36.

[3]- عبد الفتاح بيومي حجازي، التجارة الإلكترونية في القانون العربي النموذجي لمكافحة جرائم الكمبيوتر والإنترنت، المرجع السابق، ص. 271؛ عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، المرجع السابق، ص، ص. 31- 32.

[4]- سمير حامد عبد العزيز الجمال، المرجع السابق، ص. 220.

[5]- تنص المادة الثانية الفقرة 08 من القانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، سابق الإشارة إليه، بأن: " مفتاح التشفير الخاص هو عبارة عن سلسلة من الأعداد يحوزها حصريا الموقع فقط، وتستخدم لإنشاء التوقيع الإلكتروني، ويرتبط هذا المفتاح بمفتاح تشفير عمومي"..

أما المفتاح العام (clé publique) فهو أيضا يتكون من مجموعة من الرموز والأرقام التي يتم تبليغها للمرسل إليه أو المستقبل، حيث يستخدمه ليتمكن بموجبه من فك شفرة الرسالة التي تم تشفيرها بالمفتاح الخاص، والتأكد من صحة التوقيع الذي تحمله ونسبتها إلى مرسلها، وأنه لا يوجد أي تلاعب أو تغيير في مضمون الرسالة منذ إنشائها وحتى وصولها إلى المرسل إليه[1]، ولكنه يختلف عن المفتاح الخاص في أنه يكون معروفا لطرفين أو أكثر[2]، وهو ما تعرض له المشرع الجزائري في نص المادة الثانية الفقرة 09 من القانـــون رقم 15-04 المذكور أعلاه[3].

من خلال ما سبق، يتضح أن المفتاح الخاص لا يعلمه سوى المرسل، أما المفتاح العام فقد يكون معروفاً لطرفين أو أكثر والعبرة بالمفتاح الخاص.

ورغم الاختلاف بين المفتاحين إلا أن كل منهما يكمل عمل الآخر، لأن كلاهما عبارة عن متتالية رقمية متولدة في نفس الوقت من عمليات حسابية أو معطيات بيومترية، ومرتبطين ببعضهما البعض ارتباطاً فنياً على درجة عالية من الدقة[4]، ومن ثم فإن هذا النظام يعد أكثر أمان من النظام السابق، لأن معرفة تركيبة أحد المفتاحين لا تتيح معرفة أو فك تركيبة المفتاح الآخر، وبالتالي لا يمكن لمن في حوزته المفتاح العام العلم بالمفتاح الخاص، وهو ما لا يسمح له بفك شفرة الرسالة.

---

[1] - وهو ما عبّر عنه جانب من الفقه الفرنسي بقوله:
"A la clé privée de l'expéditeur correspond une clé cryptographique publique, connue du destinataire, que celui-ci va utiliser pour déchiffrer la signature électronique et comparer le résultat au message original, s'ils correspondent, c'est la garantie que le message a été signé électroniquement par le titulaire de la clé privée correspondante et qu'il n'a pas été modifié ni altéré pendant sa transmission, puisque seul le titulaire de la clé privée peut générer une signature électronique et qu'il est (quasiment) impossible de la reconstituer en connaissant uniquement la clé publique". Cf, Michel Jaccard, Problèmes juridiques liés à la sécurité des transactions sur le réseau.
http://www.signele.com.date de consultation le site 12/10/2016à 15:00.

[2]- سمير حامد عبد العزيز الجمال، المرجع السابق، ص.222.

[3]- تنص المادة الثانية الفقرة 09 من القانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، سابق الإشارة إليه، على أنه: "مفتاح التشفير العمومي هو عبارة عن سلسلة من الأعداد تكون موضوعة في متناول الجمهور بهدف تمكينهم من التحقق من الإمضاء الإلكتروني وتدرج في شهادة التصديق الإلكتروني".

[4]- مصطفى أبو مندور موسى، المرجع السابق، ص، ص. 39- 40.

رغم نجاعة تقنية التشفير اللاماثل، إلا أن جانبا من الفقه[1] انتقده، واعتبر أن هذا التشفير يضمن فقط سلامة الرسالة من الناحية الموضوعية وصدق نسبتها إلى من صدرت عنه ولكنه لا يضمن سريتها، فوفقا له أسلوب التشفير الذي يؤمن سرية الرسالة يكمن في قيام المرسل بتشفير الرسالة بالمفتاح العام للمرسل إليه الذي سيستخدم مفتاحه الخاص عندما تصله الرسالة لفك شفرتها، بمعنى أن مالك المفتاح الخاص هو وحده دون غيره الذي يستطيع فك شفرة الرسالة التي شفرها المفتاح العام.

إن أهمية هذا النوع من التشفير دفعت المشرع الجزائري إلى التعرض له في قانون التوقيع والتصديق الإلكترونيين، حيث عرف بموجب المادة الثانية منه مفتاح التشفير العام واعتبره: "سلسلة من الأعداد تكون موضوعة في متناول الجمهور بهدف تمكينهم من التحقق من الإمضاء الإلكتروني، وتدرج في شهادة التصديق الإلكتروني"[2]، كما تطرق لمفتاح التشفير الخاص في المادة من القانون آنف الذكر واعتبره: "سلسلة من الأعداد يحوزها حصريا الموقع فقط، وتستخدم لإنشاء التوقيع الإلكتروني"[3].

الفرع الثاني: التقنيات الحديثة لتأمين المستند الإلكتروني.

نتيجة للقصور الذي صاحب وسائل التأمين التقليدية (التشفير)، وعدم تحقيقها للأمان بدرجة كافية لمواجهة كافة الاعتداءات التي تواجه أجهزة الحاسب الآلية والمعلومات، ظهرت الحاجة إلى وجود وسائل تأمينية حديثة تكون لها القدرة على حماية المستندات الإلكترونية، وكذا المعطيات والمعلومات التي تتضمنها هذه المستندات، كما يكون لها القدرة على مواجهة كافة ما يستجد من أشكال وأساليب الاعتداء والمساس بأمن وخصوصية المعلومات المعالجة آلياً، فظهرت بذلك ثلاث طرق حديثة لحماية هذه البيانات والمعلومات، حيث تعتمد الطريقة الأولى على استخدام تقنية الجدران النارية، في حين تُعول الطريقة الثانية على استخدام الخصائص البيولوجية، أما الطريقة الثالثة فتعمد إلى استخدام الشبكة

[1]- مصطفى أبو مندور موسى، المرجع السابق، ص41.

[2]- المادة 02 الفقرة 08 من قانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين، سابق الإشارة إليه.

[3]- المادة 02 الفقرة 09 من قانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، سابق الإشارة إليه.

الافتراضية[1]. وعليه ما هو نظام عمل كل تقنية من هذه التقنيات؟، وهل أنها توفر الحماية اللازمة لمعطيات وبيانات المستند الإلكتروني؟

البند الأول: التأمين باستخدام تقنية الجدران النارية.

لقد أتاحت عملية الاتصال بشبكة الإنترنت سواء الاتصال الشخصي، أو عن طريق شبكة داخلية الفرصة لدى القراصنة والمتسللين لاقتحام الشبكات الداخلية والأجهزة الشخصية بمختلف الأساليب، وهذا ما أدى إلى ضرورة العمل على سد هذه الثغرات باستخدام أجهزة الجدران النارية في حالة الشبكات الداخلية، أو باستخدام برامج الجدران النارية إذا كان الاتصال بجهاز شخصي[2].

وفي هذا يتجه أغلب خبراء المعلوماتية إلى اعتبار الجدار الناري برنامج يمكن أن يكون على هيئة جهاز متكامل، أو برنامج يتم تحميله إلى الحاسب الآلي بمواصفات جيدة، هدفه حماية شبكة الحاسب الآلي الداخلية وشبكة الإنترنت، ووظيفته الرئيسية مراقبة كل البيانات الداخلية والخارجية من الشبكة[3]، والتأكد من مطابقتها لشروط المستخدم التي يحددها البرنامج من قبل، وهو بذلك يعد نظام أمن فعال لحماية الشبكات من المقتحمين والمخربين، ذلك أنه يضع الأجهزة المستخدمة للشبكة من الاتصال مباشرة مع حواسب خارج الشبكة [4].

كما تنحصر وظيفة الجدار الناري في قيامه بعملية مسح (scan) المعلومات التي تصل من شبكة الإنترنت والقيام بتحليلها، فإن وجد أن المعلومات غير مؤمنة فإنه يمنع محاولة الدخول أو الإختراق إليها، بحيث يطردها خارج الشبكة، أما إذا كانت المعلومات عادية وآمنة فإن الجهاز يسمح لها بالمرور والدخول إلى أجهزة الحاسبات الآلية[5].

---

[1]- أيمن عبد الحفيظ، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، دار النهضة العربية- القاهرة- مصر، 2005، ص. 154.

[2]- أيمن عبد الحفيظ عبد الحميد سليمان، إستراتيجية مكافحة الجرائم الناشئة عن استخدام الحاسب الآلي، دراسة مقارنة، رسالة مقدمة للحصول على درجة دكتوراه في علوم الشرطة، أكاديمية الشرطة، كلية الدراسات العليا، مصر، 2003، ص. 341.

[3]- ذياب البداينة، أمن المعلومات، دراسات مستقبلية، مجلة علمية محكمة يصدرها مركز دراسات المستقبل، جامعة أسيوط، ع8، س السادسة، يوليو (تموز) 2003، ص.28.

[4]- طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة، مصر، 2009، ص،ص. 584- 585.

[5]- أيمن عبد الحفيظ، المرجع السابق، ص. 158؛=

وعليه يكمن الهدف من الجدار الناري في التغلب على أكبر قدر ممكن من الثغرات الأمنية، من خلال بناء قناة اتصال توجه إليها المراسلات والمعلومات المتبادلة مع شبكة الإنترنت لمراقبتها، والسيطرة على خروجها أو دخولها من وإلى الشبكة الداخلية للمستخدم، ومن ثم فقد يمنع الجدار كل (أو جزء) حركة المرور من الشبكة الداخلية للمستخدم باتجاه خدمات الإنترنت باستثناء البريد الإلكتروني، أو يستخدم جدار النار لمنع الوصول إلى المواقع المشبوهة[1].

وبشكل عام، يمكن القول أن تقنية الجدران النارية عبارة عن برامج تقوم بصد محاولات الاختراق، أو الهجوم الوافد من شبكة الإنترنت لتهديد الشبكة الداخلية أو النظام المعلوماتي، وفي هذا شبه بعض الفقه برامج الجدران النارية بحرس الحدود على الساحل، حيث تزود الشبكات بحماية جيدة عن طريق التأكد من شرعية كل شخص يود زيارة الشبكة المحمية دخولاً أو خروجاً دون أن يكون مصرحاً له بذلك[2].

هذا ويتم استخدام برمجيات الجدران النارية عند الأماكن التي تتلاقى فيها الشبكة الداخلية للشركة أو المؤسسة مع شبكة الإنترنت العالمية، ويمكن القول بصفة عامة أنه كلما زاد عدد خدمات الإنترنت التي يسمح بها لمستخدمي الشبكة في المؤسسة المحلية، تزدادا الخطورة من الدخول إلى شبكة الإنترنت العالمية، ولذلك تأتي وظيفة الجدران النارية في هذه الحالة، ويكون هدفها حماية المناطق الهامة من الشبكة الداخلية للمؤسسة الخاصة أو العامة[3].

هذا وتختلف أنواع الجدران النارية، فقد يكون الجدار الناري جهازا أو برنامجا، ومن أمثلة برامج الجدران النارية برنامج شبكة (DAN)، والذي يتضمن مزايا أمنية عديدة، ومزودات بروكسي (Proxy Server) التي تحتفظ بصفحات الشبكة للويب على القرص

=Hubert Bitan, droit et expertise des contrats informatiques (contrat de communication électronique vision expertale de la protection des données), édition lamy, France, 2010, p.399.

[1]- جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات، دار البداية للنشر، الأردن، 2007، ص. 246.

[2]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الإسكندرية، مصر، 2007، ص. 49 ؛ جعفر حسن جاسم الطائي، المرجع السابق، ص. 246.

[3]- طارق إبراهيم الدسوقي عطية، المرجع السابق، ص. 585.

الصلب، وكذا مرشحات عناوين[1]، ومهما اختلفت أشكال هذه البرامج وأنواعها ومهما تعددت الشركات الصناعية، فإنها جميعها تعمل بنفس الفكرة والتقنية، وتقريباً تتساوى في قدراتها في حماية الشبكة، ويكون الاختلاف فقط في طريقة تركيبها وبرمجتها[2].

البند الثاني: التأمين باستخدام الخصائص البيولوجية.

بغية توفير حماية كافية وفعالة للمستند الإلكتروني، وما يحتويه من بيانات ومعلومات، وفي سبيل المحافظة على الخصوصية والسرية في البيئة الإلكترونية، ابتكر العلم تقنية تأمين المستندات والمعلومات المعالجة آليا باستخدام الخصائص البيولوجية للإنسان.

ولعل ما يميز هذه الخصائص أن لكل شخص سماته التي ينفرد بها عن غيره، لأن هذه السمات البيولوجية لا يشترك فيها شخصان، ولذلك طورت الشركات الأمنية أسلوب تأمين الدخول إلى أنظمة الحاسبات الآلية، باستخدام هذه السمات البيولوجية، وذلك عن طريق إنشاء أجهزة لا تتيح لأي شخص استخدام الحاسب الآلي، والاطلاع على بيانات المستندات الإلكترونية، إلا المصرح له فقط من طرف هذه الأجهزة استناداً إلى السمات البيولوجية[3].

---

[1]- فيما يخص مزودات بروكسي، فقد شبهها الفقه بالشاحنات العسكرية الخاصة بالتموين، والتي تجلب البضائع، وهي في هذه الحالة صفحات الشبكة الخارجية، حيث يعاد توزيعها داخلياً، وتساعد عملية التوزيع الداخلي على حفظ حركة المرور عبر بوابة الدخول إلى الشبكة المحلية، وتستخدم مزودات بروكسي كذلك لمنع دخول البيانات الوافدة من الإنترنت على الحاسب الآلي بالشبكة المحلية بصفة جزئية أو كلية.
أما مرشحات (URL)، فهي ببساطة عبارة عن فلتر يمنع مستخدمي الشبكة من الدخول إلى مواقع معينة على شبكة الإنترنت، وبالتالي تعطي صاحب الشبكة أو مالكها الحق في التحكم في مستخدمي الشبكة للدخول من عدمه لمواقع معينة غير مرغوب فيها على الشبكة، ولعل هذه الميزة من الأهمية بمكان فيما يتعلق بتصفح الطفل أو الحدث للإنترنت بطريقة آمنة، بحيث لا يتسلل إلى المواقع الإباحية أو تلك التي يحصل منها على خبرات ضارة. مشار اليه من طرف، جعفر حسن جاسم الطائي، المرجع السابق، ص. 247.

[2]- من أشهر تطبيقات برامج الجدران النارية ما يسمى ببرنامج (Zone alarm) وذلك نظراً لكفاءته غير المحدودة في ضبط ورصد كافة محاولات الاختراق على الأجهزة وقيامه بإعطاء إشارة عند حدوث أي اعتداء، كما أن هذا البرنامج يمكنه القيام بتفقد مرفقات البريد الإلكتروني والتي أصبحت مصادر الفيروسات بحيث يقوم باحتجازها أو طردها أو مسحها، كما يلاحظ كذلك أن هذا البرنامج قبل قيامه بحذف أي من البرامج يتيح للمستخدم فرصة تفحص الملفات ثم يقرر تشغيلها أم لا. لتفاصيل أكثر حول أشهر تطبيقات الجدران النارية. يراجع، أيمن عبد الحفيظ عبد الحميد سليمان، المرجع السابق، ص.343.

[3]- أيمن عبد الحفيظ، المرجع السابق، ص. 155.

ومن بين هذه السمات استخدام بصمة الإبهام، حدقة العين، وبصمة الصوت[1]، فبالنسبة لتأمين المستندات عن طريق استخدام بصمة الأصبع (الإبهام)، يلاحظ أن العديد من الشركات الأمنية لجأت إلى تأمين مستنداتها عن طريق استخدام بصمة الإصبع، بحيث حددت مكانا معينا في لوحة مفاتيح الحاسب الألي غرضها التحقق من تطابق بصمة الأصبع مع تلك المخزنة لديها [2].

ولئن كانت هذه إحدى التقنيات، فإنه يمكن كذلك التحقق من بصمة الإصبع عن طريق جهاز مستقل يتم توصيله بجهاز كمبيوتر خاص بذلك، حيث يقوم الجهاز بالتقاط صور الثنايا الموجودة في الإصبع المستخدم، ثم يحول البرنامج المرفق هذه الصورة إلى صورة نقطية تخزن للإحالة المستقبلية، باعتبارها كلمة سر لكي تتيح لصاحبها الدخول إلى النظام المعلوماتي، وذلك عن طريق قيام الجهاز بعمل مسح ضوئي لبصمة الأصبع، ومقارنتها بقاعدة البيانات البيولوجية المخزنة على جهاز الحاسب الآلي، وعند تطابق البصمة مع قاعدة البيانات البيولوجية يسمح للشخص باستخدام الجهاز، والاطلاع على ما يحتويه من بيانات ومستندات إلكترونية، وما يميز هذه التقنية أنها توفر درجة تأمين عالية للمستندات الإلكترونية، لأن الفحص العلمي قد أثبت على مدار سنوات طويلة أن الخطوط الحلمية التي تولد مع الشخص تظل على ذات شكلها حتى مماته، مما يمثل صفة خاصة به تميزه عن غيره[3].

وينطبق ذات الأمر على الخصائص البيولوجية بالنسبة لعين الشخص نتيجة الاختلاف في الشرايين والعلامات الموجودة على الشبكية، فبغية توفير تأمين كافي للمستندات الإلكترونية تم ابتكار بعض الأجهزة التي تتطلب استخدام حدقة العين للسماح بالدخول إلى النظام المعلوماتي وتسمى هذه التقنية (Tact Lessness)[4]، وهذا ما دفع الكثير من الشركات الأمنية إلى استخدام هذه الخاصية في عمل برامج تقوم بتسجيل صور شبكة

[1]- محمد أمين الرومي، المستند الإلكتروني، المرجع السابق، ص. 70.
[2]- جعفر حسن جاسم الطائي، المرجع السابق، ص. 242.
[3]- أيمن عبد الحفيظ عبد الحميد سليمان، المرجع السابق، ص. 336.
[4]- جعفر حسن جاسم الطائي، المرجع السابق، ص .243.

العين للأشخاص المخول لهم سلطة استخدام الجهاز، والاطلاع على المستندات الإلكترونية، حيث يقوم الجهاز المزود بشرائح إلكترونية صغيرة الحجم من خلال برنامج يتم تدعيم الجهاز به، ويوفر السرعة والدقة المطلوبة للتحكم في النظام بتحديد هوية الأشخاص عن الوقوف بالقرب منه من خلال المرآة الخاصة بالجهاز ليلتقط الصورة لحدقة العين من مسافة تتراوح ما بين ثلاثة وعشر بوصات، ثم يتولى الجهاز بعد ذلك بمعالجة هذه الصورة الرقمية من خلال شريحة متطورة تعرف باسم (شفرة إيريس)، ثم بعدها يقوم بإجراء مقارنة بينها وبين الصورة المخزنة لديه مسبقاً، وعند وجود التطابق يسمح للشخص باستخدام الجهاز والاطلاع على البيانات والمعلومات المعالجة آلياً[1].

أما فيما يخص تأمين المستندات عن طريق استخدام بصمة الصوت في بعض الحاسبات التي تتطلب ذلك، فنجد أن هذه التقنية توفر كذلك درجة تأمين عالية، وذلك نظراً لاختلاف خصائص كل شخص عن الآخر في الذبذبات الصوتية، من حيث إعدادها وطبيعتها، حيث تسمح هذه التقنية بتحويل نبرة الصوت إلى خطوط أفقية يمكن للبرنامج تسجيلها عليه، وعن طريق المقارنة بين صوت الشخص المصرح له باستخدام الجهاز، وبين النبرات المسجلة لديه يتم السماح للشخص باستخدام الجهاز في حالة التطابق في الأصوات، وذلك من خلال أجهزة استقبال هذه النبرات، والتعامل معها من خلال البرنامج المخزن داخل الجهاز[2].

البند الثالث: التأمين باستخدام الشبكة الافتراضية.

نظراً لتزايد المخاطر الناشئة عن إنشاء شبكة الإنترنت، وخاصة منها تلك الناجمة عن اقتحام المخربين والمتسللين لها والعبث بالبيانات والمعطيات المخزنة إلكترونيا، فكر خبراء المعلوماتية في ضرورة التغلب على تلك المخاطر وذلك من خلال استخدام شبكة الاتصال ذاتها، ونتيجة لذلك ابتكروا ما يُعرف بالشبكة الافتراضية، هذه الأخيرة عُرفت

[1]- أيمن عبد الحفيظ، المرجع السابق، ص. 156.

[2]- للإضافة فإن البصمة الصوتية تستخدم في بعض البنوك مثل التوقيع تماماً وذلك من خلال أنظمة التعرف الصوتي. مشار إليه من طرف، جعفر حسن جاسم الطائي، المرجع السابق، ص. 243؛ أيمن عبد الحفيظ ، المرجع السابق، ص.157.

بأنها: "شبكة خاصة بمنشأة أو شركة أو هيئة، تقوم هذه الأخيرة بإنشائها فوق شبكة عامة مستفيدة من تلك الشبكة العامة، وإن كانت الشبكة الخاصة تقوم على أسس فنية مختلفة عنها، وسُميت الشبكة بالافتراضية (dynamic) لأنها تنشأ فقط وقت الحاجة إليها، فهي ليست مستمرة طوال الوقت، وذلك بخلاف النوع الآخر الذي يظل دائما ويطلق عليه اسم (static)"[1] .

يعتمد عمل الشبكة الافتراضية على نقل البيانات عن طريق توثيقها وتشفيرها، باستخدام مفاتيح سرية تكون معلومة لدى مختلف أطراف الشبكة الخاصة، وهو الأمر الذي يُصعب على أي طرف خارجي الاطلاع على محتوى تلك البيانات وقراءتها .

الحقيقة أن فكرة الشبكة الإفتراضية راودت خبراء المعلوماتية عندما بدأت المؤسسات والشركات الكبرى تستأجر خطوطاً من شركات الاتصال، لتستخدمها في ربط شبكاتها المحلية وشبكاتها للمناطق الواسعة، بالإضافة إلى خطوط الربط بين مختلف الفروع لنقل البيانات، وكانت هذه الشبكات تقدم للشركات حلولاً تضمن لها توسيع شبكاتها الخاصة إلى نطاقات تتجاوز الحدود الجغرافية الضيقة[2].

للإشارة فإن الشبكات السالف ذكرها تتمتع بمجموعة من المميزات تجعلها تختلف عن الشبكات الدولية كالإنترنت، من حيث الأداء والأمان وإمكان الاعتماد عليها، ولكن مع الاستمرار في استخدام شبكات المناطق الواسعة كشبكة الإنترنت الدولية ظهرت الكثير من المخاطر مما تطلب ضرورة المواجهة التأمينية لتلك التجاوزات، وهنا بدأ مفهوم الشبكات الخاصة الافتراضية يفرض نفسه، معتمدا في ذلك على استثمار الاتصالات المتاحة عن طريق إنشاء مجموعة من قنوات الاتصال المستقلة في قلب الشركة الأم تعمل كشبكة اتصال منفصلة تماماً، وتُوجه لعدد من المستخدمين المحدودين وتكون مغلقة عليهم، حيث لا يستطيع أي شخص آخر استخدامها، ومن ثم تصبح هذه الشبكة وكأنها أنشئت خصيصاً لهؤلاء دون أن يكون لها وجود مادي في الواقع[3].

---

[1]- أيمن عبد الحفيظ عبد الحميد سليمان، المرجع السابق، ص.345.

[2]- المرجع نفسه، ص. 344.

[3]- المرجع نفسه، ص. 161.

من فوائد الشبكة الافتراضية قدرتها على الوصول لمجموعة من المستخدمين بشكل آمن وبسرعات عالية، وباستخدام مجموعة مختلفة من التقنيات ومن أماكن مختلفة، وهي عند تحقيقها لغايتها تتطلب نفقات تقل عن نفقات الاتصالات التليفونية العادية، خاصة إذا كانت الشبكة تربط بين مجموعة من المستخدمين في مناطق متباعدة جغرافياً، سواء في مدن مختلفة داخل الدولة الواحدة أو في مجموعة من الدول، كما هو الشأن في حالة الشركات متعددة الجنسيات.

إلى جانب هذه الميزة تعمل الشبكة الإفتراضية على تطوير جميع أنواع الاتصالات، كما أنها تسمح بتبادل المعلومات بجميع أشكالها، بحيث أنها تُمكن من إجراء محادثات تليفونية والمشاركة في التجارب العلمية والعملية والمحاضرات، وكذا البحث في قواعد البيانات عن طريق البرامج الشائعة المستخدمة في التصفح والتجوال داخل شبكة الإنترنت، بصورة آمنة لا يتم اختراقها أو التسلل إليها[1].

المطلب الثالث: حفظ المستند الإلكتروني.

نظراً لأهمية المستندات الإلكترونية في إبرام المعاملات والصفقات في شتى المجالات بما فيها مجال التجارة الإلكترونية عبر الإنترنت – حيث لا تكاد تخلو عملية من العمليات المذكورة من التبادل الإلكتروني للبيانات-، تم البحث عن وسيلة لحفظ وتخزين هذه المستندات، وذلك حتى يتمكن من له مصلحة من الرجوع إليها عند الحاجة، وكذا استعمالها كوسيلة لإثبات التصرفات القانونية الإلكترونية التي تتم عبر الوسائط الافتراضية، وذلك في حالة ما إذا وقع نزاع بشأن هذه التصرفات.

ومن ثم فإنه يمكن تعريف عملية الحفظ الإلكتروني للمستندات والبيانات المعالجة آلياً بأنها: "الحفاظ على البيانات الإلكترونية في دعامة ثابتة لا يمكن تغييرها، إلا من جانب المحتفظ بها"[2].

[1]- أيمن عبد الحفيظ، المرجع السابق، ص،ص. 162- 163.
[2]- علاء حسين مطلق التميمي، الأرشيف الإلكتروني وكيفية المحافظة على المستند الإلكتروني عبر الزمن، دراسة مقارنة، المرجع السابق، ص.160.

ولتحقيق عملية الحفظ الإلكتروني للبيانات ظهر ما يسمى بالسجل الإلكتروني، كوسيلة لحفظ المستندات المعالجة آلياً على نحو يسمح بالرجوع إليها، واستعمالها عند الحاجة[1].

فما المقصود بهذا السجل؟ ما هي المزايا التي يوفرها في مجال التبادل الإلكتروني للبيانات؟ وما هي البيانات الواجب توافرها فيها؟.

للإجابة على هذه التساؤلات سيتم التعرض إلى السجل الإلكتروني كوسيلة لحفظ المستندات **(الفرع الأول)**، على أن يتم بعدها التطرق للبيانات الواجب توافرها في السجل الإلكتروني **(الفرع الثاني)**.

الفرع الأول: السجل الإلكتروني كوسيلة لحفظ المستند الإلكتروني.

نظرا للدور الهام الذي يلعبه السجل الإلكتروني في حفظ المستندات الإلكترونية، عمد الفقه إلى تعريفه، بحيث عرفه جانب من الفقه[2] بأنه: "سجل ينشأ أو ينتج أو يتصل، أو يتم تلقيه أو حفظه بوسيلة إلكترونية"، هذا وقد وسع اتجاه آخر[3] في تعريفه بحيث اعتبره: " كل مجموعة من النصوص أو الرسوم أو البيانات أو الأصوات أو الصور أو غيرها من المعلومات تتمثل في صورة رقمية، ويتم إنشاءها أو تعديلها أو حفظها أو فهرستها أو استرجاعها أو توزيعها بواسطة نظم الكمبيوتر".

إن أساس هذا توسع هذا الاتجاه الفقهي في تعريفه للسجل الإلكتروني ربطه المدلول الاصطلاحي للسجل الإلكتروني بمعناه اللغوي[4]، وفي هذا يرى الرأي الراجح أن مثل هذا التوسع يتعارض مع النصوص التشريعية، والقواعد المنظمة للسجل الإلكتروني.

---

[1]- لزهر بن سعيد، المرجع السابق، ص. 133.

[2]- أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني –دراسة مقارنة–، ط1، المرجع السابق، ص. 56.

[3]- علاء حسين مطلق التميمي، المستند الإلكتروني، عناصره وتطوره ومدى حجيته في الإثبات المدني، المرجع السابق، ص.98؛

Hubert Bitan,op. cit, p. 389.

[4]- للإشارة فإن كلمة سجل لغةً يراد بها: بيان وضع في صورة ثابتة وبصفة خاصة كتابة ليحفظ المعرفة أو ذاكرة الأحداث أو الوقائع أو المعلومات أو البيانات والتي تم جمعها في موضوع معين". مشار إليه من طرف، أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني –دراسة مقارنة-، ط1، المرجع السابق، ص. 57.

استنادا لما تقدم، يتبين أن السجل الإلكتروني يُعد من الأمور المهمة التي يتعين مراعاتها في مجال التبادل الإلكتروني للبيانات، بحيث إذا أُثير ثار نزاع بين أطراف التعامل أمكن آنذاك إقامة دعوى لإثبات الحق بناءً على ما سجل من بيانات متبادلة داخل الكمبيوتر، ولهذا شبه بعض الفقه السجل الإلكتروني بالدفاتر التجارية التي يلتزم التجار والمنشآت التجارية بمسكها لبيان معاملاتهم التجارية[1].

ونظراً لأهمية السجل الإلكتروني في المعاملات الإلكترونية، فإن الاتفاقات الدولية والتشريعات العربية الخاصة بالتجارة الإلكترونية تشترط ضرورة وجود سجل إلكتروني لحفظ البيانات والمعلومات المعالجة آليا، فقد جاء التوجيه الأوروبي الصادر سنة 2000 على أن: "الشخص الذي يعرض منتجات وخدمات نظم معلومات يمكن للجمهور الوصول إليها، يلزم بأن يوفر وسائل لتخزين أو طباعة العقد"[2].

وليس هناك ما يخالف المنطق في اشتراط تقديم بيانات ومعلومات معينة، أو توفير وسائل تقنية لإتاحة شروط العقد بطريقة تسمح بتخزينها واستنساخها، لا سيما وأن التبادل الإلكتروني للبيانات من الممكن أن يتم في ظل عدم وجود اتفاق مسبق بين الأطراف[3].

كما تضمنت غالبية الاتفاقات النموذجية للتبادل الإلكتروني للبيانات نصاً يلتزم بموجبه الأطراف بالاحتفاظ بسجل لرسائل التبادل الإلكتروني للبيانات، وقد نص عدد من هذه الاتفاقيات على أن طرق التسجيل المستخدمة ينبغي أن تحافظ على كل من الرسائل المرسلة والمسلمة، وأن يوفر سجلاً ذا تسلسل زمني وتاريخي لهذه الرسائل، وأن تضمن إمكانية الوصول إلى الرسالة المسجلة بالتبادل الإلكتروني للبيانات، بشكل يمكن للإنسان قراءته.

[1]- علاء حسين مطلق التميمي، الأرشيف الإلكتروني وكيفية المحافظة على المستند الإلكتروني عبر الزمن، المرجع السابق، ص. 168.

[2]- نص المادة 10 الفقرة 01 من التوجيه الأوروبي الصادر عام 2000. نقلا من مرجع، محمد أمين الرومي، المستند الإلكتروني، المرجع السابق، ص. 155.

[3]- علاء حسين مطلق التميمي، المستند الإلكتروني، عناصره وتطوره ومدى حجيته في الإثبات المدني، المرجع السابق، ص.100.

ولعل أهم الاتفاقات الواردة في هذا المجال الإتفاق النموذجي الأوروبي للتبادل الإلكتروني للبيانات (TEDIS)، حيث نص على أنه: "يجب على كل طرف من أطراف التعاقد أن يخزن بدون تعديل أو تحريف، باستخدام وسائل أمان، سجلاً متسلسلاً لجميع رسائل البيانات التي يتبادلها الأطراف إلكترونياً أثناء القيام بالعملية التجارية، وفقاً للشروط والمواصفات المنصوص عليها في قانونه الوطني".

كما يجب على كل طرف الاحتفاظ بهذا الشكل الإلكتروني لمدة لا تقل عن ثلاث سنوات تبدأ من تاريخ إتمام الصفقة (م1/8)، كذلك يجب على المرسل أن يخزن الرسالة الإلكترونية المرسلة من قبله بالشكل نفسه الذي أرسلت به، وعلى المستلم الاحتفاظ بها بالشكل الذي تسلمها به ما لم تنص القوانين الوطنية على خلاف ذلك (المادة 2/8)، ويلتزم أطراف التعاقد بتسهيل الاطلاع على السجلات الإلكترونية، وإمكانية استنساخها بشكل يمكن الإنسان من قراءتها وطبعها (المادة 3/8)[1].

أما عن مفهوم السجل الإلكتروني من الناحية التشريعية، فيلاحظ أن بعض التشريعات العربية الخاصة بالمعاملات الإلكترونية قد تطرقت إلى وضع تعريف له، ومن ذلك قانون المعاملات الالكترونية الأردني، بحيث عرفت المادة 7/02 منه السجل الإلكتروني بأنه: "القيد أو العقد أو رسالة المعلومات التي يتم إنشاؤها أو إرسالها أو تسليمها أو تخزينها بوسائل إلكترونية"[2].

للإشارة فقد حلت محل هذا النص المادة 7/2 من قانون رقم 15 لسنة 2015[3]، وفيها عرف السجل الإلكتروني بأنه: "رسالة المعلومات التي تحتوي على قيد أو عقد أو أي مستند أو وثيقة من نوع آخر يتم إنشاء أي منها أو تخزينها أو استخدامها أو نسخها أو إرسالها أو تبليغها أو تسلمها باستخدام الوسيط الإلكتروني."

[1]- محمد أمين الرومي، المستند الإلكتروني، المرجع السابق، ص. 155؛ علاء حسين مطلق التميمي، الأرشيف الإلكتروني وكيفية المحافظة على المستند الإلكتروني عبر الزمن، المرجع السابق، ص، ص. 169- 170.
[2]- قانون رقم 85 لسنة 2001 المتعلق بالمعاملات الالكترونية الأردني، سابق الإشارة إليه.
[3]- قانون رقم 15 لسنة 2015 المتعلق بالمبادلات الالكترونية الأردني، سابق الإشارة إليه.

كما عرفته المادة الثانية من قانون المعاملات الإلكترونية لإمارة دبي بدولة الإمارات العربية المتحدة، بأنه: "سجل يتم إنشاؤه أو تخزينه أو استخراجه أو نسخه أو إرساله أو استلامه بوسيلة إلكترونية على وسيط ملموس، أو على وسيط إلكتروني آخر، ويكون قابلاً للاسترجاع بشكل يمكن فهمه"[1].

كما عرفته المادة الأولى فقرة رابعة من قانون المعاملات الإلكترونية البحريني[2] بأنّه: "السجل الذي يتم إنشاؤه أو إرساله أو تسلمه أو بثه أو حفظه بوسيلة إلكترونية"، وقد عرف القانون ذاته وسيط الشبكة فيما يتعلق بالسجل الإلكتروني في المادة 7/1أنه: "الشخص الذي يقوم نيابة عن شخص آخر بإرسال واستقبال وبث أو تخزين ذلك السجل الإلكتروني، أو يقدم خدمات أخرى بشأن ذلك السجل".

للإشارة فقد ألغى المشرع البحريني القانون آنف ذكره بحيث عرف السجل الإلكتروني في المادة3/1 من قانون رقم 54 لسنة 2018[3] واعتبره: "معلومات يتم إنشاؤها أو إرسالها أو تسلمها أو تخزينها بوسيلة إلكترونية ، وتشمل بحسب الأحوال، كافة المعلومات التي تقترن أو ترتبط منطقيا بالسجل على نحو يجعلها جزءا منه سواء أنشئت في وقت متزامن أم لا"، كما أورد تعريفا مماثلا لوسيط الشبكة في المادة 40/1.

ولئن كانت جل التشريعات العربية المنظمة للمعاملات الالكترونية أوردت تعريفا صريحا للسجل الالكتروني إلا أن قانون المبادلات والتجارة الالكترونيين التونسي لم يورد مثل هذا النص بل اكتفى في المادة 14منه بإلزام كل شخص طبيعي مختص بخدمة المصادقة والتوثيق بمسك سجل الكتروني خاص بشهادة المصادقة على ذمة المستعملين، على أن يكون ذلك السجل مفتوحا للاطلاع الكترونيا بصفة مستمرة على المعلومات المدونة به كما وأشار ذات القانون إلى ضرورة حماية هذا السجل الالكتروني من كل تغيير أو تحريف غير مرخص به[4].

---

[1]- قانون إمارة دبي رقم 2 لسنة 2002 بشأن المعاملات والتجارة الالكترونية، سابق الإشارة إليه.
[2]- مرسوم بقانون رقم (28) لسنة 2002 بشأن المعاملات الالكترونية البحريني، سابق الإشارة إليه.
[3]- مرسوم بقانون رقم (54) لسنة 2018 المتعلق بإصدار قانون الخطابات والمعاملات الإلكترونية، سابق الإشارة إليه.
[4]- قانون رقم 83 لسنة 2000 المتعلق بالمبادلات والتجارة الإلكترونية، سابق الإشارة إليه.

أما بالنسبة للموقف الجزائري من السجل الإلكتروني، فإذا تصفحنا نصوص التشريع الجزائري بما فيها تعديل 2015 المتضمن القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين[1]، نجد أنه لم يضع تعريفاً لهدا السجل، واكتفى بموجب قانون التجارة الإلكترونية 18-05 بإلزام المورد الإلكتروني بحفظ سجلات المعاملات التجارية المنجزة وتواريخها مع إلزامه بضرورة إرسالها إلكترونيا إلى المركز الوطني للسجل التجاري[2].

من خلال التعريفات الفقهية والتشريعية السابقة يتضح أن السجل الإلكتروني يشمل أي حامل أو وسيط، أو دعامة معدة لإنشاء البيانات والمعلومات أو حفظها أو إرسالها أو استلامها إلكترونياً، وأن الهدف من استخدام السجل الإلكتروني يتمثل في توثيق المعلومات بطريقة تضمن سلامتها، واسترجاعها كاملة عند اللزوم لأطراف التعاقد أو الأشخاص المرخص لهم بذلك، وهو ما يقتضي تهيئة بيئة تحمي السجل من كافة المؤثرات السلبية الطبيعية أو البشرية، وتوفر الصيانة المستمرة والمنتظمة[3].

الفرع الثاني: البيانات الواجب توافرها في السجل الإلكتروني.

المعلوم أن السجل الإلكتروني لا يمكنه ان يؤدي دوره المنوط به كأرشيف إلكتروني يمكن الرجوع إليه عند الحاجة ليكون حجة في إثبات واقعة أو تصرف معين، إلا اذا تضمن بيانات معينة تضمن الثقة في مضمونه وتبعث على الاعتقاد بسلامة محتواه[4].

وفي سبيل تحقيق ذلك اشترطت بعض التشريعات المعنية بالمعاملات الإلكترونية في نصوصها عدد من البيانات التي ينبغي أن ترد بالسجل الالكتروني، ولا ريب في أن هذه البيانات لها أهميتها عند نشوء النزاع، ناهيك عن أنها تسمح بمعرفة محتوى المستند الالكتروني في حال ضياعه، أو تلفه وهي بذلك حجة في الاثبات[5].

---

[1]- القانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، سابق الإشارة إليه.
[2]- قانون رقم 18-05 المتعلق بالتجارة الإلكترونية، سابق الإشارة إليه.
[3]- لزهر بن سعيد، المرجع السابق، ص، ص. 135- 136.
[4]- أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني –دراسة مقارنة–، ط1، المرجع السابق، ص.59.
[5]- محمد أمين الرومي، المستند الإلكتروني، المرجع السابق، ص. 153.

إن من بين البيانات التي ينبغي أن يتضمنها السجل الإلكتروني التوقيع عليه من طرف شخص أو أشخاص معينين، مع ذكر أسمائهم وصفاتهم وتاريخ وضع توقيعاتهم على المستند، كما يجب تحديد المغزى من التوقيع، إذا كان يعني إنشاء المستند أو مراجعته أو التصديق عليه[1].

ولئن كانت هذه البيانات ترد في معظم معاملات البيئة الالكترونية، فإنه ينبغي الذكر أن سجل العمليات التجارية الإلكترونية والذي هو عبارة عن ملفات للمعلومات خاصة برسائل البيانات الإلكترونية المتبادلة بين أطراف العقد[2]، يجب أن تحتوي على العديد من البيانات الخاصة بالمعاملات الإلكترونية، من أهمها :

1- الاسم والعنوان والهوية والجنسية والبريد الإلكتروني لكل من الطرفين في العملية.

2- تاريخ وزمان ومكان إرسال واستلام الرسائل الإلكترونية، والمستندات الإلكترونية الخاصة بإبرام المعاملة.

3- حجم التعامل بين الأطراف كما هو مبين في الرسائل الإلكترونية.

4- بيان البروتوكول والمعايير الخاصة بالتبادل الإلكتروني للبيانات (EDI)، التي تم تسليم الرسائل بموجبها، وذلك كصيغة نموذجية يستخدمها الأطراف فيما بينهم بعد ذلك في المعاملات المستقبلية.

5- بيانات ومعلومات عن الفواتير أو المستندات الخاصة بالمعاملة الإلكترونية (العملية التجارية).

6- اعتبار أن الرسالة الإلكترونية مرسلة من مصدرها إذا وافق على ذلك.

7- القانون الواجب التطبيق على المعاملة الإلكترونية.

---

[1]- علاء حسين مطلق التميمي، الأرشيف الإلكتروني وكيفية المحافظة على المستند الإلكتروني عبر الزمن، المرجع السابق، ص. 174.

[2]- علاء حسين مطلق التميمي، المستند الإلكتروني، عناصره وتطوره، وحجيته في الإثبات المدني، المرجع السابق، ص.99.

8- مكان وزمان إبرام العقد.

9- ملف إضافي يحتوي على أية معلومات أخرى ترتبط بالتعاملات.

10- نسخة طبق الأصل من السجل يحتفظ بها في الأرشيف[1].

لا شك البيانات السابق ذكرها لها أهمية كبيرة في إثبات بعض الوقائع، فمثلاً في المجال البنكي يكون لتحديد تاريخ إتمام التحويل المصرفي الإلكتروني أهمية كبيرة في القول بنفاذ أو عدم نفاذ التحويل في حالة إفلاس أحد أطرافه، كما أن لحظة تمام التحويل تعني أن الآمر لم يعد لديه الحق في التصرف في المبلغ المالي محل الأمر بالتحويل، ومن ثم فإنه إن أصدر شيكاً عن ذات المبلغ كان مرتكباً لجريمة إصدار شيك بدون رصيد[2].

هذا ويتم حفظ السجل الإلكتروني بما يحتويه من مستندات على أوعية إلكترونية من خلال الحاسب الآلي ذاته، وبشكل لا يقبل القراءة إلا من خلال إحدى مخرجاته، ومن أهم الوسائط الإلكترونية المستخدمة في هذا الشأن الأقراص المغناطيسية[3].

وبغية تأمين حفظ المستند الإلكتروني، قامت الجمعية الفرنسية للتوحيد القياسي (A.F.N.O.R) بوضع معيار خاص بالسجلات الإلكترونية أطلق عليه معيار أفنور للسجل الإلكتروني، الغرض منه تحديد الشروط اللازمة والملامح الفنية الواجب توافرها في البيانات المسجلة إلكترونياً في أنظمة المعلومات، ومدة وشروط صلاحية حفظ المستند إلكترونياً، ويوجد في هذا المعيار العديد من الاختيارات لنظم تأمين السجل الإلكتروني من خلال عمليات التحكم والتشفير[4].

---

[1]- محمد أمين الرومي، المستند الإلكتروني، المرجع السابق، ص. 154.

[2]- أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني –دراسة مقارنة–، ط1، المرجع السابق، ص. 60.

[3]- للإشارة فإن الأقراص المغناطيسية تعتبر من أفضل أنواع الوسائط الإلكترونية التي يمكن استخدامها للتخزين المباشر أو العشوائي، وتتميز بقدرتها الاستيعابية الكبيرة، وسرعة تداول المعلومات المخزنة عليها، ومن أهم خواصها إمكانية القراءة أو التسجيل على أي قطاع منها، كذلك يمكن تغيير أو تعديل أي ملف مسجل عليها دون حاجة إلى إنشاء ملف جديد، إذ يتم تعديل السجل وهو في موضعه. وتوجد أنواع عديدة منها لعل من أهمها: القرص المرن، القرص الصلب، وقرص الخرطوش، والمصغرات الفيلمية.
مشار إليه من طرف، هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دار النهضة العربية، القاهرة، 1997، ص. 18؛ علاء حسين مطلق التميمي، الأرشيف الإلكتروني وكيفية المحافظة على المستند الإلكتروني عبر الزمن، المرجع السابق، هامش ص،ص. 165- 166.

[4]- محمد أمين الرومي، المستند الإلكتروني، المرجع السابق، ص. 156.

هذا وقد وضعت لجنة أفنور للسجل الإلكتروني مجموعة من التوصيات التي تعتبر الإطار العام للمواصفات الفنية التي تبين كيفية إتمام عملية التسجيل إلكترونياً، واسترجاع الوثائق الإلكترونية بالحالة التي حفظت عليها[1]، وإن كان هذا المعيار غير ملزم قانوناً فهو عبارة عن معيار استرشادي، أو بالأحرى هو دليل نموذجي الغرض منه توحيد المعايير في مختلف دول العالم[2].

من خلال ما سبق كله، يمكن القول أن السجل الإلكتروني قد أصبح في عصرنا الحالي يتمتع بمميزات وإيجابيات لا تتوافر في السجلات التقليدية الورقية، ومن بين مميزاته صعوبة تغييره أو تحريفه أو تزويره مقارنة بالسجلات الورقية، ولك لأنه يعتمد على تكنولوجيا التأمين والتشفير التي تُصَعِّب على أي شخص غير مرخص له أن يصل أو يغير، أو يزور مستندات محفوظة إلكترونياً، إلا إذا قام باختراق الشفرة[3].

زيادة على ذلك، فإن حفظ هذه السجلات يحتاج إلى حيز مكاني أقل مقارنة بالسجلات الورقية، حيث يتم حفظها على دعامات إلكترونية كالأقراص المغناطيسية والأسطوانات المضغوطة التي لا تشغل أي حيز يذكر، وهو الأمر الذي يؤدي إلى توفير مساحات كافية للتخزين والحفظ[4].

ولعل من إيجابيات السجل الإلكتروني اعتباره دليلاً في الإثبات يقدم إلى المحاكم، وذلك في حالة وجود شك أو خلاف بين الأطراف المتعاقدة، على أن يكون للقاضي الحق في تقدير وتقييم حجية تلك السجلات الإلكترونية في الإثبات، ويمكن له الاستعانة بأهل الخبرة لاستجلاء الأمر[5].

---

[1]- من بين التوصيات التي تم وضعها من طرف الجمعية الفرنسية للتوحيد القياسي:
1) ضرورة وضع نظام فني مرن الغرض منه التأكد من إتمام عملية الحفظ اليومية بطريقة آمنة وخالية من سوء النية وليس فيها تحايل على القانون.
2) إلزام المؤسسات والمنشآت التجارية بالفحص الدوري والمنتظم لأنظمة السجلات الإلكترونية وذلك بغرض اكتساب ثقة العملاء في عمليات التسجيل الإلكتروني.
لتفاصيل أكثر يراجع، علاء حسين مطلق التميمي، الأرشيف الإلكتروني وكيفية المحافظة على المستند الإلكتروني عبر الزمن، المرجع السابق، ص. 172.

[2]- محمد أمين الرومي، المستند الإلكتروني، المرجع السابق، ص،ص. 156- 157.

[3]- لزهر بن سعيد، المرجع السابق، ص. 136.

[4]- محمد أمين الرومي، المستند الإلكتروني، المرجع السابق، ص. 156.

[5]- علاء حسين مطلق التميمي، الأرشيف الإلكتروني وكيفية المحافظة على المستند الإلكتروني عبر الزمن، المرجع السابق، ص. 173.

المبحث الثاني: القوة الثبوتية للمستند الإلكتروني.

لقد سمحت التقنية الحديثة للمعلوماتية والاتصالات بزيادة التعاملات بين الأفراد، وكذا التعاقد عن بعد، وهذا الأمر أصبح يفرض نفسه وبات يدفع إلى ضرورة مواكبة هذه الإمكانات الهائلة التي أصبح يتم فيها التعاقد من خلال الحواسب، وعبر الشبكات المفتوحة[1].

ولعل المشكلة الأساسية في مجال استخدام تقنية المعلوماتية، والتعاقد عن بعد تكمن في الإثبات بالدرجة الأولى، خاصة وأن المعاملات والعقود تتم في شكل غير عادي ودون الحاجة إلى مستندات ودعائم ورقية[2].

ولقد كان لهذه التطورات التكنولوجية الهائلة أثرها المباشر على قوانين الكثير من الدول، والتي توسعت فيها النظرة إلى المستندات وما تحتويه من كتابة وتوقيع، بحيث أصبحت تشمل الكتابة الإلكترونية والتوقيع الإلكتروني، ومن ثم فإنه يثار التساؤل عن ما هي القوة الثبوتية للمستندات الإلكترونية؟، وهل يمكن قبول الكتابة الإلكترونية، والتوقيع الإلكتروني كبديل ونظير للكتابة والتوقيع الخطي المتطلب توافره في الإثبات؟.

وكيف يمكن الإثبات بالوثائق والمستندات الإلكترونية؟، وما هي حجيتها في الإثبات؟

للإجابة على هذه التساؤلات سوف يتم التطرق إلى الشروط اللازمة للاعتماد على المستند الإلكتروني كوسيلة للإثبات، وذلك بعنصريه المتمثلين في الكتابة التوقيع الالكترونيين **(المطلب الأول)**، ثم بعد ذلك سيتم دراسة حجية عناصر المستند الإلكتروني في الإثبات المدني **(المطلب الثاني)**، كما سوف يتم إلقاء الضوء على حجية عناصر المستند في الإثبات من الناحية الجزائية **(المطلب الثالث)**.

[1]- باطلي غنية، المرجع السابق، ص. 181.
[2]- يوسف أحمد النوافلة، حجية المحررات الإلكترونية في الإثبات، دار وائل للنشر، الأردن، 2007، ص، ص. 103-104؛ باطلي غنية، المرجع السابق، ص. 180.

المطلب الأول: الشروط اللازمة للاعتماد على المستند الالكتروني كوسيلة للإثبات.

يشترط في المستند الإلكتروني عدة شروط حتى يؤدي وظيفته القانونية في الإثبات، ونظراً لأن عنصري الكتابة والتوقيع يشكلان أهم عناصر هذا المستند، فإن معرفة الشروط اللازمة للاعتماد على هذا المستند الإلكتروني كوسيلة للإثبات يقتضي حتما ضرورة البحث في الشروط الواجب توافرها في الكتابة الإلكترونية **(الفرع الأول)**، خاصة وأن هذه الكتابة تتم على دعامة غير ورقية، كما يقتضي أيضا البحث في الشروط الواجب توافرها في التوقيع الإلكتروني **(الفرع الثاني)**، خاصة وأن هذا التوقيع أصبح يتم باستخدام الوسائل والأجهزة الإلكترونية المتقدمة.

الفرع الأول: الشروط المتعلقة بالكتابة الإلكترونية على المستند

إن الكتابة على المستند تتمثل في البيانات التي يقوم صاحب الشأن بمعنى محرر المستند بتدوينها فيه، ذلك أن التوقيع على المستند المكتوب يقتضي بالضرورة أن يشتمل هذا المستند على بيانات لها مضمون معين[1]، ومن ثم فإنه من شروط هذه الكتابة حتى تؤدي وظيفتها القانونية في الإثبات أن تكون مقروءة **(البند الأول)**، بحيث تدل على مضمون التصرف القانوني، أو البيانات المدونة بالمستند، وأن تكون مستمرة **(البند الثاني)**، وذلك بتدوين الكتابة على دعائم تحفظها بصورة مستمرة، بحيث يمكن لأطراف العقد أو أصحاب الشأن الرجوع إليها عند الضرورة، كما يشترط فيها أيضاً أن تضمن عدم التعديل في مضمونها سواءً بالإضافة أو الحذف **(البند الثالث)**، وهذا كله حتى تتمتع بالثقة والأمان من جانب المتعاملين في التجارة الإلكترونية[2].

[1]- الأنصاري حسن النيداني، حجية المحررات الإلكترونية في الإثبات في المواد المدنية وسلطة القاضي إزاءها، مجلة الفكر القانوني والاقتصادي، مجلة فصلية محكمة تصدرها كلية الحقوق جامعة بنها، جمهورية مصر العربية، عدد خاص بالمؤتمر العلمي السنوي الرابع لكلية الحقوق بجامعة بنها، 2010، ص. 371.

[2]- لزهر بن سعيد، المرجع السابق، ص. 145؛ يوسف أحمد النوافلة، المرجع السابق، ص. 55 وما يليها.

البند الأول: أن تكون الكتابة مقروءة (lisible).

حتى يمكن الاعتداد بمضمون المستند المكتوب في مواجهة الآخرين، فإنه يشترط في هذا المستند المعد لإثبات أن يكون مقروءاً، وأن تكون كتابته واضحة بحيث يمكن فهمها وإدراك محتواها[1]، ومن ثم فإنه يجب أن يكون هذا المستند الكتابي مدوناً بحروف أو رموز مفهومة ومعروفة للشخص الذي يراد الاحتجاج به عليها[2]، ويستوي في ذلك أن تكون هذه الكتابة على دعامة ورقية أو إلكترونية، أما إذا كانت الكتابة غير مقروءة فإنه لا يعتد بالمستند الكتابي ولو كان موقعاً[3].

وبالرجوع إلى طريقة تدوين المستند الإلكتروني فإن تدوينه يتم على وسائط إلكترونية بلغة الآلة المكونة من توافق وتبادل بين رقم الصفر ورقم الواحد، مما يعجز معه الإنسان عن فهم هذه اللغة اللوغاريتمية المعقدة، غير أنه ولتجنب هذه العقبة قد تم إيجاد برامج خاصة يجري تحميلها على جهاز الحاسب لتقوم بترجمة لغة الآلة إلى لغة الإنسان، من خلال تحويل رموز الآلة إلى حروف مقروءة وواضحة[4].

وعليه فإن شرط القراءة يتحقق ويتوافر في المستندات الإلكترونية، ما دام أن اللغة التي تظهر على شاشة الجهاز هي لغة مفهومة ومقروءة لأطراف العقد ولو أن ذلك يتم

---

[1]- في الشريعة الإسلامية يجب أن تكون الكتابة مستبينة على وجه يمكن معه قراءتها وفهمها، وفي هذا يقسم الفقه الإسلامي الكتابة إلى ثلاث مراتب:
- مستبينة مرسومة بحيث تكون معنونةً: أي مصدراً بعنوان، وهو أن يكتب في صدره من فلان إلى فلان على ما جرت به العادة فهذا كالنطق فلزم حجة.
- ومستبينة غير مرسومة كالكتابة على الجدران وأوراق الأشجار لا على الوجه المعتاد فلا تكون حجة إلا بانضمام شيء آخر كالنية والإشهاد عليه والإملاء على الغير حتى يكتبه لأن الكتابة قد تكون للتجربة ونحوها، وبهذه الأشياء تتعين الجهة وقبل الإملاء بالإشهاد لا يكون حجة والأول أظهر.
- غير مستبينة كالكتابة على الهواء أو الماء، وهو بمنزلة كلام غير مسموع ولا يثبت به شيء من الأحكام.
مشار إليه من طرف، الأنصاري حسن النيداني، حجية المحررات الإلكترونية في الإثبات في المواد المدنية وسلطة القاضي إزاءها، المرجع السابق، هامش ص. 372.

[2]- علاء حسين مطلق التميمي، المستند الإلكتروني، عناصره، تطوره، ومدى حجيته في الإثبات المدني، المرجع السابق، ص. 47.

[3]- الأنصاري حسن النيداني، حجية المحررات الإلكترونية في الإثبات في الإثبات المواد المدنية وسلطة القاضي إزاءها، المرجع السابق، ص.372.

[4]- علاء حسين مطلق التميمي، المستند الإلكتروني، عناصره، تطوره، ومدى حجيته في الإثبات المدني، المرجع السابق، ص.47.

بطريق غير مباشر، عن طريق استخدام الحاسب الآلي أو الهاتف المحمول أو أية وسيلة أخرى، حيث تظهر الكتابة على شاشة الجهاز في صورة واضحة[1].

من أجل حسم المسألة السابقة الذكر، حرصت قوانين المعاملات الإلكترونية المختلفة على التأكيد على هذا الشرط بالنسبة لأي سجل أو مستند أو رسالة إلكترونية، بحيث نص المشرع الفرنسي في المادة 1365 من القانون المدني المعدلة بموجب الأمر رقم 131- 2016 المؤرخ في 10 فيفري 2016 على ضرورة توفر هذا الشرط، وذلك من خلال تعريفه للكتابة في نص هذه المادة، والتي جاء فيها أنه: " تتكون الكتابة من تتابع حروف أو أشكال أو أرقام أو أي علامات أو رموز، تمثل معنى مفهوم مهما كانت دعامتها"[2].

كما نصت قوانين الدول العربية على ضرورة توافر هذا الشرط في الكتابة، وفي القانون المصري[3]، والقانون الإماراتي[4] والبحريني[5]، ونفس الاتجاه انتهجه التشريع الجزائري، وذلك بموجب القانون رقم 05-10 المتضمن القانون المدني الجزائري المعدل والمتمم، بحيث نص في المادة 323 مكرر منه على أنه: " ينتج الإثبات بالكتابة من تسلسل

---

[1]- الأنصاري حسن النيداني، حجية المحررات الإلكترونية في الإثبات في المواد المدنية وسلطة القاضي إزاءها، المرجع السابق، ص. 373؛ لزهر بن سعيد، المرجع السابق، ص. 146.

[2] -Article 1365 c.civ.fr (modifié par ordonnance n°2016-131 du 10 février 2016 – art .4) dispose que : «L'écrit consiste en une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quel que soit leur support ».

[3]- تنص المادة الأولى من القانون رقم 15 لسنة 2004 بشأن تنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات، سابق الإشارة إليه.الكتابة الإلكترونية : " كل حروف أو أرقام أو رموز أو أي علامات أخرى تثبت على دعامة إلكترونية أو ورقية أو ضوئية أو أية وسيلة أخرى مشابهة وتعطي دلالة قابلة للإدراك".

[4]- تنص المادة الأولى قانون إمارة دبي رقم 2 لسنة 2002 بشأن المعاملات والتجارة الالكترونية، سابق الإشارة إليه. السجل أو المستند الإلكتروني: "سجل أو مستند يتم إنشاؤه أو تخزينه أو استخراجه أو نسخه أو إرساله أو إبلاغه أو استلامه بوسيلة إلكترونية، على وسيط ملموس أو على أي وسيط إلكتروني آخر، ويكون قابلاً للاسترجاع بشكل يمكن فهمه".

[5]- تنص المادة 3/1 من مرسوم بقانون رقم (28) لسنة 2002 بشأن المعاملات الالكترونية البحريني، سابق الإشارة إليه. في تعريفها للسجل بأنه: "المعلومات التي تدون على وسط ملموس، أو تكون محفوظة على وسط إلكتروني أو على أي وسط آخر، وتكون قابلة للاستخراج بشكل قابل للفهم". كما تنص المادة 3/09 من نفس القانون على أنه: " يشترط أن تكون المعلومات التي تضمنها السجل الإلكتروني الذي تم حفظه قابلة لأن يتم لاحقاً الدخول عليها وعرضها واستخراجها بشكل قابل للفهم". هذا وتنص المادة 07 /ب منه على أنه: " في حالة الإلزام بتقديم أصل المستند إلى شخص معين، فإنه يجب أن يكون السجل الإلكتروني قابلاً للدخول عليه واستخراجه وحفظه وعرضه بشكل قابل للفهم من قبل ذلك الشخص".
للإشارة فإن هذا القانون بعد إلغائه وإحلال مرسوم بقانون رقم 54 لسنة 2018 المتعلق بإصدار قانون الخطابات والمعاملات الإلكترونية، أضحت المادة 7/ب منه المادة 8/ب وقد نصت هذه الأخيرة على أنه: "في حالة الإلزام بتقديم المستند أو السجل أو المعلومات إلى شخص معين، يجب أن يكون السجل الإلكتروني قابلا لأن يتم عرضه على ذلك الشخص."
هذا وقد أضحت المادة 3/9 من القانون الملغى المادة 10/أ/1 والتي نصت: "أن تكون المعلومات الواردة في السجل الإلكتروني قابلة لأن يتم النفاذ إليها بما يمكن من استعمالها عند الرجوع إليها لاحقا."

الحروف أو أوصاف أو أرقام أو أية علامات أو رموز ذات معنى مفهوم، مهما كانت الوسيلة التي تتضمنها وكذا طرق إرسالها".

البند الثاني: استمرارية الكتابة ودوامها (Durabilité.)

من الشروط الواجب توافرها بالمستند الإلكتروني المعد للإثبات الاستمرارية، فاستمرارية الكتابة تعني أن يتم التدوين على وسيط يسمح بثبات الكتابة عليه، واستمرارها، بحيث يمكن الرجوع إليها وقت الحاجة[1]، لاستعمالها لمراجعة بنود العقد مثلاً أو لعرضها على القضاء عند حدوث خلاف بين أطرافه.

وببحث هذا الشرط ومدى توافره في كل من المستند العادي الورقي والمستند الإلكتروني، يتبين أن طبيعة وتكوين الورق يسمح بتحقق هذا الشرط، وبغض النظر عن العوامل الاستثنائية التي قد تحد من ذلك كالرطوبة، أو تآكل الأوراق نتيجة لسوء التخزين أو لحرقها، بخلاف المستندات الإلكترونية ذلك أن الخاصية الكيميائية والمادية التي تتكون منها الشرائح الممغنطة التي يجري تحميل وتخزين البيانات الإلكترونية عليها، تمتاز بحساسية عالية تجعلها عرضة للتلف السريع، الأمر الذي لا يستوي معه اعتماد هذه الوسائط في الإثبات، ما لم يجرى العمل على تجاوز هذه العقبة.

وبالرجوع للتطورات التقنية والتحسينات التي طرأت على مبتكرات الوسائط الإلكترونية، يتبين أنه تم التغلب على هذه العقبة، وذلك لما تم ابتكاره من وسائط تتمتع بقدرة تحميل هائلة، تسمح بالاحتفاظ بالبيانات المخزنة لمدة طويلة قد تتجاوز بذلك قدرة الأوراق العادية المعرضة للتلف والتآكل بعوامل الرطوبة، وبالتالي يمكن تحقيق هذا الشرط من خلال التكنولوجيا المتقدمة[2].

---

[1]- لزهر بن سعيد، المرجع السابق، ص. 146؛
S. Caidi, la preuve et la conservation de l'écrit dans la société de l'information, Faculté des études supérieures, université de Montréal, Décembre 2002, p.20.

[2]- علاء حسين مطلق التميمي، المستند الإلكتروني، عناصره، تطوره، ومدى حجيته في الإثبات المدني، المرجع السابق، ص. 49.

ولقد أكدت قوانين المعاملات الإلكترونية المختلفة على ضرورة توافر هذا الشرط في المستند الإلكتروني ومن ذلك المادة (1/10/أ) من قانون الأونيسترال النموذجي للتجارة الإلكترونية والتي نصت على أن: "الإطلاع على المعلومات الواردة فيها على نحو يتيح استخدامها والرجوع إليها لاحقا"، كما نصت المادة (1/6) من ذات القانون على أنه: "عندما يشترط القانون أن تكون المعلومة مكتوبة تستوفي رسالة البيانات ذلك الشرط إذا تيسر الاطلاع على البيانات الواردة فيها، على نحو يتيح استخدامها بالرجوع إليها لاحقا"[1].

هذا وقد تأثرت القوانين العربية بقانون الأونيسترال، ومنها القانون الأردني حيث نص في المادة 9/أ من قانون المعاملات الإلكترونية: "إذا اتفق الأطراف على إجراء معاملة بوسائل إلكترونية يقتضي التشريع الخاص بهذه المعاملة تقديم المعلومات المتعلقة بها، أو إرسالها أو تسليمها إلى الغير بوسائل خطية، فيجوز لهذه الغاية اعتبار إجراؤها بوسائل إلكترونية متفقاً مع متطلبات تلك التشريعات، إذا كان المرسل إليه قادراً على طباعة تلك المعلومات وتخزينها والرجوع إليها في وقت لاحق بالوسائل المتوفرة لديه"[2].

هذا وقد حلت محل هذا النص المادة 6/أ-ب من قانون المعاملات الإلكترونية رقم 15 لسنة 2015[3] والتي ورد فيها: "مع مراعاة أحكام الفقرة (ب) من المادة (3) من هذا القانون، إذا استوجب أي تشريع تقديم أي قيد أو عقد أو مستند أو وثيقة بشكل خطي أو كتابي فيعتبر تقديم السجل الإلكتروني الخاص بأي منها منتجا للآثار القانونية ذاتها شريطة ما يلي:

أ- إمكانية الإطلاع على معلومات السجل الإلكتروني.

ب-إمكانية تخزين السجل الإلكتروني والرجوع إليه في أي وقت دون إحداث أي تغيير عليه."

بهذا يلاحظ أن المشرع الأردني اشترط في الكتابة أن تحقق الوظيفة التقليدية، وهي حفظ الكتابة وإمكانية استرجاعها عند الحاجة.

[1]- قانون الأونيسترال النموذجي بشأن التجارة الإلكترونية لسنة 1996، سابق الإشارة إليه .
[2]- قانون رقم 85 لسنة 2001 المتعلق بالمعاملات الالكترونية الأردني، سابق الإشارة إليه.
[3]- قانون رقم 15 لسنة 2015 المتعلق بالمبادلات الالكترونية الأردني، سابق الإشارة إليه.

هذا وقد تبنى قانون المبادلات والتجارة الإلكترونية التونسي ذات الحكم، حيث نص الفصل الرابع منه على أنه: "يعتمد قانونا حفظ الوثيقة الإلكترونية، كما يعتمد حفظ الوثيقة الكتابية، ويلتزم المرسل بحفظ الوثيقة الإلكترونية بالشكل المرسل به، ويلتزم المرسل إليه بحفظ هذه الوثيقة في الشكل الذي تسلمها به، ويتم حفظ الوثيقة الإلكترونية على حامل إلكتروني يمكن من الاطلاع على محتواها طيلة مدة صلاحيتها، حفظها في شكلها النهائي بصفة تضمن سلامة محتواها، حفظ المعلومات الخاصة بمصدرها ووجهتها، وكذلك تاريخ ومكان إرسالها واستلامها"[1].

وقد نص المشرع الجزائري، هو الآخر على ضرورة توافر هذا الشرط في الكتابة وذلك من خلال نص المادة 323 مكرر1 من قانون 05-10 المتضمن القانون المدني الجزائري المعدل والمتمم، والتي ورد فيها عبارة: " أن تكون الكتابة في الشكل الإلكتروني معدة ومحفوظة في ظروف تضمن سلامتها"[2].

بهذا يكون المشرع الجزائري قد إشترط في الكتابة الإلكترونية أن تكون ثابتة ومحفوظة في ظروف تضمن وتمكن من له مصلحة من الرجوع إليها واستخدامها عند الحاجة.

البند الثالث: عدم قابلية الكتابة للتعديل .

يشترط في الكتابة حتى تصلح دليلاً في الإثبات أن تكون خالية من أي عيب يؤثر في صحتها، وبالتالي ينبغي أن تكون خالية من أي كشط أو محو أو تحشير، فإذا كانت هناك أية علامات تدل على التعديل في بيانات المستند، فإن هذا ينال من قوته في الإثبات[3].

للإشارة فإن هذا الشرط يتحقق بسهولة بالنسبة للمستندات الورقية التي تكتب بالقلم الجاف أو بالحبر أو على الآلة الكاتبة، وما ييسر ذلك أن هذه المواد تلتصق بالدعامة التي

[1]- الفصل الرابع من قانون رقم 83 لسنة 2000 المتعلق بالمبادلات والتجارة الإلكترونية، سابق الإشارة إليه.
[2]- القانون 05-10 المتضمن تعديل القانون المدني الجزائري، سابق الإشارة إليه.
[3]- لزهر بن سعيد، المرجع السابق، ص.147؛ علاء حسين مطلق التميمي، المستند الإلكتروني، عناصره وتطوره وحجيته في الإثبات المدني، المرجع السابق، ص. 50.

كتبت عليها، وتتصل كيميائيا بالتركيب المادي لهذه الأوراق، بحيث لا يمكن فصل الكتابة عن الورق إلا من خلال إتلافه (إتلاف الورق)، أو إحداث تغيير فيه، بحيث يمكن التعرف على هذا التغيير بمجرد النظر، أو بالاستعانة بالخبرة الفنية إذا استصعب ذلك[1].

وذلك بخلاف المستند الإلكتروني، حيث يعتمد شرط الدوام وعدم القابلية للتعديل على نوع وطبيعة الدعامات المثبتة عليها المعلومات والبيانات، ذلك أن الكتابة على الوسائط الإلكترونية من أقراص وشرائط ممغنطة، قد تمكن كل طرف من تعديل مضمون المستند وإعادة تنسيقه بالإضافة أو الإلغاء، ودون أن يظهر لهذا التعديل أي أثر مادي[2].

الواقع أنه قد تم تجاوز هذه العقبة، إذ قد أدى التطور التقني إلى ابتكار وسائل وتقنيات وبرامج حاسوب تعمل على تثبيت البيانات الإلكترونية، وتحافظ على بقاء النص في صورته التي تم عليها[3]، كما تعمل على حفظ المستند بطريقة تمكنها من كشف أي تعديل في البيانات الإلكترونية، وتسمح لها أن تحدد بدقة البيانات المعدلة ووقت تعديلها، ومن بين هذه التقنيات نظام التشفير والتوقيع الإلكتروني باستخدام تقنية المفتاح الواحد أو المفتاحين، وهو نظام يسمح باكتشاف أي تعديل أو تغيير في بيانات المستند الإلكتروني[4].

كما أن هناك بطاقات ذاكرة يمكن حفظ البيانات الإلكترونية عليها وفي هذه الأخيرة يبرز شرط الدوام في أعلى صوره، ذلك أن المعلومات المسجلة عليها يتعذر محوها، أو تعديلها ولا يمكن تغييرها أو محوها بأي وسيلة ماعدا بإعدامها تماما، هذا ويمكن الاستعانة بجهات التصديق الإلكتروني لحل هذه المشكلة بحيث يمكن اللجوء إليها عند ادعاء أي طرف من الأطراف المتعاقدة أن هناك عبثاً أو تعديلاً في بيانات المستند الإلكتروني[5]، وهذا لتحقيق

---

[1]- الأنصاري حسن النيداني، حجية المحررات الإلكترونية في الإثبات في المواد المدنية وسلطة القاضي إزاءها، المرجع السابق، ص. 375.

[2]- علاء حسين مطلق التميمي، المستند الإلكتروني، عناصره، نطوره ومدى حجيته في الإثبات المدني، المرجع السابق، ص.50.

[3]- Cf. T.P.Coudol, La signature électronique, introduction technique et juridique a la signature électronique sécurisée, prevue et écrit électronique , edition litec, 2001, p.57.

[4]- الأنصاري حسن النيداني، حجية المحررات الإلكترونية في الإثبات في المواد المدنية وسلطة القاضي إزاءها، المرجع السابق، ص. 376.

[5]- لزهر بن سعيد، المرجع السابق، ص. 148.

أقصى درجات الأمان فيما يتعلق بعدم قابلية المستند الإلكتروني للتعديل، فقوة المستند في الإثبات تتقرر بمدى سلامته من أي عيب قد يؤثر في شكله الخارجي.

ونظراً لأهمية هذا الشرط، فإن قوانين المعاملات الإلكترونية المختلفة، قد أكدت على وجوب حفظ المستند من أي تعديل، آخذة في الحسبان العمل على الإنقاص من قيمته وإسقاطه إذا ما تجاوز التعديل حداً معيناً يتشكك معه في صحة المستند، كما نصت على ضرورة إيجاد إجراءات معينة يمكن عن طريقها التحقق من أن المعلومات لم يتم تغييرها منذ إنشائها[1]، ومن أمثلة هذه التشريعات قانون الأونيسترال النموذجي بشأن التجارة الإلكترونية بحيث نصت المادة (1/10/ب) في معرض حديثها عن المستند الإلكتروني، وشرط الاستناد إليه في قدرته على: "الاحتفاظ برسالة البيانات بالشكل الذي أنشئت أو أرسلت به، أو بشكل يمكن إثبات أنه يمثل بدقة المعلومات التي أنشئت أو أرسلت أو استلمت"[2].

كما نصت المادة 30 من قانون المعاملات الإلكترونية الأردني[3] على أنه: "لمقاصد التحقق من أن قيداً إلكترونياً لم يتعرض إلى أي تعديل منذ تاريخ معين، فيعتبر هذا القيد موثقا من تاريخ التحقق منه، إذا تم بموجب إجراءات توثيق معتمدة أو إجراءات توثيق مقبولة تجارياً، أو متفق عليها بين الأطراف ذوي العلاقة.

ب- وتعتبر إجراءات التوثيق مقبولة تجارياً إذا تم عند تطبيقها مراعاة الظروف التجارية الخاصة بأطراف المعاملة بما في ذلك:

1- طبيعة المعاملة،

2- درجة دراية كل طرف من أطراف المعاملة،

3- حجم المعاملات التجارية المماثلة التي ارتبط بها كل طرف من الأطراف...".

[1]- علاء حسين مطلق التميمي، المستند الإلكتروني، عناصره، تطوره ومدى حجيته في الإثبات المدني، المرجع السابق، ص.50.

[2]- قانون الأونيسترال النموذجي بشأن التجارة الإلكترونية لسنة 1996، سابق الإشارة إليه.

[3]- قانون رقم 85 لسنة 2001 المتعلق بالمعاملات الالكترونية الأردني، سابق الإشارة إليه.

كما نصت المادة 19 من قانون المعاملات الإلكترونية الإماراتي على أنه: "إذا تم بطريقة صحيحة تطبيق إجراءات توثيق محكمة، منصوص عليها في القانون أو معقولة تجارياً ومتفق عليها بين الطرفين، على سجل إلكتروني للتحقق من أنه لم يتم تغييره منذ وقت معين من الزمن، فإن هذا السجل يعامل كسجل إلكتروني محمي منذ ذلك الوقت إلى الوقت الذي تم فيه التحقق،

2- لأغراض هذه المادة والمادة (20) من هذا القانون ولتقرير ما إذا كانت إجراءات التوثيق المحكمة معقولة تجارياً، ينظر لتلك الإجراءات والظروف التجارية وقت استخدامها بما في ذلك:

أ- طبيعة المعاملة،

ب- معرفة ومهارة الأطراف،

ج- حجم المعاملة المماثلة التي قام بها أي من الطرفين أو كلاهما،

د- وجود إجراءات بديلة،

هـ- تكلفة الإجراءات البديلة،

و- الإجراءات المستخدمة عموماً لأنواع مماثلة من المعاملات"[1].

كما نص المشرع الجزائري على ضرورة توافر هذا الشرط في الكتابة الإلكترونية، ويظهر ذلك في الشرط الفني الذي أورده في نص المادة 323 مكرر من القانون رقم 05-10 المتضمن القانون المدني المعدل والمتمم، والذي بموجبه اشترط في الكتابة " أن تكون معدة ومحفوظة في ظروف تضمن سلامتها"، بمعنى أن تدون الكتابة الإلكترونية بتقنيات تضمن حفظها ، وتضمن سلامتها من أي تعديل أو تبديل في مضمونها ومحتواها.

[1]- قانون إمارة دبي رقم 2 لسنة 2002 بشأن المعاملات والتجارة الالكترونية، سابق الإشارة إليه.

الفرع الثاني: الشروط المتعلقة بالتوقيع الإلكتروني على المستند.

لا يقوم التوقيع الإلكتروني بدوره الكامل في مجال الإثبات الإلكتروني إلا إذا اشتمل على مجموعة من الضمانات والشروط، هذه الأخيرة تسعى كلها إلى تحقيق هدف واحد، وهو توفير الثقة والأمان في المعاملات الإلكترونية، وذلك بإسباغ الحماية المدنية والحجية الثبوتية لهذا التوقيع[1].

ولعل السبب في اشتراط مواصفات فنية معينة للتوقيع الإلكتروني قبل ممارسته تكمن في أن مشكلة الأمن والخصوصية على شبكة الإنترنت أصبحت تشغل حيزاً كبيراً من الاهتمام، وهو الأمر الذي أثار قلق الكثير من المتعاملين، وذلك بسبب انعدام الثقة في هذه الشبكة، لذلك ظهرت الحاجة إلى ضرورة المحافظة على سرية المعلومات أو على أية رسالة مرسلة من شخص لآخر، حتى تنعدم قدرة هذا الأخير على الاطلاع أو تعديل أو تحريف الرسالة، وفي الوقت ذاته تكون رسالة المرسل الموقعة بتوقيعه الإلكتروني محددة لشخصيته وهويته، وبالتالي يمكن لمستقبل الرسالة أن يكشف أي تلاعب أو تحايل يدور حول تزوير ذلك التوقيع[2].

وعليه فإنه من بين الشروط الواجب توافرها في التوقيع الإلكتروني على المستند أن يكون هذا التوقيع متميزاً ومرتبطاً بشخص صاحبه ومعبراً عنه **(البند الأول)**، وأن يكون منشأ بواسطة وسائل تكون تحت التحكم الحصري للموقع **(البند الثاني)**، كما يشترط فيه أن يكون مرتبطاً بالمستند الإلكتروني ارتباطاً وثيقاً وأن يكون موثقا **(البند الثالث)**، على نحو يسمح بإمكانية كشف أي تبديل أو تعديل في بيانات التوقيع الإلكتروني، بمعنى أن يكون مرتبطاً بالبيانات الخاصة به، بحيث يمكن الكشف عن التغييرات اللاحقة بهذه البيانات ولأهمية هذه الشروط سيتم التعرض لها.

[1]- إبراهيم الدسوقي أبو الليل، التوقيع الإلكتروني ومدى حجيته في الإثبات، المرجع السابق، ص .115 وما يليها.
[2]- عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، المرجع السابق، ص، ص. 100- 101.

البند الأول: ارتباط التوقيع بالموقع وحده دون غيره.

يتطلب هذا الشرط أن يكون التوقيع خاصا بصاحبه دالاً على شخصيته ينفرد به على غيره، والموقع حسب ما عرّفه قانون الأونيسترال النموذجي للتوقيعات الإلكترونية هو كل: "شخص حائز على بيانات إنشاء التوقيع، ويوقع عن نفسه أو عن من ينيبه قانوناً"[1].

هذا وقد عرف المشرع الجزائري الموقع كل: "شخص طبيعي يتصرف لحسابه الخاص أو لحساب الشخص الطبيعي أو المعنوي الذي يمثله، ويضع موضع التنفيذ جهاز إنشاء التوقيع الإلكتروني"[2].

للإشارة فإن المشرع الجزائري تبنى تقريبا ذات التعريف في قانون التوقيع والتصديق الإلكترونيين، بحيث عرفه في نص المادة الثانية منه بأنه: " شخص طبيعي يحوز بيانات إنشاء التوقيع الإلكتروني ويتصرف لحسابه الخاص، أو لحساب الشخص الطبيعي أو المعنوي الذي يمثله "[3]، هذا وقد عرّف بيانات إنشاء التوقيع الإلكتروني في نص المادة الثانية الفقرة 03 من ذات القانون على أنها: "بيانات فريدة مثل الرموز أو مفاتيح التشفير الخاصة التي يستعملها الموقع لإنشاء التوقيع الإلكتروني".

وبخصوص مدى إمكانية توافر هذا الشرط في التوقيع الإلكتروني، يمكن القول أن التوقيع الإلكتروني بصوره المختلفة -التي تم دراستها سابقاً- إذا تم إنشاؤه بصورة صحيحة، فإنه يعد من قبل العلامات المميزة والخاصة بالشخص وحده ودون غيره، بمعنى أنه إذا قام أكثر من شخص باستعمال بعض أدوات إنشاء التوقيعات تمتلكها مؤسسة أو شركة ما، فإن تلك الأداة يجب أن تكون قادرة على تحديد هوية مستعمل واحد، تحديداً لا لبس فيه .

[1]- المادة الثانية الفقرة - د- من القانون النموذجي للأمم المتحدة بشأن التوقيعات الإلكترونية الأونيسترال لسنة 2001، سابق الإشارة إليه.

[2]- المادة 3 مكرر من المرسوم التنفيذي رقم 07-162 المعدل والمتمم للمرسوم التنفيذي رقم 01-123 والمتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية، وعلى مختلف خدمات المواصلات السلكية واللاسلكية، سابق الإشارة إليه.

[3]- القانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، سابق الإشارة إليه.

ولعلّ أفضل مثال على ذلك هو التعامل مع البنوك عن طريق استخدام الرقم السري، وذلك بإدخال بطاقة الائتمان المصرفية داخل جهاز السحب الآلي، وإعطاء حامل البطاقة موافقته الصريحة على سحب المبلغ المطلوب، فإن ذلك يعتبر بمثابة تعبير عن إرادته الصريحة برضائه بهذا التصرف، على الرغم من أنه قد استخدم مجرد رموز وأرقام في تعامله مع جهاز السحب الآلي[1].

هذا وقد أكدت غالبية التشريعات المتعلقة بالمعاملات الإلكترونية على ضرورة توافر هذا الشرط في التوقيع الإلكتروني، وذلك حتى يكون موثوقاً فيه ومؤمناً، وفي هذا السياق نجد إشترطت المادة 2/2 من التوجيه الأوروبي رقم 93 لسنة 1999 في التوقيع الإلكتروني حتى يكون محمي ومعزز: "1- أن يرتبط هذا التوقيع بالشخص الموقع حصراً، أو أن يكون قادراً على تحديد شخصية الموقع"، كما نص قانون الأونيسترال النموذجي المتعلق بالتوقيعات الإلكترونية لسنة 2001 على ذلك في المادة 3/6 التي قضت على أن: "التوقيع يكون موثوقاً به إذا توافرت فيه المتطلبات الآتية:

1- أن تكون بيانات إنشاء التوقيع مرتبطة بالموقع"[2].

وقد تبنت التشريعات العربية ذات المبدأ، وحذت حذو التوجيه الأوروبي وقانون الأونيسترال النموذجي المتعلق بالتوقيعات الإلكترونية، وأكدت على ضرورة توافر هذا الشرط في التوقيع، حتى يكون له القوة والأمان ويعتد به في الإثبات، ومن ذلك قانون إمارة دبي بشأن المعاملات والتجارة الإلكترونية[3]، بحيث نص في المادة 10 منه أنه من بين المتطلبات الواجب توافرها في التوقيع الإلكتروني حتى يكون محمي، أن ينفرد به الشخص الذي استخدمه، وأن يكون من الممكن أن يثبت هوية مستخدمه.

كما نص المشرع التونسي صراحة على ضرورة مراعاة الشروط الفنية للتوقيع الإلكتروني، قاصداً بذلك ضرورة توافر ضوابط ومواصفات معينة تتعلق بكيفية حصول

---

[1]- علاء حسين مطلق التميمي، المستند الإلكتروني، عناصره وتطوره ومدى حجيته في الإثبات المدني، المرجع السابق، ص.144.

[2]- المادة السادسة الفقرة 03 من القانون النموذجي بشأن التوقيعات الإلكترونية الأونيسترال لسنة 2001، سابق الإشارة إليه.

[3]- المادة 10 من قانون إمارة دبي رقم 2 لسنة 2002 بشأن المعاملات والتجارة الالكترونية، سابق الإشارة إليه.

التوقيع الإلكتروني الخاص بصاحب التوقيع، وذلك حتى يمكن الحفاظ على مصداقية هذا التوقيع لصاحبه وللآخرين الذين يوقع لهم على وثائق إلكترونية، كما أنه اعتبر كذلك أن هذه الشروط الفنية هي بمثابة السمات الشخصية التي تميز توقيعاً عن آخر، باعتبار أن التوقيع دال على صاحبه ويفيد نسبة المحرر أو المستند الذي وقعه إلى ذلك الشخص الموقع[1].

أما عن موقف المشرع الجزائري فيلاحظ أنه هو الآخر قد نص على ضرورة توافر هذا الشرط في التوقيع الإلكتروني، وذلك بداية في سنة 2007 حيث نص في المادة 3 مكرر من المرسوم التنفيذي رقم 07-162 المتعلق بخدمات المواصلات السلكية واللاسلكية على التوقيع الإلكتروني المؤمن، والتي أورد فيها أنه: "من بين المتطلبات الواجب توافرها في هذا التوقيع :

1- أن يكون خاصا بالموقع..."[2].

ثم بعد ذلك جاء في سنة 2015 وخاصة بموجب القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين، واشترط في نص المادة 07 منه ضرورة توافر هذا الشرط قي التوقيع الإلكتروني، غير أنه استبدل كلمة مؤمن الواردة في المرسوم التنفيذي رقم 07-162 بكلمة موصوف وسماه بالتوقيع الإلكتروني الموصوف، بحيث جاء في المادة 07 من القانون المذكور بأن: "التوقيع الإلكتروني الموصوف، هو التوقيع الإلكتروني الذي تتوفر فيه المتطلبات الآتية:

1- أن ينشأ على أساس شهادة تصديق إلكتروني موصوفة[3]،

---

[1]- عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، المرجع السابق، ص. 100.

[2]- المادة 3 مكرر من المرسوم التنفيذي رقم 07-162 المعدل والمتمم للمرسوم التنفيذي رقم 01-123 والمتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية، وعلى مختلف خدمات المواصلات السلكية واللاسلكية، سابق الإشارة إليه.

[3]- قد عرّف المشرع الجزائري شهادة التصديق الإلكتروني الموصوفة في نص المادة 15 من قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، سابق الإشارة إليه بأنها: "شهادة تتوفر فيها المتطلبات الآتية:

1) أن تمنح من قبل طرف ثالث موثوق أو من قبل مؤدي خدمات تصديق إلكتروني، طبقا لسياسة التصديق الإلكتروني الموافق عليها.

2) أن تمنح للموقع دون سواه.

3) يجب أن تتضمن على الخصوص:=

2- أن يرتبط بالموقع دون سواه،

3- أن يمكّن من تحديد هوية الموقّع...".

البند الثاني: سيطرة الموقع على الوسيط الإلكتروني.

يعتبر شرط انشاء التوقيع بوسائل تبقى تحت الرقابة الحصرية للموقع من الشروط الواجب توافرها في التوقيع الإلكتروني حتى تكون له مصداقية وقوة في الإثبات، ويقصد به سيطرة الموقع على الوسيط الإلكتروني بمعنى قدرة الموقع على الإحتفاظ بالتوقيع الإلكتروني والسيطرة عليه بشكل حصري، ولتحقق هذا الشرط ينبغي أن يكون صاحب التوقيع الإلكتروني منفرداً به، بحيث لا يستطيع أي شخص معرفة فك رموز التوقيع الخاص به أو الدخول عليه، سواء عند استعماله لهذا التوقيع أو عند إنشائه[1].

هذا وقد عبر قانون الأونيسترال النموذجي للتوقيعات الإلكترونية لسنة 2001 على هذا الشرط صراحة، حيث أكد على ضرورة سيطرة الموقع وحده دون غيره على الوسيط الإلكتروني، وذلك بموجب نص المادة السادسة الفقرة الثالثة، والتي أورد فيها أنه من بين المتطلبات الواجب توافرها في التوقيع الإلكتروني حتى يكون موثوقا به " أن تكون بيانات إنشاء التوقيع خاضعة لسيطرة الموقع..."[2].

كما أكدت تشريعات المعاملات الإلكترونية العربية على ضرورة توافر هذا الشرط في التوقيع الإلكتروني حتى يكون مؤمناً، ومن ذلك قانون إمارة دبي بشأن المعاملات

= أ- إشارة تدل على أنه تم منح هذه الشهادة على أساس أنها شهادة تصديق إلكتروني موصوفة.
ب- تحديد هوية الطرف الثالث الموثوق أو مؤدي خدمات التصديق الإلكتروني المرخص له المصدر لشهادة التصديق الإلكتروني وكذا البلد الذي يقيم فيه.
ج- اسم الموقِّع أو الاسم المستعار الذي يسمح بتحديد هويته.
د- إمكانية إدراج صفة خاصة للموقع عند الاقتضاء، وذلك حسب الغرض من استعمال شهادة التصديق الإلكتروني.
ه- بيانات تتعلق بالتحقق من التوقيع الإلكتروني وتكون موافقة لبيانات إنشاء التوقيع الإلكتروني.
و- الإشارة إلى بداية ونهاية مدة صلاحية شهادة التصديق الإلكتروني.
ز- رمز تعريف شهادة التصديق الإلكتروني.
ح- التوقيع الإلكتروني الموصوف لمؤدي خدمات التصديق الإلكتروني أو الطرف الثالث الموثوق الذي يمنح شهادة التصديق الإلكتروني".

[1]- عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، المرجع السابق، ص. 444.

[2] - قانون الأونيسترال النموذجي للأمم المتحدة بشأن التوقيعات الإلكترونية لسنة 2001، سابق الإشارة إليه.

الإلكترونية الذي نص في المادة العاشرة منه أنه: "من بين المتطلبات الواجب توافرها في التوقيع الإلكتروني حتى يكون محميا :

1- أن يكون تحت سيطرة الموقع التامة، سواء بالنسبة لإنشائه أو بالنسبة لوسيلة استعماله وقت التوقيع"[1].

وقد أكد قانون التوقيع الإلكتروني المصري على ذلك الشرط بعد ما عرف الوسيط الإلكتروني في المادة 1/د منه بإعتباره أداة أو أدوات أو أنظمة إنشاء التوقيع الإلكتروني[2]، للإشارة فإن المشرع المصري قد بين في المذكرة الإيضاحية لقانون التوقيع الإلكتروني بعض أنواع الوسيط الإلكتروني و أوردها على سبيل المثال لا الحصر، فاتحاً بذلك المجال لإمكانية إفراز التكنولوجيا لوسائط أخرى، ومن هذه الوسائط التي ذكرتها المذكرة أجهزة تسجيل البصمات والمجسمات وأجهزة وأنظمة التشفير، وشبكات الاتصال التي تربط بين هذه الأدوات والأنظمة، إضافة إلى البرامج المستخدمة في التشغيل وما في حكمها.

أما عن موقف المشرع الجزائري من هذا الشرط فيلاحظ أنه قد استلزم ضرورة سيطرة الموقع على بيانات إنشاء التوقيع بدايتا سنة 2007 ، بموجب نص المادة 03 مكرر الفقرة 02 من المرسوم التنفيذي رقم 07-162، حيث نصت على أن: "التوقيع الإلكتروني المؤمن هو توقيع يفي بالمتطلبات التالية: ... 2- أن يتم إنشاؤه بوسائل تبقى تحت رقابة الموقع الحصرية"، وقد إشترط هذا الشرط بعد أن عرف معطيات إنشاء التوقيع بأنها: "العناصر الخاصة بالموقع مثل الأساليب التقنية التي يستخدمها الموقع نسبة لإنشاء التوقيع الإلكتروني"[3].

وما تجدر الإشارة إليه، أن المشرع الجزائري واجه العديد من الانتقادات خلال هذه الفقرة، ذلك أنه لم يكن يبين من الناحية الفنية والتقنية كيف يتمكن الموقع من السيطرة على

[1]- المادة 10 من قانون إمارة دبي رقم 2 لسنة 2002 بشأن المعاملات والتجارة الالكترونية، سابق الإشارة إليه.
[2]- المادة 01 الفقرة - د- من القانون المصري رقم 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات، سابق الإشارة إليه.
[3]- المادة 3 مكرر من المرسوم التنفيذي رقم 07-162 المعدل والمتمم للمرسوم التنفيذي رقم 01-123 والمتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية، وعلى مختلف خدمات المواصلات السلكية واللاسلكية، سابق الإشارة إليه.

الوسيط الإلكتروني، مكتفيا بذكر قواعد عامة وتعريفات عامة وتاركا مسألة التفسير والتحليل لاجتهاد الفقه، وهذا الامر الذي يجعل الكثير من الباحثين يتساءلون حول الضوابط الفنية، والطرق والتقنيات والوسائل الواجب استعمالها لتمكين الموقع من السيطرة على الوسيط الإلكتروني، وهو في هذا يكون قد خالف بعض تشريعات المعاملات الإلكترونية ومنها المشرع المصري الذي شرح بموجب لائحته التنفيذية تلك المسائل الفنية، فحسب المشرع المصري مثلا تكمن هذه السيطرة في حيازة الموقع لأداة حفظ المفتاح الشفري الخاص متضمنة البطاقة الذكية المؤمنة، والكود السري المقترن بها[1].

بسبب الانتقادات التي واجهها المشرع الجزائري عمد بموجب قانون 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين إلى حسم الجدل و الغموض، فأكد على ضرورة توافر هذا الشرط وذلك بموجب نص المادة 07 من هذا القانون، والتي أورد فيها أنه من بين المتطلبات التي لا بد أن تتوفر في التوقيع الإلكتروني حتى يكون موصوفا: "... 4- أن يكون مصمماً بواسطة آلية مؤمنة خاصة بإنشاء التوقيع الإلكتروني،

5- أن يكون منشأ بواسطة وسائل تكون تحت التحكم الحصري للموقع"[2].

كما عرّف أيضا بيانات إنشاء التوقيع في نص المادة الثانية الفقرة 03 من القانون المذكور على أنهاّ: "بيانات فريدة، مثل الرموز أو مفاتيح التشفير الخاصة، التي يستعملها الموقع لإنشاء التوقيع الإلكتروني"، أما آلية إنشاء التوقيع فقد عرّفها في نفس المادة على أنها: " جهاز أو برنامج معلوماتي معد لتطبيق بيانات إنشاء التوقيع الإلكتروني"[3].

أما من الناحية التقنية فقد جاء المشرع الجزائري في نص المادة 11 من هذا القانون وبيّن بالتفصيل المتطلبات الواجب توافرها في آليات إنشاء التوقيع الإلكتروني الموصوف المؤمنة، بحيث نصت المادة 11 على أنه: "الآلية المؤمنة لإنشاء التوقيع الإلكتروني، هي آلية إنشاء توقيع إلكتروني تتوفر فيها المتطلبات الآتية:

[1]- محمد حسين منصور، الإثبات التقليدي والإلكتروني، دار الفكر الجامعي، الإسكندرية، 2006، ص. 280.
[2]- قانون رقم15-04 ا المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ص.08، سابق الإشارة إليه.
[3]- قانون رقم15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين ، ص.07، سابق الإشارة إليه.

1- يجب أن تتضمن بواسطة الوسائل التقنية والإجراءات المناسبة على الأقل ما يأتي:

أ- ألا يمكن عملياً مصادقة البيانات المستخدمة لإنشاء التوقيع الإلكتروني إلا مرة واحدة، وأن يتم ضمان سريتها بكل الوسائل التقنية المتوفرة وقت الاعتماد.

ب- ألا يمكن إيجاد البيانات المستعملة لإنشاء التوقيع الإلكتروني عن طريق الاستنتاج، وأن يكون هذا التوقيع محميا من أي تزوير عن طريق الوسائل التقنية المتوفرة وقت الاعتماد.

ج- أن تكون البيانات المستعملة لإنشاء التوقيع الإلكتروني محمية بصفة موثوقة من طرف الموقع الشرعي من أي استعمال من قبل الآخرين.

2- يجب أن لا تعدل البيانات محل التوقيع، وأن لا تمنع من تعرض هذه البيانات على الموقع قبل عملية التوقيع"[1].

هذا وقد نص كذلك في المادة 13 من القانون المذكور على المتطلبات الواجب توافرها في آلية التحقق من التوقيع الإلكتروني الموثوقة[2]، وهذا إن دل على شيء إنما يدل على أن النصوص التي استحدثها المشرع بموجب هذا القانون هي نصوص أكثر تفصيلا، وأكثر وضوحا مما نص عليه في المرسوم التنفيذي لسنة 2007.

وهذا كله رغبة من المشرع في عصرنة القطاعات الإدارية و الحكومية وتجسيدا لفكرة التجارة الإلكترونية والإدارة الإلكترونية، وكذا الحكومة الإلكترونية التي تعتمد على الوثائق والمستندات الإلكتروني الموقعة بتوقيعات إلكترونية كبديل للمستندات الورقية التقليدية.

[1]- قانون رقم15-04 المحدد للقواعد المتعلقة بالتوقيع والتصديق الإلكترونيين، سابق الإشارة إليه.
[2]- المادة 13 من القانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، سابق الإشارة إليه.

البند الثالث: ارتباط التوقيع الإلكتروني بالمستند.

يشترط في التوقيع الإلكتروني لكي يؤدي وظيفته في إثبات إقرار الموقع بما ورد في مضمون المستند، أن يكون هذا التوقيع متصلاً بالمستند على نحو لا يمكن فصله عنه، وأن يكون هذا الاتصال مستمراً ويمكن حفظه، واسترجاعه بطريقة معلوماتية آمنة طوال الفترة الزمنية الكافية لاستخدامه في الإثبات[1].

ولا شك أن هذا الشرط يتحقق بسهولة بالنسبة للتوقيع التقليدي على المستند الورقي، حيث يكون التوقيع فيه متصلاً بالمستند اتصالاً مادياً وكيميائياً، بحيث لا يمكن فصل أحدهما عن الآخر إلا بإتلاف المستند، أو إحداث تعديل في التركيب الكيميائي لكل من الأحبار، ومادة الأوراق المستخدمة، وهو الأمر الذي يمكن كشفه بالمناظرة، أو بالاستعانة بأهل الخبرة الفنية في هذا المجال، أما فيما يتعلق بالتوقيع الإلكتروني فقد يبدو لأول وهلة أن هذا الأمر غير ميسور، حيث أن المستندات الإلكترونية تتخذ شكل رموز وبيانات ومعلومات غالباً ما تكون على دعائم إلكترونية، بحيث يمكن إحداث تعديل وإدخال بيانات أخرى، مما يتفق مع مصالح مستعمل جهاز الحاسوب، والذي يخضع لسيطرة مستخدمه دون أن يترك ذلك أي أثر مادي يمكن أن يدل عليها[2].

زيادة على ذلك فإن شرط ارتباط التوقيع الإلكتروني بالمستند يتناول مسألة مهمة وضرورية، وهي سلامة المستند الإلكتروني الموقع من أي تعديل قد يطرأ عليه بعد توقيعه، ذلك أن حماية التوقيع الإلكتروني ليس غرضاً في ذاتها، وإنما هي حماية أيضاً للمستند الموقع عليه، والذي يتضمن انصراف مضمون المستند إلى الموقع[3]، ففي عقود التجارة

---

[1]- Art 1366 c.civ .fr (modifié par ordonnance n°2016-131 du 10 février 2016-art.4) dispose que :« ….Qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité »
Plus information. V.Yves Bismuth, Droit de l'informatique, éléments de droit à l'usage des informations, Nouveau édition, l'Harmattan, paris, Mise à jour au 1er octobre 2014, p. 185.

[2]- علاء حسن مطلق التميمي، المستند الإلكتروني، عناصره، تطوره، ومدى حجيته في الإثبات المدني، المرجع السابق، ص،ص. 146- 147.

[3]- عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، المرجع السابق، ص، ص. 444- 445.

الإلكترونية أو غيرها من العقود، فإن وضع التوقيع الإلكتروني على هذا العقد يعني اتجاه إرادة الموقع إلى انصراف آثار العقد والتزامه به.

وعليه فإن هذا الشرط يستلزم ضرورة تكامل البيانات المتعلقة بالتوقيع الإلكتروني، بحيث يكون أي تغيير يلحق برسالة البيانات أو المستند بعد توقيعه قابلاً للكشف، خاصة وأن إحداث أي تعديل على التوقيع الموضوع على المستند الإلكتروني قد يؤدي إلى تعديل بيانات المستند كاملة، وهو الأمر الذي قد يؤثر على سلامة وصلاحية المستند في الإثبات، كما قد يترتب عنه كذلك زعزعة سلامة هذه البيانات والتوقيع الإلكتروني أيضاً[1].

غير أنه سبق وأن تم التوضيح عند دراسة الشروط الواجب توافرها في الكتابة على المستند الإلكتروني، أن هذه المخاوف يمكن التغلب عليها في ظل التطور التقني الهائل في مجال نظم المعلومات والاتصالات، وما يبذله المختصون في هذا المجال من جهود كبيرة لتوفير أكبر قدر من الأمان والحماية والسرية لمثل هذه المعاملات، وأن هناك تقنيات تمكن من تسجيل وحفظ جميع البيانات الإلكترونية على دعائم إلكترونية غير قابلة للتعديل، وتتيح إمكانية استرجاعها عند الضرورة، كما يتيح التوقيع عليها بوسائل مشفرة يصعب معها فصل التوقيع عن المستند أو تعديله[2].

أما من الناحية التشريعية فيلاحظ أن قانون الأونيسترال النموذجي للأمم المتحدة المتعلق بالتوقيعات الإلكترونية لسنة 2001 قد نص صراحة في المادة 1/6 على ضرورة توافر هذا الشرط في التوقيع الإلكتروني، والتي أورد فيها أنه من المتطلبات الواجب توافرها في التوقيع الإلكتروني حتى يكون موثوقاً به: "إمكان اكتشاف أي تغيير في التوقيع يطرأ عليه، أو على المعلومات التي يوثقها"[3].

هذا وقد حذت التشريعات العربية المنظمة للمعاملات الإلكترونية حذو قانون الأونيسترال النموذجي، وأكدت على ضرورة توافر هذا الشرط في التوقيع الإلكتروني، ومن

---

[1]- علاء حسن مطلق التميمي، المستند الإلكتروني، عناصره، تطوره، ومدى حجيته في الإثبات المدني، المرجع السابق، ص.147.

[2]- إبراهيم الدسوقي أبو الليل، التوقيع الإلكتروني ومدى حجيته في الإثبات، دراسة مقارنة، المرجع السابق، ص. 118.

[3]- المادة السادسة من القانون النموذجي للأمم المتحدة الأونيسترال بشأن التوقيعات الإلكترونية لسنة 2001، سابق الإشارة إليه.

ذلك قانون إمارة دبي المتعلق بالتجارة الإلكترونية، بحيث نص في المادة العاشرة منه أنه من بين المتطلبات الواجب توافرها في التوقيع الإلكتروني حتى يكون محمي أن يرتبط بالرسالة الإلكترونية ذات الصلة[1]، ونفس الاتجاه سلكه المشرع المصري في نص المادة 18 من القانون المتعلق بالتوقيع الإلكتروني، وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات[2].

أما المشرع الجزائري فقد نص هو الآخر صراحة على ضرورة توافر هذا الشرط في التوقيع الإلكتروني، وهذا بموجب نص المادة 3 مكرر من المرسوم التنفيذي رقم 07-162، والذي اشترط فيها أنه من متطلبات التوقيع الإلكتروني المؤمن أن يضمن مع الفعل المرتبط به صلة، بحيث يكون كل تعديل لاحق للفعل قابلاً للكشف عنه[3].

كما أكد على ضرورة توافر هذا الشرط في التوقيع بموجب القانون رقم 15-04 المتضمن القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، وذلك من خلال المادة 7 منه الفقرة السادسة والتي اشترط فيها أنه: "من متطلبات التوقيع الإلكتروني حتى يكون موصوف:

- أن يكون مرتبطاً بالبيانات الخاصة به، بحيث يمكن الكشف عن التغييرات اللاحقة بهذه البيانات"[4].

وباستقراء نصوص هذا القانون يتبين أنه يتم من الناحية الفنية والتقنية كشف أي تعديل أو تبديل على بيانات المستند الإلكتروني الموقع إلكترونياً، باستخدام تقنية شفرة المفتاحين العام والخاص[5]، وبمضاهاة أو مطابقة شهادة التصديق الإلكتروني مع بيانات إنشاء

---

[1]- المادة 10 من قانون إمارة دبي رقم 2 لسنة 2002 بشأن المعاملات والتجارة الالكترونية، سابق الإشارة إليه.

[2]- تنص المادة 18 القانون المصري رقم 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات، سابق الإشارة إليه: "إمكانية كشف أي تعديل أو تبديل في بيانات المحرر الإلكتروني أو التوقيع الإلكتروني".

[3]- المرسوم التنفيذي رقم 07-162 المعدل والمتمم للمرسوم التنفيذي رقم 01-123 والمتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية، وعلى مختلف خدمات المواصلات السلكية واللاسلكية، سابق الإشارة إليه.

[4]- قانون رقم15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، سابق الإشارة إليه.

[5]- لقد عرّف المشرع الجزائري مفتاح التشفير الخاص في المادة الثانية الفقرة 08 من القانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، سابق الإشارة إليه: "عبارة عن سلسلة من الأعداد يحوزها حصرياً الموقع فقط، وتستخدم لإنشاء التوقيع الإلكتروني، ويرتبط هذا المفتاح بمفتاح تشفير عمومي".
كما عرف مفتاح التشفير العمومي في الفقرة 09 من ذات المادة بأنه: "عبارة عن سلسلة من الأعداد تكون موضوعة في متناول الجمهور بهدف تمكينهم من التحقق من الإمضاء الإلكتروني، وتدرج في شهادة التصديق الإلكتروني".

التوقيع بأصل الشهادة أو تلك البيانات أو بأي وسيلة مشابهة، وبهذا يكون المشرع الجزائري قد حسم كل غموض، وكل لبس كان يثار حول طريقة وتقنية إمكانية كشف أي تعديل أو تعديل على بيانات المستند الإلكتروني الموقع إلكترونياً.

من خلال ما سبق ذكره يمكن القول أن التوقيع الإلكتروني حالياً قد أصبح علما وليس فناً، وذلك لاعتماده على برامج معلوماتية متطورة تعمل على تشفيره وتحصينه من عبث العابثين، وهذا بخلاف التوقيع التقليدي الذي يعتبر فناً وليس علماً، وذلك مادام أنه عبارة عن رسم يقوم به الشخص ويكون عرضة للتبديل والتغيير.

المطلب الثاني: حجية عناصر المستند الإلكتروني في الإثبات المدني.

يقصد بالحجية القانونية للوثائق والمستندات الإلكترونية، القوة القانونية للبيانات والمعلومات المستخرجة عن طريق الوسائل الحديثة للاتصالات[1].

ويثور التساؤل عن مدى حجية هذه المستندات في الإثبات، خاصة وأن كتابتها وتوقيعها وإرسالها وحفظها يتم في بيئة إلكترونية دون تدخل أدوات الكتابة الورقية، إلا في حالة الرغبة في تحويل الكتابة الإلكترونية إلى ورقية، لما تقدم يتضح أن المستندات الإلكترونية لا تحمل توقيعا يدويا، بل التوقيع عليها يكون إلكترونيا، ولسبب هذا الأمر ترددت الهيئات القضائية كثيرا في قبول المستندات الإلكترونية لإثبات المعاملة مصدر الحق المدعى به أمامها ولكن سرعان ما تحول الوضع، إذ بعدما أصبحت التكنلوجيا الحديثة واقعا قائما في إبرام المعاملات المدنية والتجارية عمدت الهيئات المختصة على المستوى الدولي والوطني إما بتعديل قواعدها القانونية بما يتلاءم والتطورات التكنولوجية، أو بسن تشريعات جديدة تخص هذه المرحلة، وهذا كله من أجل إيجاد ضمانات تكفل حقوق الأفراد وتحافظ عليها، خاصة بعد أن أوجدت هذه التقنيات الحديثة فراغاً قانونياً نظراً للطبيعة الغير المادية التي ترتكز عليها[2].

[1]- عباس العبودي، الحجية القانونية لوسائل التقدم العلمي في الإثبات المدني، المكتبة القانونية، عمان، 2002، ص. 144.
[2]- تامر محمد سليمان الدمياطي، إثبات التعاقد الإلكتروني عبر الإنترنت- دراسة مقارنة-، ط1، منشأة المعارف، الإسكندرية، مصر، 2009، ص، ص. 101- 102.

وبما أن عناصر المستند الإلكتروني المعد للإثبات ينحصران في الكتابة والتوقيع الإلكترونيين، فإن بخصوص التساؤل مدى حجية الكتابة الإلكترونية في الإثبات؟، وهل تعتبر نظيرا للكتابة التقليدية؟

هذا ما سيتم بيانه بالتعرض إلى حجية الكتابة الإلكترونية في الإثبات **(الفرع الأول)**، وإلى حجية التوقيع الإلكتروني في الإثبات **(الفرع الثاني)**.

الفرع الأول: حجية الكتابة الإلكترونية في الإثبات.

من المتعارف عليه أن الكتابة على أي مستند تثبت التصرف المتفق عليه ما بين الأشخاص، سواء أثبت هذا التصرف بمستند رسمي أو عادي[1]، ومع التطور الذي حصل في المجال التكنولوجي، وما نتج عنه من تغير في دعامة الكتابة، ومع ظهور الكتابة الإلكترونية التي تختلف كلياً عن الكتابة المتعارف عليها (الكتابة العادية الورقية)، سارعت تشريعات أغلب الدول إلى المساواة بين الكتابة الإلكترونية والكتابة التقليدية، فمنحتها الحجية القانونية الكاملة في الإثبات، وكذا القوة الثبوتية الكاملة شأنها في ذلك شأن الكتابة العادية، وهو ما عبّر عنه الفقه والتشريع بمبدأ التكافؤ الوظيفي بين الكتابة الإلكترونية والكتابة العادية على الورق[2]، وقد تقرر هذا كله بغية مسايرة التطور التكنولوجي وحتى لا يقف مفهوم الكتابة حجر عثرة أمام التصرفات التي تبرم عبر التقنيات الحديثة.

ولعل من بين التشريعات التي أقرت مبدأ التكافؤ الوظيفي بين الكتابة الإلكترونية والكتابة الخطية قانون الأونيسترال النموذجي للأمم المتحدة المتعلق بالتجارة الإلكترونية لسنة 1996، بحيث نص في المادة 09 منه على قبول رسائل البيانات وأعطاها القوة والحجية في الإثبات، إذ أورد في هذه المادة أنه: " في أية إجراءات قانونية لا يطبق أي حكم من أحكام قواعد الإثبات من أجل الحيلولة دون قبول رسالة البيانات كدليل إثبات:

---

[1]- للإشارة فإن الكتابة تعتبر أفضل وسيلة لتحديد إرادة الالتزام ومحتواه ودوامه، كما أن اشتراط إعداد الكتابة لإثبات التصرفات القانونية يضمن المساواة بين الأطراف فيما يتعلق بالإثبات الذي يعتبر ضمانة مهمة للحفاظ على الحقوق، وهي بهذا الصدد أكثر موثوقية من طرق الإثبات الأخرى. مشار إليه من طرف، تامر محمد سليمان الدمياطي، المرجع السابق، ص،ص. 106- 107.

[2]- لزهر بن سعيد، المرجع السابق، ص،ص. 149- 150.

أ- لمجرد أنها رسالة بيانات،

ب- بدعوى أنها ليست في شكلها الأصلي، إذا كانت هي أفضل دليل يتوقع بدرجة معقولة من الشخص الذي يستشهد بها أن يحصل عليه"[1].

هذا وقد نص في الفقرة الثانية من هذه المادة على أن: " يعطى للمعلومات التي تكون في شكل رسالة بيانات ما تستحقه من حجة في الإثبات..."[2].

أما المشرع الفرنسي فقد أقر هذا المبدأ في نص المادة 1366 من القانون المدني الفرنسي المعدل بموجب الأمر رقم 131-2016 المؤرخ في 10 فيفري 2016، بحيث نصت هذه المادة على أنه: "للكتابة الإلكترونية نفس القوة والحجية الثبوتية للكتابة على الورق، بشرط إمكانية إثبات الشخص الذي أصدرها، وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها وصحتها"[3].

بموجب هذه المادة يلاحظ أن المشرع الفرنسي قد ساوى بين الكتابة على الدعامات الإلكترونية، وبين تلك المدونة على الدعامات الورقية في حجية الإثبات[4].

أما التشريعات العربية الخاصة بالمعاملات الإلكترونية فقد أقرت هي الأخرى هذا المبدأ، ومنحت للكتابة الإلكترونية نفس قوة وحجية الكتابة العادية في الإثبات، وذلك بدءاً بالتشريع التونسي الذي كان من بين الدول العربية السبّاقة في وضع تشريع ينظم به التجارة الإلكترونية والمعاملات الإلكترونية، هذا وقد أولى المشرع للتونسي للكتابة الإلكترونية مكانة متميزة ضمن النظرية العامة للإثبات حيث عمل على تنقيح مجلة الالتزامات والعقود

---

[1]- المادة 1/09 من قانون الأونيسترال النموذجي للأمم المتحدة المتعلق بالتجارة الإلكترونية لسنة 1996، سابق الإشارة إليه.

[2]- المادة 09/ 2من قانون الأونيسترال النموذجي للأمم المتحدة المتعلق بالتجارة الإلكترونية لسنة 1996، سابق الإشارة إليه.

[3]- Art 1366 c.civ.fr (modifié par ordonnance n°2016-131 du 10 février 2016-art.4) 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. »

[4]- Cf. Yves Bismuth, op.cit, p .185.

بموجب قانون 57 لسنة2000[1]، الذي أدرج فيه أحكاماً خاصة بالوثيقة الإلكترونية، وأورد لها تعريفاً في الفقرة الأولى من الفصل 453 مكرر، كما علق المشرع التونسي هذا الاعتراف صراحة بتحقق بعض الضوابط الفنية والتقنية، وذلك لضمان سلامة المستند من أي تغيير أو إتلاف، هذا وقد جاء بالفصل 453 مكرر على أن تكون الوثيقة الإلكترونية ذات محتوى يمكن فهمه ومحفوظة على حامل إلكتروني يمكن من قراءتها والرجوع إليها عند الحاجة، وأن اعتراف القانون بالوثيقة الإلكترونية يفترض استجابتها إلى شروط الفصل 453 مكرر[2].

أما المشرع الإماراتي فقد ساوى هو الآخر بين حجية الكتابة الخطية والكتابة الإلكترونية من حيث الوظيفة والإثبات، إذ نصت المادة 09 من قانون المبادلات والتجارة لإمارة دبي رقم 02 لسنة 2002 على أنه: "إذا اشترط القانون أن يكون خطياً أي بيان أو مستند أو سجل أو دعامة أو بينة، أو نص على ترتيب نتائج معينة في غياب ذلك، فإن المستند أو السجل الإلكتروني يستوفي هذا الشرط طالما تم الالتزام بأحكام الفقرة 1 من المادة السابقة"، وقد علّق المشرع الإماراتي هذه الحجية على استيفاء الكتابة الإلكترونية لبعض الشروط الفنية والتقنية التي سبق شرحها وبيانها في السابق[3].

ونفس الاتجاه سلكه المشرع المصري، بحيث منح بموجب المادة 15 من قانون التوقيع الإلكتروني للكتابة الإلكترونية الحجية القانونية الكاملة، حيث أورد في هذه المادة أنه: "للكتابة الإلكترونية والمحررات الإلكترونية، في نطاق المعاملات المدنية والتجارية ذات الحجية المقررة للكتابة والمحررات الرسمية والعرفية في أحكام قانون الإثبات في

---

[1]- القانون عدد 57 لسنة 2000 المؤرخ في 13 جوان 2000 المتعلق بتنقيح وإتمام بعض فصول من مجلة الالتزامات والعقود، سابق الإشارة إليه.

[2]- تنص المادة 453 مكرر من قانون عدد 57 لسنة 2000 المؤرخ في 13 جوان 2000 المتعلق بتنقيح وإتمام بعض فصول من مجلة الالتزامات والعقود، سابق الإشارة إليه. على أنه: "الوثيقة الإلكترونية هي الوثيقة المتكونة من مجموعة أحرف وأرقام وأي إشارات رقمية أخرى، بما في ذلك تلك المتبادلة عبر وسائل الاتصال، تكون ذات محتوى يمكن فهمه ومحفوظة على حامل إلكتروني يؤمن قراءتها والرجوع إليها عند الحاجة.
وتعد الوثيقة الإلكترونية كتبا غير رسمي إذا كانت محفوظة في شكلها النهائي بطريقة موثوقة بها ومدعمة بإمضاء إلكتروني".

[3]- يراجع في ذلك، ص 145 إلى ص 152 من هذه الأطروحة.

المواد المدنية والتجارية، متى استوفت الشروط المنصوص عليها في هذا القانون، وفقاً للضوابط الفنية والتقنية التي تحددها اللائحة التنفيذية لهذا القانون"[1].

كما نص في المادة 16 من ذات القانون على أن: "للصورة المنسوخة على الورق من المحرر الإلكتروني الرسمي حجية على الكافة بالقدر الذي تكون فيها مطابقة لأصل هذا المحرر، وذلك ما دام المحرر الإلكتروني الرسمي، والتوقيع الإلكتروني موجودين على الدعامة الإلكترونية"[2].

أما بخصوص موقف المشرع الجزائري من حجية الكتابة الإلكترونية في الإثبات، فيلاحظ أن المشرع ساير التشريعات الأجنبية والعربية، حيث إعترف بالكتابة الإلكترونية في نص المادة 323 مكرر من القانون 05-10 المتضمن القانون المدني المعدل والمتمم[3]، كما أقر مبدأ التكافؤ الوظيفي بين الكتابة الإلكترونية والعادية وأعطى لها الحجية الكاملة في الإثبات، ويظهر ذلك جلياً من خلال نص المادة 323 مكرر، والتي جاء فيها بأنه: "ينتج الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق، بشرط إمكانية التأكد من هوية الشخص الذي أصدرها، وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها"[4]،

---

[1]- تنص المادة 08 من قرار رقم 109 لسنة 2005 بتاريخ 15-05-2005 المتعلق بإصدار اللائحة التنفيذية للتوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة وتكنولوجيا المعلومات المصري، سابق الإشارة إليه. على أنه: "مع عدم الإخلال بالشروط المنصوص عليها في القانون، تتحقق حجية الإثبات المقررة للكتابة الإلكترونية والمحررات الإلكترونية الرسمية أو العرفية لمنشئها، إذا توافرت الضوابط الفنية والتقنية الآتية:

أ- أن يكون متاحاً فنياً وقت وتاريخ إنشاء الكتابة الإلكترونية أو المحررات الإلكترونية الرسمية أو العرفية، وأن تتم هذه الإتاحة من خلال نظام حفظ إلكتروني مستقل وغير خاضع لسيطرة منشئ هذه الكتابة أو تلك المحررات، أو لسيطرة المعني بها.

ب- أن يكون متاحاً فنياً تحديد مصدر إنشاء الكتابة الإلكترونية أو المحررات الإلكترونية الرسمية، ودرجة سيطرة منشئها على هذا المصدر وعلى الوسائط المستخدمة في إنشائها.

ج- في حالة إنشاء وصدور الكتابة الإلكترونية أو المحررات الإلكترونية الرسمية أو العرفية بدون تدخل بشري، جزئي أو كلي، فإن حجيتها تكون متحققة متى أمكن التحقق من وقت وتاريخ إنشائها ومن عدم العبث بهذه الكتابة أو تلك المحررات".

[2]- المادة 16 من القانون رقم 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني، وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات، سابق الإشارة إليه.

[3]- تنص المادة 323 مكرر من القانون 05-10 المتضمن تعديل القانون المدني الجزائري، سابق الإشارة إليه: "ينتج الإثبات بالكتابة من تسلسل الحروف أو أوصاف أو أرقام أو أية علامات أو رموز ذات معنى مفهوم مهما كانت الوسيلة التي تتضمنها، وكذا طرق إرسالها".

[4]- المادة 323 مكرر 1 من القانون 05-10 المتضمن تعديل القانون المدني الجزائري، سابق الإشارة إليه .

وهي تقريبا نفس المادة التي أوردها المشرع الفرنسي الذي سبق بيانها المادة 1366 من القانون المدني الفرنسي.

الفرع الثاني: حجية التوقيع الإلكتروني في الإثبات.

إن الكتابة على المستند لا تعتبر دليلاً كاملاً في الإثبات إلا إذا كانت ممهورة بالتوقيع، والذي يعتبر بمثابة العنصر الثاني من عناصر الدليل الكتابي المعد أصلا للإثبات، ذلك أنه هو الذي يحدد هوية الشخص ويعبر عن قبوله الالتزامات الواردة في المستند، كما أنه هو الذي ينسب الورقة إلى من وقعها حتى ولو كانت مكتوبة بخط يده[1]، ومع التوجه نحو عالم الرقميات كبديل لعالم الماديات، عالم البيانات والملفات المخزنة في أنظمة المعلومات كبديل للبيانات المحررة على الورق وحوافظ الملفات التقليدية، فإنه يزداد الاهتمام بمدى حجية وقوة التوقيع الإلكتروني في الإثبات وهل أنه يؤدي نفس وظائف التوقيع الخطي التقليدي؟[2].

فبالنسبة للمساواة من حيث المنظور الوظيفي، فإنه بالرغم من الاختلاف بين التوقيع التقليدي والتوقيع الإلكتروني من حيث طريقة إنشاء كل منهما، كون الأول عبارة عن رسم يقوم به الشخص (الموقع)، ويظهر في شكل بصمة أو إمضاء أو ختم أو طباعة أو غير ذلك، في حين يتم إنشاء الثاني بأشكال مغايرة عن الأشكال التي تم ذكرها سابقاً، ذلك أنه عبارة عن رقم أو رمز أو كتابة بالقلم الإلكتروني أو صورة لخصائص بيولوجية في الإنسان، وهذا حسب الطريقة البيوميترية أو التوقيع البيوميتري الذي سبق التطرق إليه، والذي يتم على إثر مجموعة من الإجراءات وليس نتيجة إمضاء أو ختم[3].

إلا أن التشريعات الدولية والوطنية اتجهت نحو تحقيق المساواة بين التوقيع التقليدي والالكتروني من حيث المنظور الوظيفي، حيث وسعت من دائرة التوقيع، الطريقة المستعملة في إنشاءه ، فأجازت أن يكون التوقيع بأي شكل، بمعنى أنها لم تحصر الأشكال التي يتم بموجبها التوقيع، بحيث أصبح التوقيع يتم إلى جانب الوسائل العادية التقليدية السالفة الذكر

[1]- عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، المرجع السابق، ص،ص. 126- 127.
[2]- تامر محمد سليمان الدمياطي، المرجع السابق، ص، ص. 115- 116.
[3]- عبد الفتاح بيومي حجازي، التجارة الإلكترونية في القانون النموذجي لمكافحة جرائم الكمبيوتر والإنترنت، المرجع السابق، ص،ص. 252- 253.

كالختم والتثقيب، بأي وسيلة آلية أو إلكترونية أخرى[1]، وهو ما أخذ به المشرع الجزائري سنة 2005، بموجب نص المادة 323 مكرر من القانون 05-10 المتضمن القانون المدني المعدل و المتمم[2].

أكثر من ذلك يمكن أن يؤدي التوقيع في الشكل الكتابي مجموعة متنوعة من الوظائف حسب طبيعة المستند الذي يحمل التوقيع، فيكون دليلاً على نية الموقع لإقراره بتحريره نص المستند للإثبات في حالة قيام نزاع مستقبلي بين الأطراف، كما أنه يعد وسيلة لتوثيق العقد وتأمينه من التعديل[3].

أما التوقيع الإلكتروني فزيادة على قيامه بالوظائف السابقة فهو يمتاز على التوقيع التقليدي من ناحية الاستيثاق أو الوثوق من شخصية صاحب التوقيع كلما استخدم في ذلك الرقم السري أو المفتاح الخاص، وبالتالي فإنه لا مجال للانتظار حتى ينشب النزاع للبحث في مدى صحة التوقيع كما هو الشأن في معظم الأحوال بخصوص المستندات الموقعة بخط اليد[4].

ومن ثم فإن المساواة من حيث الوظائف التي يؤديها التوقيع التقليدي والتوقيع الإلكتروني (مبدأ التكافؤ الوظيفي) قد أصبحت من المبادئ المعترف بها من الناحية التشريعية.

أما عن قوة وحجية التوقيع الإلكتروني في الإثبات، فيلاحظ أن التشريعات الدولية والوطنية إلى جانب إقرارها لمبدأ المساواة بين التوقيع العادي والإلكتروني من حيث المنظور الوظيفي، أقرت كذلك في نصوصها التشريعية مبدأ المماثلة والمساواة بين التوقيعين (الإلكتروني والتقليدي) من حيث القوة والحجية في الإثبات[5].

---

[1]- خالد ممدوح إبراهيم، إبرام العقد الإلكتروني، المرجع السابق، ص.247.

[2]- تنص المادة 323 مكرر من القانون 05-10 المتضمن تعديل القانون المدني الجزائري، سابق الإشارة إليه: "ينتج الإثبات بالكتابة من تسلسل الحروف أو أوصاف أو أرقام أو أية علامات أو رموز ذات معنى مفهوم، مهما كانت الوسيلة التي تتضمنها، وكذا طرق إرسالها".

[3]- نجوى أبو هيبة، التوقيع الإلكتروني، تعريفه ومدى حجيته في الإثبات، دار النهضة العربية، مصر، 2004، ص.83 ؛ خالد ممدوح إبراهيم، إبرام العقد الإلكتروني، المرجع السابق، ص.246.

[4]- خالد ممدوح إبراهيم، إبرام العقد الإلكتروني، المرجع السابق، ص. 246؛ لزهر بن سعيد، المرجع السابق، ص. 166.

[5]- للإشارة لقد ميزت التشريعات التي نظمت الإثبات الإلكتروني بين نوعين من التوقيع الإلكتروني الأول سمته بالتوقيع الإلكتروني البسيط، أما الثاني فقد أطلقت عليه تسمية التوقيع الإلكتروني المتقدم أو المعزز أو المؤمن أو الموصوف، كما سماه المشرع الجزائري في القانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.=

بحيث منح قانون الأونيسترال المتعلق بالتوقيعات الإلكترونية للتوقيع الإلكتروني الحجية القانونية للإثبات شأنه في ذلك شأن التوقيعات العادية، وأورد ذلك في نص المادة 06 منه، والتي جاء فيها أنه: "عندما يشترط القانون وجود توقيع من شخص، يستوفي ذلك الشرط بالنسبة إلى رسالة البيانات، إذا استخدم توقيع إلكتروني موثوق بالقدر المناسب للغرض الذي أنشئت، أو بلغت من أجله رسالة البيانات، بما في ذلك أي اتفاق ذي صلة"[1].

كما اعترف التوجيه الأوروبي بشأن التوقيعات الإلكترونية بحجية التوقيع الإلكتروني، وحث الدول الأعضاء في الاتحاد الأوروبي على منحه الحجية القانونية في التعاملات الإلكترونية، بحيث نص على ذلك في المادة (1/5) منه، والتي جاء فيها بأنه: "على سائر الدول الأعضاء، بشأن التوقيعات الإلكترونية المسبقة (المتقدمة) القائمة على شهادة موصوفة، والمنشئة بطريق منظومة آمنة لإنشاء التوقيع على الآتي:

1- أن تستجيب للمتطلبات الشرعية للتوقيع حيال البيانات الإلكترونية على ذات النحو الذي يستجيب به التوقيع التقليدي للمتطلبات حيال البيانات الخطية، أو المطبوعة على الورق.

2- أن تكون مقبولة كأدلة أمام القضاء"[2].

وقد انتهج التشريع الفرنسي ذات النهج الذي اعتمده قانون الأونيسترال النموذجي للتوقيعات الإلكترونية لسنة2001، وكذا التوجيه الأوروبي فمنح هو الآخر للتوقيع الإلكتروني الحجية الكاملة في الإثبات[3]، ويظهر ذلك جلياً في نص المادة 4/1367 من

= كما ميزت ما بين الحجية المقررة للتوقيع الإلكتروني البسيط والحجية المقررة للتوقيع الإلكتروني المتقدم أو المؤمن، فبينما أقرت التشريعات صراحة حجية التوقيعات الإلكترونية المتقدمة وجعلتها مساوية لحجية التوقيع التقليدي، فإنه في المقابل اختلفت فيما بينها على الحجية المقررة للتوقيعات الإلكترونية البسيطة، فمثلاً لم ينكر التوجيه الأوروبي بشأن التوقيعات الإلكترونية حجية التوقيع الإلكتروني البسيط إذا قدم صاحبه الدليل على صحة منظومة إنشائه، بمقابل ذلك لم تقرر بعض التشريعات العربية أي حجية للتوقيع الإلكتروني البسيط، ومثالها التشريع الإماراتي والأردني وحتى التشريع الجزائري، ذلك أن المشرع الجزائري يعترف بحجية التوقيع الإلكتروني المؤمن أو الموصوف وهذا ما نص عليه في المادة 08 من القانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين. لتفاصيل أكثر يراجع، علاء حسين مطلق التميمي، المستند الإلكتروني، عناصره، تطوره، ومدى حجيته في الإثبات المدني، المرجع السابق، ص، ص.238- 239.

[1]- قانون الأونيسترال النموذجي للأمم المتحدة بشأن التوقيعات الإلكترونية لسنة 2001، سابق الإشارة إليه.

[2] - Art 5al 1 du Directive 1999/93/CE du parlement européen et du conseil, du 13 décembre 1999 ,sur un cadre communautaire pour les signatures électroniques.

[3]- Cf. Sophie Sontag- Koenig, la signature électronique en procédure pénale, une évolution amorcée n°3, AJ pénal, mensuel, Dalloz, mars 2014, p.123.

القانون المدني الفرنسي والتي جاء فيها أن: "التوقيع ضروري لإتمام العقد القانوني، ولتحديد هوية من وصفه، كما يكشف عن رضاء الأطراف بالالتزامات الناشئة عن العقد...، حينما يكون التوقيع الإلكتروني، فإنه يتمكن من استخدام طريقة جاهزة لتحديد الهوية بما يضمن ارتباطه مع العقد الذي وضع عليه التوقيع..."[1].

وقد منحت التشريعات العربية للتوقيع الإلكتروني القوة والحجية الكاملة في الإثبات، ومن ذلك التشريع الأردني إذ قد أورد في قانون المعاملات الإلكترونية مادتين ساوى فيهما بين حجية التوقيع الإلكتروني والتوقيع التقليدي، وهما المادة 7 الفقرة أ والتي تنص على أنه: "يعتبر السجل الإلكتروني والعقد الإلكتروني والرسالة الإلكترونية والتوقيع الإلكتروني منتجاً للآثار القانونية ذاتها المترتبة على الوثائق والمستندات الخطية والتوقيع الخطي، بموجب أحكام التشريعات النافذة من حيث إلزاميتها لأطرافها أو صلاحيتها في الإثبات"، أما المادة الثانية فهي المادة (10/أ) والتي جاء فيها أنه: "إذا استوجب تشريع نافذ توقيعاً على المستند أو نص على ترتيب أثر على خلوه من التوقيع، فإن التوقيع الإلكتروني على السجل الإلكتروني يفي بمتطلبات ذلك التشريع"[2].

للإشارة فإن قانون المعاملات الإلكترونية الأردني رقم 15 لسنة 2015، اتجه إلى إقرار مبدأ المعادل الوظيفي بين التوقيع الإلكتروني والتوقيع الخطي، وهو ما نص عليه في المادة 17-1-2[3].

---

[1]- Article 1367 c.civ .fr (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 opposée par un officier public, elle confère l'authenticité à l'acte.
Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable 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 crée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en conseil d'état ».

[2]- المادة 07 والمادة 10 من قانون رقم 85 لسنة 2001 المتعلق بالمعاملات الالكترونية الأردني، سابق الإشارة إليه.

[3]- تنص المادة 17 من قانون رقم 15 لسنة 2015 المتعلق بالمبادلات الالكترونية الأردني، سابق الإشارة إليه.:" أ- يكون للسجل الإلكتروني المرتبط بتوقيع إلكتروني محمي الحجية ذاتها المقررة للسند العادي ويجوز لأطراف المعاملة الإلكترونية الاحتجاج به.
ب- يكون للسجل الإلكتروني المرتبط بتوقيع إلكتروني موثق الحجية ذاتها المقررة للسند العادي ويجوز لأطراف المعاملة الإلكترونية والغير الاحتجاج به.=

ونفس الاتجاه سلكه المشرع البحريني في نص المادة (2/6) من قانون المعاملات الإلكترونية[1]، وكذا المشرع الإماراتي في المادة (1/10) من قانون المبادلات والتجارة الإلكترونية لإمارة دبي[2].

كما استجاب القانون المصري بموجب قانون التوقيع الإلكتروني، لمتطلبات المعاملات الإلكترونية، فأورد نصوصا تضمن مبدأ المساواة بين التوقيع الإلكتروني والتوقيع الخطي التقليدي من حيث الحجية المقررة للتوقيعات التي تتم عبر الوسائط الورقية، شريطة أن يستوفي التوقيع الشروط والضوابط الفنية المطلوبة وفق اللائحة التنفيذية، بحيث نصت المادة 14 من القانون المذكور: "للتوقيع الإلكتروني في نطاق المعاملات المدنية والتجارية والإدارية، ذات الحجية المقررة للتوقيعات في أحكام قانون الإثبات في المواد المدنية والتجارية، إذا روعي في إنشائه وإتمامه الشروط المنصوص عليها في هذا القانون والضوابط الفنية والتقنية التي تحددها اللائحة التنفيذية لهذا القانون"، كما نصت المادة 18 من ذات القانون على أنه: "يتمتع التوقيع الإلكتروني، والكتابة الإلكترونية، والمحررات الإلكتروني بالحجية في الإثبات إذا ما توافرت فيها الشروط الآتية:... وتحدد اللائحة التنفيذية لهذا القانون الضوابط الفنية، والتقنية اللازمة لذلك"[3].

وقد سار المشرع الجزائري على نهج التشريعات المقارنة الأجنبية منها والعربية، فأقر الحجية الكاملة للتوقيع الإلكتروني في الإثبات شأنه في ذلك شأن التوقيع التقليدي، ويظهر ذلك جليا في نص المادة 323 مكرر من القانون رقم 05-10 المتضمن القانون المدني المعدل والمتمم، بشرط أن يُمكِّن من التأكد من هوية الشخص الذي أصدره، وأن

=ج- في غير الحالات المنصوص عليها في الفقرتين (أ) (ب) من هذه المادة يكون للسجل الإلكتروني الذي يحمل توقيعا إلكترونيا الحجية ذاتها المقررة للسند العادي في مواجهة أطراف المعاملة الإلكترونية، وفي حال الإنكار يقع عبء الإثبات على من يحتج بالسجل الإلكتروني."

[1]- تنص المادة 6 فقرة 2 من مرسوم بقانون رقم (28) لسنة 2002 بشأن المعاملات الالكترونية البحريني، سابق الإشارة إليه. على أنه: "إذا أوجب القانون التوقيع على مستند أو رتب أثرا قانونياً على خلوه من التوقيع فإنه إذا استعمل سجل إلكتروني في هذا الشأن، فإن التوقيع الإلكتروني عليه يفي بمتطلبات هذا القانون".

[2]- تنص المادة 10فقرة1 من قانون إمارة دبي رقم 2 لسنة 2002 بشأن المعاملات والتجارة الالكترونية، سابق الإشارة إليه. على أنه: "إذا اشترط القانون وجود توقيع على مستند أو نص على ترتيب نتائج معينة في غياب ذلك، فإن التوقيع الإلكتروني الذي يعول عليه في إطار المعنى الوارد في المادة 20 من هذا القانون يستوفي ذلك الشرط".

[3]- القانون رقم 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات، أما اللائحة التنفيذية فيقصد بها اللائحة التنفيذية الصادرة بالقرار رقم 109 لسنة 2005 الصادرة في 15 ماي 2005.

يكون معد ومحفوظ في ظروف تضمن سلامته، وهذا ما أكده في نص المادة 327 الفقرة 02 من القانون المدني والذي جاء فيها أنه: "يعتد بالتوقيع الإلكتروني، وفق الشروط المذكورة في المادة 323 مكرر أعلاه".

كما أكد مبدأ المماثلة بين التوقيع التقليدي والتوقيع الإلكتروني في نص **المادة** 08 من القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين، حيث نص بأنه: "يعتبر التوقيع الإلكتروني الموصوف وحده مماثلاً للتوقيع المكتوب، سواء كان لشخص طبيعي أو معنوي"[1]، بهذا يلاحظ أن المشرع الجزائري أعطى التوقيع الإلكتروني المؤمن كما سماه في المرسوم التنفيذي رقم 07-162[2]، أو الموصوف كما سماه في قانون التوقيع والتصديق الإلكترونيين رقم 15- 04 القوة في الإثبات، واعتبره وحده له الحجية الكاملة في الإثبات.

هذا وقد نص المشرع الجزائري في المادة 09 من القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين بأنه: "لا يمكن تجريد التوقيع الإلكتروني من فعاليته القانونية، أو رفضه كدليل أمام القضاء بسبب:

1- شكله الإلكتروني أو،

2- أنه لا يعتمد على شهادة تصديق إلكتروني موصوفة أو،

3- أنه لم يتم إنشاؤه بواسطة آلية مؤمنة لإنشاء التوقيع الإلكتروني"[3].

من خلال استقراء النصوص القانونية السابقة، يتضح أن التشريعات المختلفة قد أولت للإثبات الإلكتروني اهتماماً بالغاً، وساوت بين التوقيع الإلكتروني والتوقيع التقليدي، كما أقرت للتوقيع الإلكتروني حجية مساوية لحجية التوقيع التقليدي، لذا لم يعد إحداث التوقيع بواسطة وسيلة إلكترونية عقبة أمام الاعتراف به وقبوله كعنصر في دليل الإثبات، وهذا ما

[1]- قانون 15- 04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، سابق الإشارة إليه.
[2]- المرسوم التنفيذي رقم 07-162 المعدل والمتمم للمرسوم التنفيذي رقم 01-123 والمتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية، وعلى مختلف خدمات المواصلات السلكية واللاسلكية، سابق الإشارة إليه.
[3] - قانون 15- 04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، سابق الإشارة إليه.

أخذ به التشريع الجزائري في نص المادة 9 من القانون 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين السابقة الذكر.

زيادة على ذلك فقد أصبح التوقيع الإلكتروني – بعد مساواته بالتوقيع التقليدي- أداة تصلح لتوثيق التصرفات التي تتم بواسطة الوسائط الإلكترونية، فضلا عن ذلك فإن مساواة التوقيع الإلكتروني بالتوقيع التقليدي قد أنهت سلطة القاضي التقديرية في الأخذ بالتوقيع الإلكتروني أو رفضه.

المطلب الثالث: حجية المستند الالكتروني في الإثبات الجزائي .

يقصد بالإثبات الجزائي إقامة الدليل لدى السلطات المختصة بالإجراءات الجزائية على حقيقة واقعة ذات أهمية قانونية ، وذلك بالطرق التي حددها القانون و وفق القواعد التي أخضعها لها ، ذلك أن الدليل في القانون هو أساس كشف الحقيقة [1].

وللإثبات في العلاقات القانونية أهمية فائقة، فهو يعد الوسيلة العملية التي يعتمد عليها الأفراد في صيانة حقوقهم المترتبة على الوقائع القانونية، والأداة الضرورية التي يعول عليها القاضي في التحقق من تلك الوقائع، وتظهر أهمية الإثبات بصفة واضحة وجلية في ساحة القضاء حين تتصارع المصالح، فإن استطاع صاحب الحق إثباته قضي له به، وإلا ضاعت عليه مزية هذا الحق[2].

ونظرا للتطور المتزايد في استخدام الحاسب الآلي، وظهور المستندات الالكترونية وما صاحبها من ظهور طوائف جديدة من الجرائم لم يكن لها من قبل تسمية (الجرائم المعلوماتية)، أصبح متطلبا من القاضي الجزائي أن يتعامل مع أشكال مستحدثة من الأدلة في مجال الإثبات الجزائي، فظهرت الحاجة إلى تطوير وسائل الإثبات بما يواكب هذه الطفرة التي حدثت في الجرائم الالكترونية، وما يستلزمه ذلك من ضرورة قبول الأدلة الناتجة عن التطور، ومن أهمها المستندات الالكترونية بأنواعها المختلفة، وقد كانت هذه المسألة محل

[1]- سليمان محمد أحمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الانترنت)، رسالة لنيل شهادة الدكتوراه في علوم الشرطة، كلية الدراسات العليا، القاهرة، 2007، ص. 352؛
Sophie Sontag- Koenig, op. cit, p.124.

[2]- تامر محمد سليمان الدمياطي، المرجع السابق، ص. 100.

اهتمام، وبحث العديد من الدول من خلال المؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات، والذي عقد في ريو دي جانيرو بالبرازيل في الفترة الممتدة من 4 إلى 06 سبتمبر 1994[1].

عرف القانون المقارن نظم مختلفة في الإثبات، يسمى النظام الأول، بنظام الإثبات الحر أو المطلق (système de la preuve libre)، ويسود هذا النظام القوانين ذات النزعة اللاتينية[2].

أما النظام الثاني فهو نظام الإثبات المقيد (système de la preuve legal)، وأخيرا يوجد نظام الإثبات المختلط (système de la preuve mixte) و الذي يتخذ موقفا وسطا بين النظامين السابقين ، بحيث يأخذ ما في النظامين من مزايا، و يتجنب ما يشوبهما من عيوب .

لأهمية هذه المسألة سيتم بحث حجية المستند الالكتروني جزائيا، في كل نظام من أنظمة الإثبات المذكورة، بحيث سيتم التطرق إلى حجية المستند الالكتروني في ظل نظام الإثبات الجزائي الحر **(الفرع الأول)**، ثم إلى حجية المستند الالكتروني في ظل نظام الإثبات الجزائي المقيد **(الفرع الثاني)**، كما سيتم التطرق إلى حجية المستند الالكتروني في ظل نظام الإثبات الجزائي المختلط **(الفرع الثالث)**.

الفرع الأول: حجية المستند الالكتروني في نظام الإثبات الجزائي الحر.

إن نظام الإثبات الجزائي الحر يقوم على أساس أن القانون لا يحدد طرقا معنية للإثبات يتقيد بها القاضي الجنائي، بل يترك للخصوم الحرية الكاملة في أن يختاروا ويقدموا ما يرونه مناسبا من الأدلة المؤدية إلى إقناع القاضي ومساعدته للوصول إلى الحقيقة[3]،

[1]- أحمد عاصم عجلية ، الحماية الجنائية المحررات الالكترونية ، دراسة مقارنة ، دار النهضة العربية ، القاهرة ، 2014، ص. 508.

[2]- هلالي عبد اللاه احمد، حجية المخرجات الكمبيوترية في المواد الجنائية (دراسة مقارنة)، المرجع السابق، ص، ص.26-27.

[3]- هلالي عبد اللاه أحمد، حجية المخرجات الكمبوتيرية في المواد الجنائية، دراسة مقارنة، المرجع السابق ، ص. 29 ؛ تامر محمد حسين الدمياطي، المرجع السابق ، ص. 104؛ راشد بن حمد البلوشي، الدليل في الجريمة المعلوماتية، مجلة الحقوق للبحوث القانونية والاقتصادية، مجلة فصلية محكمة تصدرها كلية الحقوق، جامعة الإسكندرية، ع1، 2008، ص.25.

فجوهر هذا النظام يتمثل في أن الاقتناع الشخصي هو وحده الذي يتحكم في قرار القاضي الجزائي، وهذا الاقتناع بدوره من اللزوم أن يصدر بكل حرية من ضمير القاضي الذي يجب أن يكون حرا من ناحية اختيار الدليل من جهة، وأن يكون حرا في تقييم هذا الدليل من جهة أخرى، لما تقدم يتضح أن نظام الإثبات الحر يكرس مبدأ حرية القاضي في الاقتناع، بمعنى أن القاضي حر في تكوين عقيدته من أي دليل يراه يقينيا ويقتنع به[1].

ومن تم فإن هذا النظام يعطي للقاضي دورا ايجابيا في تسيير الدعوى وتكوين الأدلة، والحكم بناءا على ما يصل إليه من حقائق على نحو يكون به حرا في أن يستعين بكل طرق الإثبات للبحث عن الحقيقة والكشف عنها[2]، وهو بذلك يختلف عن القاضي المدني الذي يكون دوره في الدعوى المدنية المنظورة أمامه سلبي يقتصر على الموازنة بين أدلة الخصوم الذين يلعبون دورا ايجابيا، ويقدمون للمحكمة الأدلة التي يرون أنها مفيدة في تدعيم مراكزهم القانونية، وهكذا فان القاضي المدني لا يملك أن يبحث بنفسه فيما يعتقد أنه مفيد لإظهار الحقيقة، بل يجب عليه أن يكتفي بعناصر الإثبات التي قدمها الأطراف، وهذا يرجع في الواقع إلى أن الإثبات في المادة الجزائية ينصب على الوقائع المادية ذات الصلة بالجريمة، ولا ينصرف إلى التصرفات المدنية المرتبطة بالمصالح الشخصية، بالإضافة إلى أن البحث عن الحقيقة يفرض على القاضي الجنائي الاستعانة بجميع السلطات التي تمكنه من الوصول إليها، ومفاد ذلك أنه في الإثبات الحر تكون حجية الاتهام ملزمة بإقامة الدليل على ثبوت الجريمة في حق المتهم [3] .

غير أن هذه الحرية في اختيار أدلة الإثبات ليست مطلقة كليا، فالقانون وإن اعترف للقاضي بسلطة واسعة في تقدير الدليل، فإنه قد قيده من حيث القواعد التي تحدد كيفية

---

[1]- محمد مروان، نظام الاثبات في المواد الجنائية في القانون الوضعي الجزائري، ج1، ديوان المطبوعات الجامعية، الجزائر، 1999 ، ص. 39.

[2]- المقصود بالدور الايجابي للقاضي هو عدم التزامه بما يقدمه أطراف الدعوى من أدلة، وإنما تكون له سلطة فيها، ويجب عليه أن يتخذ بنفسه الإجراءات المناسبة للتحقيق في الدعوى و الكشف عن الحقيقة ، كما أن القاضي غير ملزم بأن يقتنع بما يقدمه له أطراف الدعوى، بل عليه أن يبحث بنفسه عن الأدلة اللازمة التي يكون من خلالها قناعته، فالقاضي الجنائي من واجبه التحري و البحث عن الحقيقة بشتى الوسائل، سواء نص عليها القانون أم لا. مشار إليه من طرف، هلالي عبد اللاه احمد، حجية المخرجات الكمبيوترية في الإثبات الجنائي، المرجع السابق ، ص، ص. 30-31.

[3]- محمد زلايجي، حجية دليل الحاسوب الآلي في النطاق الجنائي، دراسات قانونية ، مجلة سداسية تصدر عن مخبر القانون الخاص الأساسي ، كلية الحقوق، جامعة أبو بكر بلقايد، تلمسان، ع، 07، س 2010، ص. 63.

حصوله عليه والشروط التي يتعين عليه تطلبها فيه، ومخالفة هذه الشروط قد تهدر قيمة هذا الدليل وقد تشوب قضاءه بالبطلان[1].

وبما أن القوانين ذات الصياغة اللاتينية هي التي تبنت هذا النظام، فإن التساؤل المطروح يكمن في مدى إمكانية اعتماد مخرجات الكمبيوتر كالمحررات والمستندات الالكترونية كدليل إثبات أمام القضاء، وهل هذا النوع من المستندات يحقق مبدأ الاقتناع وتكون له حجية أمام القاضي الجزائي ؟

إن الإجابة على هذه التساؤلات لا يتم إلا ببيان موقف بعض التشريعات التي تبنت هذا النظام (التشريعات ذات الصياغة اللاتينية) سواء الغربية منها كالتشريع الفرنسي، أو العربية كالتشريع المصري، وكذا الجزائري.

فالنسبة لموقف المشرع الفرنسي من حجية هذه المستندات من الناحية الجزائية، يتضح أنه قد تبنى مبدأ حرية الأدلة، وحرية القاضي الجنائي في تقديرها، أما الفقه الفرنسي فقد تناول حجية الدليل الالكتروني (المستند الالكتروني) في المواد الجنائية ضمن مسألة أعم وأشمل، وهي مسالة قبول الأدلة الناشئة عن الآلات الحديثة بوجه عام والأدلة العلمية كأجهزة التصوير وأشرطة التسجيل وأجهزة التنصت[2].

وقد قبل القضاء الفرنسي هذه الأدلة (المستندات) في الإثبات إذا توفرت فيها مجموعة من الشروط، ومن أهمها أن يتم الحصول عليها بطريقة شرعية ونزيهة، وأن يتم مناقشتها في حضور الأطراف، وعلى هذا الأساس قضت محكمة النقض الفرنسية بأن أشرطة التسجيل الممغنطة التي يكون لها قيمتها كدليل في الإثبات يمكن أن تكون صالحة للتقديم أمام القضاء الجزائي[3].

وتطبيقا لذلك قضي في فرنسا بخصوص حجية المستندات الصادرة عن الآلات الحديثة في الإثبات أمام القضاء الجنائي، بأن التسجيلات الممغنطة لها قيمة الأدلة التي يمكن

---

[1]- هلالي عبد اللاه احمد، حجية المخرجات الكمبيوترية في المواد الجنائية، المرجع السابق، ص. 30.

[2]- محمد زلايجي، المرجع السابق، ص. 63؛ راشد بن حمد البلوشي، المرجع السابق، ص.43.

[3] -Cass crim 1987 BULL crim n° 173.
مشار إليه من طرف، هلالي عبد اللاه احمد، حجية المخرجات الكمبيوترية في المواد الجنائية، المرجع السابق، ص. 43؛ راشد بن حمد البلوشي، المرجع السابق، ص.43.

الاطمئنان إليها كأدلة إثبات أمام القضاء الجنائي، فإذا اطمأنت محكمة الموضوع وفقا لاقتناعها الذاتي و القواعد العامة إلى ما أسندت إليه النيابة من قرائن بشان خطأ سائق سيارة منسوب إليه تجاوز السرعة، وهو الأمر الذي يثبت لها من خلال جهاز آلي التقط صورة السيارة متجاوزة السرعة، فإنها لا تكون ملزمة بتحديد ما استندت إليه من عناصر الواقعة في تبرير اقتناعها[1].

على هذا فإن يمكن الاعتداد بالمستندات الالكترونية كدليل إثبات، و تكون له الحجية في الإثبات أمام القاضي الجزائي الفرنسي، وذلك متى اقتنع القاضي الفرنسي بها و بحجيتها، هذا ولقد انتهج المشرع البلجيكي[2] نفس نهج المشرع الفرنسي، وأعطى هو الآخر لهذه المستندات والأدلة الالكترونية الحجية في الإثبات أمام القضاء الجزائي.

أما عن موقف التشريعات العربية من حجية الأدلة الالكترونية بما فيها المستندات من الناحية الجزائية، فنلاحظ أن المشرع المصري قد خلا تشريعه الإجرائي من التعرض لحجية المخرجات الكمبيوترية بما فيها المستندات الالكترونية في الإثبات الجزائي، غير أنه ورغم من عدم إيراده لنصوص صريحة إلا أنه يمكن الاستناد إلى الدليل الالكتروني، وكذا المخرجات الكمبيوترية في إثبات أو نفي الجريمة، وتكون لها قوة القرائن في الإثبات، ذلك أن المشرع المصري أخذ بمبدأ الإثبات الحر، ويظهر ذلك جليا من خلال نصه في المادة 303 من قانون الإجراءات الجزائية المصري على أنه: "يحكم القاضي في الدعوى حسب العقيدة التي تكونت لديه بكامل حريته "، كما نص في المادة 291 من نفس القانون بأنه : "للمحكمة أن تأمر ولو من تلقاء نفسها إثناء نظر الدعوى بتقديم أي دليل تراه مناسبا لظهور

---

[1] - Crim 3 jan 1978 (2 arréts) BULL crim n° 1.

مشار إليه من طرف، أحمد عاصم عجيلة، المرجع السابق، ص.519.

[2]- للإشارة فإن التشريع البلجيكي هو الآخر يتبنى نظام الإثبات الحر في ميدان الأدلة الناتجة عن الحاسوب و هذا طبقا للمادة 461 عقوبات و يعد الحكم الصادر عن محكمة (anvers) بتاريخ 13 دجنبر 1984 أول حكم صدر في هذا الخصوص ، حيث اعتبر أن قيام المتهم بنسخ ثلاثة برامج تعود ملكيتها للشركة يعد فعلا مجرما تنطبق عليه العقوبة المقررة في المادة المذكورة بدعوى أنه كان يهدف إلى تحقيق منفعة شخصية، كما اعتبر كلمة شيء التي وردت في معرض المادة 461 ذات مفهوم واسع يجعلها تتوافق مع مدلول اختلاس الأشياء المملوكة للغير، وهو ما تحقق حسب الحكم في قضية الاستنساخ ما دامت أن البرامج تدخل ضمن عناصر الذمة المالية للشركة ، بالرغم من أن المتهم نفى ذلك مدعيا بأن النسخ التي استخرجها مجرد معلومات ذات طابع مهني لا تكون محلا للاختلاس، و بالتالي لا تخضع لأحكام المادة 461 من قانون العقوبات البلجيكي . مشار إليه من طرف، محمد زلايجي، المرجع السابق، ص. 64.

الحقيقة "، وعلى ذلك فإنه يكون للمحكمة أن تستند إلى المخرجات الكمبيوترية لإثبات وقوع الجريمة أو نفيها [1].

أما عن موقف المشرع الجزائري من حجية هذه المستندات في الإثبات الجزائي، فانه يمكن القول بأن التشريع الجزائري قد انتهج نفس نهج التشريع الفرنسي والمصري وأخذ بمبدأ حرية الإثبات الجنائي، ويظهر ذلك جليا من نص المادة 202 من قانون الإجراءات الجزائية، والتي جاء فيها بأنه: "يجوز إثبات الجرائم بأي طريق من طرق الإثبات، ماعدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص، ولا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات، والتي حصلت المناقشة فيها حضوريا أمامه " [2] .

حسب هذه المادة، يستخلص أن المشرع الجزائري قد تبنى مبدأ تكافؤ قيمة الأدلة كقاعدة عامة، كما أنه لم يفرق بين قوة الدليل سواء كان كتابيا أو شفويا، مباشرا أو غير مباشر، فالعبرة فقط بمدى تأثيره وإقناعه للقاضي، ومن تم فإن الغاية النهائية من جمع الأدلة وتقديمها ليس الوصول إلى الدليل القاطع بحد ذاته، وإنما الوصول إلى إقناع القاضي[3]، هذا وقد نص المشرع على مبدأ الاقتناع الشخصي، بموجب نص المادة 307 من قانون الإجراءات الجزائية.[4].

أما عن حجية المستندات الالكترونية في الإثبات الجزائي، ومدى توفيرها لقناعة القاضي الجزائي، فيلاحظ أن المشرع الجزائري لم يتطرق إلى هذه المسألة بنصوص

---

[1]- سليمان أحمد محمد فضل، المرجع السابق، ص. 366.

[2]- الأمر رقم 66-155 المؤرخ في18 صفر عام 1386 الموافق 8 يونيو 1966، المتضمن قانون الإجراءات الجزائية الجزائري المعدل والمتمم، ج.ر، ع.48، س.1966، المعدل والمتمم.

[3]- بوعناد فاطمة زهرة، مشروعية الدليل الالكتروني في مجال الاثبات الجنائي، أطروحة دكتوراه في العلوم، تخصص علوم قانونية، فرع علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة جيلالي اليابس، سيدي بلعباس، 2013-2014، ص. 258.

[4]- تنص المادة 307 من ق.إ.ج.ج، المعدل والمتمم، سابق الإشارة إليه : " يتلو الرئيس قبل مغادرة المحكمة في قاعة الجلسة التعليمات الآتية التي تعلق فضلا من ذلك بحروف كبيرة في اظهر مكان من غرفة المداولة:
إن القانون لا يطلب من القضاة أن يقدموا حسابا عن الوسائل التي بها قد وصلو الى تكوين اقتناعهم، و لا يرسم لهم قواعد بها يتعين عليهم أن يخضعوا لها على الأخص تقدير تمام او كفاية دليل ما ، و لكنه يأمرهم أن يسألوا أنفسهم في صمت وتدبر وأن يبحثوا بإخلاص ضمائرهم في أي تأثير قد أحدثته في إدراكهم الأدلة المسندة إلى المتهم و أوجه الدفاع عنها، و لم يضع لهم القانون سوى هذا السؤال الذي يتضمن كل نطاق واجباتهم ، هل لديكم اقتناع شخصي ؟ ".

صريحة، لكن تبنيه لمبدأ الإثبات الحر في المادة الجنائية يدفع إلى القول بإقراره الضمني بعدم قدرة الأدلة التقليدية في مواجهة الجرائم المستحدثة، ومنها الجريمة الالكترونية، ومن تم فتح المجال أمام الأدلة الحديثة للاستفادة من الوسائل العلمية الحديثة للكشف عن الأدلة ومنها الأدلة الالكترونية، وعليه فإن المستندات الالكترونية مادام أنه تم الحصول عليها بصورة قانونية، و طالما أنها دقيقة و لم يطرأ عليها أي تغيير خلال فترة حفظها، فإنه يمكن الاستعانة بها كدليل إثبات له القوة والحجية في إثبات الجريمة، أو نفيها أمام القضاء الجزائي.

الفرع الثاني : حجية المستند الالكتروني في ظل نظام الإثبات الجزائي المقيد.

إن نظام الإثبات المقيد بصفة عامة هو ذلك النظام الذي يطلق عليه نظام الأدلة القانونية أو نظام الإثبات المحدد، وفي ظل هذا النظام تكون الأدلة محصورة ومحددة سلفا من قبل المشرع[1]، كما أن قوتها التدليلية محددة، ولا يجوز للقاضي أن يخرج عليها أو يبني حكمه على خلافها[2] .

ومن تم فإن هذا النظام يملي على القاضي أن يتقيد في حكمه بالإدانة أو بالبراءة بأنواع معنية من الأدلة، أو بعدد منها طبقا لما يرسمه التشريع المطبق، ودون أن يأبه في ذلك بمدى اقتناع القاضي بصحة ثبوت الواقعة أو عدم ثبوتها، وعليه إذا توافرت أدلة الادانة بالشروط التي يحددها القانون إلتزم القاضي بإدانة المتهم، ولو كان غير مقتنع بإدانته، وإذا لم تتوافر الأدلة فلا يجوز له أن يحكم بالإدانة، بل يحكم باستبعاد الدليل حتى ولو اقتنع بأن المتهم مدان[3].

بهذا يتضح أن دور القاضي في ظل هذا النظام دور آلي لا يتعدى مراعاة توفر الأدلة وشروطها القانونية، وهو على ذلك لا يستطيع التحري عن الحقيقية بطرق أخرى لم ينص

[1]- راشد بن حمد البلوشي، المرجع السابق، ص.26؛
F. jacques et autres, Droit civil , les obligations, 8ème éd, sirey, Paris, 2013, p.11.

[2]- بن فردية محمد، الدليل الجنائي الرقمي وحجيته أمام القضاء الجزائي، المجلة الأكاديمية للبحث القانوني، مجلة تصدر عن كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة، بجاية، الجزائر، ع 2014، ص. 287.

[3]- سليمان أحمد محمد فضل، المرجع السابق، ص،ص. 366-367 ؛ هلالي عبد اللاه احمد، حجية المخرجات الكمبيوترية في المواد الجنائية، المرجع السابق، ص. 49.

عليها المشرع ولا أن يطلب إكمال أدلة ناقصة، بل عليه أن يلتزم بما حدده المشرع[1]، فهذا النظام يخرج القاضي عن وظيفته الطبيعية، ويسمح للمشرع أن يتدخل في نطاق لا يملكه، بحيث يقنن اليقين في قواعد عامة محددة، رغم أن اليقين مسألة واقع ترتبط بظروف كل قضية وتترك لتقدير قاضي الموضوع .

كما أن وضع القاضي في قالب جامد قد يترتب عليه إفلات حالات كثيرة من العقاب، رغم أن من واجبه أن يقيم موازنة معتدلة بين حق الإنسان في الخصوصية، وحق المجتمع في العقاب[2].

أن التساؤل عن عن حجية المستند الالكتروني، والدليل الالكتروني بصفة عامة في ظل هذا النظام، يستلزم تحديد موقف القوانين التي تبنت هذا النظام كالقانون الانجليزي والأمريكي، وكذا الكندي.

فبالنسبة لموقف التشريع الانجليزي يلاحظ أنه قبِل المستندات الالكترونية في الإثبات منذ سنة 1984، وذلك في حالات محددة بنصوص صريحة غير أنه قيد مسألة قبولها و قوتها الثبوتية بشروط معينة، حيث حدد المشرع الانجليزي في المادة 69 من قانون الشرطة والإثبات الجنائي لسنة 1984 الشروط الواجب توافرها في المستند الناتج عن الحاسوب حتى يقبل كدليل في الإثبات، و تتمثل هذه الشروط في :

1- عدم وجود أسباب معقولة للاعتقاد بأن البيان يفتقر إلى الدقة بسبب الاستخدام غير المناسب، أو الخاطئ للحاسب.

2- أن الحاسب كان يعمل في جميع الأحوال بصورة سليمة، وإن لم يكن كذلك فإنه لم يثبت أن هناك جزء منه لم يكن يعمل فيه بصورة سليمة، أو كان عدم انتظامه ناتجا عن عيب لم يكن مؤثرا في استخراج المستند أو دقة محتوياته.

[1]- راشد بن حمد البلوشي، المرجع السابق، ص.43.
[2]- بوعناد فاطمة زهرة، المرجع السابق، ص، ص.261-262؛ هلالي عبد اللاه احمد، حجية المخرجات الكمبيوترية في المواد الجنائية، المرجع السابق، ص. 51.

3- الوفاء بأية شروط متعلقة بالمستند محددة طبقا لقواعد المحاكمة المتعلقة بالطريقة أو بالكيفية التي يجب أن تقدم بها المعلومات الخاصة بالبيان المستخرج عن طريق الحاسب[1].

ولم يكتف قانون الشرطة والإثبات الجنائي لسنة 1984 بتحديد الشروط الواجب توافرها في مخرجات الحاسب كي تكون أدلة مقبولة أمام القضاء، بل تضمن كذلك توجيهات لكيفيه تقدير قيمة أو وزن البيان المستخرج عن طريق الحساب، فأوصت المادة 11 من الجزء الثاني من الملحق الثالث من القانون المذكور بمراعاة كل الظروف عند تقييم البيانات الصادرة عن الحاسب المقبولة في الإثبات طبقا للمادة 69 من القانون، وبوجه خاص مراعاة ما إذا كانت المعلومات المتعلقة بأمر قد تم بتزويد الحاسب بها في وقت معاصر لهذا الأمر أم لا، وكذلك مسألة ما إذا كان للشخص المتصل الذي قام بإخراج البيان من الحاسب دافع لإخفاء الوقائع أو تشويهها[2].

هذا وقد تم اقتراح أنه في حالة ما إذا كان الحاسب موضوعا للاستخدام غير المصرح به، فإن أي أدلة مستندية ناتجة عن الحاسب بخصوص أصل و مدة هذا الاستعمال، لن تكون مقبولة ، لأن سوء استخدام الحاسب في حد ذاته أدى إلى عدم عمل الجهاز كما ينبغي[3].

هذا عن القانون الإنجليزي، أما بخصوص موقف القانون الأمريكي فيُلاحظ أنه قد حسم حجية المستند الالكتروني والدليل الالكتروني بصفة عامة في القوانين الخاصة بالولايات المتحدة الأمريكية، حيث نص قانون الحاسب الآلي لسنة 1984 في ولاية آيوا (IOWA) أن مخرجات الحاسب الآلي تكون مقبولة بوصفها أدلة إثبات بالنسبة لبرامج وبيانات الحاسب الآلي والمخزنة بداخله، كما نص قانون الإثبات الصادر سنة 1983 في

[1]- شيماء عبد الغني محمد عطا الله، الحماية الجنائية للمعاملات الالكترونية، دار الجامعة الجديدة، الإسكندرية، 2007، ص،ص. 389-390 .

[2]- هشام رستم، الجوانب الإجرائية للجرائم المعلوماتية، ط1، مكتبة الآلات الحديثة، مصر، سنة 1994، ص .178؛ بوعناد فاطمة زهرة، المرجع السابق، ص. 267.

[3]- بوعناد فاطمة زهرة، المرجع السابق، ص. 267.

ولاية كاليفورنيا من أن النسخ المستخرجة من المعلومات التي يحتويها الحاسب الآلي تكون مقبولة بوصفها أفضل الأدلة المتاحة لإثبات هذه المعلومات[1].

ولم يظل الأمر حبيس النصوص القانونية، بحيث عمد القضاء الأمريكي في أحكامه المختلفة إلى التأكيد على قبول المخرجات الكمبيوترية كأدلة إثبات، طالما كان الحاسب المتولدة عنه يؤدي وظائفه بصورة سليمة، وكان القائم عليه تتوافر فيه الثقة والطمأنينة[2].

نتيجة لما سبق ذكره، عبر الفقيه الأمريكي إدوار وايز (edward wise) بالنسبة لمدى قبول الأدلة الناتجة عن الحاسب، بما فيها المستندات الالكترونية بقوله:" أن الصعوبات الحقيقية في الولايات المتحدة الأمريكية نابعة من عدم الألفة مع تكنولوجيا الحاسب الآلي أكثر من كونها صعوبات قانونية، ولذا فمن غير المعتقد –حسب رأيه– على وجه العموم أن تكون هناك حاجة ماسة إلى سن تشريعات بخصوص التعامل مع مدى قبول السجلات المعالجة بواسطة الحاسب"[3].

وقد حسم المشرع الكندي هو الآخر حجية المستند الالكتروني، والدليل الالكتروني حيث نص صراحة على قبول السجلات والمستندات الناجمة عن الحاسب الآلي إذا توافرت فيه شروط معينة، وذلك بموجب المادة 29 من قانون الإثبات الكندي، والخاصة بسجلات المؤسسات المالية، حيث حددت المادة المذكورة عددا من الشروط التي يجب توافرها قبل عمل صورة من السجل الذي يضاف إلى الأدلة، ومن هذه الشروط أن تكون الصورة حقيقية من المدخل الأصلي[4].

وتطبيقا لذلك نصت محكمة استئناف اونتاريو الكندية في قضية مكميلان (McMullen)، بأنه يشترط لكي تكون سجلات الحاسب مقبولة بوصفها نسخا حقيقية من السجلات الالكترونية، أن تكون مستكملة بوصف كامل لنظام حفظ السجلات السائد في

[1]- هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، المرجع السابق، ص. 54.
[2]- شيماء عبد الغني محمد عطا الله، المرجع السابق، ص. 408 ؛ هلالي عبد اللاه احمد، حجية المخرجات الكمبيوترية في المواد الجنائية، المرجع السابق، ص. 55.
[3]- هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، المرجع السابق، ص. 55.
[4]- هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، المرجع السابق، ص.ص. 55-56 ؛ شيماء عبد الغني محمد عطا الله، المرجع السابق، ص،ص. 405-406.

المؤسسات المالية، كما ينبغي أن تتضمن وصفا للإجراءات والعمليات المتعلقة بإدخال البيانات وتخزينها واسترجاعها، حتى يتبين أن المخرج الكمبيوتري موثوق به بشكل كافي.

وقد تعرضت المحكمة ذاتها في قضية بيل وبروس (Bel et Bruce) لذلك، وتتلخص وقائع القضية السالفة في استخدام البنك للمخرجات المطبوعة على أنها الأصل، بسبب بقاء مخرجات الطابعة دون المعلومات الواردة بقاعدة البيانات التي تعرضت للمحو، وعليه استخدامها من البنك في مثل هذه الظروف يجعلها تنزل منزلة الأصل، فتصبح هي السجل الأصلي حسبما ورد في المادة 29 من قانون الإثبات الكندي.

كما أضافت أن السجل قد يتخذ عدة أشكال سواء أكانت مقروءة وواضحة أم لا، ناهيك عن الشكل الذي سُجلت عليه المعلومات قد يتغير من وقت لآخر، إذ قد يتم تجميعها أو دمجها، لكن في كل الحالات يصبح الشكل الجديد سجلا بنفس مقومات السجل السابق[1].

وعليه فان المشرع الكندي قد انتهج نفس اتجاه التشريع الانجليزي والأمريكي بخصوص قبول المستندات الالكترونية كأدلة لها القوة والحجية أمام القضاء الجزائي، بالرغم أنهم اعتنقوا في تشريعاتهم نظام الإثبات المقيد.

بعد أن تم التطرق إلى حجية المستند الالكتروني في الإثبات الجزائي في ظل القوانين ذات النزعة اللاتينية، وكذا القوانين ذات النزعة الأنجلوساكسونية، فإن دراسة هذه الحجية لا تكتمل، إلا باستعراض موقف القوانين ذات الصياغة المختلطة من حجية وقوة هذه الأدلة الالكترونية في الإثبات.

الفرع الثالث: حجية المستندات الالكترونية في نظام الإثبات الجزائي المختلط.

يقصد بالقوانين ذات الصياغة المختلطة القوانين التي تجمع بين النظامين اللاتيني والأنجلوسكسوني، فهي قوانين تتبع نظاما وسطا بين الإثبات الحر والإثبات المقيد.

[1]- هلالي عبد اللاه احمد، حجية المخرجات الكمبيوترية في المواد الجنائية، المرجع السابق، ص. 56.

وفقا لهذا النظام يتولى المشرع تحديد الأدلة المقبولة في الإثبات الجنائي، بحيث يُحدد أدلة إثبات بعض الوقائع دون البعض الأخر، كما يُحدد الشروط التي يجب توافرها في الدليل، ليمنح بعدها للقاضي الحرية في تقدير الأدلة القانونية وقيمتها التبوثية[1].

بهذا يبدو أن نظام الإثبات المختلط نظام يسعى للتوفيق بين النظامين، وفيه يتم تلافي ما وُجه لنظام الإثبات الحر من خشية تعسف القاضي وانحرافه عن الصواب، وكذا ما وُجه لنظام الإثبات المقيد الذي يجعل من دور القاضي سلبيا في عملية الإثبات، بحيث لا تكون له حرية تقدير ما يعرض عليه من عناصر الإثبات[2].

ورغم سعي نظام الإثبات المختلط إلى الإستفادة من مزايا النظامين السابقين، والتخفيف من سلبياتهما، إلا أنه في الواقع مُنتقد كون أنه لا يراعي التوازن بين مصلحة المتهم في البراءة ومصلحة المجتمع في العقاب، حيث يهدف إلى تحقيق مصلحة المتهم فقط، وهو ما يبرز من امتناع القاضي عن الحكم بإدانة المتهم في غياب وجود دليل قانوني، ولو كان هناك دليل آخر يُساهم في تكوين اقتناعه الشخصي[3].

ولئن كان هذا هو تقدير النظام من حيث دور القاضي في الحكم بالإدانة والبراءة، فإن معرفة القوة الثبوتية للمستندات الإلكترونية من الناحية الجزائية، لا يتقرر إلا باستعراض موقف القوانين التي تبنت نظام الإثبات المختلط، والتي من بينها القانون الياباني وقانون الشيلي .

فالنسبة للقانون الياباني يُلاحظ أنه قد عمل على تحديد وسائل الإثبات من جهة، كما وأخذ من جهة أخرى بقاعدة الاقتناع الذاتي للقاضي، وبناء على ذلك فقد حصر المشرع الياباني طرق الإثبات المقبولة في: 1- أقوال المتهم، 2- أقوال الشهود، 3- القوانين، 4- الخبرة، أما بالنسبة للمستندات الالكترونية وغيرها من الأدلة المستخرجة من الحاسب والانترنت، فقد قرر المشرع الياباني بأن السجلات الإلكترومغناطيسية، تكون غير مرئية في

[1]- سليمان أحمد محمد فضل، المرجع السابق، ص. 369.
[2]- هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، المرجع السابق، ص. 57.
[3]- بوعناد فاطمة زهرة، المرجع السابق، ص. 268.

حد ذاتها، ولذلك لا يمكن أن تستخدم كدليل في المحكمة إلا إذا تم تحويلها إلى صورة مرئية ومقروءة عن طريق مخرجات الطباعة لمثل هذه السجلات، وفي مثل هذه الحالة يتم قبول هذه الأدلة الناتجة عن الحاسب سواء كانت هي الأصل أم كانت نسخة من الأصل[1]، وبموجب هذه المادة يكون المشرع الياباني قد اعترف بإمكانية الأخذ بالسجلات المستخرجة من الحاسب الآلي، والاعتماد عليها كدليل أمام القضاء.

هذا عن موقف القانون الياباني، أما بخصوص موقف قانون الشيلي فيُلاحظ أنه عمد بموجب نص المادة 475 من قانون الإجراءات الجنائية إلى حصر طرق الإثبات في ستة، وتشمل كل من: شهادة الشهود، تقرير الخبراء، المعاينة، المستندات الرسمية والعرفية، الاعتراف، والقرائن. كما ونص في المادة 456 مكرر من نفس القانون على عدم جواز إدانة أي شخص بجريمة، ما لم تصل المحكمة المختصة من خلال الوسائل القانونية للإثبات إلى الاقتناع بأن الفعل المستوجب للعقاب قد ارتكب، وأن الشخص المدان ساهم في ارتكاب هذا الفعل، وأن مساهمته تلك معاقب عليها قانونا[2] .

ما يمكن استخلاصه من هذا كله، تمسك القانون الإجرائي الشيلي بنظام التحديد الحصري لوسائل الإثبات في المواد الجنائية على نحو تكون فيه الوسائل المحددة والمنظمة قانونا وسائل مشروعة يجوز استخلاص الحقيقة عن طريقها، وفي ظل هذا التحديد يمكن أن يكون الدليل الناشئ عن الحاسب بما فيه المستند الالكتروني مقبولا في الإثبات الجنائي استنادا إلى تقرير الخبير المقدم بشأن البيانات المعنية المعالجة آليا، فللقاضي وفقا للمادة 221 من قانون الإجراءات أن يطلب تقريرا من الخبير عند حدوث أي من الحالات التي يحددها القانون في مجالات العلم أو الفن أو التجارة، وكذا عند وجود حالة لازمة أو ضرورية لتقييم واقعة أو ظرف مؤثر في الدعوى، وكذا في حالة البيانات والعناصر الأخرى التي يقدمها أو يوفرها جهاز الحاسب، ويكون الرأي للخبير الفني المتخصص مهما لمساعدة القاضي على كشف الحقيقة[3].

[1]- سليمان أحمد محمد فضل، المرجع السابق، ص، ص. 369-370.
[2]- هشام فريد رستم، المرجع السابق ، ص. 162.
[3]- هشام فريد رستم، المرجع السابق، ص. 163 ؛ بوعناد فاطمة زهرة، المرجع السابق، ص. 269.

للإشارة، لم يظل قانون الشيلي محصورا في هذه المواد، بل أصدر بعدها بعض القوانين الخاصة، بحيث وسع بموجبها من نطاق وسائل الإثبات المقبولة أمام المحاكم الجنائية على نحو يجعلها أعم وأشمل من تحديدها الحصري الوارد بقانون الإجراءات، ومن بين هذه القوانين القانون الخاص بالإتجار غير المشروع في المواد المخدرة، والذي نص فيه على أنه يجوز للمحاكم أن تقبل كوسائل للإثبات، الأفلام السينمائية، والصور الفوتوغرافية، والنظم الخاصة بتسجيل الصوت والصورة، وبصفة عامة أية وسيلة يمكن أن تكون ملائمة ووثيقة الصلة وتفضي إلى إضفاء الشرعية على وسيلة الإثبات[1] .

وعلى ضوء ذلك فإن الدليل المتولد عن جهاز الحاسب الآلي، بما فيه المستندات الالكترونية يمكن أن يكون مقبولا، أمام المحاكم الجزائية بإعتباره دليلا مستنديا، ومثله أيضا النظم الحديثة الأخرى لجمع وتسجيل المعلومات، تسجيل وإنتاج الحقائق كالتصوير الفوتوغرافي، التصوير بالأقمار الصناعية، الصور الضوئية وصور الأشعة، وجميع تسجيلات الصوت والصورة، فهذه الوسائل العلمية جميعها يمكن اعتبارها مستندات بالمعنى الواسع لهذا المصطلح، خاصة وأن التقدم الفني والتكنولوجي قد تجاوز المفهوم التقليدي للمستند كورقة مكتوبة، وأصبح يسمح بالحصول على وسائل أخرى من التسجيلات التي تمثل فكرة أو حقيقة أكثر سلامة ودقة وبأسلوب موثوق به[2].

[1]- هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، المرجع السابق، ص. 64.
[2]- هشام فريد رستم، المرجع السابق، ص،ص. 163 -164 ؛ هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، المرجع السابق، ص. 65.

الباب الثاني

الأحكام التنظيمية والإجرائية
للمستند الالكتروني من الناحية الجزائية

الباب الثاني: الأحكام التنظيمية والإجرائية للمستند الالكتروني من الناحية الجزائية

يثير التنظيم الموضوعي والإجرائي للجرائم الماسة بالنظم المعلوماتية بصفة عامة والجرائم الواقعة على المستندات الالكترونية بصفة خاصة جملة من الإشكالات القانونية، ذلك أن الأفعال الإجرامية التي قد تطال هذه المستندات تتصف بسمات وخصائص تميزها عن غيرها من الجرائم التقليدية، وتنبع هذه الصفات الخاصة من أطراف هذه الجريمة، فالجاني فيها أو ما يطلق عليه بالمجرم المعلوماتي -والذي قد يكون فرد أو منظمة أو حتى دولة- يتميز بالذكاء في غالب الأحيان، وبقدرته على التكيف الاجتماعي مع المجتمع الذي يعيش فيه.

ناهيك عن أن دوافع ارتكاب الجريمة كثيرة ومتنوعة، إذ قد أظهرت الدراسات والأبحاث الخاصة بظاهرة الإجرام المعلوماتي، أن المجني عليه يغلب عليه الطابع المالي، بحيث يفوق العائد من إرتكاب جريمة معلوماتية نظيره بأضعاف في حالة إرتكاب جريمة تقليدية، ولا ريب في أن هذه الأسباب هي التي أدت إلى إرتفاع معدل إرتكاب الجريمة المعلوماتية من جهة، وإلى إرتفاع حجم الخسائر الناشئة عنها من جهة أخرى[1]، ولمجابهة هذا الوضع سعت التشريعات إلى إستحداث نصوص عقابية رادعة للحد من هذا النوع من الجرائم.

ولم يكن الأمر كافيا، فمحاربة الجرائم المعلوماتية لا يقتصر على إيجاد نصوص قانونية تجرم الأفعال الماسة بالمستندات الإلكترونية، بل يتطلب أحكام إجرائية تسمح بفك لغز الجريمة المعلوماتية التي تمس كيانات منطقية ومستندات الكترونية ليس لها وجود مادي ملموس إلا إذا تم طباعتها على الورق، وهو الأمر الذي يضع الكثير من العقبات أمام القائمين بالتحقيق وغالبا ما تبرز هذه العقبات في مجال جمع الأدلة المعلوماتية وتحديد مرتكب الفعل، ذلك أن الأدلة الإلكترونية أدلة قابلة للمحو والإتلاف في وقت قصير، كما

[1]- عادل عبد الله خميس المعمري، التفتيش في الجرائم المعلوماتية، الفكر الشرطي، دورية ربع سنوية، عملية محكمة ومفهرسة تعنى بالأبحاث الشرطية، تصدر عن مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، الإمارات العربية المتحدة، مج الثاني والعشرون، ع3، العدد رقم (86) – يوليو 2013، ص.252؛

Céline Castets-Renard,op. cit ,p.427.

أنها متداخلة، ناهيك على أن الحصول عليها يتطلب تكوينا فنيا وتدريبا ميدانيا لرجال متخصصين على المستوى الوطني وتعاونا على المستوى الدولي[1].

أمام سعي التشريعات إلى إستحداث نصوص قانونية للكشف عن الجريمة المعلوماتية ومعاقبة المجرم المعلوماتي، يبقى السؤال مطروحا في ما مدى وفقت التشريعات في مواجهة الجرائم الماسة بالمستندات الإلكترونية؟ هذا ما سيتم بيانه في هذا الباب ببيان الأحكام التنظيمية للمستند الالكتروني من الناحية الجزائية **(الفصل الأول)**، والأحكام الإجرائية للمستند الالكتروني من الناحية الجزائية بين التنظيمين الدولي والداخلي **(الفصل الثاني)** .

[1]- Cf. Philippe Baumard, la cybercriminalité comportementale:historique et régulation, revue française de criminologie et de droit pénal, n°02, octobre 2014,p. p.41-42.

الفصل الأول: الأحكام التنظيمية للمستند الالكتروني من الناحية الجزائية

تعد المستندات الإلكترونية وما تتضمنه من بيانات ومعلومات سواء كانت هذه المستندات مخزنة داخل الأنظمة المعلوماتية أو خارجها على وسيط خارجي كالأسطوانات والشرائط الممغنطة، مستهدف رئيسي من جانب الجريمة المعلوماتية، فجرائم الاعتداء عليها في تزايد يوما بعد يوم حيث لا يتوانى محترفو النظم المعلوماتية في إبتكار وسائل متطورة من أجل الإعتداء على هذه المعلومات، فضلا عن ذلك فإن هذه الاعتداءات قد تطال البيانات الإلكترونية المكتوبة آليا، كما قد تطال التوقيعات الإلكترونية الواردة على هذه المستندات، وهو الأمر الذي قد يسبب خسائر للمتعاملين، كما قد يهدد الثقة والخصوصية في المعاملات الإلكترونية[1]، ولا شك أن الجرائم الواقعة على المستندات الإلكترونية شأنها شأن كافة أنواع الجرائم تتطلب لتحققها توافر النموذج القانوني للجريمة حتى يمكن مساءلة مرتكبيها، بالإضافة إلى ما تتفرد به هذه الأفعال الإجرامية من ذاتية خاصة باعتبارها من الجرائم الآلية التي تتم في بيئة إفتراضية مقوماتها بيانات ومعلومات وأرقام.

لكل هذا سيتم التعرض للأحكام التنظيمية الجزائية لمواجهة المساس بمحتوى المستند الإلكتروني **(المبحث الأول)**، والأحكام التنظيمية المقررة لمواجهة المساس بخصوصية المستند الإلكتروني **(المبحث الثاني)**.

المبحث الأول: الأحكام التنظيمية لمواجهة المساس بمحتوى المستند الإلكتروني.

أدى التطور المذهل للمعلوماتية في شتى المجالات إلى التعامل بالمستندات الإلكترونية، بحيث شكلت هذه الأخيرة قفزة نوعية في عالم المال والأعمال، كما وكان لها الأثر البالغ في مجال الحكومة الإلكترونية، ونظرا لأهمية المعلومات التي تحويها تلك المستندات توجهت الأنظار إليها، فسعى هواة الإجرام إلى تعلم أبجديات الحاسب الآلي لتنفيذ مخططاتهم الإجرامية والمساس بمحتوى المستندات الإلكترونية، والتلاعب بالمعلومات

[1] - Cf. Emmanuel Dreyer, sur internet, tout ce qui n’est pas permis est interdit, hebdomadaire, n °44, recueil dalloz, décembre 2012, p.3006.

الواردة بها عن طريق السرقة، التزوير والإتلاف، ولا يخفى على أحد حجم الضرر الذي قد يلحق أصحاب تلك المستندات نتيجة الإعتداء[1].

أمام هذه المسألة أضحى القانون الجزائي يواجه أزمة حقيقية، وبات من الضروري على التشريعات اللحاق بالرغب ومواجهة واقع العالم الرقمي بكل خصائصه ومميزاته بدون المساس بمبادئ القانون الجنائي وعلى رأسها مبدأ شرعية الجرائم والعقوبات، وما يتفرع عنه من ضرورة التفسير الضيق لقواعد القانون الجزائي وحظر القياس في التجريم والعقاب[2].

وبما أن المستندات الإلكترونية تعتبر وليدة البيئة الرقمية، زيادة عن كونها أصبحت أداة تتم بموجبها المعاملات الإلكترونية المختلفة، فقد تطالها بعض الأفعال التي قد تنال من صحة محتوياتها وقوة البيانات التي تتضمنها، وهو الأمر الذي قد يلحق أضرار ويكبد خسائر بالمتعاملين بها، كما قد يهدد الثقة في التعامل بهذا النوع المستحدث من المستندات، وهو الأمر الذي جعل الكثير من التشريعات تسعى جاهدة للحاق بالركب باستحداث نصوص قانونية عقابية وجزائية محاولة منها للحد من هذا النوع الجديد من الإجرام الذي بات يهدد المال والتجارة والإدارة وكذا الاقتصاد.

ومن ثم فإننا سنحاول من خلال هذا المبحث أن نلقي الضوء على بعض الأفعال التي تمس بمحتوى المستند الإلكتروني وما يتضمنه من معلومات وبيانات، بحيث سيتم التطرق أولاً إلى جريمة التزوير المعلوماتي أو التزوير في محتوى وبيانات المستند الإلكتروني **(المطلب الأول)**، ثم بعد ذلك سيتم إلقاء الضوء على جريمة إتلاف بيانات المستند الإلكتروني **(المطلب الثاني)**، كما سيتم التعرض كذلك إلى جريمة السرقة المعلوماتية أو سرقة المستند الإلكتروني وما يتضمنه من بيانات ومعلومات **(المطلب الثالث)**، وسوف نحاول من خلال دراسة هذه الجرائم الثلاثة، أن نتساءل عن مدى كفاية النصوص القانونية الجزائية سواء

[1] -Cf. Jaques Larrieu, Christian Le Stanc, et Pascal Tréfigny, droit du numérique, recueil dalloz, hebdomadaire, , n° 40, novembre 2014, p,p.2317-2318.

[2] - آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص. 13.

التقليدية أو الحديثة في الحد من هذه الجرائم؟ وهل أن المشرع الجزائري تصدى لهذا النوع المستحدث من الإجرام؟

المطلب الأول: جريمة تزوير المستند الإلكتروني واستعمال المزور.

يشهد التزوير في مجال نظم المعلومات بوصفه أحد أنماط الغش المعلوماتي تزايداً سريعاً في الآونة الأخيرة، بحيث برز تزوير المستخرجات الإلكترونية، وتزوير المعلومات المخزنة بداخل الأنظمة المعلوماتية[1]، وللإشارة فإن التزوير المعلوماتي استفحل في عديد المجالات فشمل مجال إدارة المنشآت -من دفع أو محاسبة أو طلبات أو فواتير- ومجال برمجة أعمال قلم كتاب المحكمة وصحيفة السوابق القضائية، والأحوال المدنية، والقوائم الانتخابية... وغيرها[2]، وقد إنتشر في المجالات المذكورة سلفا بقدر إنتشار الدعامات الإلكترونية وحلولها محل الدعامات الورقية، سيما بعد أن أثبت الواقع العملي أن المستندات والمحررات التقليدية لا تضاهي الدعامات المعلوماتية، سواءً من حيث السعة التخزينية، أو من حيث سرعة استرجاع المعلومات محل التخزين، أو من حيث حسن تبويبها[3].

ولعل ما ساهم في إنتشار هذه الجريمة سهولة الولوج إلى المستندات الإلكترونية والمساس بمحتواها، إما بالإضافة أو الحذف وهو الأمر الذي يشكل خطرا جسيما يهدد سلامة البيانات، ونظرا لأن فعل التزوير يلجأ إليه الجاني إما لتغيير الحقائق في المعلومات والبيانات التي يتضمنها المستند بغية الوصول إلى نتيجة معينة أو تحقيق مكسب معين، وإما من أجل استعمال المستند المزور لتحقيق أغراض غير مشروعة مخالفة للقانون[4].

---

[1]- عمر أبو الفتوح عبد الحفيظ الحمامي، الحماية الجنائية للمعلومات المسجلة إلكترونياً، دراسة مقارنة، دار النهضة العربية، القاهرة، 2010، ص. 873.

[2]- خثير مسعود، المرجع السابق، ص. 134.

[3]- عمر أبو الفتوح عبد الحفيظ الحمامي، المرجع السابق، ص. 873.

[4]- يتخذ التزوير في المحررات الإلكترونية إحدى صورتين؛ تتمثل الأولى في التلاعب في معلومات المحرر أو المستند داخل نظام الحاسب الآلي، وذلك لتغيير الحقيقة في المحرر، سواء بتعديل المعلومات أو محوها أو جزء منها.
في حين تتمثل الثانية في إدخال معلومات غير صحيحة لخلق محرر غير صحيح، وكلتا الطريقتين تتم بنية استعمال المستند فيما زور من أجله. لتفاصيل أكثر يراجع، إيهاب فوزي السقا، المرجع السابق، ص. 47؛ جعفر مشيمش، جريمة التزوير- دراسة مقارنة-، ط1، منشورات زين الحقوقية، بيروت- لبنان، 2009، ص.84 .

لأهمية هذا كله سيتم التعرض إلى جريمة تزوير المستند الإلكتروني **(الفرع الأول)**، وكذا لجريمة استعمال مستند إلكتروني مزور **(الفرع الثاني)**.

الفرع الأول: جريمة تزوير المستند الإلكتروني.

تعتبر جرائم التزوير بمختلف صورها جرائم مخلة بالثقة[1] فهي تقوم على تغيير الحقيقة[2]، والتزوير مهما كانت وسيلته جوهره كذب، ومرماه اغتيال عقيدة الغير[3]، لذلك يعرف بأنه تغيير الحقيقة في بيانات محرر ما بإحدى الطرق المحددة مع ترتب ضرر للغير، ومع نية استعمال المحرر فيما زُور من أجله[4]، كما يعرف بأنه تغيير للحقيقة بقصد الغش في محرر بإحدى الطرق المقررة قانونا، تغييراً من شأنه أن يسبب ضرراً للغير[5]، وهو باختصار إظهار الكذب في محرر بمظهر الحقيقة غشا لعقيدة الغير، كما عرفه جانب من الفقه الفرنسي على أنه تغيير الحقيقة في وقائع، أعِدّ المحرر لإثباتها كان من شأنه أن يسبب ضرراً، أو ارتكب بقصد الغش[6].

غير أنه بعد ظهور التكنولوجيات الحديثة وتقنية الحاسوب الآلي اكتسب التزوير شكلاً جديداً وأضحى يطلق عليه التزوير المعلوماتي، وقد أطلقت هذه التسمية عليه لأنه أصبح يرد على وثائق ومحررات معلوماتية، أي تلك التي يتم الحصول عليها بواسطة جهاز إلكتروني أو كهرومغناطيسي أو أشرطة ممغنطة، ويعرف التزوير المعلوماتي بأنه التلاعب في المعلومات المخزنة في أجهزة الحاسب الآلي المرتبطة بالشبكة أو اعتراض المعلومات بقصد تخزينها[7].

---

[1]- أورد المشرع الجزائري جرائم التزوير بصورها المختلفة في المواد من 197 إلى 241 من قانون العقوبات، وقسمها إلى أربع مجموعات وهي: تزوير النقود وما يتصل بها، تقليد أختام الدولة والطوابع والعلامات، التزوير في المحررات، وشهادة الزور وما شابهها. يراجع، أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، ج2، جرائم الفساد- جرائم المال والأعمال- جرائم التزوير، منقحة ومتممة في ضوء قانون 20 فبراير 2006 المتعلق بالفساد، ط9، دار هومة، الجزائر، 2008، ص. 307.

[2]- المرجع نفسه، ص. 307.

[3]- عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص. 875.

[4]- فائزة يونس الباشا، السياسة الجنائية لجرائم الكمبيوتر في التشريع الليبي (نموذجا ومقارنا)، دار النهضة العربية، القاهرة، 2013،ص37؛ عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص. 876.

[5]- محمد حسين علي محمود، التزوير بإستخدام الوسائل الالكترونية، رسالة ماجستير في الحقوق، كلية الحقوق، جامعة القاهرة، 2011 ، ص36، إيهاب فوزي السقا، المرجع السابق، ص. 48.

[6]- نجوى أبو هيبة، المرجع السابق، ص.3؛ إيهاب فوزي السقا، المرجع السابق، ص. 49.

[7]- محمد نصر محمد، الوسيط في الجرائم المعلوماتية، ط1، مركز الدراسات العربية للنشر والتوزيع، سنة 2015، ص.13؛ عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والأنترنت (الجرائم الإلكترونية) دراسة مقارنة في النظام=

كما يعرف كذلك بأنه تغيير للحقيقة في المستندات المعالجة آلياً والمستندات المعلوماتية، وذلك بنية استعمالها وهو يتم من خلال خلق أو تعديل غير مصرح به للبيانات المسجلة وذلك بطريقة تجعلها تحوز قوة وحجية بما يؤدي إلى خداع لأصحاب الحقوق القانونية المحمية في أمن وسلامة وإمكانية تشغيل البيانات الإلكترونية[1]، وهو الأمر الذي أوردته المذكرة التفسيرية للاتفاقية الأوربية لمكافحة الجريمة المعلوماتية المسماة باتفاقية بودابست التي تطرقت للتزوير المعلوماتي في نص المادة 07 منها[2].

إن العلة من تجريم تزوير المستندات الإلكترونية ترجع إلى رغبة التشريعات المختلفة في حماية الثقة التي نبعت من هذه المستندات بوصفها وسيلة للتعبير عما تتضمنه من بيانات، بحيث أصبحت في نظر الناس معبرة عن الحقيقة فيقدموا على التعامل بها بثقة واطمئنان، وأيضاً لكي يؤدي المستند الإلكتروني دوره بوصفه وسيلة السلطة العامة في مباشرة اختصاصاتها، ووسيلة الأفراد لإثبات علاقاتهم، وكذلك إثبات حقوقهم المتنازع عليها[3].

ولإلقاء الضوء على جريمة التزوير المستند الإلكتروني لا بد من التطرق أولاً إلى أركان هذه الجريمة **(البند الأول)**، ثم بعد ذلك إلى العقوبات المقررة لها **(البند الثاني)**.

البند الأول: أركان جريمة تزوير المستند الإلكتروني.

يستلزم التزوير المعلوماتي الذي يتم بوسيلة معلوماتية في مستند أو محرر معلوماتي تحقق ركنين أساسيين؛ ركن مادي، وآخر معنوي[4].

=القانوني لمكافحة جرائم المعلوماتية والأنترنت مع الإشارة إلى جهود مكافحتها محليا وعربيا ودوليا، ط1، منشورات الحلبي الحقوقية، لبنان، 2007، ص.112.

[1]- محمد حسين علي محمود، المرجع السابق، ص.38.

[2]- هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها، المرجع السابق، ص. 97.

[3]- عبد الفتاح بيومي حجازي، التزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، 2008، ص. 154.

[4]- خثير مسعود، المرجع السابق، ص. 134؛ خالد محمد كدفور المهيري، جرائم الكمبيوتر والإنترنت والتجارة الإلكترونية، ط2، معهد القانون الدولي، دار الغرير للطباعة والنشر، دبي، د.س.ن، ص. 634.

أولاً: الركن المادي لجريمة تزوير المستند الإلكتروني.

لقيام الركن المادي لجريمة التزوير المعلوماتي يشترط ضرورة توافر عناصر ثلاثة أساسية وهي:

1- تغيير الحقيقة في مستند أو محرر بإحدى الطرق المنصوص عليها قانونا وأن يكون من شأن ذلك إحداث ضرر للغير.

2- وجود مستند أو وثيقة أو محرر إلكتروني (محل الجريمة)[1].

3- استخدام جهاز إلكتروني.

فبالنسبة للعنصر الأول فهو يتضمن شقين:

شق أول يتمثل في تغيير الحقيقة، وعليه لا تقوم جريمة التزوير إلا إذا حدث تغيير الحقيقة في المستند، بحيث يترتب على انتفاء هذا العنصر عدم قيام هذه الجريمة[2]، ويعتبر تغييرا للحقيقة إبدالها بما يغايرها[3] ويتم ذلك في التزوير المعلوماتي بإدخال بعض البيانات والمعلومات إلى البرامج والمستندات المعلوماتية، وهو الأمر الذي يتحقق من خلال إستغلال الثغرات والعيوب المنطقية التي تحتويها، والتي لا يمكن إكتشافها إلا عند استخدامها، ويمكن استخدام هذه المستندات المعيبة فنياً بإضافة أي معلومات إليها، ولا يتطلب القانون أن تتغير الحقيقة برمتها وإنما يكتفي بتغيير أقل قدر منها[4].

فتغيير الحقيقة يراد به كل إبدال أو تحريف لها بما يخالفها، ويتم ذلك بمحو بعض أو كل البيانات الوارد ذكرها في المستندات أو البرامج من خلال الحذف أو الشطب أو

---

[1]- إيهاب فوزي السقا، المرجع السابق، ص. 49؛
Jean Pradel, Michel Danti-Juan, droit pénal spécial,3ème éd, CUJAC, paris, 2004, p.790.

[2]- عبد الفتاح بيومي حجازي، التزوير في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص. 156.

[3]- خثير مسعود، المرجع السابق، ص. 136.

[4]- أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، ج2، المرجع السابق، ص. 339؛ جعفر مشيمش، المرجع السابق، ص.86.

الإضافة[1]، أو عن طريق التلاعب بتعديل المعلومات والبيانات الإلكترونية، ومن ذلك مثلا إستبدال كلمة بكلمة أو رقم برقم بهدف خلق مستند إلكتروني غير صحيح[2].

ويتجسد تغيير الحقيقة في بيانات المستند الإلكتروني في ثلاثة صور أساسية: فعل الإدخال والذي يقصد به إضافة معطيات جديدة على الدعامة الخاصة سواءً كانت الدعامة مملوءة أو فارغة من البيانات والمعلومات، فعل المحو والذي يراد به إزالة جزء من المعطيات المسجلة على الدعامة الإلكترونية والموجودة داخل النظام أو تحطيم تلك الدعامة، أو نقل وتخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة، فعل التعديل الذي يراد به تغيير المعطيات الموجودة داخل النظام واستبدالها بأخرى.

إن الأفعال السابق ذكرها هي التي وردت على سبيل الحصر في معظم القوانين المقارنة[3]، وإذا كان تغيير الحقيقة يتم بفعل إيجابي فإنه يمكن أن يتحقق بفعل سلبي كالترك إذا ترتب عنه تغير جوهري، ويقصد بالتزوير بطريق الترك امتناع الشخص عن إثبات واقعة يتعين إثباتها، بحيث يترتب عن عدم ذكرها تغير المعنى الإجمالي للمستند[4].

ومن ثم فإن تغيير الحقيقية يعتبر عنصر من عناصر الركن المادي لجريمة التزوير المعلوماتي تقع على البيانات والمعلومات بأي لغة كانت وبأي طريقة وجدت حيث لا يهم المادة التي كانت عليها ولا يهم شكلها (صوراً، رموزاً، علامات...)، ويستوي أن يكون التغيير مادياً أو معنويا، فالحاسب الآلي جهاز إلكتروني يقوم بأداء عمليات حسابية ومنطقية وفقاً للتعليمات الممنوحة له.

ولئن كان هذا هو الشق الأول للركن المادي لجريمة التزوير المعلوماتي، فإن الشق الثاني يتمثل في إحداث ضرر، وعليه لا يكفي لاكتمال الركن المادي في هذه الجريمة تغيير

---

[1]- باسم رمزي معروف دياب، المرجع السابق، ص.55.

[2]- ضياء يحي السادات، مبادئ استخدام الحاسب الآلي والإنترنت وجهود مكافحة الجرائم الناشئة عنها، منشأة المعارف، سنة 2012، ص ص. 168- 169.

[3]- عبد الإله محمد النوايسية، جريمة الدخول غير المشروع في تشريعات الجرائم الإلكترونية العربية، المجلة القانونية والقضائية، مجلة متخصصة محكمة نصف سنوية، تصدر عن مركز الدراسات القانونية والقضائية، وزارة العدل، دولة قطر، ع1، س العاشرة، جوان 2016، ص. 09.

[4]- باسم رمزي معروف دياب، المرجع السابق، ص.55.

الحقيقة في المستند، وإحداث هذا التغيير بإحدى الطرق التي بينها القانون، وإنما ينبغي أن يكون من شأن ذلك التغيير إلحاق ضرر بالغير، وعليه يعتبر الضرر عنصرا أساسيا وجوهريا لقيام جريمة التزوير وتخلفه يؤدي إلى إنتفاء الجريمة ولو توافرت كل أركانها ولأهميته عرفه الفقه بأنه: « فقد أو نقص أو مساس بمال أو مصلحة يحميها القانون»[1]، ومن ثم فإن الضرر هو عنصر أساسي وجوهري في جريمة التزوير ذلك أنه إذا تخلف الضرر انتفى التزوير ولو توافرت كل أركانه[2].

ولا يشترط القانون وقوع ضرر بالفعل بل يمكن احتمال وقوعه[3]، ويستوي أن يكون مادياً أو أدبياً، فردياً أو جماعيا، كما أن مسألة توافر الضرر من عدمه تعد من المسائل الموضوعية التي تقدرها محكمة الموضوع حسب ظروف كل دعوى[4].

أما بالنسبة للعنصر الثاني الواجب توافره لتكوين الركن المادي لجريمة التزوير المعلوماتي، فيتمثل في الوثيقة أو المحرر بمعنى الشيء الذي ينصب ويقع عليه فعل التزوير، وأن يكون (المستند الإلكتروني) هو الذي تأثر بالتغيير الذي أحدث عليه سواءً بالإضافة أو الحذف أو التعديل، أو أي فعل من شأنه تغيير حقيقة المعطيات والبيانات الواردة في هذا المستند على نحو يسبب به ضرراً لصاحبه الأصلي، بمعنى أن النشاط الإجرامي في هذا النوع من الجرائم يرد على محل أو موضوع محدد هو المستند الإلكتروني، وما يتضمنه من معطيات ومعلومات تمت معالجتها آليا[5].

ومن ثم فإنه يلزم في هذا المستند أن يتخذ شكل الكتابة بحيث لا يهم بأي خط دونت، وبأي لغة كتبت، وبصرف النظر عمن دونها وعن المادة التي كتبت عليها، كما يلزم أن يكون

---

[1]- إيهاب فوزي السقا، المرجع السابق، ص، ص. 56- 57.

[2]- خثير مسعود، المرجع السابق، ص. 137.

[3]- يرى بعض الفقه أن الضرر في جريمة التزوير هو مضمون لمصطلح اللا مشروعية، حيث أن اللامشروعية لا تقتصر على الوجهة الشكلية، أي التعارض بين الواقعة والقاعدة القانونية، بل لها مضمون أساسي وهو الاعتداء على المصلحة التي يحميها المشرع. يراجع في ذلك، إيهاب فوزي السقا، المرجع السابق، ص.57.

[4]- عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص. 930.

[5] - عبد الفتاح بيومي حجازي، التزوير في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص، ص. 209- 210.

مصدر المستند ظاهراً فيه وأن يتضمن تعبيراً متكاملاً عن مجموعة من المعاني والأفكار المترابطة فيما بينها[1].

ويستفاد مما سبق أن المقصود بالمستند الإلكتروني كمحل لجريمة التزوير المعلوماتي ذلك المستند بمميزاته التقنية والقانونية الواردة في النصوص التشريعية وبمفاهيمه، وعناصره[2].

لقيام الركن المادي لجريمة التزوير المعلوماتي، ينبغي تحقق العنصر الثالث والمتمثل في إستخدام جهاز إلكتروني، ذلك أن التغيير أو التلاعب الذي يتم بتعديل أو تحوير، إضافة، أو حذف المعطيات والبيانات يكون بإتباع إجراءات إلكترونية معينة بإستخدام الحاسب الآلي، أو أي جهاز إلكتروني متصل بشبكة اتصالات مفتوحة أو داخلية[3]، وعليه فإن عدم إستخدام جهاز إلكتروني يؤدي إلى انتفاء توفر الركن المادي للتزوير المعلوماتي، فالعلاقة ترابطية بين تغيير الحقيقة والوسيلة المستعملة والمتمثلة في الجهاز الإلكتروني.

ثانياً: الركن المعنوي لجريمة تزوير المستند الإلكتروني.

يتمثل الركن المعنوي في جريمة تزوير المستندات الإلكترونية في القصد الجنائي، على اعتبار أن هذه الجريمة من الجرائم العمدية، وبالتالي يتخذ القصد الجنائي فيها صورة القصد العام ، ناهيك عن تطلبها للقصد الخاص [4].

ويتمثل القصد العام في هذه الجريمة في علم الجاني على وجه اليقين بفعل تغيير الحقيقية في المستند، مع إرادة إلحاق ضرر بشخص ما، بمعنى أن يكون الجاني مدركا وقت تغيير الحقيقة أن من شأن هذا التغيير إلحاق ضرر مادي أو أدبي حال أو محتمل الوقوع بالأفراد أو بالصالح العام[5].

---

[1]- أحمد أبو الروس، جرائم التزييف والتزوير والرشوة واختلاس المال العام من الوجهة القانونية والفنية، المكتب الجامعي الحديث، الإسكندرية، مصر، 2004، ص. 62.
[2]- يراجع في ذلك، ص. 18 وما يليها من هذه الأطروحة.
[3]- إيهاب فوزي السقا، المرجع السابق، ص. 65.
[4]- خثير مسعود، المرجع السابق، ص. 138.
[5]- عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص. 940.

وعليه فإن تخلف هذان الشرطان يؤدي إلى إنتفاء القصد العام، ومن تم إنتفاء الركن المعنوي لجريمة التزوير وهو ما يستتبع عدم قيامها، وعليه فقيام هذه الجريمة يفترض علم الجاني بأن ما حصل من تغيير فيه يعتبر مستنداً أو محرراً في نظر القانون، وأنه لا يجوز أن يقع عليه أي تغيير للحقيقة، ضف إلى ذلك ضرورة علم الجاني بأن الطريقة التي حصل بها التزوير هي من الطرق المنصوص عليها في القانون، ذلك انه ليس للجاني أن يعتذر بجهله للقانون في هذا الصدد[1].

إلى جانب القصد الجنائي العام، فإنه يجب أن يتوافر لدى الجاني قصداً خاصاً والمتمثل في نية الغش، بمعنى أن تتجه نية الجاني وقت ارتكاب الفعل إلى استعمال المستند المعلوماتي المزور فيما زور من أجله –أي الاحتجاج به على اعتبار أنه صحيح، أو دفع مضرة عنه أو عن غيره–[2].

وفي هذا يلاحظ أن المشرع الفرنسي يتطلب لقيام هذه الجريمة قصداً خاصاً يتمثل في نية الجاني إحداث ضرر- سواء حقيقي أو احتمالي- للغير[3].

بعد أن تم التطرق إلى العناصر المكونة للركن المادي لجريمة التزوير المعلوماتي، وكذا إلى الركن المعنوي، فإن دراسة هذه الجريمة لا تكتمل إلا بعرض العقوبات المقررة لها، سواء في التشريع الفرنسي أو في التشريع الجزائري.

البند الثاني: العقوبات المقررة لمواجهة جريمة تزوير المستند الإلكتروني.

يتبادر منذ الوهلة الأولى عند معالجة التزوير المعلوماتي التساؤل الآتي: هل يسري على المستند الإلكتروني النصوص العامة لجريمة تزوير المحررات العادية، أم أن هناك عقوبات أخرى تطبق على هذه الجريمة؟

[1]- خثير مسعود، المرجع السابق، ص. 138.
[2]- عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص. 941.
[3]- فؤاد حسين العزيزي، الجرائم المعلوماتية -دراسة مقارنة-، دار الفكر الجامعي، الإسكندرية، مصر،2014، ص، ص.364- 365؛ خثير مسعود، المرجع السابق، ص. 139.

الإجابة على هذا التساؤل لا تتم إلا باستعراض موقف التشريعات بما فيها التشريع الفرنسي والجزائري من هذه الجريمة، وكذا بيان طبيعة العقوبات المقررة لجريمة التزوير المعلوماتي في كل من التشريعين المذكورين.

أولاً: العقوبات المقررة في التشريع الفرنسي.

نتيجة لخطورة الإجرام المعلوماتي اعترف المشرع الفرنسي بجريمة التزوير المعلوماتي بما فيها تزوير المستندات المعلوماتية، وقد تقرر ذلك منذ سنة 1988 بموجب القانون 88/19 الصادر في 1988/01/05 المتعلق بالغش المعلوماتي[1]، والمعروف بقانون كود فران (CODE FRAIN)[2]، والمتتبع لترسانة النصوص العقابية الفرنسية يدرك أن إقرار المشرع الفرنسي لهذه الجريمة لم يتم إلا بعد صراع طويل داخل البرلمان الفرنسي، والذي تجسد بدايةً بالاقتراح الذي تقدم به النائب الفرنسي (كود فران)، والذي تضمن فيه مشروع تعديل قانون العقوبات الفرنسي، حيث اقترح فيه إدخال تعديل على جريمة التزوير في المحررات بحيث تشمل التسجيلات المعلوماتية، غير أن البرلمان الفرنسي هاجم اقتراح هذا النائب بشدة على أساس أن الأخذ به يؤدي إلى تشويه مفهوم التزوير في المحررات والسماح بقيام الجريمة رغم عدم توافر محرر أو مكتوب، نتيجة لذلك اقترحت لجنة إعداد القوانين في الجمعية العامة تشديد عقوبة جريمة الاعتداء العمدي على المعطيات إذا نتج عن التعديل أو الإدخال أو المحو تغيير للحقيقة.

في حين إقترح مجلس الشيوخ تعديلاً آخراً من خلال اعتبار تزوير المستندات المعالجة آلياً جريمة مستقلة عن التزوير في المحررات، وكذا مستقلة عن جريمة استعمال تلك المستندات المزورة، وهو الأمر الذي وافق عليه البرلمان بمجلسيه[3].

---

[1]- أحمد عاصم عجيلة، المرجع السابق، ص. 208.

[2]- يرجع إسم هذا القانون إلى النائب الفرنسي (Jacques Codfrain) الذي عرف هذا التشريع باسمه. مشار إليه من طرف، عبد الفتاح بيومي حجازي، التزوير في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص. 160؛
Eric Przyswa, cybercriminalité et contrefaçon, fyp édition, France,2010, p.125.

[3]- قارة آمال، الجريمة المعلوماتية، رسالة ماجستير في القانون الجنائي والعلوم الجنائية، كلية الحقوق -بن عكنون-، جامعة الجزائر، السنة الجامعية 2001- 2002، ص. 55؛ أحمد عاصم عجيلة، المرجع السابق، ص،ص. 208- 209، عبد الفتاح بيومي حجازي، التزوير في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص، ص. 160- 161.

وبناءاً على ذلك تضمن القانون رقم 88/19 المذكور المادة 462-5، والتي جاء فيها: «يعاقب بالحبس لمدة تتراوح ما بين سنة وخمس سنوات وبالغرامة بين عشرين ألف فرنك إلى مليونين فرنك، كل من زور أية مستندات معالجة آلياً[1]، أياً كان شكلها إذا سبب ذلك ضرر للغير»[2].

غير أنه بصدور قانون العقوبات الفرنسي الجديد في 1992/12/16[3] ألغيت المادة السابقة، حيث قرر المشرع الفرنسي عدم ضرورة الإبقاء على التجريم الخاص بتزوير المستندات المعالجة آلياً واستعمالها، والاكتفاء بإضافة تعديل على جريمة التزوير العادية، أي العودة إلى الاقتراح القديم الذي تقدم به النائب الفرنسي (كود فران)، وهو ما تقرر فعلا حيث تم تعديل المادة (441-1) في الكتاب الرابع من قانون العقوبات الفرنسي لكي تفي بهذا الغرض[4]، والتي ورد نصها كالتالي: «التزوير هو كل تغيير بطريق الغش في الحقيقة يكون من شأنه إحداث ضرر، ويرتكب بأي طريقة كانت سواء كان ذلك بالكتابة أو بأي إفصاح آخر للتعبير عن الفكر، والذي يكون الغرض منه أو كنتيجة له إحداث شأن في إثبات حق أو واقعة لها آثار قانونية، ويعاقب على جريمة التزوير واستعمال المزور بالسجن لمدة ثلاث سنوات وبغرامة مالية تقدر بـ 45000 أورو»[5].

---

[1]- يلاحظ أن هذا النص الجديد قد استخدم تعبيراً حديثاً وهو المستندات المعالجة (les documents informatisés) ولم يستخدم مصطلح المحررات المعلوماتية (les écritures informatiques)، والواقع أن تعبير المستندات المعالجة آليا الذي استخدمه المشرع الفرنسي هو التعبير الأصح من وجهة النظر التقنية في الحاسب الإلكتروني، حيث يقصد بتعبير المستندات المعالجة آليا، أنها مستندات تم بالفعل خضوعها لمعالجة آلية، وبمعنى آخر أن هذه المستندات قد تمت صياغتها في صورة إحدى لغات الحاسب، وبالتالي فلفظ المحررات المعلوماتية هي الخطوة الأولى التي يتم بعدها الانتقال إلى عملية المعالجة الآلية، وللإشارة فإن التزوير يقع على هذه المستندات المعالجة آليا. يراجع في ذلك، عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص. 891.

[2]- Art. 462-5 du C.P.F créé par Loi 88-19 1988-01-05 art.1 JORF 6 janvier 1988 Abrogé par Loi n°92-1336 du 16 décembre 1992-art .372 (V) JORF 23 décembre 1992 en vigueur le 1er mars1994 disposse que : « Quiconque aura procédé la falsification de documents informatisés, quelle que soit leur forme, de nature à causer un préjudice à autrui, sera puni d'un emprisonnement d'un an à cinq ans et d'une amende de 20.000 F à 2.000.000 F ».

[3]- للإشارة فإن قانون العقوبات الفرنسي الصادر بتاريخ 1992/12/16 لم يدخل حيز التنفيذ إلا مع بدايةً 01 مارس 1994. مشار إليه من طرف، عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص. 891.

[4]- خثير مسعود، المرجع السابق، ص، ص. 132- 134.

[5]- Art. 441 -1 c.p.fr (modifié par Ordonnance n°2000-916 du 19 septembre 2000-art.3 (v) JORF 22septembre2000 en vigueur le 1 er janvier 2002) dispose que : «constitué un faux toute vérité de nature à causer un préjudice et accompli 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.=

والجديد الذي إستحدثه المشرع الفرنسي من خلال هذا التعديل، أنه وسع من محل التزوير (وسع من مفهوم المحرر) بحيث أصبح لا يقتصر على ما يصدق عليه وصف المكتوب فقط، وإنما يمتد ليشمل أي دعامة أخرى للتعبير عن الفكر، وهذا لا ينطبق فقط على المستندات المعالجة آليا، بل يشمل أيضاً البرامج أياً كان نوعها، والمعلومات المسجلة على أقراص أو شرائط ممغنطة ولو لم يتم معالجتها بعد، أو لم يتم إدخالها بعد إلى جهاز الحاسب الآلي، والتعليمات المتعلقة بكيفية تشغيل البرامج، وكذلك تذاكر المترو والبطاقات البنكية (بطاقات السحب وبطاقات الائتمان أو الدفع...) حتى ولو لم تدخل الخدمة[1].

وبذلك تتضح أهمية هذا التعديل في أنه لم يقصر الحماية على المستندات المعالجة آلياً فقط، بل وسع منها لتشمل المستندات المعلوماتية وسواءً كانت هذه الأخيرة خاضعة للمعالجة الآلية أم غير خاضعة لها[2].

الملاحظ أن المشرع الفرنسي حقق من وراء هذا التعديل هدفين مهمين يكمن الأول في توسيعه لجريمة التزوير لتشمل كل من التزوير التقليدي والتزوير المعلوماتي[3]، في حين يكمن الثاني في إخراجه لجريمتا تزوير المستندات المعالجة آليا واستعمالها من بين جرائم الاعتداء على نظام المعالجة الآلية للمعطيات، وهو أمر منطقي حسب رأي الفقه ويجد مبرره في اختلاف المصلحة المحمية قانونا والتي تقف وراء تجريم كل منهما، إذ أن المصلحة المحمية من تجريم الاعتداء على نظام المعالجة الآلية للمعطيات هي مصلحة فردية تخص صاحب هذا النظام المعلوماتي ومن يسيطر عليه فردا أو شركة، في حين أن المصلحة التي يحميها القانون بصدد جريمة التزوير في المستندات والمحررات، ومنها تزوير المستندات المعلوماتية هي حماية الثقة العامة المقترحة في هذه المستندات أيا كان شكلها[4].

=Le faux et l'usage de faux sont punis de trois ans d'emprisonnement et de 45000 Euros d'amende ».

[1]- علي عبد القادر القهوجي، الحماية الجنائية لبرامج لبرامج الحاسب الآلي، المرجع السابق، ص، ص.144- 145؛ قارة أمال، الجريمة المعلوماتية، المرجع السابق، ص، ص. 58- 59.

[2]- خثير مسعود، المرجع السابق، ص. 133.

[3]- حطاب كمال، الحماية الجنائية للتجارة الإلكترونية، أطروحة دكتوراه في العلوم تخصص علوم قانونية، فرع علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة جيلالي ليابس- سيدي بلعباس، السنة الجامعية 2014- 2015، ص. 159.

[4]- عبد الفتاح بيومي حجازي، التزوير في جرائم لكمبيوتر والإنترنت، المرجع السابق، ص، ص 162- 163؛ خثير مسعود، المرجع السابق، ص.133؛ علي عبد القادر القهوجي، الحماية الجنائية لبرامج لبرامج الحاسب الآلي، المرجع السابق، ص. 143.

ثانياً: موقف المشرع الجزائري من جريمة تزوير المستند الإلكتروني.

أورد المشرع الجزائري النصوص المتعلقة بجرائم التزوير بصفة عامة في قانون العقوبات[1]، وتطرق إلى جريمة تزوير المحررات بصفة خاصة في نفس القانون المذكور من نص المادة 214 إلى غاية المادة 229[2]، حيث نص في المادة 214 بأنه: « يعتبر مرتكبا لجريمة التزوير كل موظف أو قائم بوظيفة عمومية أو خاصة، يغير في حقيقة المحررات العمومية أو الرسمية أثناء تأدية وظيفته وذلك بوضع توقيعات مزورة، أو إحداث تغيير في المحررات أو الخطوط أو التوقيعات أو انتحال شخصية الغير أو الحلول محلها، أو الكتابة في السجلات أو غيرها من المحررات العمومية، أو التغيير فيها بعد إتمامها وقفلها»[3].

كما نص في المادة 216 من ذات القانون على التزوير في المحررات الرسمية أو العمومية[4] المرتكب من طرف الأشخاص العاديين غير الذين عينتهم المادة 214 الآنف ذكرها، أما المادة 219 فنظم فيها المشرع فعل التزوير في المحررات العرفية أو التجارية أو المصرفية[5].

---

[1]- وردت جرائم التزوير بأنواعها في المواد من 197 إلى 241 ق.ع.ج مقسمة إلى أربع مجموعات وهي: تزوير النقود وما يتصل بها، تقليد أختام الدولة والطوابع والعلامات، التزوير في المحررات، وشهادة الزور وما شابهها. مشار إليه من طرف، أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، ج2، المرجع السابق، ص. 307.

[2]- أدرجت النصوص الخاصة بتزوير المحررات في كل من القسم الثالث والرابع والخامس من الفصل السابع من الباب الأول من الكتاب الثالث من قانون العقوبات الجزائري في المواد من 214 إلى 229.

[3]- الأمر رقم 66-156 المؤرخ في 18 صفر سنة 1386 الموافق 8 يونيو 1966 المتضمن قانون العقوبات الجزائري المعدل والمتمم،ج.ر.ع. 49، س 1966.

[4]- إستحدث المشرع هذه المادة بموجب القانون رقم 06-23 المؤرخ في29 ذي القعدة عام 1427 الموافق 20 ديسمبر 2006 المعدل والمتمم للأمر رقم 66-156المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات الجزائري، ج.ر، ع. 84،س. 2006. وفيها نص: «يعاقب بالسجن المؤقت من عشر (10) سنوات إلى عشرين (20) سنة وبغرامة من 1.000.000 دج إلى 2.000.000 دج كل شخص، عدا من عينتهم المادة 215، ارتكب تزويراً في محررات رسمية أو عمومية:

1- إما بتقليد أو بتزييف الكتابة أو التوقيع.
2- وإما باصطناع اتفاقات أو نصوص أو التزامات أو مخالفات أو بإدراجها في هذه المحررات فيما بعد.
3- وإما بإضافة أو إسقاط أو بتزييف الشروط أو المقررات أو الوقائع التي أعدت هذه المحررات لتلقيها أو لإثباتها.
4- وإما بانتحال شخصية الغير أو الحلول محلها»

[5]- تنص المادة 219 /1 من ق.ع.ج :المعدل والمتمم: « كل من ارتكب تزويراً بإحدى الطرق المنصوص عليها في المادة 216 في المحررات التجارية أو الصرفية، أو شرع في ذلك يعاقب بالحبس من سنة إلى خمس سنوات وبغرامة من 500 إلى 20.000 دينار».

الملاحظ أن هذه النصوص جاءت تخص التزوير في المحررات العادية، ومن تم يبقى السؤال مطروحا ما إذا كان في الإمكان تطبيق ذات النصوص على المحررات المعلوماتية؟ بمعنى آخر هل تشمل هذه النصوص إلى جانب التزوير المادي التزوير المعلوماتي؟ .

إن المتتبع لترسانة النصوص العقابية الجزائرية يدرك أن المشرع الجزائري قد جعل من جريمة التزوير تنصب على المحررات العادية فقط، ولم يتخذ أي موقف للتوسيع من مفهوم المحرر ليشمل المحررات والمستندات المعلوماتية ضمن المحررات محل جريمة التزوير[1]، كما أنه لم يورد نصاً في قانون العقوبات يعرف فيه جريمة التزوير.

مما سبق يتبين أن المشرع الجزائري لم يواكب نظيره الفرنسي بحيث لم يورد نصا مستقلا للتزوير المعلوماتي بصفة عامة والتزوير في المستندات الإلكترونية بصفة خاصة، كما وأنه لم ينص عليها كجرائم ضمن القواعد العقابية العامة التي تجرم فعل التزوير ولا كأفعال معاقب عليها ضمن جرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات[2]، وذلك رغم محاولاته العديدة لسد الفراغ التشريعي في مجال حماية نظم المعلومات، ومكافحة الجريمة المعلوماتية، التي تجسدت بدايةً بإصداره القانون رقم 04-15 المعدل والمتمم لقانون

[1]- سوير سفيان، جرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، السنة الجامعية 2010- 2011، ص. 109؛ آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص، ص. 138- 139.

[2]- إن مصطلح نظام المعالجة الآلية للمعطيات هو تعبير فني تقني يصعب على المشتغل بالقانون إدراك حقيقته بسهولة، فضلاً عن أنه تعبير متطور يخضع للتطورات السريعة والمتلاحقة في مجال فن الحاسبات الآلية، ولذلك فالمشرع الجزائري على غرار التشريع الفرنسي لم يعرف نظام المعالجة الآلية للمعطيات بل مهمة تعريفه لكل من الفقه والقضاء ،وبناءاً عليه عرّف الفقه الفرنسي نظام المعالجة الآلية للمعطيات والبيانات بأنه كل مركب يتكون من وحدة أو مجموعة وحدات معالجة، والتي تتكون كل منها من الذاكرة والبرامج والمعطيات وأجهزة الإدخال والإخراج وأجهزة الربط، والتي يربط بينها مجموعة من العلاقات، التي عن طريقها تتحقق نتيجة معينة وهي معالجة المعطيات، على أن يكون هذا المركب خاضع لنظام الحماية الفنية. كما ورد تعريف للنظام المعلوماتي ضمن المادة الثانية من الاتفاقية الدولية للإجرام المعلوماتي على النحو التالي:

- "Système informatique désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données."

مشار إليه من طرف، خليفي مريم، الرهانات القانونية للتجارة الإلكترونية، رسالة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد ،تلمسان، السنة الجامعية 2011- 2012، ص. 169.

العقوبات[1] والذي بموجبه استحدث قسما سابع مكرر في تقنين العقوبات سماه المساس بأنظمة المعالجة الآلية للمعطيات[2]، حيث نص فيه على حماية جزائية للأنظمة المعلوماتية من خلال تجريم بعض أنواع الاعتداء التي تستهدف أنظمة المعالجة الآلية للمعطيات كالدخول غير مشروع للأنظمة المعلوماتية والتلاعب بالمعطيات الخاصة لأنظمة المعلومات[3]، إلا أنه لم يفرد نصاً خاصاً يتضمن التزوير المعلوماتي وتزوير المستندات والمحررات الإلكترونية، وظل المشرع الجزائري على موقفه إلى غاية سنة 2014 حيث أصدر القانون 14-03 المتعلق بمستندات ووثائق السفر[4]، والذي فرض فيه ضمن أحكامه الجزائية بعض العقوبات على فعل التزوير الذي يمكن أن يطال البيانات الإلكترونية الخاصة بوثائق السفر المخزنة في النظام البيومتري الإلكتروني بحيث جاء في المادة 17 منه على أن: « كل شخص يزور... عمداً سنداً أو وثيقة سفر... يتعرض إلى العقوبات المنصوص عليها في قانون العقوبات.

وإذا مست الأفعال المذكورة أعلاه البيانات المخزنة في النظام البيومتري الإلكتروني فتطبق العقوبات المنصوص عليها في قانون العقوبات، لا سيما تلك المنصوص عليها في المواد 394 مكرر إلى 394 مكرر 7".

---

[1]- قانون 04-15 المؤرخ في 27 رمضان عام 1425 الموافق ل 10 نوفمبر سنة 2004 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات، سابق الإشارة إليه.

[2]- للإشارة فإن هذا القانون قد تم تعديله سنة 2006 بموجب القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون العقوبات الجزائري، وقد مس التعديل ثلاث مواد من القانون رقم 04-15 وهي المادة 304 مكرر إلى غاية المادة 304 مكرر 2.

[3]- تنص المادة 394 مكرر من ق.ع.ج المعدل والمتمم: "يعاقب بالحبس من ثلاثة (3)أشهر إلى سنة (1) وبغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك.

تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة.

وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة (6) أشهر إلى سنتين (2) والغرامة من 50.000 دج إلى 150.000 دج.

وبخصوص جريمة التلاعب بمعطيات أنظمة المعلوماتية فنص عليها المشرع الجزائري بالمادة 394 مكرر1 من قانون العقوبات الجزائري وجاء فيها: « يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها».

[4]- قانون رقم 14-03 مؤرخ في 24 ربيع الثاني عام 1435 الموافق 24 فبراير سنة 2014 المتعلق بسندات ووثائق السفر، ج.ر. ع. 16، س. 2014.

وبهذا يكون المشرع قد أحال إلى تطبيق العقوبات المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات، باعتبار أن النظام البيومتري الإلكتروني ما هو إلا نظام من أنظمة المعالجة الآلية.

وقد إستحدث المشرع الجزائري قانون 14-03 المتعلق بمستندات ووثائق السفر رغبة منه في مواكبة التطورات التي شهدتها البيئة الرقمية وكذا كتمهيدا لمصادقته على الإتفاقية العربية لمكافحة جرائم تقنية المعلومات التي تمت بموجب المرسوم الرئاسي 14-252، إذ وبالرجوع لهذه الأخيرة يلاحظ أنها خصت التزوير المعلوماتي بالمادة 10 منها بحيث إعتبرته: "إستخدام وسائل تقنية المعلومات من أجل تغيير الحقيقة في البيانات تغييرا من شأنه إحداث ضرر....".

الملاحظ المشرع الجزائري بالرغم من مصادقته على الإتفاقية العربية لمكافحة جرائم تقنية المعلومات إلى أنه لم يورد في قانون 04/15 المتعلق بالتوقيع والتصديق الإلكترونيين نصا يعالج تزوير التوقيع الإلكتروني [1].

أمام النقص التشريعي الوارد في أحكام قانون العقوبات ينبغي على المشرع الجزائري أن يحذو حذو نظيره الفرنسي بحيث يوسع من المحل الذي يقع عليه فعل التزوير بحيث يشمل المحرر التقليدي وأي محرر آخر مهما كانت طبيعته، كما يتوجب عليه التوسيع من طرق التزوير بحيث لا يحصرها في طرق محددة كما فعل في المادة 214 وما يليها من قانون العقوبات وهذا كله لمسايرة الأحداث المتغيرة باستمرار.

لتحقيق هذا كله يتوجب عليه أن يضيف في قانون العقوبات نصا إلى باب التزوير في المحررات يعرف فيه التزوير على النحو التالي: « كل تغيير في الحقيقة بطريق الغش في مكتوب أو أي دعامة أخرى تحتوي تعبيراً على الفكر»، وبهذا التعديل يكون النص أشمل حيث يمكن أن تدرج فيه كل المستندات المعلوماتية حتى وإن كانت غير معالجة آلياً وهو ما يضمن حماية جزائية فعالة.

[1]- يراجع في ذلك نصوص القانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، سابق الإشارة إليه.

الفرع الثاني: جريمة استعمال مستند معلوماتي مزور.

إذا كان التزوير في مدلوله العام يعني تغيير الحقيقة أيا كانت وسيلته، فإن هذا التغيير يمكن أن يقترن بنية استعمال ما زُوِر لتحقيق أغراض غير مشروعة وإلحاق ضرر بالغير[1]، ومن ثم فإن استعمال المستندات والمحررات المزورة يعد قانوناً جريمة مستقلة عن جريمة التزوير، وهذا ما أقرته أغلب التشريعات المقارنة بما فيها التشريع الفرنسي[2].

ويترتب على هذه الاستقلالية بين الجريمتين (أي بين التزوير وفعل استعمال المزور) أن مرتكب التزوير يعاقب على فعله إذا توافرت أركان الجريمة ولو لم يستعمل المحرر المزور، في حين أنه يسأل من يستعمل المستند المزور مع العلم بتزويره عن جريمة الإستعمال ولو لم يكن قد ساهم في تزويره[3]، وفي هذا الإطار ونظراً لخصوصية التزوير المعلوماتي وخصوصية جريمة إستعمال المستندات المزورة، فإنه كان لا بد من إلقاء الضوء على هذه الجريمة والتي قلما تعرض لها الشراح في كتاباتهم بصدد المستندات الإلكترونية، ولا يتأتى ذلك إلا باستعراض أركان هذه الجريمة **(البند الأول)** وكذا العقوبة المقررة لها سواء في التشريع الفرنسي أو الجزائري **(البند الثاني)**.

البند الأول: أركان جريمة استعمال مستند إلكتروني مزور.

يتطلب قيام جريمة استعمال مستند إلكتروني مزورة ضرورة توافر ركنين أساسيين؛ ركن مادي وهو السلوك الإجرامي المتمثل في فعل الاستعمال، وأن ينصب هذا الفعل على مستند إلكتروني مزور **(أولا)** ، وركن معنوي يتمثل في القصد الجنائي والذي مفاده أن يكون الجاني على علم وبصيرة بأن المستند الذي يستعمله مزور **(ثانيا)** [4].

أولاً: الركن المادي لجريمة استعمال مستند إلكتروني مزور.

يعد فعل الاستعمال الركن المادي لجريمة استعمال المستندات الإلكترونية المزورة في مجال المعلوماتية، بل هو القاعدة الأساسية التي تقوم عليها الجريمة[5]، وعن معنى فعل

[1]- أحمد عاصم عجيلة، المرجع السابق، ص، ص. 186- 187.
[2]- فؤاد حسين العزيزي، المرجع السابق، ص. 365.
[3]- إيهاب فوزي السقا، المرجع السابق، ص، ص. 77- 78.
[4]- علي عبد القادر القهوجي، الحماية الجنائية لبرامج لبرامج الحاسب الآلي، المرجع السابق، ص. 142.
[5]- أحمد عاصم عجيلة، المرجع السابق، ص 216- 217؛ خثير مسعود، المرجع السابق، ص. 140.

الاستعمال المعاقب عليه من الناحية التشريعية يلاحظ أن المشرع الفرنسي وكذا الجزائري لم يحددا معناه ومفهومه في نصوصهما القانونية، بل تركا للقاضي حرية ما يدخل في نطاق الاستعمال[1]، الأمر الذي يجعل من الضروري اللجوء إلى آراء الفقه وأحكام القضاء التي تناولت مفهوم الاستعمال للمستندات التقليدية المزورة، وذلك من أجل الوصول إلى ماهية فعل الاستعمال في المستندات الإلكترونية المزورة، وفي هذا يعرف الفقه المصري الاستعمال بأنه يعني إبراز المستند المزور والتمسك به على اعتبار أنه صحيح[2]، في حين يتجه الفقه والقضاء الفرنسيين في تحديدهما لمعنى الاستعمال بالنسبة للمستند التقليدي المزور إلى اتجاهين:

الأول: نادى به الفقيه الفرنسي جارو (Garraud) الذي اعتنق المفهوم الضيق، وذهب إلى وجوب أن تكون هناك علاقة تزامن بين فعل التزوير وفعل الاستعمال، بحيث يكون هناك ارتباط بين فعل الاستعمال والتزوير[3].

أما الثاني فنادى به الفقيه الفرنسي جارسون (Garçon) الذي اعتنق المفهوم الواسع لفعل الاستعمال حيث يرى أن كل فعل يستعمل أو يستخدم فيه المستند المزور يشكل جريمة استعمال دون اشتراط أن يستخدم المحرر فيما زور من أجله[4]، غير أن إتباع هذا النهج فيما يتعلق بالمستندات الإلكترونية لا يتطابق وذاتية المعلومات، الأمر الذي يدفع الباحث إلى بيان ذاتية الاستعمال للمستندات الإلكترونية المزورة، والتي تظهر في أنها تتميز بعدة خصائص منها اختلاف مفهوم الاستعمال عن مفهوم التزوير ذاته، وما يؤكد ذلك أن معظم التشريعات قد أقرت للجريمتين نصين قانونيين مستقلين[5]، ويترتب على هذا نتائج عديدة أهمها أن الفاعل

---

[1]- عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص. 950.

[2]- عرفت محكمة النقض المصرية فعل الاستعمال بأنه: « كل فعل إيجابي يستخدم به المحرر المزور، والاستناد إلى ما دون فيه ويستوي في ذلك أن يكون هذا الاستعمال قد بوشر على جهة رسمية أو على موظف عام أو كان حاصلاً في معاملات الأفراد»، كما عرفه بعض الفقه بأنه: « كل فعل لاستخدام ورقة مزورة من شأنه أن يرتب آثارا قانونية، أو يوهم الغير بصحة الورقة المزورة لترتيب آثار معينة». مشار إليه من طرف، إيهاب فوزي السقا، المرجع السابق، ص. 79.

[3]- عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص. 951.

[4]- خثير مسعود، المرجع السابق، ص. 140.

[5]- نفس الاتجاه سلكه المشرع الفرنسي وكذا المشرع الجزائري في نصوص قانون العقوبات.

الفاعل في جريمة الاستعمال قد يختلف عن الفاعل في جريمة التزوير، كما أن الفاعل في جريمة الاستخدام لا تطبق عليه عقوبة الاشتراك في التزوير[1].

فضلاً عن ذلك فإن فعل الاستعمال يعد تاماً أو مكتملاً في حالة تقديم وإبراز المستند المزور واستعماله فيما زور من أجله بغض النظر عن النتيجة المرجوة[2]، كما قد تكون جريمة الاستعمال جريمة مستمرة أو وقتية، وذلك حسب الوقت الذي يستغرقه تحقق النشاط الإجرامي للاستعمال، والغالب فيها أن تكون مستمرة خاصة وأن طبيعة الأمور تقتضي أن يستمر الاحتجاج بالمستند المزور فترة طويلة[3].

إلى جانب فعل الاستعمال كشرط جوهري في الجريمة محل الدراسة، فإنه يشترط كذلك أن ينصب الاستعمال على مستند إلكتروني مزور حيث أن هذه الجريمة لا تقوم إلا إذا كان نشاطها الإجرامي منصباً على مستند إلكتروني ثبت تزويره، ومن ثم فلا يجوز الاستناد في إدانة المتهم من أجل استعمال مستند إلكتروني مزور على جريمة تزوير لم تثبت قانوناً[4].

ثانياً: الركن المعنوي لجريمة استعمال مستند إلكتروني مزور.

تعتبر جريمة استعمال مستند إلكتروني مزور جريمة عمدية يتخذ ركنها المعنوي صورة القصد الجنائي الذي يقوم على العلم بعناصر الجريمة وإرادة تحقيقها[5]، فالقصد الجنائي في هذه الجريمة يتحقق باتجاه إرادة الجاني إلى تقديم المستند والتمسك به على أنه صحيح مع العلم بتزويره[6].

ولا يكفي القول بتوافر العلم أن يتمسك الجاني بالمستند المزور، إذ قد يتمسك به على الرغم من جهله بتزويره، لذلك فإنه يجب إثبات علم الجاني اليقيني بتزوير المستند، وأن

---

[1]- عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص، ص. 952- 953.

[2]- للإشارة فإنه في هذه الحالة لا يشترط أن يؤدي هذا الاستعمال إلى تحقيق النتيجة المطلوبة، كما يعد العدول اللاحق عن الاستخدام نتيجة الندم أو التوبة غير مؤثر في قيام المسؤولية الجنائية. مشار إليه من طرف، خثير مسعود، المرجع السابق، ص. 141.

[3]- فؤاد حسين العزيزي، المرجع السابق، ص. 365؛ أحمد عاصم عجيلة، المرجع السابق، ص. 217.

[4]- أحمد عاصم عجيلة، المرجع السابق، ص. 217.

[5]- المرجع نفسه، ص. 218.

[6]- خثير مسعود، المرجع السابق، ص. 141.

يكون على علم بتغير الحقيقة فيه حيث ينتفي القصد الجنائي في هذه الجريمة إذا تبين أن مرتكب الفعل كان يجهل تزوير المستند (أي إذا انتفى العلم بالتزوير) حتى ولو كان جهله بالتزوير راجع إلى إهماله أو تقصيره في تحري الحقيقة، كما ينتفي القصد الجنائي كذلك إذا لم تتجه إرادة الجاني إلى استعمال المستند، وإنما ضبط معه وادعى صحته[1].

ومن ثم يستفاد مما سبق أنه من يستخدم أو يستعمل مستند إلكتروني وهو عالم علم اليقين أنه مزور ويستخدمه كدليل ويتمسك به للحصول على حقوق قانونية، فإنه يعدّ بذلك مرتكباً لجريمة استعمال مستند إلكتروني مزور.

البند الثاني: العقوبة المقررة لجريمة استعمال مستند إلكتروني مزور.

جريمة استعمال مستند إلكتروني مزور من الجرائم المعاقب عليها و لمعرفة العقوبة المقررة على هذه الجريمة سيتم إلقاء الضوء على العقوبات المقررة لها في التشريع العقابي الفرنسي **(أولا)**، ثم بعد ذلك سيتم البحث عن مدى وجود هذه العقوبات في التشريع الجزائري سواء نصوص قانون العقوبات أو في نصوص قوانين أخرى **(ثانيا).**

أولاً: العقوبة المقررة في التشريع الفرنسي.

لقد كان المشرع الفرنسي سباقاً في النص على هذه الجريمة والعقاب عليها، ويظهر ذلك بدايةً في سنة 1988 حين أفرد لها بموجب القانون رقم 19 لسنة 1988 المتعلق بالغش المعلوماتي[2] نصاً مستقلاً وفيه عاقب على إستخدام المستندات المعالجة آلياً (المستندات المعلوماتية) المشوبة بالتزوير، وجعل عقوبتها مساوية لعقوبة التزوير ذاته حيث نص في المادة 462-6 من القانون المذكور بأنه: «كل من استخدم بتبصر[3] المستندات المعلوماتية

[1]- إيهاب فوزي السقا، المرجع السابق، ص. 81؛ أحمد عاصم عجيلة، المرجع السابق، ص. 218؛ فؤاد حسين العزيزي، المرجع السابق، ص. 365.

[2]- خثير مسعود، المرجع السابق، ص. 139.

[3]- يلاحظ على المادة 6/462 من قانون رقم 19 لسنة 1988 أن المشرع الفرنسي استخدم بدقة لفظاً دالاً على التبصر بكون المحرر مزور، فاستعمل التبصير الدال عليه (sciement) ليدل على أن الجاني المعلوماتي على علم تام بكون المحرر مشوباً بالتزوير، ورغم ذلك يستعمله متعمداً، وهذا المفهوم يتطابق مع القصد الجنائي العام، أما فيما يتعلق بالقصد الجنائي الخاص فإن هذا النص لم يشر إطلاقاً إلى البحث عن اتجاه إرادة الجاني إلى إحداث الضرر بالغير من عدمه، الأمر الذي يعطي الإيحاء بأن هذا النص لا يتطلب سوى القصد الجنائي العام، إلا أن بعض الفقه استقر على أن لفظ التبصر الوارد =

المنصوص عليها في المادة 462-5 فإنه سيعاقب بالسجن من سنة إلى 5 سنوات وبغرامة من 20.000 فرنك إلى 2.000.000 فرنك أو بإحدى هاتين العقوبتين»[1].

بموجب هذه المادة يكون المشرع الفرنسي قد جرم فعل استخدام المستندات المزورة المنصوص عليها في المادة 5/462 من القانون المذكور، وهذا يفيد أن جريمة الإستعمال المنصوص عليها تفترض وجود تزوير سابق، أو على الأقل تلازم بين الاستخدام وبين المستندات المعلوماتية المزورة.

غير أنه بعد صدور قانون العقوبات الفرنسي الجديد في 1992/12/16،ألغى المشرع الفرنسي نص المادة 6/462 وأصبح ينص على هذه الجريمة في نص المادة 2/441 من قانون العقوبات الفرنسي، التي تضمنت العقاب على فعل الاستخدام للمستندات المزورة ومنها الإلكترونية، حيث اعتبرت المادة المذكورة أن من يستخدم مستند مزور أياً كان وبأي وسيلة تم تزويره، وهو عالم بتزويره بقصد تحقيق غرض ما فإنه يعد مرتكباً لجريمة استعمال مستند معلوماتي مزور، ويعاقب بالعقوبة التي قررتها هذه المادة، وهي السجن لمدة خمس سنوات وغرامة تقدر بـ 75000 أورو، وتطبق هذه العقوبة في حالة استخدام محرر عرفي مزور، أما في حالة استخدام مستند رسمي مزور فإن العقوبة تشدد لتصل إلى07 سنوات سجن والغرامة المقدرة بـ 100.000 أورو[2]، وهو ما ورد ذكره في الفقرة الثانية من المادة آنفة الذكر.

=في النص يتطلب توافر القصدين معاً العام والخاص .مشار إليه من طرف، عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص. 954.

[1] - Art. 462-6 c.p. fr (créé par Loi 88-19 1988 -01-05- art .1 JORF 6 janvier 1988 Abrogé par Loi n°92-1336 du 16 décembre 1992 – art .372 (V) JORF 23 Décembre 1992 en vigueur le 1er mars 1994) dispose que: « quiconque aura sciemment fait usage des documents informatisés visés à l'article 462-5 sera puni d'un emprisonnement d'un an à cinq ans et d'une amende de 20.000 F à 2.000.000 F ou de l'une de ces deux peines ».

[2]- Article 441-2 du c. p.fr (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 faux commis dans un document délivré par une administration publique aux fins de constater un droit, une identité ou une qualité ou d'accorder une autorisation et puni de cinq ans d'emprisonnement et de 75000 euros d'amende.

l'usage du faux mentionné à l'alinéa précédent est puni des mêmes peines.

Les peines sont portées à sept ans d'emprisonnement et à 100.000 euros d'amende lorsque le faux ou l'usage de faux est commis :=

ثانياً: العقوبة في التشريع الجزائري.

نص المشرع الجزائري على جريمة استعمال المحررات المزورة في نصوص قانون العقوبات، بحيث نص على استعمال الأوراق العمومية أو الرسمية في المادة 218 من قانون العقوبات، كما نص على استعمال المحررات العرفية أو التجارية أو المصرفية المزورة في المادة 221 من قانون العقوبات، وعلى استعمال الوثائق الإدارية والشهادات المزورة في المواد 1/222 و223 و2/227 و3/228 من قانون العقوبات، إلا أنه لم يتعرض إلى جريمة إستعمال المستندات الإلكترونية المزورة وهو أمر منطقي طالما لم ينص على جريمة التزوير المعلوماتي في قانون العقوبات عند إستحداثه لنصوص تشريعية حديثة تعالج المعاملات الإلكترونية وتحمي نظم المعلومات المختلفة، كالقانون رقم 04-15 المعدل والمتمم لقانون العقوبات المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات[1]، وكذا القانون 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين الصادر في سنة 2015[2]، فنصوص هذه القوانين جاءت خالية من النص على هذه الجريمة، رغم مصادقة الجزائر على الإتفاقية العربية لمكافحة جرائم تقنية المعلومات سنة 2014، والتي أورد فيها نصا يعالج جريمة إستعمال المحررات الإلكترونية المزورة، بحيث ذكر في المادة 10 منها أن جريمة التزوير هي : "استخدام وسائل تقنية المعلومات من أجل تغيير الحقيقة في البيانات تغييرا من شأنه إحداث ضرر، وبنية إستعمالها كبيانات صحيحة".

أمام النقص التشريعي الوارد في أحكام قانون العقوبات يتوجب على المشرع الجزائري أن يحذو حذو المشرع الفرنسي وبعض التشريعات العربية التي انتهجت نفس نهج

=1. Soit par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public agissant dans l'exercice de ses fonctions.

2. Soit de manière habituelle.
3. Soit dans le dessin de faciliter la commission d'un crime ou de procurer l'impunité à son auteur. »

[1]- القانون رقم 04-15 المعدل والمتمم لقانون العقوبات والمتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات، سابق الإشارة إليه.

[2]- قانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، سابق الإشارة إليه.

التشريع الفرنسي (كالتشريع المصري)[1]، ويستحدث نصوصا ينظم فيها جريمة استعمال المستندات المعلوماتية المزورة، وذلك نظراً للأهمية القصوى التي أصبحت تكتسيها خاصة مع انتشار ثقافة استخدام الكمبيوتر وتوجه الدول إلى خلق وتجسيد فكرة التجارة الإلكترونية والحكومة الإلكترونية وكذا الإدارة الإلكترونية.

المطلب الثاني: جريمة إتلاف المستند الإلكتروني.

تتضمن أنظمة المعالجة الآلية للمعلومات عناصر مادية[2] يمكن أن تكون ملكاً للغير ومنها شاشات العرض، الأشرطة، الأسطوانات، الأقراص الممغنطة، الكابلات ومعدات الإدخال والإخراج، وبخصوص هذه العناصر ينعقد إجماع الفقه على تطبيق الأحكام الخاصة بجريمة الإتلاف عليها وذلك لإعتبارها أموالاً منقولة، ومرد هذا التكييف أن النصوص التشريعية المختلفة تطرقت لهذه الجريمة تحت مسمى إتلاف المنقولات المادية[3].

إن أهمية هذه المسألة لا تغطي مسألة إتلاف المستندات الإلكترونية التي تعد محور دراسة جريمة الإتلاف، ذلك أنها تتضمن بيانات ومعلومات تكيف على أنها مال معنوي غير مادي، ويشكل الفعل المؤثر فيها إعتداءا على بيانات المستند الإلكتروني ذاته، خاصة وأن المجرم المعلوماتي قد لا يكتفي بالولوج أو الدخول غير المشروع والبقاء في الأنظمة الآلية

---

[1]- تطرق المشرع المصري إلى جريمة استعمال المستندات الإلكترونية المزورة في قانون التوقيع الإلكتروني المصري رقم 15 لسنة 2004، حيث نص في هذا القانون على عقوبتين أصليتين لهذه الجريمة وعقوبة تكميلية وعقوبة في حالة كون المتهم عائداً، وتتمثل العقوبات الأصلية لهذه الجريمة في الحبس والغرامة أو إحداهما، حيث جاء في المادة 23 فقرة ج من قانون تنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات، سابق الإشارة إليه على أنه: « مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات، أو أي قانون آخر يعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين كل من...
(ج) استعمل توقيعا أو وسيطا أو محررا إلكترونيا معيباً أو مزوراً مع علمه بذلك».
كما أضاف المشرع المصري إلى العقوبة السابقة عقوبة تكميلية وجوبية وهي النشر، وذلك بنشر حكم الإدانة الصادر ضد المتهم في جريدتين يوميتين واسعتي الانتشار، وعلى شبكة الإنترنت على نفقة المحكوم عليه.
كما نص على عقوبة خاصة كون المتهم عائداً، وهي أنه تزاد بمقدار المثل العقوبة الأصلية المقررة لهذه الجريمة في حديها الأدنى والأقصى. مشار إليه من طرف، أحمد عاصم عجيلة، المرجع السابق، ص ص. 218- 219.

[2]- إن المصطلح الانجلوسكسوني الشائع للدلالة على المكونات المادية للحاسبات الآلية "Hardware"، ويقصد بها مجموعة الأجهزة المادية التي تكون الحاسب الآلي وملحقاته. مأخوذ من، محمد سامي الشوا، الحماية الجنائية للكيانات المنطقية "برامج الحاسب الآلي"، مجلة البحوث القانونية والإقتصادية، مجلة نصف سنوية محكمة تصدرها كلية الحقوق، جامعة المنوفية، ع4، س2، أكتوبر 1993، ص.101.

[3]- نائلة عادل محمد فريد قورة، جرائم الحاسب الآلية الاقتصادية، ط1، منشورات الحلبي الحقوقية، لبنان، 2005، ص، ص. 190- 191.

لمعالجة المعلومات، بل قد يتجاوز بفعله الغرض الإجرامي بإتلافه المستندات والمعلومات المسجلة إلكترونيا والمخزنة بداخل هذه الأنظمة[1].

إستنادا لما تقدم ينبري التساؤل التالي: هل يخضع فعل الإتلاف المعلوماتي وإتلاف المكونات المعنوية لا المادية للنظام المعلوماتي بما فيه المستندات الإلكترونية وما تحتويه من معلومات لنفس النصوص التقليدية لجريمة الإتلاف، أم أن التشريعات أفردت لها نصوصاً قانونية خاصة؟، وما هي الأركان المتطلب توافرها لقيام هذه الجريمة، وكذا العقوبة المقررة لها؟

الإجابة على هذه التساؤلات تتطلب تبيان عناصر جريمة إتلاف المستند الإلكتروني **(الفرع الأول)**، ليتم بعدها تحديد العقوبات المقررة لهذه الجريمة سواءً في التشريع الفرنسي أو الجزائري **(الفرع الثاني)**.

الفرع الأول: عناصر جريمة إتلاف المستند الإلكتروني.

يعرف الإتلاف المعلوماتي بصفة عامة بما فيه إتلاف المستندات الإلكترونية بأنه: "محو المعلومات أو البرامج كلياً أو تدميرها إلكترونيا وكذا تشويه المعلومات أو البرامج على نحو يؤدي إلى إتلافها ويجعلها غير صالحة للاستعمال"[2].

وعليه فإن الإتلاف هو تعييب الشيء على نحو يفقده قيمته الكلية أو الجزئية[3]، وهو بكل بساطة إخفاء لمادة الشيء أو على الأقل إحداث تغيير شامل عليها، بحيث تصبح غير صالحة للاستعمال في الغرض المخصص لها، ناهيك عن أن قيمتها تضيع على المالك[4].

جريمة الإتلاف قد تقع عن طريق شبكة الإنترنت، وذلك بالاعتداء على الوظائف الطبيعية للحاسب الآلي، وعن طريق التعدي على البرامج والبيانات المخزنة والمتبادلة عن

[1]- أحمد عاصم عجيلة، المرجع السابق، ص. 240.
[2]- مدحت محمد عبد العزيز إبراهيم، الجرائم المعلوماتية الواقعة على النظام المعلوماتي، ط1، دراسة مقارنة، دار النهضة العربية، القاهرة، 2015، ص. 95؛ عبد الله عبد الكريم عبد الله، المرجع السابق، ص.113.
[3]- عادل علي المانع، إشكالية الحماية الجنائية لملكية المعطيات المعالجة آليا، مجلة البحوث القانونية والإقتصادية، كلية الحقوق، جامعة المنصورة، ع التاسع والعشرين، أفريل 2001، ص.487.
[4]- ضياء يحي السادات،المرجع السابق، ص. 152.

طريق شبكة الإنترنت، وكذا بالتلاعب بالبيانات وإتلاف المعلومات المخزنة بالمستندات الإلكترونية بمحوها أو تعديلها أو تغيير نتائجها، أو التشويش على النظام المعلوماتي، وإعاقة سير عمل هذا النظام، أو بتدمير البيانات إلكترونياً على نحو فيه إتلاف بما يجعلها غير صالح للاستعمال[1].

انطلاقاً مما سبق، يتبين أن جريمة إتلاف المستند الإلكتروني تتطلب لقيامها توفر ركن مادي **(البند الأول)**، وركن معنوي **(البند الثاني)**.

البند الأول: الركن المادي لجريمة إتلاف المستند الإلكتروني.

غالبا ما يتم إتلاف المعلومات والمستندات الإلكترونية داخل النظام المعلوماتي أثناء تشغيل جهاز الحاسب الآلي أو عند تشغيله، ويتم ذلك بأحد أساليب الإتلاف المكونة للركن المادي، وللإشارة فإن هذه الأساليب تستلزم من مرتكبيها صفات خاصة كالذكاء وإحتراف التعامل مع الأنظمة المعلوماتية، ذلك أن إتلافها لا ينشأ بأسلوب العنف والتحطيم أو التكسير التقليدي، وإنما يتم من خلال تقنيات التدمير الناعمة[2].

ونظراً للطبيعة الخاصة التي تتسم بها المكونات غير المادية للمعلومات والبيانات الإلكترونية والتي يغلب عليها الطابع المعنوي، فقد أطلق عليها بعض الفقه مصطلح "تدمير نظم المعلومات"[3]، ويقصد بهذا المصطلح إتلاف أو محو أو تعديل المكونات المعنوية[4] مثل البرامج المعلوماتية والمعلومات المخزنة بداخل هذه النظم، بهدف إحداث ضرر بالنظام المعلوماتي وإعاقته عن أداء وظيفته[5].

---

[1]- محمد أمين الشوابكة، جرائم الحاسوب والانترنت (الجريمة المعلوماتية)، ط1، دار الثقافة، الأردن ،2006، ص. 219؛ محمد عبيد الكعبي، المرجع السابق، ص. 382.

[2]- عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص، ص. 989- 990.

[3]- مصطفى محمد موسى، أساليب اجرامية بالتقنية الرقمية ماهيتها ومكافحتها، دار الكتب القانونية، مصر،2005، ص.58.

[4]- إن المصطلح الأنجلوسكسوني الشائع للدلالة على المكونات المعنوية أو ما يعرف بالكيان المنطقي هو مصطلح "Logiciel أو software"، وللإشارة فقد عرف المنشور الفرنسي الصادر في 22 نوفمبر 1981 هذه الكيانات بأنها: "مجموعة البرامج والأساليب والقواعد وعند الإقتضاء الوثيقة المتعلقة بتشغيل وحدة معاجة البيانات.". مأخوذة من، محمد سامي الشوا، الحماية الجنائية للكيانات المنطقية "برامج الحاسب الآلي"، المرجع السابق، ص.103.

[5]- عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص. 988.

بهذا يتضح أن قيام الركن المادي لجريمة إتلاف المستندات الإلكترونية يتم من خلال قيام الجاني بإرتكاب فعل المحو أو التعديل بإستخدام وسيلة معينة، وقد تكون هذه الوسيلة إستخدام تقنية الفيروسات كوسيلة للإتلاف والتعييب، كما قد يتم الإتلاف بأساليب أخرى غير الفيروسات.

لأهمية هذه المسألة سيتم التعرض لها بالتطرق للإتلاف بواسطة الفيروسات **(أولا)**، وللإتلاف بغير الفيروسات **(ثانيا)**.

أولاً: إتلاف المستند الإلكتروني بواسطة الفيروسات.

تعتبر الفيروسات المعلوماتية من وسائل إتلاف المستندات الإلكترونية، وهي تختلف من حيث أنواعها وقوتها التدميرية[1]، كما أنها تعد وسيلة تكنيكية حديثة أصبحت تستخدم لإرتكاب جرائم معينة، والفيروسات هي برامج مشفرة مصممة بقدرتها على التكاثر والانتشار من نظام إلى آخر بواسطة قرص ممغنط أو عبر شبكة الاتصالات، بحيث يمكن أن تنتقل عبر الحدود من أي مكان إلى آخر في العالم، كما لها القدرة على الاختفاء داخل برنامج سليم بحيث يصعب اكتشافها، وقد تكون الفيروسات مصممة لتدمير برامج أخرى أو تغيير معلومات، لتقوم بعد الإنتهاء من عملها بتدمير نفسها ذاتياً دون أن تترك أي أثر يدل عليها[2].

وعلى الرغم من قدرة الفيروسات على تدمير البرامج والمعلومات وكذا المستندات إلا أنها لا تسبب عادة تدميراً لمكونات النظام المادي للحاسب الآلي[3]، وللإشارة فإن الفيروسات المعلوماتية تتميز في جانب كبير بخصائص المجرم المعلوماتي فهي تختفي كخطوة أولى ثم تبدأ في الظهور كخطوة ثانية لتدمر في خطوة ثالثة، كالمجرم تماما الذي يضع خطته لإرتكاب الجريمة[4].

---

[1]- محمد عبد الله محمد العوا، المسؤولية الجنائية الناشئة عن جرائم الاموال عبر الانترنت، أطروحة لنيل درجة دكتوراه في الحقوق، كلية الحقوق، قسم الدراسات العليا، القانون الجنائي، جامعة الإسكندرية، 2012، ص.218.

[2]- رشدي محمد علي محمد عيد علي، الحماية الجنائية للمعلومات على شبكة الإنترنت، دراسة مقدمة لنيل درجة الدكتوراه في الحقوق، كلية الحقوق، قسم القانون الجنائي، جامعة القاهرة، سنة 2009، ص. 250؛ ماجد عمار، المسؤولية القانونية الناشئة عن استخدام فيروس برامج الكمبيوتر ووسائل حمايتها، دار النهضة العربية، القاهرة، 1989، ص، ص. 72- 73.

[3]- نائلة عادل محمد فريد قورة، المرجع السابق، ص. 192؛ رشدي محمد علي محمد عيد علي، المرجع السابق، ص.250.

[4]- ماجد عمار، المرجع السابق، ص.76؛

Philippe Baumard, op. cit,p.42.

ونظراً لأن الفيروس المعلوماتي (Le virus informatique) يتمتع بصفة الخفاء فإنه يبدأ بالإضرار بنظام عمل الحاسب الآلي وشبكات المعلومات، ثم يمتد هذا الضرر إلى المعلومات الكامنة في هذا النظام والمخزنة بالمستندات الإلكترونية، حيث يقوم بتعديلها أو إحداث إلغاء لها، وهو ما يؤدي إلى إجراء خلل في السير الطبيعي لها بحيث يجعلها غير قادرة على أداء دورها، وبهذا يصف القضاء الفرنسي العيب الفيروسي في البرامج بأنه العيب الخفي[1].

بهذا يمكن القول أن الفيروسات عبارة عن مجموعة من التعليمات التي تتكاثر بمعدل سريع جداً لدرجة تصيب النظام المعلوماتي بالشلل التام، أو هي عبارة عن خلية كهرومغناطيسية نائمة ومبرمجة بحيث تنشط في وقت محدد لتخريب البرنامج الأصلي، وتنتشر في الأجهزة الأخرى التي تضمها الشبكة بحيث تفسد ما تحويه من معلومات وملفات ومستندات إلكترونية[2]، ونظرا لدقتها وخطورتها فإن إعداد هذه الفيروسات وبثها يكون من طرف فئة من خبراء البرامج أو الهكرة[3]، وهدفهم في ذلك الدعاية وإثبات الذات أو إيذاء الآخرين، وللإشارة فإن هذه الفيروسات يمكن إنتاجها من طرف بعض الشركات الكبرى

[1]- رشدي محمد علي محمد عيد علي، المرجع السابق، ص. 250- 251؛
Myriam Quéméner, Joel Ferry, cyber criminalité défi mondial ,2eme éd, édition economica, paris, 2009, p. 77 ; Frédéric-Jérome Pensier et Emmanuel Jez, la criminalité sur l'internet, 1ere édition, puf, paris 2000, p.p.105-106.

[2]- محمد محمود المكاوي، الجوانب الاخلاقية والاجتماعية والمهنية للحماية من الجرائم المعلوماتية (جرائم الكمبيوتر والانترنت) المكتبة العصرية للنشر، مصر، 2010، ص، ص 314-315؛ محمد عبد الله محمد العوا، المرجع السابق، ص.218.

[3]- المحترفون أو الهاكرز (Haker) هواة حاسب آلي، ويدل هذا المصطلح على الشخص الذي يمارس برمجة الحاسب الإلكتروني، واستخدام إمكانياته كهواية، بما في ذلك محاولاته للدخول في شبكات المعلومات للتعامل مع الآخرين سواء بطريقة مشروعة أو غير ذلك. وذهب رأي إلى أن المخترق (Haker) كلمة تطلق على المبرمج المتفوق الذي يستخدم طاقاته في الاتجاه غير الشرعي، بحيث يخترق ويعتدي على أنظمة الحاسب الآلي إما بهدف إثبات الذات، أو الأهداف الإجرامية كتدمير البيانات أو الابتزاز. وتوجد حالياً جمعيات ومؤسسات للمخترقين، توظفها شركات لمحاولة اختراق الاحتياطات الأمنية في أنظمتها الكمبيوترية، وذلك بهدف كشف نقاط الضعف فيها والتأكد من مناعتها. لتفاصيل أكثر يراجع، ضياء يحي السادات، المرجع السابق، ص.139؛ محمد قدري حسن عبد الرحمن، جرائم الإحتيال الإلكتروني، الفكر الشرطي، دورية ربع سنوية- علمية محكمة ومفهرسة تعنى بالأبحاث الشرطية، تصدر عن مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، الإمارات العربية المتحدة، مج العشرون، ع الرابع، العدد رقم (79)، أكتوبر 2011، ص.119.

وذلك بغرض حماية برامجها من النقل غير المشروع، الذي يهدد استثماراتها في هذا المجال[1].

غير أن الفيروسات المعلوماتية كوسيلة لإتلاف المستندات الإلكترونية وإن كانت تتفق جميعها في كونها وسائل تدميرية وتخريبية للبيانات والمعلومات الإلكترونية، إلا أنها تختلف فيما بينها في طريقة عملها في الهجوم وطريقة إحداث النتيجة الإجرامية[2]، ومن ثم فهي تختلف من حيث أنواعها حيث يوجد من بين هذه الأنواع ما يسمى بفيـــروس الـدودة (virus worm) الذي هو عبارة عن برامج تعمل على استغلال أي فجوات في نظم التشغيل لكي تنتقل من حاسب إلى آخر[3]، أو من شبكة إلى أخرى عبر الوصلات التي تربط بينها وتتكاثر أثناء عملها وأثناء انتقالها بإنتاج نسخ منها مثل البكتيريا، وتهدف هذه البرامج إلى شغل أكبر حيز ممكن من سعة الشبكة ومن ثم العمل على خفض أو تعطيل كفاءتها، وأحيانا تتعدى هذا الهدف لتبدأ بعد التكاثر والانتشار في التخريب الفعلي للملفات والمستندات والبرامج ونظم التشغيل[4].

---

[1]- للإشارة فإن للفيروس أهداف متعددة يقصدها مصممه أو مبرمجه من إنشائه ومنها استخدام هذه الفيروسات بهدف عدواني للاطلاع على إمكانية الغير المنافس وإضعافها وتكبيده خسائر مالية في القطاع السياسي أو العسكري أو الاقتصادي، أو لابتزاز الشركات الكبرى والبنوك، كما قد يكون الهدف الرغبة في الانتقام من قبل بعض المبرمجين المطرودين من أعمالهم والناقمين على شركاتهم، وقد يكون التشجيع على شراء البرامج المضادة للفيروسات. لتفاصيل أكثر يراجع، محمد عبيد الكعبي، المرجع السابق، ص، ص. 402- 403.

[2]- رشدي محمد علي محمد عيد علي، المرجع السابق، ص. 252.

[3]- ظهر برنامج الدودة لأول مرة في 02 نوفمبر سنة 1988 على يد العبقري (Robert Tappan Morris) وهو طالب دكتوراه في علوم الحاسوب بجامعة كورنيل بولاية نيويورك بالولايات المتحدة الأمريكية، وتتلخص وقائع هذه القضية في قيام الطالب الأمريكي موريس (Morris) بإعاقة أكثر من ستة آلاف حاسب آلي عن العمل من بينها حاسبات آلية خاصة بوكالة الفضاء الأمريكية (NASA)، وذلك باستخدام برنامج الدودة (Worn) على شبكة الإنترنت وقد ترتب على انتشار هذا البرنامج إتلاف بعض المعلومات، وقد قدرت الخسائر من جراء ذلك بحوالي 12 مليون دولار، وقُدِمَ موريس (Morris) للمحاكمة بتهمة الدخول العمدي غير المصرح به إلى حاسب آلي له أهمية فيدرالية وإعاقة المستخدمين الشرعيين من الدخول إلى نظام الحاسب الآلي والتسبب في خسائر مالية كبيرة، وقد حكم على (Morris) بالسجن مدة 3 سنوات و 10 آلاف دولار غرامة. مشار إليه من طرف، عمر محمد أبو بكر بن يونس، المرجع السابق، 2004، ص،ص. 366-369؛ محمد أمين الشوابكة، المرجع السابق، ص،ص.339-340؛ هروال نبيلة هبة، ماهية جرائم الإنترنت، المعيار، مجلة دورية تصدر عن المركز الجامعي تيسمسيلت، الجزائر، ع5، جوان 2012، ص.327؛ عادل علي المانع، المرجع السابق، ص.488؛ تركي بن محمد العطيان، جرائم الحاسب الآلي "دراسة نفسية تحليلية"، مجلة البحوث القانونية والإقتصادية، مجلة فصلية محكمة يصدرها أساتذة كلية الحقوق، جامعة المنصورة،ع السابع والثلاثون، أبريل 2005، ص.323.

[4]- سنة 2000 ظهرت واحدة من أشهر أشكال الدودة عبر شبكة الإنترنت وسميت بدودة الحب (Love Bug) والتي صنعها (Onel Du Goju Zman) وهو فلبيني الجنسية ويبلغ من العمر 22 سنة، وهي عبارة عن ملصق على رسالة إلكترونية تهبط في الجهاز بمجرد فتح الرسالة المعنونة بعبارات الحب والإغراء، وقد تسببت هذه الدودة في إحداث خسائر بملايين الدولارات في العديد من المؤسسات. مشار إليه من طرف، رشدي محمد علي محمد عيد علي، المرجع السابق، ص. 405؛ Myriam Quéméner, Joel Ferry, op cit, p.p.77-78.

أما النوع الثاني من الفيروسات فقد أطلق عليه مصطلح حصان طـــروادة[1] (Cheval de Troie) وهو عبارة عن برنامج فيروسي لديه القدرة على الاختراق وتدمير أجهزة الحاسبات الآلية، حيث يقوم بنسخ نفسه داخل الملفات والمستندات الإلكترونية، كما يمكن أن يدخل في الأماكن المشفرة وينتشر فيها ليتمكن من تحقيق غرضه في التخريب والتدمير، وهو بذلك أقرب إلى برنامج الاختراق منه إلى الفيروسات، وذلك لكونه يساعد الهكرة على دعم أنشطتهم الاختراقية، فهو برنامج يختبئ داخل البرامج الموجودة بالذاكرة ثم ينشط في الوقت المحدد له ويعمل على تنفيذ الأمر المعطى له إما بإتلاف المستندات أو محو البيانات أو تشويهها[2].

وما يمكن ملاحظته أن حصان طروادة يتميز عن غيره من الفيروسات في أنه لا يستطيع تنشيط نفسه بل يحتاج إلى من يقوم بتنشيطه[3].

أما النوع الثالث من الفيروسات المعلوماتية التي أصبحت تستعمل كوسيلة لارتكاب جريمة الإتلاف فيطلق عليها اصطلاح القنبلة المنطقية (La bombe informatique)، وهي عبارة عن برنامج ينفذ في لحظة محددة أو كل فترة زمنية منتظمة، يتم وضعه في الشبكة المعلوماتية بغرض تسهيل تنفيذ عمل غير مشروع حيث يعمل على تخريب وإتلاف البيانات الإلكترونية[4].

---

[1]- نظرا للقدرة الفائقة لهذا الفيروس في الاختباء والاختفاء عن أعين المستخدم والتمويه عليه فقد شبه بحصان طروادة الذي استخدمه الإغريق حوالي عام 1200 ق.م.، إذ تحكي ملحمة الإلياذة لهوميروس قصة حصار طروادة الذي استمر تسع سنوات دون أن يظفر اليونانيون بها، وحين غلبهم اليأس والحنين إلى الوطن لجئوا إلى خدعة وقاموا بصنع هيكل حصان كبير ووضعوا في داخله مجموعة من جنودهم وانسحبوا وتركوا الحصان خلفهم، وعندما وجدت قوات طروادة الحصان فرحوا به وأدخلوه داخل الحصن، وفي الليل تسلل الجنود المختفون داخل الحصان وهاجموا الحصن وفتحوا أبوابه لإدخال القوات الإغريقية.
مشار إليه من طرف، محمد عبد الله محمد العوا، المرجع السابق، ص.210؛ ضياء يحي السادات، المرجع السابق، ص. 132؛ عادل علي المانع، المرجع السابق، ص.488.

[2]- نعيم مغبغب، حماية برامج الكمبيوتر الأساليب والثغرات، دراسة في القانون المقارن، ط1، منشورات الحلبي الحقوقية، بيروت- لبنان، 2006، ص. 243؛ رشدي محمد علي محمد عيد علي، المرجع السابق، ص، ص . 254- 255؛
Alain Buquet, op. cit, p.p.327-328.

[3]- عمر محمد أبو بكر بن يونس، المرجع السابق، ص. 367؛ نعيم مغبغب، المرجع السابق، ص.243.

[4]- محمد عبد الله محمد العوا، المرجع السابق، ص.215؛ محمد محمود المكاوي، المرجع السابق، ص. 304؛ محمد أمين الشوابكة، المرجع السابق، ص.231؛

Alain Buquet, op cit, p.329.

والملاحظ أن فيروس القنبلة المنطقية يطلق عليه مصطلح القنبلة الموقوتة، كما يعرف بمصطلح الشفرة المعيقة، وهي من حيث شكلها ليست ملفاً متكاملاً، ولكنها شفرة تنضم إلى مجموعة ملفات البرمجية بتقسيمها إلى أجزاء هنا وهناك، وذلك حتى لا يمكن التعرف عليها، وبحيث تجتمع فيما بينها بحسب الأمر المعطى لها في زمن محدد، على نحو يؤدي إجتماعها إلى تخريب المستندات الإلكترونية وما تحويه من بيانات[1]، ومن الأمثلة على ذلك ما قام به خبير في نظم المعلومات وهو يعمل محاسب بإحدى المنشآت في فرنسا، حيث عمد إلى وضع قنبلة زمنية في شبكة المعلومات الخاصة بالمنشأة انتقاماً لفصله منها، وقام ببرمجتها لتنفجر بعد مضي ستة أشهر من تركه العمل بالمنشأة، وقد ترتب على هذا العمل إتلاف كل البيانات والمعلومات المتعلقة بشبكة المعلومات بهذه المؤسسة[2].

إلى جانب هذه الأنواع الثلاثة من الفيروسات الشائعة في مجال الاعتداء على نظم المعلومات، توجد أنواع أخرى من الفيروسات التي تم رصدها والتعامل معها في هذا المجال والتي بات مجرمو المعلوماتية يستخدمونها لإتلاف البيانات والمستندات الإلكترونية منها على سبيل المثال لا الحصر فيروس القردة[3]، الفيروس الإسرائيلي[4]، فيروس الجنس[5]، فيروس الكريسماس[6]، فيروس مايكل

---

[1]- عمر محمد أبو بكر يونس، المرجع السابق، ص. 371؛
Jean Larguier, Phillippe conte, Stéphanie Fournier, droit pénal spécial, 15éd , édition dalloz, France, 2013, p.251.

[2]- من بين الأمثلة الشائعة على استخدام القنبلة المنطقية في حالة البرامج المؤجرة التي يقوم مالكها بتأجيرها للغير مقابل قيمة إيجارية معينة، ففي حالة عدم قيام المستأجر بالوفاء بالأجرة يقوم مالك البرنامج بإرسال قنبلة منطقية توقف نشاطه. مشار إليه من طرف، رشدي محمد علي محمد عيد ، المرجع السابق، ص، ص . 256- 257.

[3]- تتمثل طريقة عمل فيروس القردة في الإتلاف في أنه يعرض على شاشة بها مجموعة من القردة تقوم بعمل بعض الألعاب البهلوانية، ثم يقوم بنسخ نفسه في أكثر من مكان وتدمير الفهرس الرئيسي للقرص الصلب لجهاز الحاسب الآلي محدثا بذلك تخريب المستندات الإلكترونية وما تحويها من بيانات، والتي تكون مخزنة داخل ذلك القرص. مشار إليه من طرف، عايد رجا الخلايلة، المسؤولية التقصيرية الإلكترونية - المسؤولية الناشئة عن إساءة إستخدام اجهزة الحاسوب والأنترنت- دراسة مقارنة، ط1، دار الثقافة، الأردن، 2009، ص.112.

[4]- تم اكتشاف هذا الفيروس في الجامعة العبرية في القدس، وتتمثل طريقة عمله في أنه يقوم بإبطاء تشغيل النظام المعلوماتي إلى نصف زمن التشغيل تقريباً، وذلك بعد نصف ساعة من تشغيل الجهاز. مشار إليه من طرف، محمد عبد الله محمد العوا، المرجع السابق، ص.208.

[5]- يعمل هذا الفيروس على تصوير مجموعة من الصور الجنسية المثيرة للغرائز لجذب انتباه مستخدم النظام، وفي هذه الأثناء ينسخ البرنامج نفسه داخل القرص ويمسح جدول توزيع الملفات. مشار إليه من طرف، عايد رجا الخلايلة، المرجع السابق، ص.111.

[6]- يتمثل هذا الفيروس في صورة رسالة ترسل إلى أحد الأشخاص كتهنئة بمناسبة أعياد الكريسماس، وفي الوقت نفسه يقوم يقوم بقراءة عناوين المشتركين في البريد الإلكتروني ثم ترسل هذه الرسالة إلى تلك العناوين، الأمر الذي يترتب عليه أن=

أنجلو[1]، فيروس الجمعة 13[2]، فيروس نازا (**NASA**)[3]، وفيروس كليتزاتش[4]، وهي تؤدي في مجملها إلى تعطيل وتدمير وكذا تخريب البيانات والمستندات الإلكترونية، كما قد تؤدي إلى إحداث شلل في عمل النظام المعلوماتي بصفة عامة.

ثانياً: إتلاف المستند الإلكتروني بغير الفيروسات.

إلى جانب وسائل الإتلاف غير مباشرة المتمثلة في إستخدام الفيروسات الحديثة والديدان كوسيلة لإتلاف المستندات الإلكترونية داخل الحاسبات الآلية، فإنه توجد وسائل أخرى يتم الاستعانة بها من أجل إحداث هذا التلف، منها على سبيل المثال محو البيانات التي يحتويها المستند الإلكتروني على نحو يتم به إحداث تلف للبيانات الإلكترونية عن طريق تعريض الأسطوانات أو الأقراص الممغنطة المسجل عليها المستندات الإلكترونية لقوى مغناطيسية، أو قطع التيار أثناء معالجة البيانات أو عن طريق التلاعب في البيانات بتغييرها بحيث تفقد قيمتها وحقيقتها التي كانت عليها[5]، وفعل المحو المؤدي إلى الإتلاف المعلوماتي يمكن أن يعرف بأنه: "إزالة جزء من المعلومات المسجلة على الدعامة والموجودة داخل

=يتوقف النظام بأكمله لحين القضاء على هذا الفيروس. مشار إليه من طرف، ماجد عمار، المرجع السابق، ص. 78؛ محمد عبيد الكعبي، المرجع السابق، ص. 405.

[1]- ظهر هذا الفيروس في 26 مارس 1992 بمناسبة الاحتفال بذكرى ميلاد الرسام الإيطالي الشهير مايكل أنجلو، وهو يقوم بمسح معلومات القرص الصلب للأجهزة المصابة محدثا بذلك تخريب وإتلاف المستندات الإلكترونية. مشار إليه من طرف، محمد عبد الله محمد العوا، المرجع السابق، ص. 207.

[2]- ظهر هذا الفيروس في يناير 1988 وتسبب في إصابة الحاسبات الآلية في انجلترا حيث يعمل هذا الفيروس على مسح جميع البرامج والمستندات الإلكترونية. مشار إليه من طرف، عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص.264.

[3]- أطلق هذا الفيروس احتجاجاً على نتائج الأسلحة النووية وكان هدفه اختراق الحاسب الآلي لوكالة الفضاء الأمريكية ناسا (NASA) وتدمير ما تحتويه من بيانات ومستندات إلكترونية. مشار إليه من طرف، محمد عبيد الكعبي، المرجع السابق، ص.405؛ محمد عبد الله محمد العوا، المرجع السابق، ص.208.

[4]- تربع هذا الفيروس عرش فيروسات الكمبيوتر وأصبح أكثرها خطراً على الإطلاق حيث يعمل هذا الفيروس على إبطال مفعول البرامج المضادة للفيروسات، كما يعمل على مهاجمة البريد الإلكتروني ويرسل نفسه إلى أي عنوان يعثر عليه في دفتر العناوين في الجهاز الذي يصيبه، كما أنه يستطيع الوصول إلى هدفه بواسطة 18 رسالة مختلفة كملف ملحق، وهو الأمر الذي يسبب إتلاف وتخريب البيانات الإلكترونية. مشار إليه من طرف، عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص، ص. 267- 268.

[5]- خالد حربي السعدي، جريمة إتلاف برامج ومعلومات الحاسب الآلي في التشريعين الكويتي والمقارن، ط1، دار النهضة العربية، القاهرة، مصر، 2012، ص .85؛ نائلة عادل محمد فريد قورة، المرجع السابق، ص،ص. 193- 194.

النظام المعلوماتي، أو تحطيم تلك الدعامة أو نقل وتخزين جزء من المعلومات على نحو يفقدها قيمتها وجديتها"[1].

إلى جانب فعل المحو فإنه يمكن أن يلجأ مجرمو المعلوماتية إلى إستخدام تقنية تعديل البيانات والمعلومات الإلكترونية على نحو يحقق تلف وتخريب المستندات الإلكترونية، وفعل التعديل المؤدي إلى إحداث الإتلاف المعلوماتي يمكن أن يعرف بأنه: "كل تغيير غير مشروع للمعلومات والبرامج يتم عن طريق استخدام إحدى وظائف الحاسب الآلي"[2].

هذا ويعد تعديل المعلومات والبيانات الإلكترونية بصورة غير مشروعة من أكثر صور الإتلاف شيوعاً، فالتعديل وفق هذا المعنى يتمثل في تغيير حالة المعلومات الموجودة داخل النظام بشكل يؤدي إلى تبديلها واستبدالها بغض النظر عن الطريقة التي وقع بها، وعليه فإنه يقتضي حظر قيام الغير بتبديل المعلومات بأي شكل كان، ذلك أن الأمر يترتب عليه تخريب وإتلاف البيانات الإلكترونية، كما يفقدها قيمتها وجديتها[3].

وفضلاً عن فعل المحو والتعديل المؤديين إلى تخريب بيانات المستندات الإلكترونية، فإنه يمكن أن يتحقق فعل الإتلاف المعلوماتي للبيانات بوسائل أخرى، كاستعمال لوحة المفاتيح الخاصة بالحاسب، وإجراء بعض التغييرات على المعلومات الموجودة في نظامه بصورة مباشرة، أو من خلال استخدام الشبكة المعلوماتية كوسيلة للوصول إلى الحاسب الآلي، والعبث بما يحويه من بيانات ومستندات إلكترونية[4].

ولا يشترط لقيام الركن المادي لهذه الجريمة اجتماع الأفعال المذكورة سابقاً معاً، بل يكفي توافر إحداها، فالقاسم المشترك بين هذه الأفعال يكمن في انطوائها على تلاعب في البيانات والمعلومات التي تتخذ دعامة لها المستندات الإلكترونية[5].

---

[1]- مدحت محمد عبد العزيز إبراهيم، المرجع السابق، ص. 102؛ علي عبد القادر القهوجي، الحماية الجنائية لبرامج لبرامج الحاسب الآلي، المرجع السابق، ص. 134.

[2]- نائلة عادل محمد فريد قورة، المرجع السابق، ص. 217.

[3]- مدحت محمد عبد العزيز إبراهيم، المرجع السابق، ص،ص. 105- 106.

[4]- خالد حربي السعدي، المرجع السابق، ص،ص.75- 76؛ مدحت محمد عبد العزيز إبراهيم، المرجع السابق، ص،ص.106- 107.

[5]- مدحت محمد عبد العزيز إبراهيم، المرجع السابق، ص، ص. 96- 97.

بعد تحديد الركن المادي لجريمة إتلاف المستند الإلكتروني، فإنه ينبغي التعرض للركن المعنوي لهذه الجريمة.

البند الثاني: الركن المعنوي لجريمة إتلاف المستند الإلكتروني.

تعتبر جريمة إتلاف المستندات الإلكترونية من الجرائم العمدية التي تتطلب لقيامها توافر القصد الجنائي العام بعنصريه العلم والإرادة، وعليه ينبغي لتحقق الركن المعنوي أن ينصرف علم مرتكب الفعل إلى أن القيام بتخريب البيانات التي تتضمنها المستندات الإلكترونية أو تعديل أو محو المعلومات، يشكل نشاطا غير مشروع كما يشكل اعتداءاً على صاحب الحق في المعلومات والبيانات الإلكترونية، أو إعتداء على من له السيطرة عليها، مع علمه بأن نشاطه هذا يؤدي إلى نتيجة وهي تغيير حالة المعلومات[1]، وتخريب البيانات التي تتضمنها المستندات الإلكترونية وجعلها غير صالحة للاستعمال في الغرض المحدد له أو على الأقل إذهاب قيمتها[2].

ومما لا شك فيه أن الأضرار الناشئة عن تدمير المستندات الإلكترونية والمعلومات التي تتضمنها تفوق نظيرتها الناتجة عن إتلاف المعدات المادية الخاصة بنظم المعلومات، بل وتفوق إتلاف الأشياء المادية، ولعل ذلك يرجع إلى التكلفة الاقتصادية المرتفعة لإعداد البرامج والمستندات الإلكترونية والإمكانيات الفنية المخصصة لإعدادها[3].

أما بخصوص القصد الجنائي العام الواجب توافره في هذا النوع من الجرائم فإنه لا يشترط أن يكون مباشراً، أي أن تتجه الإرادة إلى النتيجة المتحققة، وإنما قد يكون هذا القصد غير مباشر أو ما يسمى بالقصد الاحتمالي، بحيث يستوي أن تتجه إرادة الجاني إلى وقوع النتيجة من عدمها[4].

---

[1]- شمسان ناجي صالح الخليلي، الجرائم المستخدمة بطرق غير مشروعة لشبكة الأنترنت، دراسة مقارنة، دار النهضة العربية ، القاهرة 2009، ص.240؛ مدحت محمد عبد العزيز إبراهيم، المرجع السابق، ص. 109.

[2]- خالد حربي السعدي، المرجع السابق، ص. 16؛ محمد أمين الشوابكة، المرجع السابق، ص.221.

[3]- أحمد عاصم عجيلة، المرجع السابق، ص، ص. 207- 208.

[4]- فضلاً عن ذلك فإنه يمكن أن نتصور تحقق الشروع في ارتكاب هذه الجريمة إما في صورة الشروع الخائب أو في صورة الشروع الموقوف، فقد يشرع الجاني في ارتكاب هذه الجريمة بفعل الإتلاف والتخريب في البيانات الإلكترونية=

إضافة إلى ضرورة توافر القصد الجنائي العام في جريمة إتلاف المستندات الإلكترونية، فإن بعض التشريعات تتطلب زيادة على ذلك اتجاه إرادة مرتكب الفعل إلى تحقيق قصد خاص، كقصد الإضرار بالغير أو قصد تحقيق ربح مادي غير مشروع للجاني أو للغير ومن بين هذه التشريعات القانون البرتغالي والفنلندي[1].

للإشارة، فقد انتقد جانب من الفقه تطلب القصد الخاص في جريمة الإتلاف المعلوماتي، وبخاصة قصد تحقيق ربح مادي غير مشروع ذلك أن تكريس هذا المبدأ سيؤدي إلى استبعاد جميع الحالات التي لا تتجه فيها نية الجاني إلى تحقيق ربح مادي غير مشروع، وذلك رغم أهمية المعلومات التي قد يتم إتلافها، كما هو حال إتلاف معلومات علمية أو طبية.

هذا عن القصد الخاص المتمثل في تحقيق ربح مادي غير مشروع، أما فيما يخص القصد الخاص المتمثل في الإضرار بالغير فيجب -حسب رأي ذات الفقه- أن يفسر تفسيراً واسعاً حيث لا يقتصر على مجرد الخسائر والأضرار المادية التي قد تصيب المجني عليه[2].

وإذا كانت جريمة إتلاف المستند الإلكتروني عمدية فهذا لا يعني أن الخطأ فيها غير متصور، بل يمكن أن تقع هذه الجريمة بطريق الخطأ غير العمدي أي بدون أن يتوافر قصد الإتلاف، وفي هذا يلاحظ أن قانون العقوبات الفرنسي الجديد عاقب على تعديل البيانات والمعلومات أو محوها إذا ما تم بطريق الخطأ، وقد أشار المشرع الفرنسي إلى ذلك في نص المادة 1/323 من قانون العقوبات الفرنسي ضمن جريمة الدخول أو البقاء بدون تصريح في النظام المعلوماتي حيث شدد العقوبة إذا ما ترتب على ذلك الدخول أو البقاء تعديل المعلومات

=ويستنفذ نشاطه الإجرامي كاملاً، إلا أن النتيجة لا تتحقق لسبب خارج عن إرادته كما لو كان النظام المعلوماتي به برامج حماية متطورة تمنع مثل هذه السلوكيات فهنا يتحقق السلوك الإجرامي في صورة الشروع في ارتكاب جريمة الإتلاف المعلوماتي ،ويوصف بأنه جريمة خائبة. كما يتصور أيضا أن يقوم الجاني ويشرع في فعل التخريب والإتلاف إلا أنه يقبض عليه قبل إتمام هذا السلوك، فهنا يتحقق الشروع في صورة الجريمة الموقوفة، غير أنه لا بد للتشريعات أن تنص صراحة على العقاب على الشروع في هذه الجريمة وإلا يفلت الجاني من العقاب. مشار إليه من طرف، مدحت محمد عبد العزيز إبراهيم، المرجع السابق، ص.109وما يليها.

[1]- نص قانون العقوبات البرتغالي على ذلك في المادتين الخامسة والسادسة من قانون العقوبات البرتغالي لسنة 1991. مشار إليه من طرف، أحمد عاصم عجيلة، المرجع السابق، ص. 258؛ مدحت محمد عبد العزيز إبراهيم، المرجع السابق، ص. 112.

[2]- نائلة عادل محمد فريد قورة، المرجع السابق، ص. 224.

الموجودة داخل النظام، وطبقاً للنص السابق الذكر فإن الركن المعنوي لجريمة الدخول أو البقاء بدون تصريح يكون مزدوج التكوين، ففعل الدخول أو البقاء بدون تصريح يكون عمدياً في حين أن إتلاف المعلومات المترتب على هذا الدخول يكون مبنياً على الخطأ[1].

بعد بيان الأركان الواجب توافرها لقيام جريمة إتلاف المستندات الإلكترونية، فإنه سيتم تحديد العقوبات المقررة لهذه الجريمة.

الفرع الثاني: العقوبات المقررة لجريمة إتلاف المستند الإلكتروني.

نظرا لأن جريمة إتلاف المستندات الإلكترونية من الجرائم المعلوماتية المستحدثة التي تستهدف المعلومات والبيانات المعالجة إلكترونيا، فإنه يصعب القول بانطباق النصوص العقابية التقليدية عليها، ذلك أن تلك النصوص جرمت فعل الاعتداء الموجه إلى المال المادي، وهو الأمر الذي وإن كان ينطبق على حالات الاعتداء المنصبة على العناصر المادية للأنظمة المعلوماتية -كما سبق بيانه- كشاشات العرض ووحدة المعالجة المركزية والأقراص الممغنطة، كونها ذات طبيعة مادية ملموسة، إلا أنه لا يمتد للجرائم المعلوماتية التي تتحقق بالاعتداءات الواقعة على المعلومات والبيانات الإلكترونية ونظم معالجتها[2]، بسبب هذا الفراغ القانوني حاول التشريع المقارن التصدي لهذه المسألة ومواجهة حالات الإتلاف التي تطال العناصر المعلوماتية ذات الطبيعة المعنوية غير الملموسة، أو عن طريق تعديله للنصوص القائمة من خلال سنه لنصوص جديدة.

ومن ثم فإنه سيتم التطرق إلى موقف التشريع المقارن من هذه الجريمة وكذا العقوبة المقررة لها، حيث سيتم التركيز على موقف التشريع الفرنسي كنموذج من التشريعات المقارنة **(البند الأول)**، كما سيتم بيان موقف التشريع الجزائري من هذه الجريمة **(البند الثاني)** وذلك من ناحية مدى وجود جزاءات من عدمه.

[1]- مدحت محمد عبد العزيز إبراهيم، المرجع السابق، ص، ص. 113- 114.
[2]- نائلة عادل محمد فريد قورة، المرجع السابق، ص، ص. 190- 191.

البند الأول: العقوبات المقررة لجريمة إتلاف المستند الإلكتروني في التشريع الفرنسي.

تطرق المشرع الفرنسي إلى جريمة إتلاف المستند الإلكتروني (الإتلاف المعلوماتي) بدايةً بموجب القانون رقم 19 لسنة 1988 المتعلق بجرائم المعلوماتية[1]، وذلك في كل من المادتين 462-3 و462-4 منه بحيث جاء في نص المادة 462-3 بأنه: « يعاقب الحبس لمدة تتراوح من 3 أشهر إلى 3 سنوات وبغرامة من عشر آلاف إلى مائة ألف فرنك فرنسي أو بإحدى هاتين العقوبتين، كل من أضر أو زيف بطريقة عمدية وإضراراً بحقوق الغير نظام المعالجة الآلية للمعلومات»[2].

أما المادة 462-4 من القانون المذكور فقد أورد فيها بأنه: «يعاقب بالحبس لمدة تتراوح من ثلاثة أشهر إلى ثلاثة سنوات وبغرامة من عشرين إلى خمسمائة ألف فرنك أو بإحدى هاتين العقوبتين، كل من قام عمداً بطريقة مباشرة أو غير مباشرة وإضراراً بحقوق الغير بإدخال معلومات إلى نظام معلوماتي معين أو تعديل أو إلغاء بث المعلومات التي يحويها»[3].

ولم يكتف المشرع الفرنسي بهذا النص بل قام سنة 1992 بتعديل قانون العقوبات الفرنسي وضمّنه أحكاما جديدة للحد من هذا النوع من الجرائم، وبموجب هذا القانون الجديد

---

[1]- إستحدث المشرع الفرنسي هذا القانون من أجل وضع حد للخلاف الفقهي الذي وقع بشأن التعدي على الجرائم الواقعة على النظام المعلوماتي، حيث أضاف نصوص القانون رقم 19 لسنة 1988 إلى نصوص قانون العقوبات وذلك من خلال الباب الثاني الفصل الثاني منه، تحت عنوان "جرائم الغش المعلوماتي"، وهذه النصوص عبارة عن تسع مواد تبدأ من المادة 1/462 وتنتهي بالمادة 9/462. مشار إليه من طرف، عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص. 974؛
Eric Przyswa, op. cit, p.p.125-126.

[2]- Art 462-3 c.p.fr (créé par Loi 88-19 1988-01-05 art .1 JORF 6 janvier 1988 Abrogé par Loi n° 92-1336 du 16 décembre 1992-art.372 (V) JORF 23 décembre 1992 en vigueur le 1er mars 1994) dispose que : « Quiconque aura, intentionnellement et au mépis des droits d'autrui, entravé ou faussé le fonctionnement d'un systéme de traitement automatisé de données sera puni d'un emprisonnement de trois mois à trois ans et d'un amende de 1 0000F à 100 000F ou de l'une de ces deux peines. »

[3]- Art 462-4 c.p.fr (créé par Loi 88-19 1988-01-05 art .1 JORF 6 janvier 1988 Abrogé par Loi n° 92-1336 du 16 décembre 1992-art.372 (V) JORF 23 décembre 1992 en vigueur le 1er mars 1994) dispose que : « Quiconque aura, intentionnellement et au mépis des droits d'autrui, directement ou indirectement, introduit des données dans un système de traitement automatisé ou supprimé ou modifié les données qu'il contient ou leurs modes de traitement ou de transmission, sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 2000 F à 500 000 F ou de l'une de ces deux peines. »

تم استبدال المادة المذكورة سابقاً بالمادة 323-2 من قانون العقوبات الفرنسي الجديد، والتي جاءت تقريباً بنفس المحتوى مع تشديد العقوبات المقررة في المادة السابقة[1]، حيث نصت المادة 323-2 من القانون المذكور بأنه: «يعاقب بالحبس مدة خمس سنوات وبغرامة قدرها 75000 يورو كل من قام بإعاقة أو إفساد نظام المعالجة الآلية للمعلومات»، وللإشارة فقد تم تشديد العقوبات مرة أخرى على إثر تعديل قانون العقوبات سنة 2015[2]. وقد مرت المادة 323-3 بذات التعديلات، حيث نصت بموجب قانون 1992 على أن: « يعاقب بالحبس مدة خمس سنوات وبغرامة قدرها 75000 يورو كل من أدخل غشاً إلى نظام المعالجة الآلية للمعلومات أو قام بمحو أو تعديل البيانات التي يحتوي عليها»، أما تعديلها لسنة 2015 فقد شدد من الغرامة بحيث رفعها إلى150.000 أورو[3].

من خلال هذا التعديل يلاحظ على المشرع الفرنسي لم يضع شروطاً تتعلق بطبيعة المعلومات محل الإتلاف بل ترك النص عاماً ليشمل كافة أنواع المعلومات، كما أنه ترك الباب مفتوحاً لطرق إتلاف المعلومات لتشمل كافة أشكال الاعتداء على المعلومات، بما في ذلك الفيروسات والبرامج الخبيثة أياً كانت وسيلة إدخالها إلى الحاسب الآلي[4].

هذا وينبغي الذكر أن النص السالف الذكر يشمل إتلاف المعلومات الموجودة في الذاكرة أو على الأسطوانة، حيث يؤدي إدخال البيانات إلى شغلها بالكامل، فتعجز عن التعامل مع هذه المعطيات بمعالجتها أو باستخراجها مطبوعة على الورق[5].

---

[1]- أحمد عاصم عجيلة، المرجع السابق، ص. 262.

[2]- Art. 323-2 Al 1 c.p.fr (Modifié par Loi n° 2015-912 du 24 juillet 2015- art.4) dispose que: « Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé des données est puni de cinq ans d'emprisonnement et de 150.000 euros d'amende ».

[3] - Art. 323-3 Al 1 c.p. fr (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'xtraire, 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 150000 euros d'amende ».

[4]- مدحت محمد عبد العزيز إبراهيم، المرجع السابق، ص. 122؛ أحمد عاصم عجيلة، المرجع السابق، ص. 262.

[5]- جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي، الأحكام الموضوعية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، 2012، ص.73.

ونفس اتجاه المشرع الفرنسي تبنته اتفاقية بودابست لمكافحة الإجرام المعلوماتي الموقعة بتاريخ 8 نوفمبر 2001، حيث نصت على جريمة الإتلاف المعلوماتي في نص المادة الرابعة منها تحت عنوان: "الاعتداء على سلامة البيانات"[1]، والتي جاء فيها أنه: «يجب على كل طرف أن يتبنى الإجراءات التشريعية، أو أية إجراءات أخرى يرى أنها ضرورية لتجريم، تبعاً لقانونه المحلي، إذا حدث ذلك عمداً، ودون حق، أي أضرار أو محو، أو تعطيل، أو إتلاف أو طمس لبيانات الحاسب».

أما الفقرة الثانية من هذه المادة فجاء فيها أنه: « يمكن لأي طرف أن يحتفظ بحق اشتراط أن يكون السلوك المنصوص عليه في الفقرة الأولى يؤدي إلى أضرار جسيمة»[2]. وحسب المذكرة التفسيرية لهذه الاتفاقية، فإن الهدف من تقرير هذا النص هو أن تكون بيانات وبرامج الحاسب مكفولة بحماية مماثلة لتلك التي تتمتع بها الأشياء المادية من الأضرار التي تحدث عمدا، والمصلحة المحمية هنا هي سلامة وحسن تشغيل أو حسن استخدام البيانات أو برامج الحاسب المسجلة[3].

البند الثاني: العقوبة المقررة لجريمة الإتلاف المعلوماتي في التشريع الجزائري.

بالرغم من خطورة فعل الإتلاف المعلوماتي الذي يطال المستندات الإلكترونية وما تحويه من بيانات ومعلومات، وبالرغم من جسامة الأضرار والخسائر التي يلحقها هذا الإتلاف بالمكونات المعنوية للحاسب والتي تفوق بكثير الأضرار التي يلحقها إتلاف الوسائل والمكونات المادية الأخرى، إلا أن المتتبع لترسانة النصوص القانونية الجزائرية يجد أن المشرع الجزائري قد حذا حذو نظيره الفرنسي وعمل على تجريم فعل إتلاف المستندات

[1]- هلالي عبد اللاه أحمد، جرائم الحاسب والإنترنت بين التجريم الجنائي وآليات المواجهة، دار النهضة العربية، مصر، 2015، ص. 200.

[2]-Art 4 du Convention sur la cybercriminalité : Atteinte à l'intégrité des données 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'alerter ou de supprimer des données informatiques.

1- Une partie peut se réserver le droit d'exiger que le comportement décrit au paragraphe 1 entraine des dommages sérieux ».

[3]- مدحت محمد عبد العزيز إبراهيم، المرجع السابق، ص،ص. 122- 123؛ هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقاً عليها، المرجع السابق، ص. 69.

الإلكترونية بطريقة غير مباشرة، وذلك تبعاً لمعالجة تجريم إتلاف المعلومات أو البيانات الإلكترونية أو أنظمة معالجة البيانات والمعطيات الآلية، ويظهر ذلك جلياً في البداية من خلال القانون رقم 04-15 المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات[1] والذي عبر فيه بطريقة غير مباشرة عن هذه الجريمة تحت مصطلح "التخريب الذي يطال منظومة المعالجة الآلية للمعطيات" حيث جاء في نص المادة 394 مكرر من القانون المذكور بأنه: «يعاقب بالحبس من 3 أشهر إلى سنة وبغرامة من 50.000 دج إلى 200.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك، وأنه تتضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة، أما إذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة فتكون العقوبة الحبس من 6 أشهر إلى سنتين والغرامة من 50.000 دج إلى 300.000 دج»[2].

وباستقراء نصوص هذا القانون من المادة 394 مكرر إلى غاية المادة 394 مكرر 7 يتبين أن المشرع الجزائري لم يورد مادة صريحة يعاقب فيها على أفعال الإتلاف التي تطال المستندات الإلكترونية، وما تحويه من بيانات ومعلومات.

ولعل ما يؤخذ على المشرع الجزائري أنه لم يشر شأنه شأن التشريع الفرنسي إلى استخدام الفيروسات والبرامج الخبيثة لإتلاف المكونات المنطقية للحاسبات الآلية من مستندات وبيانات وبرامج بإعتبارها أحد وسائل الركن المادي للجريمة، وفي هذا يرى جانب من الفقه[3]إمكانية تطبيق هذه النصوص على حالة استخدام تلك الفيروسات والبرامج الخبيثة طالما ترتب على إدخالها الإضرار بالمستندات الإلكترونية وما تحويه من معلومات وبيانات.

إذا كان هذا موقف المشرع الجزائري سنة 2004 ، فإنه ينبغي الذكر أنه سنة 2014 نص المشرع الجزائري بموجب المادة 17 من القانون 14-03 المتعلق بوثائق وسندات السفر على جريمة الإتلاف التي تطال البيانات المخزنة في النظام البيومتري، وأشار إلى

[1]- قانون رقم 04-15 المعدل والمتمم لقانون العقوبات الجزائري الصادر بموجب الأمر رقم 66-156 المؤرخ في 08 يونيو 1966، سابق الإشارة إليه.

[2]- المادة 394 مكرر من القانون رقم 04-15 المعدل والمتمم بالقانون رقم 06-23 المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات، سابق الإشارة إليه.

[3]- نائلة عادل محمد فريد قورة، المرجع السابق، ص. 205.

تطبيق العقوبات المنصوص عليها في المواد 394 مكرر إلى 394 مكرر 7 من قانون العقوبات، أي تلك العقوبات المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات السابق بيانها، والواقع أن هذا الأمر منطقي طالما أن النظام البيومتري للبيانات ما هو إلا نظام من نظم المعالجة الآلية حيث نصت المادة 17 من القانون المذكور أنه: « كل شخص... يتلف عمداً سنداً أو وثيقة سفر أو يستعمل عمداً سندا أو وثيقة سفر... محرفة يتعرض إلى العقوبات المنصوص عليها في قانون العقوبات، وإذا مست الأفعال المذكورة البيانات المخزنة في النظام البيومتري الإلكتروني، فتطبق العقوبات المنصوص عليها في قانون العقوبات،

وإذا مست الأفعال المذكورة أعلاه البيانات المخزنة في النظام البيومتري، فتطبق العقوبات المنصوص عليها في قانون العقوبات،لا سيما تلك المنصوص عليها في المواد 394 مكرر إلى 394 مكرر 7».

أما بخصوص موقف المشرع الجزائري من هذه الجريمة فيلاحظ أن قانون التوقيع والتصديق الإلكترونيين[1] لم يسد الفراغ التشريعي الذي أثار الكثير من الجدل الفقهي والتردد القضائي، فنصوص هذا القانون جاءت خالية من كل نص ينظم جريمة إتلاف المستندات الإلكترونية.

وعليه فإنه ومن هذا المقام نناشد المشرع الجزائري بضرورة استحداث نصوص قانونية تكون فيها حماية المستند الإلكتروني من الإتلاف والتخريب والتدمير حماية أصلية مباشرة وليست حماية تبعية لحماية البرامج والمعلومات، وأن تتضمن النصوص عبارات ومصطلحات دقيقة ومباشرة تنص على فعل إتلاف وتخريب البيانات والمستندات الإلكترونية وذلك أسوة بغيره من التشريعات، كما نناشده بتشديد العقوبة المقررة لهذا النوع من الإجرام المستحدث الذي أصبح يهدد أنظمة المعلومات مثلما فعلت بعض التشريعات العربية[2].

[1]- قانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، سابق الإشارة إليه.

[2]- للإشارة فإنه من بين التشريعات العربية التي شددت العقوبة على جريمة الإتلاف المعلوماتي نظام مكافحة جرائم المعلوماتية السعودي الذي عاقب بالسجن مدة لا تزيد عن أربع سنوات، وبغرامة لا تزيد عن ثلاثين ريالا أو بإحدى هاتين العقوبتين على إيقاف الشبكة المعلوماتية عن العمل أو تعطيلها أو تدمير أو مسح البرامج والبيانات الموجودة أو المستخدمة فيها أو حذفها أو تسريبها أو إتلافها أو تعديلها»، في حين قرر التشريع العماني الصادر بالمرسوم السلطاني رقم 12 لسنة 2011 المتعلق بإصدار قانون مكافحة جرائم المعلوماتية، في المادة الثالثة منه عقوبة السجن لمدة لا تقل عن شهر =

المطلب الثالث: جريمة سرقة بيانات المستند الإلكتروني.

تعتبر جريمة السرقة بوجه عام من أهم جرائم الأموال التي تتشكل من كل فعل يمثل إعتداءاً حالاً أو محتملاً على الحقوق ذات القيمة المالية، أو على أحد عناصر الذمة المالية للشخص[1].

وإذا كان الكل يجمع بأن التكنولوجيا الحديثة قد قدمت خدمات جليلة للمجتمع حيث عن طريقها تم توفير المجهود الذهني للإنسان وتم ربح الوقت والمال، إلا أنها من ناحية أخرى خولت لمجرمي المعلوماتية ولمحترفي القرصنة[2] إختراق الشبكات المعلوماتية والأنظمة الإلكترونية وإنتهاك ما تتضمنه من بيانات ومعلومات إلكترونية، واستغلالها في أغراض غير مشروعة.

والواقع أن لجرائم الاعتداء على المال المعلوماتي[3] أهمية متزايدة، لا سيما وأن هذا النوع من الإجرام أصبح يستهدف بشكل مباشر التعامل الإلكتروني للبنوك والمؤسسات المصرفية، خاصة مع تطور وسائل الدفع الإلكتروني[4]، وانتشار عملية التجارة الإلكترونية وظهور نظم التحويلات المالية التي أصبحت في الوقت الحالي تعتمد على استخدام الحاسب الآلي وشبكات المعلومات، وعلى تبادل البيانات والمعلومات ذات الطابع الإلكتروني،

=ولا تزيد على ستة أشهر وبغرامة لا تقل عن مائة ريال عماني ولا تزيد عن خمسمائة ريال عماني أو بإحدى هاتين العقوبتين على إلغاء أو تغيير أو تعديل تشويه ،أو إتلاف أو نسخ أو تدمير أو نشر، أو إعادة نشر بيانات أو معلومات إلكترونية مخزنة في النظام المعلوماتي، أو وسائل تقنية المعلومات، أو تدمير ذلك النظام أو الشبكة المعلوماتية أو إلحاق الضرر بالمستخدمين أو المستفيدين»...مشار إليه من طرف، خالد حربي السعدي، المرجع السابق، ص، ص. 127- 128.

[1]- شمسان ناجي صالح الخليلي، المرجع السابق، ص. 172؛ أحمد عاصم عجيلة، المرجع السابق، ص. 271.

[2]- هناك من يعبر عن السرقة المعلوماتية بالقرصنة، وتعرف القرصنة بأنها «سرقة المعلومات من برامج وبيانات مخزنة في دائرة الكمبيوتر بصورة غير شرعية، أو نسخ برامج معلوماتية بصورة غير شرعية، بعد تمكن مرتكب هذه العملية من الحصول على كلمة السر أو بواسطة التقاط الموجات الكهرومغناطيسية الصادرة عن الحاسب الآلي أثناء تشغيله، وباستخدام هوائيات موصلة بحسابات خاصة...». مشار إليه من طرف، محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، ط1، دار الثقافة، عمان- الأردن، 1430هـ-2009م، ص. 39.

[3]- يقصد بالمال المعلوماتي الحاسوب بكل مكوناته، وهو عبارة عن مجموعة من الكيانات التي تسمح بدخول المعلومات ومعالجتها وتخزينها عند الطلب، وهو يتكون من كيانين؛ الكيان المادي للحاسب الإلكتروني ويتمثل في وحدات الإدخال ووحدات التشغيل ووحدات الإخراج، والكيان المنطقي أو المعنوي الذي يتمثل في البرامج.

[4]- يقصد بالدفع الإلكتروني مجموعة الأدوات والتحويلات الإلكترونية التي تصدرها المصارف والمؤسسات كوسيلة دفع، وتتمثل في البطاقات البنكية والنقود الإلكترونية، والشبكات الإلكترونية، والبطاقات الذكية وغيرها.

فالحسابات البنكية والمبالغ المودعة في الحسابات وأرقام بطاقات الائتمان معرضة للسلب والاختلاس الإلكتروني[1].

بهذا يتضح أن الإستخدام غير القانوني للتكنولوجيا يؤدي إلى السرقة، وهو ما من شأنه إنتهاك الثقة والصلاحية في العمليات المالية المتبادلة عن طريق الوسائل الإلكترونية، ولأهمية هذه المسألة يتم التساؤل عن مدى إعتبار المستند الإلكتروني وما يتضمنه من بيانات ومعلومات مالاً يندرج ضمن جرائم الأموال؟، وما مدى إمكانية تطبيق النصوص التقليدية المتعلقة بجريمة السرقة الواردة في قانون العقوبات على سرقة المستند الإلكتروني وما يتضمنه من بيانات ومعلومات؟

الإجابة على هذه التساؤلات تقتضي أولا البحث عن أركان جريمة السرقة المعلوماتية **(الفرع الأول)**، ثم التطرق إلى العقوبات المقررة لهذه الجريمة **(الفرع الثاني)**.

الفرع الأول: أركان جريمة سرقة المستند الإلكتروني.

تنشأ جريمة سرقة المستندات الإلكترونية وما تضمنه من بيانات ومعلومات، وغيرها من البرامج التي تستخدم في عملية المبادلات الإلكترونية بصفة عامة والتجارة الإلكترونية بصفة خاصة، بكل فعل من شأنه الاستيلاء على مستندات أو برامج أو معلومات أو بيانات مملوكة للغير[2]، وقد عرّفت المادة 350 من قانون العقوبات الجزائري السرقة كما يلي: «كل من اختلس شيئا غير مملوك له يعد سارقا»، ويقابلها نص المادة 311 فقرة 01 من قانون العقوبات الفرنسي[3] التي نصت على أن: «السرقة هي الأخذ الإحتيالي للشيء من الآخرين».

[1]- من أشهر جرائم سرقة الأموال التي جرت أحداثها في إمارة دبي بدولة الإمارات العربية المتحدة في أواخر عام 2001 ما قام به مهندس حاسبات آسيوي يبلغ من العمر 31 عاما، وقد وقعت الجريمة في أفريل من عام 2003 ،حيث قام ذلك المهندس بالعديد من السرقات المالية لحسابات عملاء في 13 بنكاً محلياً وعالمياً، فاستولى على الأموال من الحاسبات الشخصية، وحولها إلى حسابات وهمية قام هو بإنشائها، كما قام أيضا بشراء العديد من السلع والخدمات عبر شبكة الإنترنت مستخدما بطاقات الائتمان، والحسابات الشخصية لعدد كبير من الضحايا. كل ذلك تم من خلال الدخول للشبكة عبر إحدى المقاهي العامة المنتشرة في دبي، وقد بلغت قيمة الأموال المستولى عليها حوالي 300 ألف درهم من البنوك المحلية بالإمارات فقط . مشار اليه من طرف، خليفي مريم، المرجع السابق، ص. 200.

[2]- حطاب كمال، المرجع السابق، ص. 144.

[3]- Article 311-1 du c.p.fr dispose que: « Le vol est la soustraction frauduleuse de la chose d'autrui ».

وما يمكن ملاحظته أن التعريف الوارد في قانون العقوبات الجزائري يهتم بالجانب الموضوعي للسرقة، حيث يتطلب لقيام هذه الجريمة أن يرتكب الجاني فعلاً مادياً محدداً هو الاختلاس، وأن ينصب هذا الاختلاس على شيء منقول مملوك للغير، غير أن المادة 311 فقرة 01 من قانون العقوبات الفرنسي قد أشارت إلى الركن المعنوي للجريمة وهو القصد الجنائي، إذ يتطلب النص المتقدم وقوع الاختلاس بقصد الغش، وبذلك تكون أركان جريمة السرقة التقليدية هي؛ محل السرقة وهو شيء منقول مملوك للغير، النشاط المادي المتمثل في الاختلاس والقصد الجنائي.

وفي معرض البحث حول أركان الصورة المستحدثة لجريمة السرقة والمتمثلة في سرقة المستند الإلكتروني أو السرقة المعلوماتية بصفة عامة سيتم بيان مدى تطابق القواعد القانونية العامة لجريمة السرقة التقليدية مع القواعد الخاصة للسرقة المعلوماتية (سرقة المستند الإلكتروني)، وذلك من خلال التعرض لمحل سرقة المستند الإلكتروني **(البند الأول)**، وإيضاح الركن المادي في هذه الجريمة **(البند الثاني)**، ثم التعرض للركن المعنوي المتمثل في القصد الجنائي **(البند الثالث)**.

البند الأول: محل جريمة سرقة المستند الإلكتروني.

وفقاً للقواعد العامة للسرقة، فإن محل هذه الجريمة يجب أن ينصب على مال منقول مملوك للغير وأن يكون ذا طبيعة مادية[1]، والمال هو كل شيء يصلح للحيازة والنقل والتملك وتكون له قيمة، أما الشيء المادي فيقصد به الشيء الذي ينتمي إلى عالم المحسوسات بحيث يمكن لمسه مباشرة واستغلاله على الوجه الذي يحقق منفعة لصاحبه أو لحائزه، وبعبارة أخرى يقصد به الشيء المادي الذي يتقبل السلطات المالية التي تنطوي عليها الملكية والحيازة[2].

[1]- تتطلب بعض التشريعات صراحة أن يكون المحل مادياً، وذلك بالإشارة إلى المنقول المملوك للغير، ومن ذلك على سبيل المثال قانون العقوبات المصري، حيث نصت المادة 311 منه على: «كل من اختلس منقولاً مملوكاً لغيره فهو سارق» ، وعلة تطلب هذا الشرط أن الشيء ذو الطبيعة المادية هو الذي يصلح موضوعاً للحق العيني بصفة عامة، وحق الملكية بصفة خاصة، ذلك أن الملكية باعتبارها سلطة شاملة للمالك لا تتصور إلا على شيء له كيان مادي، وبالإضافة إلى ذلك فإن الحيازة التي تنالها السرقة بالاعتداء يراد بها الحيازة المادية التي تتمثل في سيطرة الجاني على الشيء، وهي بدورها لا تتصور إلا إزاء شيء مادي. مشار اليه من طرف، شمسان ناجي صالح الخليلي، المرجع السابق، ص. 176؛ محمد أمين الشوابكة، المرجع السابق، ص. 144.

[2]- شمسان ناجي صالح الخليلي، المرجع السابق، ص. 177.

ولتوضيح مدى التطابق ما بين محل السرقة في القواعد العامة، ومحل السرقة في المجال المعلوماتي، يجب تحديد طبيعة المال وطبيعة المنقول في مجال المعلوماتية، فبالنسبة لطبيعة المال في مجال المعلوماتية فيمكن القول أن المال المعلوماتي، والذي يقصد به الحاسوب بكل مكوناته هو عبارة عن مجموعة من الكيانات التي تسمح بدخول المعلومات ومعالجتها وتخزينها واسترجاعها عند الطلب، وهو يتكون من كيانين؛ الكيان المادي أو ما يسمى بالمال المعلوماتي الطبيعي[1]، والذي له كيان مادي ظاهري ملموس، ويتمثل في كل من وحدات الإدخال[2]، وحدات التشغيل[3]، وحدات الإخراج[4]، شاشات العرض، الطابعات، وسائط التخزين وخلافه، وبشأن هذا النوع يجمع الفقه على أن المال المعلوماتي الطبيعي يصلح لأن يكون محلاً للسرقة باعتباره مالا ماديا ملموسا، ويمكن نقله وحيازته والاستيلاء عليه[5].

هذا عن الكيان المادي، أما عن الكيان المنطقي أو المال المعلوماتي المعنوي، والمتمثل في العناصر المنطقية للنظام المعلوماتي وما تحتويه من برامج ومستندات إلكترونية وبيانات صالحة للاستخدام أي المعالجة آلياً[6]، فيثار التساؤل عن ما إذا كان يصلح أن يكون محلاً للسرقة؟.

في الحقيقة يرجع طرح التساؤل حول مدى إمكانية تطبيق القواعد العامة للسرقة في مجال سرقة البيانات والمستندات الإلكترونية إلى الطبيعة المعنوية لهذه الأخيرة، وفي هذا الشأن إستقر جانب من الفقه على وجوب أن يكون موضوع السرقة منقولاً ماديا، وعليه لا

---

[1]- آمال قارة، الحماية الجنائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص. 14.

[2]- وحدات الإدخال: تسمى كذلك لأنها تستخدم في إدخال البيانات والبرامج إلى وحدة التشغيل الرئيسية، وتشمل مشغل الأسطوانات ولوحة المفاتيح والفأرة. مشار إليه من طرف، ضياء يحي السادات، المرجع السابق، ص. 27.

[3]- وحدات التشغيل: تتكون من الذاكرة التي تستخدم لحفظ البيانات والمعلومات والبرامج حفاظاً دائماً أو مؤقتا، ووحدة الحساب أو المنطق التي تقوم بإنجاز العمليات الحسابية والمنطقية، وهي عبارة عن ذاكرة سريعة، ووحدة التحكم التي تقوم بالتنسيق بين وحدات النظام المعلوماتي. مشار إليه من طرف، أحمد خليفة الملط، الجرائم المعلوماتية، ط2، دار الفكر الجامعي، الإسكندرية، 2006، ص. 36.

[4]- وحدات الإخراج: هي الوسائط المستخدمة لإظهار نتائج التشغيل، ويمكن إظهارها بأكثر من وسيلة، وبذلك يكون للحاسب مخرجات ورقية تتم عن طريق الطابعة بحيث تستخرج المعلومات في شكل نسخ ورقية مطبوعة، ومخرجات إلكترونية حيث يتم استخراج المعلومات على دعائم إلكترونية مثل الشريط الممغنط، والمصغرات الفيلمية. مشار إليه من طرف، ضياء يحي السادات، المرجع السابق، ص. 40 وما يليها .

[5]- أحمد عاصم عجيلة، المرجع السابق، ص. 273؛

Daniel Martin, Frederic Paul Martin, cybercrime, menace, vulnérabilité, riposte, puf, 2001, p.p.176-177.

[6]- آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص. 15؛ أحمد خليفة الملط، الجرائم المعلوماتية، المرجع السابق، ص. 235.

تصلح الأموال المعنوية لتكون محلاً للسرقة، إلا إذا اتخذت هذه الأموال مظهراً مادياً، بحيث تصبح منقولات مادية يصلح أن يرد عليها الاختلاس[1].

حسب هذه الاتجاه الفقهي تدخل المستندات الإلكترونية وما تحويه من بيانات في نطاق النصوص الخاصة بجريمة السرقة التقليدية إذا ما أفرغت في دعامة مادية كالأسطوانة أو الأشرطة الممغنطة، لإعتبار أن الجريمة تقع على محل مادي يتمثل في هذه الدعامة.

مما سبق ذكره، يتضح أنه لا خلاف حول سرقة الكيان المادي للنظام المعلوماتي والمستندات والمعلومات المعالجة بصفة عامة، إذا ما تم تحويلها إلى عناصر مادية، لكن الخلاف ينصب حول سرقة المعلومات الإلكترونية التي تتخذ دعامة لها المستند الإلكتروني سواءً أكانت موجودة داخل النظام المعلوماتي، أو على الوسائط المساعدة [2].

لا بد من التنويه إلى أن جريمة السرقة لا تقع بالنسبة للمستندات الإلكترونية، ولا على المعلومات الواردة بها إلا إذا تبث صفة المال عليها.

في سياق البحث حول مدى اعتبار المعلومات مالاً خاضعا للسرقة ينقسم الفقه إلى إتجاهين: الأول يجعل المعلومات الإلكترونية غير قابلة لأن تكون محلا للسرقة، كون أن وصف المال لا ينطبق عليها، في حين يعتبرها الإتجاه الثاني مالا يمكن سرقته، ويبرر الإتجاه الأول الذي يتزعمه بعض من الفقه الجنائي[3] موقفه بسبب أن المعلومات لا تندرج ضمن الأشياء، في حين أن جرائم المال لا تحمي إلا المنقولات، وهذه الأخيرة لا تكتسب هذه الصفة إلا إذا كانت من الأشياء، هذا بالإضافة إلى أن جرائم السرقة تقع عدواناً على الحيازة، كما وقد تقع على الملكية في حين يصعب تصور حيازة المعلومة لأن لها كيان معنوي، والحيازة غير متصورة إلا بالنسبة للأشياء التي يقع عليها الاتصال المادي[4].

---

[1]- عفيفي كامل عفيفي، المرجع السابق، ص. 120.

[2]- آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص. 15؛
Daniel Martin, Fréderic Paul Martin, op. cit, p.176.

[3]- السيد عتيق، جرائم الإنترنت، دار النهضة، مصر، 2000، ص. 88؛ آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص.42.

[4]- أحمد عاصم عجيلة، المرجع السابق، ص. 282.

وعليه ينتهي هذا الاتجاه إلى أن المعلومات والمستندات الإلكترونية لا يتحقق فيها وصف المال بالمعنى المتداول عليه، وأن تسميتها بالأموال المعلوماتية لا يتعدى فهمه على أنها قابلة للاستغلال المالي[1].

هذا عن الإتجاه الأول، أما الاتجاه الثاني (وهو الراجح) فهو يرى أن المستندات الإلكترونية وما تتضمنه من معلومات مالاً يمكن أن يكون محلاً للسرقة، وحجتهم في ذلك أن المعلومات المعالجة أو البيانات بوصفها كيانات منطقية أصبحت من القيم الاقتصادية المستحدثة[2]، نتيجة للتطور الذي حدث في مجال تقنية المعلومات الذي أعطى الأموال المعنوية قيمة اقتصادية قد تفوق قيمة الأموال المادية[3].

وعليه تعتبر المعلومات أموالاً لأنها قيمة اقتصادية، تطرح للتداول شأنها شأن أي سلعة أخرى، كما وأن لها سوقا تجاريا يخضع لقوانين السوق الاقتصادية[4].

زيادة على ذلك فإن تطور تكنولوجيا الحاسبات واستخدامها في مجال التجارة، رفع من قيمة المعلومات وجعل لها قيمة اقتصادية مثلها مثل أي سلعة، وهو ما دفع جانبا من الفقه للقول بأنها مال، لوجود حق استئثاري عليها يرتب حقوقا لصاحبها ناهيك عن أنها قابلة للانتقال، وقد لجأ الفقه في ذلك إلى معيار القيمة الاقتصادية للشيء. كون أن القانون إذا لم

---

[1]- يفرق بعض الفقه بين المعلومات والبيانات التي تمت معالجتها إلكترونيا، فيرون أن الأولى باعتبار أن عنصرها الأساسي هو الدلالة لا الدعامة التي تجسدها، لها طبيعة غير مادية ولا سبيل من تم إلى اختلاسها وسرقتها، أما البيانات التي تمت معالجتها إلكترونيا، فتتحدد في كيان مادي يتمثل في نبضات أو إشارات إلكترونية يمكن تخزينها على وسائط معينة ونقلها واستغلالها وإعادة إنتاجها، فضلاً عن إمكانية تقديرها كماً وقياساً فهي إذاً ليست شيئاً معنوياً كالحقوق والآراء والأفكار، بل شيء له في العالم الخارجي المحسوس وجود مادي. مشار إليه من طرف، آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص. 19.

[2]- محمد زهير محمد أبو العز، جرائم الكمبيوتر في مجال البنوك، مجلة البحوث القانونية والإقتصادية، دورية- علمية- محكمة، كلية الحقوق، جامعة المنصورة، ع الثامن والأربعون، أكتوبر 2010، ص.743.

[3]- وهو موقف كل من "P.Catala, Carbonnier". مشار إليه من طرف، محمد سامي الشوا، الحماية الجنائية للكيانات المنطقية "برامج الحاسب الآلي"،المرجع السابق، ص.155؛ آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص، ص .17- 18.

[4]- يعود الفضل في إضفاء وصف القيمة على المعلومة إلى كل من الأستاذين (CATALA وVIVANT)، ويستند الأول إلى أن المعلومة ترتبط بمؤلفها عن طريق علاقة قانونية تتمثل في علاقة المالك بالشيء الذي يملكه، بينما يستند الثاني إلى أن كل الأشياء المملوكة ملكية معنوية والتي يعترف بها القانون ترتكز على الاعتراف بأن للمعلومة قيمة؛
- للاطلاع أكثر على حجج الأستاذين يراجع، عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص،ص. 526- 527؛
Daniel Martin, Frederic Paul Martin, op .cit, p179.

يسبغ صفة المال على الأشياء ذات القيمة الاقتصادية فإنه يعد قانوناً منفصلاً عن الواقع كما ذهب إليه الأستاذ (Carbonnier).[1]

إلى جانب هذين الإتجاهين، يوجد إتجاه يربط بين الطبيعة المالية للمعلومات وبين الكيان المادي لها، فهو يرى أن المال المعلوماتي المعنوي لا يمكن أن يكون شيئا ملموسا أو محسوسا، ولكن يمكن أن يكون له كيان مادي يمكن رؤيته على الشاشة مترجم إلى أفكار ومعلومات، متنقلة عبر أسلاك عن طريق انتقال نبضات أو رموز تمثل شفرات يمكن حلها إلى معلومات معينة لها أصل صادرة عنه وهذا الكيان المادي يمكن سرقته[2].

إضافة إلى ما سبق، فإن الفقه الحديث يرى أن التشريعات في موضع النص على السرقة سواء في نص المادة 311 فقرة 01 من قانون العقوبات الفرنسي أو المادة 311 من قانون العقوبات المصري[3] أو المادة 350 من قانون العقوبات الجزائري، لم يذكر مصطلح المال ولم يحدد طبيعته سواءً أكان مادياً أو معنوياً، فمثلاً كلمة شيء الواردة بالنص العقابي الفرنسي والجزائري وكلمة منقول الواردة بالنص المصري، وردت بالعموم بحيث تسمح بإدراج الأشياء، أو المنقولات المادية وغير المادية أي المعنوية كالمستندات الإلكترونية وما تضمنه من معلومات، وهو الأمر الذي أخذ به الفقه الراجح للقول بصلاحية الأموال المعنوية كالمستندات الإلكترونية لأن تكون محلاً للسرقة[4].

أما بالنسبة لطبيعة المنقول في مجال المعلوماتية فقد اعتبر بعض الفقه أن المعلومات ليست منقولا، وأن المعلومات المخزنة سواءً بالنظام المعلوماتي أو على وسيط لا تعتبر في حد ذاتها أشياء مادية، وعليه فإنه لا يتصور انتزاعها وحيازتها، كما ولا يعقل أن تكون

---

[1]- آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص. 18.

[2]- أحمد خليفة الملط، المرجع السابق، ص. 240.

[3]- تنص المادة 311 من قانون العقوبات المصري رقم 58 لسنة 1938 طبقا لآخر تعديلات سنة 2018 على أنه: «كل من اختلس منقولاً مملوكاً لغيره فهو سارق».

[4]- من أمثلة السرقة المعلوماتية قضية سرقة برنامج Windows 95 قبل خروجه للعامة ،وظهور نسخ منه تباع بسعر أقل بكثير من سعره الحقيقي في بلجيكا ولكسمبورغ، حيث كان البرنامج المذكور قد شرع في بيعه، واكتشفت الشرطة الجنائية في بلجيكا أن نسخاً مزيفة من هذا النظام موجودة في هولندا وقد بلغ مقدار تلك النسخ500 ألف نسخة أصلية وضعت للاختبار التجاري الذي إستخدمه المتخصصون في مراحل التأليف المختلفة.

Cf, Daniel Martin, la criminalité informatique, cybercrime, sabotage, piratage, etc. évolution et repression, puf, 1998, p. 28.

محلاً للسرقة، غير أن هذا الرأي أُنتقد لأن المعلومات منقول وتصلح لأن تكون محلاً للسرقة خاصة وأن كلمة شيء -كما تم ذكره سابقا- الواردة في التشريعين الفرنسي والجزائري تشمل الأشياء المادية وغير مادية، وأن المعلومات كما يمكن حيازتها فإنه يمكن سلب حيازتها بالسرقة[1].

زيادة على ذلك فإن الاستيلاء على المعلومة يمكن أن يتحقق عن طريق السمع والمشاهدة، ومن ثم فإن المعلومة يمكن أن تنتقل من عقل إلى آخر، وفي هذه الحالة يمكن صب المعلومة في إطار مادي، عن طريق تحييزها داخل إطار والاستئثار به، وهذا الأمر الذي يتحقق عند تسجيلها على دعامة ثم يتم عرضها للبيع[2].

مما سبق ذكره، يخلص الفقهاء إلى أن المستند الإلكتروني وما يتضمنه من بيانات ومعلومات إلكترونية يصلح أن يكون محلا لجريمة السرقة[3].

ولئن كان هذا هو محل السرقة في مجال المستندات الإلكترونية، فما هو الركن المادي لهذه الأخيرة؟.

---

[1]- أحمد خليفة الملط، المرجع السابق، ص. 243.

[2]- عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص. 535.

[3]- ذهب بعض الفقه إلى قياس سرقة المستندات الإلكترونية على سرقة التيار الكهربائي، وذلك من حيث مدى إمكانية تطبيق النصوص الخاصة بسرقة الكهرباء على سرقة المعلومات المبرمجة آليا، غير أن الرأي الراجح في الفقه ذهب إلى عدم صحة قياس اختلاس المعلومات على اختلاس الكهرباء، وحجتهم في ذلك أن الرأي الذي يرى صلاحية قياس اختلاس المعلومات المبرمجة آلياً على اختلاس الكهرباء قد وجه إليه النقد من ناحيتين: فمن الناحية العملية يغفل هذا الرأي وجود حالات كثيرة يتم فيها الحصول على المعلومة المبرمجة دون أن يقتضي ذلك استعمالاً لكهرباء الغير، ومن ذلك على سبيل المثال، إذا ما قام الفاعل بقراءة القرص الممغنط بواسطة حاسب آلي محمول خاص به، ثم قيامه بتخزين المعلومات في ذاكرة هذا الحاسب دون الحاجة إلى استخدام الكهرباء، لأن الفاعل يمكنه شحن الحاسب المحمول الخاص به في منزله على سبيل المثال. ومن الناحية القانونية فإن هناك عقبة قانونية تحول دون تطبيق النصوص الخاصة بسرقة الكهرباء في هذه الحالة، ذلك أن الركن المعنوي لجريمة سرقة الكهرباء يتخذ صورة القصد الجنائي، وذلك بأن يعلم المتهم أن الكهرباء التي يقوم باستخدامها هي في ملكية غيره وحيازته، وأن ذلك يتم بغير رضاء المجني عليه، وهو ما لا يتحقق في حالة الحصول غير المشروع على المعلومات، فإرادة الفاعل لم تتجه حتماً إلى سرقة التيار الكهربائي، بل اتجهت إلى الحصول على المعلومات المخزنة، وهو ما يحول دون توافر عناصر القصد الجنائي، وبالتالي دون تحقق الركن المعنوي للجريمة. مشار إليه من طرف، أحمد عاصم عجيلة، المرجع السابق، ص، ص. 274- 275- 276؛ عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، المرجع السابق، ص. 439.

البند الثاني: الركن المادي لجريمة سرقة المستند الإلكتروني.

بما أن السرقة هي اختلاس مال منقول مملوك للغير بنية تملكه، فإن الركن المادي فيها يتشكل بتوافر فعل الاختلاس[1]، وهو يبدأ عادة بفعل مادي يتمثل في نقل الشيء أو أخذه أو نزعه من مالكه متضمناً تغييراً في الحيازة القانونية لهذا الشيء، وهو ما يقتضي أن يكون الشيء بطبيعته مادياً[2].

هذا ويعرف الاختلاس في جريمة السرقة بأنه الاستيلاء على الحيازة الكاملة للشيء بعنصريها المادي والمعنوي بغير رضاء مالكه أو حائزه[3]، كما عرفته محكمة النقض المصرية في ذات المفهوم السابق واعتبرته الاستيلاء على الشيء المسروق استيلاءً تاماً يخرجه من حيازة صاحبه ويجعله في قبضة السارق وتحت تصرفه[4].

ومن ثم فإن فعل الاختلاس يقتضي نقل حيازة المال موضوع الاختلاس أو السرقة من حيازة المجني عليه إلى الجاني، بمعنى أن يظهر الجاني بوصفه صاحب السلطة والسيطرة الفعلية[5]، كما لا يهم الوسيلة التي يتحقق بها الاستيلاء على الشيء محل السرقة ما دام الجاني يصل في النهاية إلى استبدال حيازة جديدة بحيازة كانت قائمة[6].

وعليه يشترط لتحقق فعل الاختلاس في جريمة السرقة ضرورة توافر عنصرين أحدهما موضوعي والثاني معنوي، حيث يتمثل العنصر الموضوعي للاختلاس في الاستيلاء على الحيازة على نحو يشكل إخراج الشيء من حيازة المجني عليه وإدخاله في حيازة

---

[1]- عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص.558.

[2]- نايل نبيل عمر، الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتية، دراسة في المحل الالكتروني المسبوغ بالحماية القانونية وبحث المفردات المشمولة بالرعاية وآلية التطبيق في القانون المصري والمقارن، دار الجامعة الجديدة، الإسكندرية 2012، ص، ص. 68-69.

[3]- عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، ط2، دار النهضة العربية، القاهرة، 2002، ص. 261.

[4]- نقض جنائي جلسة 07 مارس سنة 1998، مجموعة أحكام النقض، س 49، رقم 50، ص 358. مشار إليه من طرف، أحمد عاصم عجيلة، المرجع السابق، هامش ص.277.

[5]-عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، المرجع السابق، ص.445.

[6]- لم تهتم غالبية التشريعات بوسيلة الاستيلاء على الحيازة أو كيفيتها فكل ما يشترط فيها أن تكون بفعل الجاني، فالاستيلاء على الحيازة يمكن أن يكون فعلياً كما لو اتخذ الاستيلاء صورة الأخذ أو الانتزاع أو النقل، كما يمكن أن يكون حكميا كإلتقاط الشيء الضائع و حبسه بنية التملك، وإذا كان الاستيلاء على الحيازة فعليا فليس بشرط أن يكون الجاني قد استعمل أعضاء جسمه في أخذ الشيء أو نقله أو انتزاعه، كما يكفى أيضا لتحقيق الإستيلاء على الحيازة أن يهيئ الجاني أسباب إنتقال حيازة المال لديه دون تدخل منه لحظة انتقالها. مشار إليه من طرف: عبد الله حسين علي محمود، المرجع السابق، ص. 262

أخرى[1]، في حين يتمثل العنصر المعنوي للاختلاس في عدم رضاء المالك أو الحائز للشيء عن فعل الاختلاس الذي ارتكبه الجاني[2].

وبما أننا بصدد الحديث عن فعل الاختلاس وعناصره في نطاق المعلوماتية، فإن التساؤل يثار حيال مدى انطباق التعريف السابق بعنصريه على المستندات الإلكترونية وما تتضمنه من بيانات ومعلومات؟

بدايةً، يمكن القول أنه وبعد أن اتضح أن الإتجاه الراجح يؤكد أن المستندات المعالجة آليا يمكن أن تكون محلا للإختلاس إذا ما تم وضعها والتعامل بها عن طريق نسخها والإطلاع عليها بالبصر أو ما يطلق عليه الإلتقاط الذهني، وذلك بسبب أن فعل الإختلاس يضر بالقيمة الإقتصادية لها، فإنه ينبغي الذكر أن فكرة الإستيلاء التي تعتبر العنصر الموضوعي المكون للركن المادي محققة الوجود[3] .

ولعل ما ينبغي ذكره أن الإتجاه الفقهي السابق يعتبر أن فكرة الاستيلاء الاحتيالي كنقل ونسخ المعلومات هي إحدى صور التفسير الواسع للاختلاس، وهو الأمر الذي أكدته محكمة الإستئناف الفرنسية في قضية بوركان (bourquin) حينما أدانت عاملا بتهمة السرقة لقيامه بالنسخ الفوتوغرافي للمستندات التي كان قد إستولى عليها عن طريق الإحتيال[4].

---

[1]- عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص. 559.

[2]- إذا أخرج شخص شيئا من حيازة مالكه أو حائزه برضائه فإن جريمة السرقة لا تقوم لانتفاء الاختلاس ،لأن المالك أو الحائز في هذا الغرض يكون قد رضي بالتخلي أو التنازل عن حيازة الشيء. وإذا توافر الرضا من جانب مالك الشيء فلا تقوم السرقة حتى ولو كان ناقل الحيازة غير عالم بهذا الرضا، هذا ويشترط في الرضاء أن يكون سابقاً أو معاصراً لنقل الحيازة. مشار إليه من طرف: عبد الله حسين علي محمود، المرجع السابق، ص. 263.

[3]- يراجع في ذلك، ص. 235 وما يليها من هذه الأطروحة؛ مشار إليه كذلك من طرف، محمد زهير محمد أبو العز، المرجع السابق، ص. 748.

[4]- تتلخص وقائع هذه القضية في قيام مبرمج كان قد ترك عمله في إحدى الشركات إلى شركة أخرى، بزيارة للشركة الأولى التي كان يعمل بها وقام بتصوير مستندات تتعلق بالعملاء الأثرياء الذين يعملون مع الشركة لنفسه على مطبعة الشركة، وقام بأخذ شرائط أخرى نسخها بمعرفته في مطبعته بهدف إنشاء شركة منافسة، فحكمت عليه محكمة الاستئناف بالحبس شهراً مع إيقاف التنفيذ تطبيقا للمواد الخاصة بعقوبات تهمة السرقة، وإلى جانب هذه القضية فقد قضت محكمة النقض الفرنسية في قضية أخرى بإدانة شخص عن جريمة إخفاء أشياء مسروقة، لأنه مع علمه بالوقائع تلقى من أحد العمال معلومات تتعلق بسر التصنيع (secret de fabrication)، حيث علل هذا الحكم العقوبة التي قررها كون أن الإخفاء قد انصب في هذه الحالة على المعلومات ذاتها. مشار إليه طرف، عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص، ص. 564- 565؛ آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، هامش ص. 38.

وبهذا يمكن القول أن المعلومات الواردة في المستندات الإلكترونية يمكن أن تكون محلا لفعل الإختلاس، و يتحقق هذا الأمر بإستيلاء الجاني على المستند الإلكتروني المخزن على جهاز الحاسب الآلي لغيره و إخراجه من حيازة صاحبه لإدخاله في حيازته، وذلك عن طريق نقله خلسة إلى جهازه الشخصي أو إلى أي وسيط مادي له سيطرة مادية عليه، على أن يتم هذا كله بغير رضاء صاحب المستند الإلكتروني[1].

البند الثالث: الركن المعنوي لجريمة سرقة المستند الإلكتروني.

وفقاً للقواعد العامة فإن السرقة من الجرائم العمدية التي لا يكتفي القول بتوافرها مجرد توافر الركن المادي، وإنما يجب أن يتوافر إلى جانبه ركنا معنويا، و صورة الركن المعنوي في هذه الجريمة هو القصد الجنائي، الذي يقصد به اتجاه إرادة الجاني إلى ارتكاب الجريمة مع العلم بكافة عناصرها القانونية[2]، ولا يُكتفى في هذه الجريمة بالقصد العام بعنصري العلم والإرادة، بل يشترط إضافة إلى ذلك وجود قصد جنائي خاص يتمثل في ضرورة توافر نية التملك، تلك النية التي عبر عنها المشرع الفرنسي بكلمة (frauduleusement) أي نية الغش.

وجريمة سرقة المستند الإلكتروني وما يتضمنه من بيانات شأنها شأن جريمة السرقة عموما، بحيث تتطلب هي الأخرى لقيامها إلى جانب الركن المادي ركنا معنويا يتمثل في توافر القصد الجنائي العام والقصد الجنائي الخاص.

وللإشارة فإن القصد العام في جريمة سرقة المستندات الإلكترونية يقوم هو الآخر على عنصرين -شأنه في ذلك شأن القصد العام في ضوء القواعد العامة- وهما العلم والإرادة، بحيث يجب أن تتجه إرادة الجاني إلى الاستيلاء على المعلومات المسجلة إلكترونياً، وهي المعلومات التي خضعت لعملية المعالجة الآلية أو المعلومات المخزنة داخل النظام المعلوماتي أو المعلومات المسجلة إلكترونيا والمخزنة على دعامة خارجية مثل

[1]- أحمد عاصم عجيلة، المرجع السابق، ص. 277.
[2]- بلال أمين زين الدين، جرائم نظم المعالجة الآلية للبيانات في التشريع المقارن والشريعة الإسلامية، دار الفكر، الإسكندرية، 2008، ص. 117؛ ناير نبيل عمر، المرجع السابق، ص. 73.

الأسطوانات والشرائط الممغنطة والتي تتخذ المستندات الإلكترونية دعامة لها، مع علمه بأن المعلومات محل السرقة ليست ملكاً له[1].

وعليه لا يتحقق القصد العام بعنصريه العلم والإرادة إلا في حالة إتجاه إرادة الجاني إلى الإستحواذ على المعلومات محل السرقة مع علمه بملكية غيره لها، ومن تم فإن عدم توفر عنصر الإرادة في الفعل ينفي تحقق القصد الجنائي، فمن يقوم مثلا بأخذ أسطوانة من صاحبها بدون علمه لمعرفة البرنامج المسجل عليها، ثم يعيدها إلى صاحبها لا تتوافر لديه نية الاختلاس[2].

هذا عن القصد العام، أما القصد عن الخاص في جريمة سرقة المستندات الإلكترونية وما تتضمنه من بيانات فيتمثل في إتجاه نية الجاني إلى الإستيلاء على المعلومات الإلكترونية، بحيث يضيفها إلى ملكه و يظهر فيها بمظهر المالك[3].

وفي هذا الإطار يرى إتجاه فقهي أن القصد الخاص في هذه الجريمة، والذي يتمثل في نية التملك لا يتوافر في حالة قراءة المعلومات من خلال الشاشة أو سماعها من خلال سماعات، وكذا في حالة إلتقاط الإشعاعات التي تمثل معلومات، ذلك أن الجاني في مثل هذه الحالات لم يقصد حرمان صاحبها منها بصفة دائمة أو مؤقتة، وإنما شاركه الانتفاع بها والاطلاع عليها، وفي هذا يقترح هذا الإتجاه الفقهي ضرورة إيجاد نصوص عقابية خاصة

---

[1]- عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص. 609.

[2]- زيادة على ذلك فقد اعتبر بعض الفقه أن سحب العميل مبالغ تجاوز رصيده من جهاز التوزيع الآلي للنقود لا يعتبر سرقة على أساس أن التسليم الذي تم بواسطة الجهاز المنفذ لأوامر الصيرفي - يعني أن البنك فتح اعتمادا تلقائيا لمصلحة العميل لاعتقاد الأخير بأن المبلغ المسحوب الزائد عن رصيده ملكاً له، فهو على هذا النحو لا يتوافر لديه القصد الجنائي- والحل الذي طرحه البعض يتمثل في الربط بين هذه الأجهزة وبين حسابات العملاء، وفي هذه الحالة لن تقوم الأجهزة بصرف أوراق البنكنوت إلى العميل إلا في حدود الرصيد الذي يوجد في حسابه وقت السحب، وهو ما يجري به العمل حالياً في نظام السحب من أجهزة التوزيع الآلي للنقود. مشار إليه من طرف، جميل عبد الباقي الصغير، الحماية الجنائية والمدنية للبطاقات الإلكترونية الممغنطة، دار النهضة العربية، 1999، ص. 56.

[3]- بخصوص نية التملك نجد أن القضاء الفرنسي قد اكتفى بنية التملك المؤقتة لقيام القصد الخاص لجريمة السرقة في نطاق المعلوماتية، حيث قضت محكمة النقض الفرنسية في إحدى أحكامها بأنه: «يرتكب سرقة الشخص الذي استولى - بمناسبة تأدية واجبات وظيفته- على مستندات مملوكة للشركة التي يعمل بها وقام بنسخها لأغراض شخصية». وفي هذا الحكم نجد أن محكمة النقض الفرنسية قد اكتفت بتوافر نية التملك المؤقتة والتي من خلالها قام القصد الجنائي الخاص بالسرقة، وتحققت تلك النية منذ سلب حيازة المستندات خلال الوقت اللازم لإعادة نسخها بدون إرادة صاحب المشروع، الأمر الذي يعني بمفهوم المخالفة أن المحكمة في هذا الحكم لم تشترط توافر نية التملك المؤبدة لدى الجاني.

Crime, 1ère, mars 1989, J.C.P.

مشار إليه من طرف، عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص. 612.

لمواجهة الحالات الإجرامية الخطيرة التي يخشى إفلات الجاني فيها من العقاب لعدم إمكانية متابعة مقترفيها بنصوص جريمة السرقة [1].

الفرع الثاني: العقوبات المقررة لجريمة سرقة المستند الإلكتروني.

إذا كان المستقر عليه فقهاً أن المعلومات الواردة بالمستندات الإلكترونية تكيف على أنها مال وتخضع لجرائم الاعتداء على الأموال بما فيها السرقة، فما مدى قدرة النصوص العقابية التقليدية على توفير الحماية الفعالة لهذا المال في حال الاعتداء عليه بالسرقة[2]؟

لا ريب في أن هذا السؤال يطرح بسبب صعوبة تطبيق النصوص العقابية التقليدية على سرقة المعلومات المسجلة إلكترونيا والمخزنة بواسطة الحاسب الآلي، وذلك بسبب أن تلك النصوص وُضعت لمواجهة صور التعدي المألوفة على الأشياء المادية، بحيث يصعب تصور تطبيق العقوبات الواردة بها على أفعال التعدي الماسة بعناصر ومكونات النظم المعلوماتية ذات الطابع المعنوي، خاصة وأن تطبيق تلك النصوص قد يتعارض مع الطابع الخاص للوسائل المعلوماتية المستحدثة لتنفيذ الجريمة[3].

لمجابهة هذا الوضع عمدت النصوص العقابية للتشريعات المقارنة إلى إصدار تشريعات خاصة بالغش المعلوماتي، لتغطي العديد من أفعال التعدي التي استحدثتها تقنيات نظم المعلومات، وذلك بصرف النظر عن النصوص التي كانت موجودة من قبل والتي يمكن تطبيقها على بعض أفعال التعدي المستحدثة، ولعل من أولى تلك التشريعات القانون الفرنسي المتعلق بالغش المعلوماتي[4]، هذا وإتجهت دول أخرى إلى تنقيح النصوص الواردة بقانون العقوبات بما يتلائم والسمات المستحدثة لأساليب ارتكاب الجريمة ومن ذلك التشريع الجزائري.

[1]- خليفي مريم، المرجع السابق، ص. 208؛ عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص، ص. 612- 613.
[2]- السيد عتيق، المرجع السابق، ص. 94.
[3]- عبد الله حسين علي محمود، المرجع السابق، ص. 306.
[4]- Loi Godfran du 5 janvier 1988, ou Loi n°88-19 du 5 janvier 1988 relative à la fraude informatique.

لأهمية هذه المسألة سيتم التعرض إلى العقوبات المقررة في التشـــريع الفرنسي **(البند الأول)**، وبعدها للعقوبات المقررة في التشريع الجزائري **(البند الثاني)**.

البند الأول: العقوبة المقررة في التشريع الفرنسي.

لا شك أن المشرع الفرنسي كان دائما سباقا لمواجهة التحديات الجديدة التي أفرزتها المعلوماتية ويظهر ذلك جليا بأن أصدر سنة 1978 القانون الخاص بحماية البيانات الاسمية للمواطنين[1] في مواجهة نظم المعالجة الآلية للمعطيات والمعلومات، والذي بموجبه أكد على أن المعلوماتية يجب أن تكون في خدمة الفرد وليست وسيلة للاعتداء على الشخصية الإنسانية ولا على حق الإنسان وحياته الخاصة وحريته الفردية أو العامة[2].

ولم يكتف المشرع الفرنسي بهذا القدر بل تدخل مرة أخرى - تأكيداً لموقفه في مواجهة الجرائم المعلوماتية المستحدثة- بإصداره القانون رقم 19 الصادر في 05 يناير 1988 بشأن الغش المعلوماتي[3]، والذي جرم بموجبه الوصول بطريق التحايل إلى نظام المعالجة، وإستحدث فيه لفظ المستندات المعلوماتية (documents informatisés) عند تعرضه لجريمة تزوير المستندات المعالجة آلياً، كما وتطرق لبعض صور التعدي التي يمكن أن تطال النظم المعلوماتية بما فيها المستندات وما تحويه من بيانات ومعلومات.

لكن للأسف الشديد لم ينص هذا القانون على تجريم سرقة البرامج والمعلومات وكذا المستندات الإلكترونية[4]، بالرغم من أنه قد نص على غيرها من الجرائم التي تمثل إعتداءا على الأموال والأشخاص، ويتضح هذا جليا من خلال نص المادة 311 من قانون العقوبات

---

[1]- قانون رقم 17-78 الصادر في 06 يناير سنة 1978 المتعلق بحماية البيانات الإسمية للمواطنين.

[2]- عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص. 616.

[3]- عبد الله حسين علي محمود، المرجع السابق، ص. 309.

[4]- حاول المشرع الفرنسي في مشروع تعديل قانون العقوبات النص على تجريم سرقة المال المعلوماتي (من معلومات وبرامج ومستندات إلكترونية)، وذلك من خلال نص المادة 307 الفقرة 01، حيث استعمل مصطلح يتناسب مع الموضوع ويعبر عن الاختلاس وهو مصطلح الإلتقاط (Capter) فقرر أن كل من التقط بطريق الاختلاس والتحايل برنامج أو معلومة أو أي عنصر من عناصر نظام المعالجة الآلية للبيانات يعاقب بالحبس ثلاث سنوات وغرامة مقدارها 100.000 ألف فرنك، إلا أنه لم يوافق عليها في تعديل القانون الصادر في 5 يناير 1988 أو تعديله الصادر عام 1994 والمتعلق بالجرائم المعلوماتية. مشار إليه من طرف، أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص. 617 .

والتي لم يتطرق فيها المشرع الفرنسي لسرقة المعلومات والبرامج، وكذا المستندات الإلكترونية.

أمام هذا الفراغ التشريعي فإنه كان من الضروري على المشرع الفرنسي التدخل بنصوص قانونية تجرم سرقة المستندات الإلكترونية و المعلومات الواردة بها، ذلك أن هذه الجريمة أضحت من أخطر الجرائم في البيئة الرقمية، خاصة أنه كما سبق الذكر كان سباقا لمواجهة الجرائم المعلوماتية، والواقع أن هذا الأمر لا يخص المشرع الفرنسي فحسب، بل يشمل بعض التشريعات اللاتينية التي سارت على نهجه، ومن ذلك المشرع السويدي المشرع والدنماركي[1].

وعليه كان على المشرع الفرنسي أن يحذو حذو التشريع الأمريكي فيجرم سرقة المعلومات والمستندات المعلوماتية، وذلك حتى يكون للقضاء الفرنسي إمكانية تطبيق العقوبات المقررة لجريمة السرقة مثلما فعل القضاء الأمريكي، والذي قررت فيه محكمة تكساس في القضية المعروفة بإسم (Hancock v.Texas) تطبيق نصوص جريمة السرقة آخذة بعين الإعتبار القيمة المالية للمعلومات المحملة في الأسطوانات لا قيمة الأسطوانات التي سجلت عليها المعلومات[2].

هذا وينبغي التنويه إلى أن بعض الولايات الفيدرالية أصدرت قوانين تتبنى بموجبها المفهوم الموسع للمال بحيث يشمل كل شيء ينطوي على قيمة مالية، بما في ذلك الأموال

[1]- لم يشر القانون السويدي والقانون الدنماركي إلى مسألة سرقة المعلومات والمستندات الإلكترونية، وقصروا حماية نظم المعالجة الآلية في فعل الولوج فقط دون التطرق لفعل السرقة ،حيث ينص المشرع السويدي في المادة 21 من القانون رقم 289 الصادر في 3 أفريل سنة 1973 الخاص بالبيانات على أن: «يعاقب... كل من ولج بوسائل غير مشروعة إلى سجل مخصص لمعالجة البيانات آليا». أما في الدنمارك فإنه طبقا للمادة 263 من قانون أول يوليه 1985 يعد من قبيل الجرائم فعل الولوج في نظم المعالجة الآلية للمعلومات أو البرامج المخزنة في هذه النظم. مشار إليه من طرف، عبد الله حسين علي محمود، المرجع السابق، ص، ص. 308- 309؛ هدى حامد قشقوش، المرجع السابق،، ص. 48.

[2]- تتلخص وقائع هذه القضية في قيام أحد العاملين السابقين في شركة (Texas Instruments Automatic Computer Corp) بسرقة كمية من أسطوانات الكمبيوتر وبيعها إلى إحدى الشركات المنافسة، وبعد ما قدم كل من الأطراف حججهم رفضت المحكمة حجة المدعى عليه، والمتمثلة في أن قانون ولاية تكساس يعاقب على سرقة الأشياء المملوكة إذا بلغت خمسين دولار، وأن الجريمة تبعا لذلك لم تتوفر لأن قيمة الشرائط التي سجلت عليها المعلومات لا تساوي أكثر من خمسة وثلاثين دولار،و قد بررت المحكمة رفضها كون أن القيمة الحقيقية للبضائع المسروقة لا تتمثل في الأسطوانات وإنما فيما تحويه من معلومات، هذا ويلاحظ أن المحكمة إعتبرت أن سرقة الأسطوانات المُحمل عليها المعلومات تُعد إستيلاء على أحد حقوق الملكية في معناها الدقيق، وعليه أسست المحكمة حكمها على اعتبار أن سرقة الشرائط المحمل عليها المعلومات تعتبر استيلاء على حق من حقوق الملكية بالمعنى الدقيق. مشار إليه من طرف، عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص، ص. 628- 629.

المادية، والأموال المعنوية كالمعلومات المسجلة إلكترونياً سواء كانت مخزنة داخل النظام أو على دعائم خارجية، هذا وتعاقب هذه القوانين على الاستخدام غير المسموح به بغرض ارتكاب أفعال الغش أو الاستيلاء على المال[1].

البند الثاني: العقوبة المقررة في التشريع الجزائري.

بداية فإنه ينبغي الذكر أن المشرع الجزائري و عند تعديله لقانون العقوبات و تجريمه للأفعال الماسة بالمعالجة الآلية للمعطيات لم يتطرق بنص صريح لجريمة السرقة التي تطال البيانات والمعلومات الإلكترونية المخزنة داخل الحاسب الآلي والتي تتخذ دعامة لها المستندات الإلكترونية رغم أنه تعرض للعديد من الأفعال التي يمكن أن تطال أنظمة المعالجة الآلية للمعطيات، وكذا البيانات والمعلومات الإلكترونية شأن أفعال الدخول والبقاء عن طريق الغش، التخريب، الإتلاف والإتجار غير المشروع بالمعطيات المخزنة والمعالجة آليا، وفي ظل هذا الوضع ينبغي الرجوع إلى الحكم الوارد في المادة 350 من قانون العقوبات والتي عدلت بموجب القانون رقم 06-23[2] حيث جاء فيها بأنه: «كل من إختلس شيئاً غير مملوكا له يعد سارقاً، ويعاقب بالحبس من سنة إلى خمس سنوات وبغرامة من 100.000دج إلى 500.000 دج، تطبق العقوبة على اختلاس المياه والغاز والكهرباء».

إذا كانت العقوبات المقررة في المادة آنفة الذكر تطبق على جرائم السرقة الواقعة على الأموال الملموسة، فهل يجوز تطبيقها على سرقة البيانات والمعلومات الإلكترونية التي تتخذ من المستندات الإلكترونية دعامة لها؟.

بالرجوع إلى المادة 350 من قانون العقوبات، يلاحظ أن المشرع الجزائري لم يشترط لتطبيق أحكام هذه المادة أن يكون المال محل السرقة ماديا، وهو الأمر الذي دفع الفقه الراجح إلى التأكيد على أن وقوع جريمة السرقة على مال معنوي لا يصطدم بمبدأ شرعية الجريمة والعقوبة، ولكن مع ذلك يمكن القول أن عدم إيراد المشرع الجزائري بشكل صريح لفظ البيانات والمستندات الإلكترونية المخزنة داخل الحاسب الآلي في المادة 350 من

[1]- عبد الله حسين علي محمود، المرجع السابق، ص. 325.
[2] - قانون 06-23المؤرخ في 20 ديسمبر 2006 المتضمن تعديل قانون العقوبات الجزائري، سابق الإشارة إليه.

قانون العقوبات، وذلك بخلاف ذكره لكل من مصطلح الماء، الغاز، الكهرباء يجعله يتبنى ذات نهج المشرع الفرنسي.

وعليه فإنه لا يمكن تطبيق نص المادة 350 من قانون العقوبات على سرقة البيانات والمستندات الإلكترونية لأنها لم تتضمن أي عبارة صريحة توحي بذلك، ولا شك أن مثل هذا الأمر يحدث نوعا من الفراغ التشريعي.

لئن كان هذا هو موقف المشرع الجزائري في العشرية الأولى من سنة ألفين ، فإنه ينبغي الذكر أنه ظل على موقفه في العشرية الثانية، بحيث أنه لم يورد في قانون التوقيع والتصديق الإلكترونيين نصا يجرم سرقة المعلومات الإلكترونية، واكتفى بتجريم الأفعال الماسة بالتوقيع و التصديق الإلكترونيين .

أمام هذا الوضع فإنه يتوجب على المشرع الجزائري تدارك النقص والتدخل على وجه السرعة لسد الفراغ التشريعي بإيراده لنص صريح وواضح سواءا في قانون العقوبات أو نص مستقل يجرم فيه سرقة البيانات والمستندات الإلكترونية، وذلك لما لهذه الجريمة من أهمية وخطورة على نظم المعلومات وعلى سلامة وأمن المعاملات الإلكترونية، كما عليه أن يقوم بتعديل نص المادة 350 من قانون العقوبات بحيث تشمل إلى جانب السرقة التقليدية السرقة المعلوماتية، وهو ما لا يتقرر إلا بجعل فعل الاختلاس ينصب على الأشياء المادية وغير المادية.

المبحث الثاني: الأعمال الماسة بخصوصية المستند الإلكتروني.

لقد خلف إستخدام التقنيات الحديثة في التعامل آثاراً إيجابية لا يستطيع أحد إنكارها، خاصة في مجال التبادل الإلكتروني للبيانات.

غير أن تكريس مبدأ الثقة في التعاملات الإلكترونية، وتجسيد فكرة التخلي عن الدعامة الورقية، وإستبدالها بالدعامة الإلكترونية لا يتأتى إلا بتوفير حماية فعالة وتأمين شامل للمستندات الإلكترونية، وما تتضمنه من بيانات رقمية.

كما ويستوجب الأمر الحفاظ على خصوصية وسرية البيانات المعالجة آلياً من أي تدخل غير مشروع قد يضر بمصلحة المتعاملين في هذا المجال[1].

والمقصود بالخصوصية في المجال المعلوماتي أن يكون الدخول والإطلاع على للمعلومات والبيانات الإلكترونية التي تتخذ دعامة لها المستند الإلكتروني، مخصصا لشخص معين أو مجموعة من الأشخاص دون غيرهم لِما يثبت لهم من سلطة التصرف في هذه المعلومات أو البيانات والاستئثار بها، وبمعنى أدق يقصد بالخصوصية إرتباط البيانات والمعلومات بأطراف المعاملة الإلكترونية (المتعاقدين) من بائعين ومشترين أو منتجين ومستهلكين[2]، بحيث يُمنع إطلاع الغير عليها كما ويمنع كل تطفل أو دخول غير مشروع في هذه المستندات وكشف ما تتضمنه من بيانات وأسرار.

ولما كانت الكتابة والتوقيع الإلكتروني عناصر للمستند الإلكتروني فإنه ينبغي بالضرورة حمايتهما من كل اعتداء أو تخريب، ذلك أن الاعتداء على المعطيات الإلكترونية التي يتضمنها المستند يشكل جرائم ينبغي التصدي لها ، وهو ما عمدت إليه القوانين الحديثة بحيث جرمت الدخول غير المشروع، البقاء غير المشروع، إفشاء البيانات الإلكترونية، وكذا المساس بالتواقيع الإلكترونية .

[1] -Cf. Daniel Martin, la criminalité informatique ,op. cit, p .68.

[2]- محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، الهيئة المصرية العامة للكتاب، مصر، 2003، ص. 176.

لأهمية المسائل السالف ذكرها سيتم التعرض للأفعال الأعمال الماسة بخصوصية المستند الإلكتروني، وذلك بدءاً بتبيان الأفعال الماسة بالمعطيات الإلكترونية التي يتضمنها المستند من دخول و بقاء غير مشروعين **(المطلب الأول)**، ثم التعرض للأفعال الماسة بسرية المستند الإلكتروني **(المطلب الثاني)**، يليها فيما بعد التطرق للأفعال الماسة بالتوقيع الإلكتروني، وذلك لاعتبار هذا الأخير العنصر الثاني للمستند بعد الكتابة الإلكترونية **(المطلب الثالث)**.

المطلب الأول: الأعمال الماسة بالمعطيات الإلكترونية التي يتضمنها المستند.

لقد أدى ربط الحاسبات الآلية بعضها بالبعض الآخر عن طريق شبكات المعلومات إلى سرعة انتقال المعلومات من جهة، وإلى سهولة التطفل عليها من جهة أخرى، بحيث أضحى بإمكان المتطفلين الولوج إلى أنظمة المعلومات، وقواعد البيانات وكذا الدخول إلى المستندات الإلكترونية وما تحويه من بيانات دون ترك أي أثر يدل على انتهاك المعلومات[1].

ونظرا لخطورة الأفعال الماسة بالبيانات الإلكترونية ومساسها بالأفراد والشركات عمدت التشريعات إلى تجريم الدخول بطريق الغش لنظم المعالجة الآلية للمعطيات[2]، والتي يسرت عليها الوصول إلى البيانات المحفوظة في المستندات الإلكترونية **(الفرع الأول)**، كما وجرمت فعل البقاء في تلك الأنظمة إذا كان الغرض منه التطفل والعبث في البيانات والمعلومات المحفوظة في المستندات الإلكترونية **(الفرع الثاني)**.

[1]- محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، المرجع السابق، ص،ص. 176-177.

[2]- يقصد بنظام المعالجة الآلية للمعطيات كل مركب يتكون من وحدة أو مجموعة وحدات معالجة، والتي تتكون كل منها من الذاكرة والبرامج والمعطيات وأجهزة الإدخال والإخراج وأجهزة الربط، والتي تربط بينها مجموعة من العلاقات والتي عن طريقها تتحقق نتيجة معينة، وهي معالجة المعطيات على أن يكون هذا المركب خاضع لنظام الحماية الفنية. مشار إليه من طرف، خثير مسعود، المرجع السابق، ص، ص .108- 109؛ زيادة على ذلك فقد ورد تعريف له ضمن نص المادة الثانية من الاتفاقية الدولية للإجرام المعلوماتي التي أبرمت بتاريخ 2001/11/08 من طرف المجلس الأوروبي على النحو التالي:
-"Système informatique désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données."

الفرع الأول: جريمة الدخول غير المشروع إلى معطيات المستند الإلكتروني.

لقد سبق الذكر أن توفير الحماية الفعالة للمستندات الإلكترونية وما تحويه من بيانات ومعلومات دفع بعض التشريعات إلى تجريم الدخول غير المشروع (أو غير المصرح به) إلى المعلومات والبيانات المخزنة بواسطة نظم المعالجة الآلية للمعلومات[1].

ونظراً لحداثة هذه الجريمة في مجال البيئة المعلوماتية، فقد أثارت جدلاً فقهيا واسعا بحيث تعددت الآراء بشأنها، وعلى هدى ما تقدم سيتم التطرق إلى هذه الجريمة من خلال بيان الركن المادي **(البند الأول)**، وكذا الركن المعنوي **(البند الثاني)**، كما سيتم تحديد العقوبات المقررة لها **(البند الثالث)**.

البند الأول: الركن المادي للجريمة.

تقوم جريمة الدخول غير المشروع لمعطيات المستند الإلكتروني أو إلى البيانات والمعلومات الإلكترونية المخزنة بواسطة نظم المعالجة الآلية للبيانات بعدة أفعال، وأساس هذه الأفعال الدخول[2] غير المشروع إلى معلومات إلكترونية مخزنة بواسطة نظام المعالجة الآلية للمعطيات، سواء أكان هذا الدخول في النظام المعلوماتي كله أو في جزء منه فقط[3]، ومن ثم فإن الدخول أو الولوج المشروع في النظام المعلوماتي لا يشكل جريمة، ذلك أن وجه التجريم في الفعل يكمن في الدخول إلى النظام بدون وجه حق، بحيث يكون الإتصال بطريق الغش، وعليه يمكن القول أن عدم مشروعية الدخول تستمد في هذه الحالة في كونه غير مصرح به[4].

---

[1]- من التشريعات التي جرمت فعل الدخول غير المشروع للبيانات المخزنة بواسطة نظم المعالجة الآلية للمعطيات التشريع العقابي الفرنسي مثلاً، والتشريع العقابي الألماني، وكذلك قانون الحاسبات الآلية الانجليزي الصادر عام 1990، وكذا القانون البرتغالي لجرائم المعلوماتية لعام 1991، وقانون العقوبات الدنماركي، وكذا القانون الفيدرالي لإساءة استخدام الحاسبات الآلية في الولايات المتحدة الأمريكية...الخ، هذا بالنسبة للتشريعات الأجنبية أما بالنسبة للتشريعات العربية فنجد مثلاً القانون المصري وكذا القانون الجزائري. مشار إليه من طرف، أحمد عاصم عجيلة، المرجع السابق، ص. 301.

[2]- المعنى اللغوي لكلمة دخول يعني النفاذ وإختراق مكان مادي، وهذا المعنى لا يمكن تطبيقه بشأن الدخول إلى أنظمة المعالجة الآلية للمعطيات ذلك أنه لا يمكن الدخول إلى هذه الأنظمة لاعتبارها ظاهرة غير مادية، وعليه يعد مصطلح الولوج أكثر دقة في مجال المعلوماتية من مصطلح الدخول، وما يؤكد ذلك أن المشرع الفرنسي قد استعمل مصطلح "accès" بدلا من "entrée " لأنه أكثر ملائمة في هذا المجال. مشار إليه من طرف، محمد خليفة، المرجع السابق، ص.141.

[3]- فائزة يونس الباشا، المرجع السابق، ص.22.

[4]- تقوم هذه الجريمة سواء تم الدخول إلى النظام كله أو إلى جزء منه فقط، كما تتوافر هذه الجريمة في حالة ما إذا دخل الجاني إلى جزء من النظام المسموح له بالدخول إليه، ليستغل الفرصة ويدخل إلى جزء آخر غير مسموح له بالدخول إليه، بشرط أن يكون العنصر الذي تم الدخول إليه يدخل في برنامج متكامل قابل للتشغيل، وعليه لا تتوافر الجريمة إذا تم=

وعن مفهوم فكرة الدخول (La notion d'accès) في هذا المجال فإنه ينصرف ليشمل كافة الأفعال التي تسمح بالولوج إلى النظام المعلوماتي، وهو يتحقق بالوصول إلى المعلومات والبيانات المخزنة داخل نظام الحاسب دون رضاء المسؤول عنه، وذلك للسيطرة على المعلومات التي يتكون منها أو الإحاطة بالخدمات التي يقدمها[1].

والمقصود بالدخول هنا ليس الدخول بالمعنى المادي كالدخول إلى منزل أو حديقة أو الدخول إلى مكان وجود الحاسب الآلي، بل إن فعل الدخول المقصود هنا الدخول بمعناه المعنوي أي الدخول الذي ينطوي على نشاط ذهني يقوم به الفاعل في ذاكرة النظام المعلوماتي[2]، ويشبه الدخول في هذه الحالة الدخول إلى ذاكرة الإنسان أو ملكة التفكير لدى الفرد، وهو يفترض إقامة اتصال مع النظام المعلوماتي من قبل شخص غير مرخص له بذلك[3]، وعليه فإن قيام هذه الجريمة تفترض أن الدخول إلى البيانات يجب أن يكون غير متاح للجمهور،بحيث يكون مقصوراً على عدد محدود من الأشخاص أو الهيئات[4].

ووفقا لهذا المعنى الأخير فإن الولوج إلى النظام المعلوماتي يتحقق بأية صورة من صور التعدي سواء تم ذلك بطريقة مباشرة أو غير مباشرة[5]، ومن تلك الصور استعمال كلمة السر الخاصة بشخص مسموح له بالدخول، وتتحقق هذه الصورة ولو كان المعني بالأمر

=الدخول إلى عنصر لا علاقة له بنظام المعالجة الآلية للمعطيات مثل الدخول إلى البرنامج منعزلاً عن غيره من العناصر، كما لا تتوافر الجريمة أيضاً في الحالة التي يقتصر فيها الشخص على مجرد قراءة الشاشة. مشار إليه من طرف، علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، المرجع السابق، ص. 121.

[1]- خليفي مريم، المرجع السابق، ص. 171.

[2]- نائلة عادل فريد قورة، المرجع السابق، ص. 332.

[3]- عمر محمد بن يونس، نطاق الجريمة الإفتراضية، (تفسير الدخول والتصريح به في إطار تشريعات الإساءة إلى الحاسوب)، ط1، د.د.ن، د.ب.ن، 2005، ص.ص. 64-65؛ آمال قارة، الجريمة المعلوماتية، المرجع السابق، ص .42؛ Béatrice Clément, Gérard Clément, Frédérique Dubost, Jean- Philippe Vincentini, fiches de droit pénal spécial, ellipses édition, Paris, 2012, p. 266.

[4]- مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، ط1، دار النهضة العربية، القاهرة، 2012، ص. 50.

[5]- نتيجة لظهور التقنيات المتطورة والفائقة الدقة والتي لها صلة بالنظام المعلوماتي فقد نشأت بالمقابل إمكانات مستحدثة للدخول أو الولوج للنظام المعلوماتي والبيانات الإلكترونية بواسطة نظم المعالجة الآلية وقد يأخذ الدخول الأشكال الآتية:

أ- توصيل خطوط تحويلية لإلتقاط المعلومات المتواجدة ما بين النظام المعلوماتي والنهاية الطرفية، وإرسال المعلومات المختلسة إلى النهاية الطرفية عن طريق إشارات إلكترونية.

ب- تسجيل ثم حل شفرة الإشعاعات الإلكترومغناطيسية المثبتة بواسطة أجهزة إلكترونية لإلتقاط الإشعاعات الصادرة عن النظام المعلوماتي ،ومثال ذلك قيام شخص باختلاس أموال عن طريق التقاط أمر بتحويل مرسل من بنك إلى آخر بعدما تمكن من تزييف الرسالة بأمر دفع نفس المبلغ لحساب قام بفتحه باسمه.

ج- الولوج غير المشروع عن طريق نهاية طرفية بعيدة، عن طريق نظام معلوماتي ومعرفة كلمة السر أو مفتاح الشفرة المناسب. مشار إليه من طرف، أحمد خليفة الملط، المرجع السابق ، ص. 192.

على علم بدخول الطرف الآخر طالما أن المعني بالأمر لايملك حق منح الترخيص بالدخول[1]، ولا يقتصر الأمر على هذه الصورة بل يتعداها ليشمل إستعمال الجاني برنامج متطور يسمح له بالدخول إلى النظام كإستعماله برنامج حصان طروادة[2] مثلا، هذا ويمكن تحقق فعل الدخول عن طريق إستعمال الجاني لكلمة السر الحقيقية طالما أنه لا يملك حق إستخدامها، أو باستخدام برنامج أو شفرة خاصة، أو عن طريق استخدام الرقم السري لشخص آخر، أو عن طريق التوصل إلى الرقم السري للدخول، أو عن طريق تجاوزه لنظام الحماية الموجود في النظام[3]، وبهذا يمكن القول أن وسيلة الدخول غير الشرعي إلى النظام لا تهم، إذ الذي يهم هو ولوج الجاني النظام بطريقة غير مرخص له بها.

هذا ويعد فعل الدخول أو الولوج جريمة وقتية تقع من أي شخص، بحيث يستوي أن يكون هذا الأخير خبيرا أو فرداً عادياً، كما و تقوم الجريمة سواء كان الغرض من الدخول القيام بعمل غير مشروع أو لمجرد الفضول و حب الإستطلاع، ويستوي في قيامها الإستفادة من الدخول من عدمه[4]، وعليه يكفي لقيام هذه الجريمة أن يكون الجاني ممن ليس لديهم الحق في الدخول، أو ممن ليس لهم الحق في الدخول بالطريقة التي دخلوا بها.

هذا وتقوم هذه الجريمة في كل حالة يكون فيها الدخول مخالفاً لشروط الدخول المنصوص عليها قانوناً أو المنصوص عليها اتفاقاً، أو ضد إرادة من له حق السيطرة على النظام[5]، كأن يكون الدخول يتطلب إلزاما دفع مبلغ من النقود[6] للولوج إلى النظام المعلوماتي المعلوماتي ونسخ ملفات منه، وتم الدخول دون دفع المبلغ.

---

[1]- علي عبد القادر القهوجي، الحماية الجنائية لبرامج لبرامج الحاسب الآلي، المرجع السابق، ص. 50.

[2] - Cf. Béatrice Clément, op. cit, p.266.

[3]- حطاب كمال، المرجع السابق، ص. 78.

[4]- مدحت عبد الحليم رمضان، المرجع السابق، ص. 51؛

Frédéric-Jérome Pensier et Emmanuel Jez, op .cit, p.114.

[5]- آمال قارة، الجريمة المعلوماتية، المرجع السابق، ص. 43؛ حطاب كمال، المرجع السابق، ص. 79.

[6]- هناك من يرى أن جريمة الدخول غير المصرح به لا تقوم في حالة الدخول إلى نظام معين دون دفع ثمن الاشتراك. ويبرر ذلك بأن تجريم الدخول غير المصرح به يهدف إلى حماية المعلومات من الوصول إليها من قبل أشخاص ليس لهم الحق في ذلك وهي حماية لسرية المعلومات، ولا يتحقق ذلك في حالة الدخول مع عدم سداد الثمن لأن هذا الشرط إنما هو شرط تنظيمي للدخول إلى النظام الذي يعد في هذه الحالة مصرحاً بالدخول من قبل أي شخص سدد الثمن المطلوب مقابل هذا الدخول، فالمعلومات التي تحتوي عليها تتمتع بالسرية في مواجهة البعض، وهي المصلحة التي يحميها القانون في جريمة الدخول غير المصرح به. مشار إليه من طرف، محمد خليفة الملط ، المرجع السابق، ص. 145.

ولئن كان الهدف من تجريم الدخول غير المشروع هو منع اقتحام النظام الآلي لمعالجة المعلومات، فهل ينبغي لقيام هذه الجريمة أن يترتب على الدخول نتيجة إجرامية من خلال الوصول إلى المعطيات والبيانات المحفوظة في المستندات الإلكترونية التي يحتوي عليها النظام، أم أن الجريمة تتم بمجرد هذا الدخول بغض النظر عن الوصول إلى هذه المعطيات؟.

يتجه الرأي الراجح إلى أن قيام جريمة الدخول غير المشروع لا تستلزم نجاح الجاني في الوصول إلى المعلومات و البيانات الإلكترونية، بحيث يكفي الدخول المجرد إلى النظام، فعلى الرغم من أن العلة من تجريم الدخول إلى النظام تكمن في الحفاظ على المستندات الإلكترونية والمعلومات الواردة بها ومنع التلاعب بها، إلا أن هذه الجريمة من جرائم العدوان المحتمل على الحق، وليس من الجرائم التي ينبغي أن يتحقق فيها العدوان على الحق المحمي قانونا[1].

زيادة على ذلك فإن أغلب التشريعات التي جرمت الدخول غير المصرح به إلى نظم المعلوماتية تذهب إلى العقاب على فعل الدخول المجرد، ولو لم يترتب على هذا الدخول ضرر، وكذا إذا لم تتحقق الفائدة المرجوة من هذا الدخول غير المشروع[2]، ومن ثم فإن الركن المادي لهذه الجريمة يتكون من السلوك الإجرامي فقط، ولا يتطلب علاقة سببية، فجريمة الدخول من جرائم الخطر لا جرائم الضرر.

البند الثاني: الركن المعنوي للجريمة.

يعتبر الركن المعنوي أمراً ضرورياً لقيام جريمة الدخول غير المصرح به إلى المعلومات والبيانات الإلكترونية المخزنة بواسطة نظم المعالجة الآلية للمعطيات، لا سيما وأن الأفعال التي تقوم بها هذه الجريمة قد أضحت شائعة الحدوث، وبات يكررها الكثير من

[1]- نائلة عادل محمد فريد قورة، المرجع السابق، ص. 343.

[2]- من بين التشريعات التي أخذت بالرأي المتقدم كل من التشريع الفرنسي، اليوناني، البرتغالي، الفنلندي، السويدي، في حين توجد تشريعات أخرى تتطلب لقيام جريمة الدخول غير المصرح به للنظام الوصول إلى المعلومات التي يتضمنها النظام المعلوماتي، ومن هذه التشريعات تشريع الولايات المتحدة الأمريكية والتشريع الأسترالي. مشار إليه من طرف، خليفي مريم، المرجع السابق، ص. 173.

مستخدمي الحاسبات الآلية، وبناءً على ذلك فإن عمليات الدخول إلى الأنظمة المعلوماتية لا يمكن أن تجرم إلا إذا تحقق بشأنها القصد الجنائي.

ويتخذ الركن المعنوي لهذه الجريمة صورة القصد الجنائي العام، وذلك لاعتبارها من الجرائم العمدية، وللإشارة فإن الركن المعنوي لهذه الجريمة لا يتحقق إلا إذا توفر كل من عنصري العلم والإرادة[1]، بمعنى أن يعلم الجاني أن ليس له الحق في الدخول إلى النظام المعلوماتي وأن هذا الولوج غير مصرح به، ورغم ذلك تتجه إرادته إلى الاعتداء على الحق الذي يحميه القانون.

ولئن كانت التشريعات تعتبر هذه الجريمة من الجرائم العمدية، إلا أنها تختلف في العبارات التي تستخدمها للتعبير عن هذا الغرض، بحيث يعبر المشرع الفرنسي عن القصد العام بإستلزامه حصول الدخول إلى النظام بطريق الغش والخداع "frauduleusement"، واستخدام هذه العبارة في المادة 323-1 فقرة 01 من قانون العقوبات الفرنسي[2] يعني أن الفاعل على علم بأن دخوله إلى النظام المعلوماتي غير مصرح به[3].

هذا ويستلزم القانون الدنماركي قيام الفاعل بالدخول غير المصرح به إلى النظام على نحو مخالف للقانون[4]، كما ويتطلب كل من القانون السويسري والبرتغالي والأمريكي حصول الدخول إلى النظام بدون تصريح[5]، بل إن القانون السويدي واليوناني يتطلب حدوث

---

[1]- زيبحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى للطباعة والنشر، الجزائر، 2011، ص.119؛ شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2007، ص. 126.

[2]- Art 323-1 Al 1 du c.p.fr (Modifié par Loi n°2015-912 du 24 juillet 2015-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… ».

[3]- Cf. Christiane Feral -Schuhl, Cyber Droit, le droit a l'épreuve de l'internet, dalloz, paris, 2011-2012, p .916.

[4]- حيث يجرم قانون العقوبات الدنماركي الدخول غير المصرح به إلى المعلومات والبرامج التي يتم تخصيصها للاستعمال داخل نظام المعالجة الآلية للمعلومات، ويتسع النص لتجريم الدخول إلى شبكات المعلومات، والأفعال التي تنطوي على اعتراض المعلومات التي يمكن أن تنجم عن هذا الدخول. مشار إليه من طرف، أحمد عاصم عجيلة، المرجع السابق، ص، ص. 310- 311؛ نائلة عادل محمد فريد قورة، المرجع السابق، ص. 364.

[5]- صدر في الولايات المتحدة الأمريكية القانون الفيدرالي في شأن الاعتداء على الكمبيوتر واستغلاله Computer Fraud and Abuse act في عام 1984 وعدل في أعوام 1986 و1994 و1996، وتجرم المادة 1030/أ من القانون الفيدرالي الأمريكي إساءة استخدام الحاسبات الآلية للحصول على المعلومات عن طريق الدخول غير المصرح به إلى الحاسبات=

الدخول إلى الأنظمة المعلوماتية بدون وجه حق، أما القانون الانجليزي فيشترط أن يتم الدخول إلى النظام على نحو غير مصرح به مع العلم بذلك[1].

هذا عن الأنظمة الغربية، أما بالنسبة للمشرع الجزائري، فيلاحظ أنه جرم فعل الدخول إلى أنظمة المعالجة الآلية للمعطيات واعتبر هذه الجريمة عمدية متى تم الدخول إلى نظام المعالجة الآلية بطريق الغش وهو ما يفهم من عبارة: «كل من يدخل عن طريق الغش» الواردة في نص المادة 394 مكرر من قانون العقوبات.[2]

وعن عنصر العلم الواجب توافره لدى الجاني لقيام هذه الجريمة فإنه بالرجوع إلى المبادئ العامة للقصد الجنائي، يتوجب على الجاني أن يعلم بكل واقعة لها أهميتها في تكوين الجريمة، بحيث يشمل علمه أركان الجريمة مع إدراكه لعناصرها، وللإشارة فإن نطاق هذا العلم لا يقتصر على مجموع الوقائع التي تدخل في تكوين الجريمة، بل يتعداه إلى التكييف الذي تتصف به وتكتسي به أهميتها في نظر القانون[3].

وبتطبيق ما تقدم من مبادئ عامة على جريمة الدخول غير المشروع إلى البيانات الإلكترونية المخزنة بواسطة نظم المعالجة الآلية للمعطيات، فإنه ينبغي على الجاني أن يدرك ويعلم بجميع عناصر الركن المادي للجريمة لكي يتوافر القصد الجنائي لديه، أي يجب أن يعلم بأنه يدخل إلى نظام معلوماتي يحتوي على مستندات إلكترونية لا يجوز له الدخول إليها، ولعل من القرائن الدالة على توافر القصد إستخدام وسائل الخداع في الدخول غير المشروع، كما لو كان الدخول إلى النظام يتطلب شفرة أو بطاقة معينة ويقوم الجاني بسرقة هذه البطاقة أو بفك تلك الشفرة[4].

=الآلية، كما تجرم المادة 1030/ أ (3) الدخول إلى الحاسبات الآلية التابعة للحكومة الفيدرالية أو تلك التي يؤدي الدخول غير المصرح به إليها إلى المساس بأعمال تتعلق بالحكومة. مشار إليه من طرف، رشدي محمد علي عيد، المرجع السابق، ص. 307؛ نائلة عادل فريد قورة، المرجع السابق، ص.315.

[1]- نائلة عادل محمد فريد قورة، المرجع السابق، ص ص. 364- 365.

[2]- يلاحظ أن المشرع الجزائري قد استعمل نفس العبارة التي استعملها المشرع الفرنسي في نص المادة 323-1 فقرة 01 من ق.ع.ف.

[3]- نائلة عادل محمد فريد قورة، المرجع السابق، ص. 365؛ محمود نجيب حسني، النظرية العامة للقصد الجنائي- دراسة تأصيلية مقارنة للركن المعنوي في الجرائم العمدية-، ط3، دار النهضة العربية، القاهرة، 1988، ص. 51.

[4]- أحمد عاصم عجيلة، المرجع السابق، ص. 307؛ جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، ط1، دار النهضة العربية، القاهرة، 1992، ص. 151.

هذا ويجب على الجاني أن يعلم أن فعل الدخول ينصب على النظام المعلوماتي بما يتضمنه من بيانات ومعلومات ومستندات إلكترونية على اعتبار أن المستندات الإلكترونية المحفوظة داخل نظام المعالجة الآلية هي محل الحق المعني بالحماية.

زيادة على ما سبق، فإن فكرة القصد الجنائي لا تقتصر على العلم بالوقائع فقط، بل تتطلب العلم بإكتساب بعض هذه الوقائع تكييفا معيناً -كما سبق ذكره- فبعض الجرائم لا تقتصر عناصرها على وقائع مجردة من التكييف، بل يعد التكييف الذي تكتسبه هذه الوقائع من بين عناصرها الأساسية، وفي مثل هذه الجرائم يكون للتكييف ذات الأهمية القانونية التي تكون للوقائع في ماديتها، ولما كان القصد الجنائي يتطلب علماً محيطاً بكل عناصر الجريمة، فهو يتطلب حتما انصراف العلم إلى التكييف كما يتطلب إحاطته بالوقائع، فالتكييف عنصر في الجريمة، وبدونه ينتفي أحد أركانها، وتصبح الواقعة التي تجردت من هذا التكييف غير ذات أهمية في تكوين الجريمة، وعليه ينبغي أن يشمل علم الجاني هذا التكييف كي يتوافر القصد الجنائي[1].

وبتطبيق ما سبق على جريمة الدخول غير المشروع يتوجب أن يعلم الجاني أن دخوله إلى النظام المعلوماتي الذي يحتوي على مستندات إلكترونية غير مسموح به، وأن عدم وجود التصريح يكف لتحقق واقعة الدخول غير المشروع إلى النظام المعلوماتي، وعلى الجاني أن يكون على علم بذلك، بحيث إذا إنتفى هذا العلم أعتبر القصد الجنائي في هذه الجريمة غير متوافر[2].

هذا عن عنصر العلم، أما عن عنصر الإرادة الواجب توافره لدى الجاني لقيام الجريمة فيراد به أن يتوقع الجاني عندما يقوم بالفعل الإجرامي النتيجة التي سوف تترتب عن هذا الفعل، وعليه يعتبر توقع النتيجة الأساس النفسي الذي تقوم عليه الإرادة، ذلك أنه حين لا يكون التوقع لا تتصور الإرادة[3]، فالجاني لا يسأل عن الجريمة إلا بعد إثبات اتجاه إرادته إلى فعل يمثل إتيانه خطراً على الحق الذي يحميه القانون[4].

---

[1]- نائلة عادل محمد فريد قورة، المرجع السابق، ص. 368.
[2]- نائلة عادل محمد فريد قورة، المرجع السابق، ص. 368؛ خليفي مريم، المرجع السابق، ص. 180.
[3]- نائلة عادل محمد فريد قورة، المرجع السابق، ص 366؛ محمود نجيب حسني، المرجع السابق، ص. 65.
[4]- خليفي مريم، المرجع السابق، ص. 180.

وفي الجريمة محل الدراسة تكمن النتيجة الذي يجب أن يتجه إليها توقع الفاعل في دخوله غير المصرح به إلى نظام معلوماتي يحتوي على مستندات إلكترونية، ولا يشترط أن يتجه التوقع إلى الآثار غير المباشرة التي لا يدخلها القانون في تحديد النتيجة، فالقصد الجنائي يتوافر ولو لم يتوقع الجاني هذه الآثار[1]، وعليه يتعين أن يتوقع الجاني أنه سوف يدخل إلى نظام معالجة آلية غير مصرح له بالدخول إليه دون أن يتوقع الضرر الذي سوف يلحق بالنظام، أو الذي سوف يمس المستندات المخزنة فيه من جراء هذا الدخول[2].

زيادة على ذلك فإنه لا عبرة بالباعث أو الغاية من وراء ارتكاب فعل الدخول غير المشروع إلى الأنظمة المعلوماتية[3]، ذلك أنهما لا يعتبران من عناصر القصد الجنائي، فسواء كانت الغاية من الدخول إلى النظام المعلوماتي الحصول على الكسب المادي، أو كشف أوجه القصور في أنظمة الحماية الفنية للنظام المعلوماتي، أو إثبات الجاني لقدرته العامة في اختراق أي نظام معلوماتي، فإن ذلك لا يحول دون القول بإتجاه الإرادة لتحقيق النتيجة الإجرامية والمتمثلة في الدخول بطريق غير مشروع إلى النظام المعلوماتي الذي يحتوي على مستندات إلكترونية[4].

إلى جانب القصد العام الواجب توافره لقيام الركن المعنوي للجريمة محل الدراسة تتطلب بعض التشريعات وجود قصد جنائي خاص، ويترتب على إستلزام تحقق هذا القصد التشديد في العقوبة، مثلا يشدد القانون الدنماركي من عقوبة الدخول غير المشروع إلى نظام

---

[1]- في جريمة الدخول غير المشروع لمعطيات المستند الإلكتروني لا يشترط تحقق الضرر أو تحقق نتيجة لقيام الركن المعنوي للجريمة، فالقانون يعاقب على مجرد الدخول متى كان هذا الولوج غير مشروع، فهذه الجريمة كما سبق وأن أوضحنا عند دراسة الركن المادي لهذه الجريمة أنها تعتبر من جرائم الخطر لا الضرر. يراجع في ذلك، ص. 255 من هذه الأطروحة.

[2]- نائلة عادل محمد فريد قورة، المرجع السابق، ص. 366.

[3]- الباعث هو المولد للقوة المحركة التي تدفع الإرادة إلى العمل المجرم، ويختلف باختلاف الجرائم وقد يختلف في الجريمة الواحدة، فيكون هو السعي لتحقيق الربح أو الرغبة في قهر النظام أو مجرد إشباع الفضول إلى غير ذلك من البواعث، أما الغاية فهي الغرض النهائي الذي يرمي إليه الجاني من ارتكابه الجريمة، وهي كالباعث قد تختلف في الجريمة الواحدة، وقد تتمثل في إلحاق أضرار بنظام المعلوماتية للشركة المنافسة أو لصاحب النظام المعلوماتي. مشار إليه من طرف، خليفي مريم، المرجع السابق، ص. 181.

[4]- تطبيقا لذلك قضي بوقوع الجريمة من مهندس للكمبيوتر أراد أن يثبت لأحد البنوك قدرته الفنية على إختراق أنظمة البنك حتى يفوز بعقد تدريب كوادر البنك، بحيث قام بغرض الإلتحاق بالمنصب باختراق أنظمة من البنك على الرغم من تعدد وسائل الحماية التي وضعها هذا الأخير ضد الاختراق، ففكك جهازا إلكترونيا كان البنك قد استغنى عليه، وللإشارة فإن المخترق تمكن من القيام بعملية الإختراق والتعرف على البيانات المسجلة في الجهاز بعد حصوله على الجهاز من تاجر آخر. مشار إليه من طرف، شيماء عبد الغني محمد عطا الله، المرجع السابق، ص. 126.

المعالجة الآلية لمعطيات إذا ما حصل هذا الأخير بنية الإحاطة بمعلومات تتعلق بالأسرار المتعلقة بعمل إحدى الشركات، كما ويشدد القانون الأسترالي من العقوبة متى أُرتكب فعل الدخول غير المصرح به إلى نظام الحاسب الآلي بنية الإضرار بالغير، وبالمثل يشدد القانون النرويجي من العقوبة متى ارتكب فعل الدخول غير المصرح به بنية حصول الفاعل له أو للغير على ربح غير مشروع أو إلحاق ضرر بالغير نتيجة الاطلاع على المعلومات التي يحتوي عليها النظام، هذا ويتطلب القانون البرتغالي لجرائم المعلوماتية لعام 1991 في المادة 07 منه قصداً جنائياً خاصا، بحيث يعاقب كل من يقوم على نحو غير مصرح به بالدخول إلى أنظمة أو شبكات المعلومات، بنية الحصول له أو للغير على ربح أو فائدة غير مشروعة، على أن تشدد العقوبة متى كان الربح أو الفائدة مرتفعين بصورة كبيرة نسبياً[1].

وفي المملكة المتحدة يتضمن قانون إساءة استخدام الحاسبات الآلية لعام 1990 في مادته الثانية نصاً يجرم الدخول غير المصرح به متى توافر لدى الفاعل قصداً خاصا يتمثل في نية ارتكاب جريمة أخرى لاحقة على هذا الدخول[2].

البند الثالث: العقوبة المقررة للجريمة.

نظراً لخطورة جريمة الدخول غير المشروع إلى المعطيات المخزنة بواسطة نظم المعالجة الآلية، فقد إختلفت خطة التشريعات على المستويين الدولي والوطني في معالجتها بحيث تفاوتت من حيث النص على الركن المادي للجريمة، وكذا في تطلب قصد خاص فيها من عدمه ولم يقتصر الأمر على ذلك ، بل تعداه ليشمل العقوبة المقررة لها.

لأهمية هذه المسألة سيتم تحديد العقوبة المقررة لهذه الجريمة في ظل الإتفاقيات الدولية **(أولاً)**، وبعدها العقوبة المقررة لها في التشريعات الأجنبية والتشريع الجزائري **(ثانياً)**.

[1]- إنتقد الفقهاء النص البرتغالي لتضييقه على نحو كبير تطبيق جريمة الدخول غير المصرح به إلى الأنظمة المعلوماتية، ويرى البعض أنه لتفادي هذا التضييق يجب أن تفسر الفائدة التي يحصل عليها الفاعل من وراء دخوله إلى النظام لتشمل كل فائدة ذهنية أو معنوية، وألا تقتصر على الفائدة والربح المادي. مشار إليه من طرف، نائلة عادل محمد فريد قورة، المرجع السابق، ص. 369.

[2]- المرجع نفسه، ص، ص. 369- 370.

أولاً: العقوبة المقررة للجريمة في ظل الاتفاقيات الدولية.

لقد حظيت الجريمة محل الدراسة باهتمام اتفاقية بودابست الخاصة بحماية المعلوماتية ومنع وقمع الإجرام المعلوماتي، بحيث أشارت إليها في المادة الثانية منها تحت اسم الولوج غير القانوني والتي ورد فيها: «يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من أجل اعتبارها جريمة جنائية، وفقا لقانونه الداخلي، للولوج العمدي لكل أو لجزء من جهاز الحاسب بدون حق، كما يمكن له أن يشترط أن ترتكب الجريمة من خلال انتهاك إجراءات الأمن، بنية الحصول على بيانات الحاسب أو أية نية إجرامية أخرى، أو أن ترتكب الجريمة في حاسب آلي يكون متصلاً عن بعد بحاسب آخر»[1].

هذا وقد أشارت المذكرة التفسيرية لهذه الاتفاقية أن الولوج غير القانوني يعد الجريمة الرئيسية التي تنطوي على تهديد وتعدٍ على أمن وحرية وسلامة النظم والبيانات المعلوماتية، ولخطورة هذه المسألة فإنه ينبغي توفير حماية ملائمة لمصالح المنظمات، وبالأخص لرجال الإدارة حتى يكون بمقدورهم إدارة، إستثمار، التحكم في نظمهم بدون تشويش أو عقبة من أي نوع، ولتحقيق ما سبق ذكره ينبغي إعتبار مجرد التدخل غير المصرح به بمعنى القرصنة أو السطو أو الدخول غير المشروع في النظام المعلوماتي فعل غير قانوني، وذلك على أساس أن مثل تلك الأفعال يمكن أن تخلق عقبات أمام المستخدمين الشرعيين للنظم والبيانات، كما يمكن أن تؤدي إلى إتلاف أو تدمير باهظ التكلفة في حالة إعادة البناء، بل ويمكن أن يترتب عليها الوصول إلى بيانات سرية (مثال ذلك كلمات المرور أو معلومات عن النظام المستهدف، أو أسرار تسمح باستخدام النظام مجانا)، خاصة وأن

[1]- Art 2 du convention sur la cybercriminalité: « Chaque partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans un autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique ».

الأفعال السابقة تشجع القراصنة على إرتكاب أكثر أنواع جرائم الحاسب الآلي خطورة كالغش المعلوماتي وماعداه من جرائم[1].

وإلى جانب اتفاقية بودابست لمكافحة الإجرام المعلوماتي، عمدت الإتفاقية العربية لمكافحة جرائم تقنية المعلومات[2] إلى تجريم الدخول غير المشروع للمعطيات الإلكترونية، بحيث إستلزمت المادة 06 منها ضرورة تجريم الدخول، وكل إتصال غير مشروع في كل أو جزء من تقنية المعلومات[3] أو الاستمرار به، كما اقترحت في الفقرة الثانية من هذه المادة ظرفين مشددين للجريمة تُشدد على إثرهما العقوبة، ويشمل الظرف المشدد الأول حالة ما إذا نجم عن الدخول أو الاتصال أو الاستمرار بهذا الاتصال محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير البيانات المحفوظة والأجهزة والأنظمة الإلكترونية وشبكات الاتصال، وإلحاق الضرر بالمستخدمين والمستفيدين، في حين يشمل الظرف المشدد الثاني حالة ما إذا نجم عن الأفعال السالف ذكرها الحصول على معلومة حكومية سرية[4].

ثانياً: العقوبة المقررة في التشريعات الأجنبية والتشريع الجزائري.

إلى جانب الاهتمام بالجريمة محل الدراسة على صعيد التشريعات الدولية، سعت التشريعات الأجنبية والوطنية إلى تنظيمها ومعالجتها بمقتضى نصوص قانونية، ومن بين

---

[1]- هلالي عبد الله أحمد، المرجع السابق، ص،ص. 49-51؛ فؤاد حسين العزيزي، المرجع السابق، ص. 261.

[2]- هذه الاتفاقية تم إبرامها في جامعة الدول العربية بحيث جاء في ديباجتها أن الدول العربية ورغبة منها في تعزيز التعاون فيما بينها لمكافحة جرائم تقنية المعلومات التي تهدد أمنها ومصالحها وسلامة مجتمعاتها، واقتناعا منها بضرورة الحاجة إلى تبني سياسة جنائية مشتركة تهدف إلى حماية المجتمع العربي ضد جرائم تقنية المعلومات، وأخذا بالمبادئ الدينية والأخلاقية السامية ،ولا سيما أحكام الشريعة الإسلامية، وكذلك بالتراث الإنساني للأمة العربية التي تنبذ كل أشكال الجرائم ومع مراعاة النظام العام لكل دولة، وأنه التزاماً بالمواثيق العربية والدولية المتعلقة بحقوق الإنسان ذات الصلة من حيث ضمانها واحترامها وحمايتها فإنه تم الاتفاق على مواد هذه الاتفاقية التي تتضمن تقريبا 43 مادة موزعة على خمسة فصول، حيث نصت في المادة الأولى أنه: «تهدف هذه الاتفاقية إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، لدرء أخطار هذه الجرائم حفاظاً على أمن الدولة العربية ومصالحها وسلامة مجتمعاتها وأفرادها». وللإشارة فإن هذه الاتفاقية حررت باللغة العربية بمدينة القاهرة في جمهورية مصر العربية بتاريخ 2010/12/21 ووافق عليها مجلس وزراء الداخلية والدول العرب في اجتماعهما المشترك المنعقد بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة بتاريخ 2010/12/21، هذا ولقد وقعت الجزائر على هذه الاتفاقية بالتاريخ ذاته.

[3]- تنص المادة 1/2 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، سابق الإشارة إليها: " تقنية المعلومات: أية وسيلة مادية أو معنوية أو مجموعة وسائل مترابطة تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها وفقاً للأوامر والتعليمات المخزنة بها ،ويشمل ذلك جميع المدخلات والمخرجات المرتبطة بها سلكيا أو لاسلكيا في نظام أو شبكة".

[4]- نص المادة 06 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، سابق الإشارة إليها.

هذه التشريعات المشرع الفرنسي الذي نص عليها في المادة 323-1 من قانون العقوبات لسنة 1994 بحيث جاء فيها أنه: «يعاقب على الدخول بطريق الغش داخل كل أو جزء من نظام المعالجة الآلية للبيانات بالحبس لمدة سنتين وبغرامة قدرها 20.000 أورو، وفي حالة ما إذا نجم عن الدخول محو أو تعديل في البيانات أو إتلاف نظم تشغيل هذا النظام تكون العقوبة الحبس لمدة ثلاث سنوات وغرامة قدرها 45000 أورو»[1]، هذا وقد قرر في المادة 323-4 من ذات القانون تطبيق العقوبات السابقة في حالة مساهمة أو إتفاق جماعة من الأشخاص على التحضير لعمل أو أعمال مادية لارتكاب جريمة أو أكثر من الجرائم السابقة.

وفي هذا يرى جانب من الفقه[2] أن المادة 323-4 السالفة الذكر تمثل خروجا عن القواعد العامة حيث عاقب فيها المشرع الفرنسي على الأعمال التحضيرية للجريمة، وهي الأعمال التي تسبق البدء في التنفيذ المادي لها، وقد تم الرد على هذا الإتجاه بحجة أن المشرع يمكنه الخروج على القواعد العامة بنص خاص متى كان بحاجة ملحة لذلك، وتكمن الحاجة في هذه الحالة في ضرورة توفير حماية وقائية لنظم المعالجة الآلية للمعلومات من كل إعتداء قد يقع عليها.

لعل ما يمكن ملاحظته على المواد السالف ذكرها أن المادة 323-1 من قانون العقوبات الفرنسي تتبنى المفهوم الموسع للدخول غير المشروع إلى أنظمة الحاسبات الآلية، حيث يشمل هذا الفعل الدخول غير المصرح به للمعلومات بسبب استخدام شبكة الأنترنت، وكذا الدخول للبيانات المخزنة بطريقة إلكترونية داخل النظام، والتي قد تكون مدرجة في

[1]- للإشارة فإن هذه المادة قد تم تعديلها سنة 2012 حيث تم رفع مبلغ الغرامة، بحيث جاء النص كالتالي.
Article 323-1 du Code Pénal modifié par loi n°2012-410 du 27 mars 2012 : « Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de donnés est puni de deux ans d'emprisonnement et de 30000 euros 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 45000 euros 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'état, la peine est portée à cinq ans d'emprisonnement et à 75000 Euros d'amende ».

[2]- علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، المرجع السابق، ص.53 وما يليها.

مستندات إلكترونية، ولهذا يمكن القول أن المشرع الفرنسي لم يتطلب وجود نشاط سابق على فعل الدخول غير المشروع داخل النظام[1].

هذا عن القانون الفرنسي، أما بخصوص القانون الانجليزي فيلاحظ أنه عاقب بموجب المادة الأولى من قانون إساءة استخدام الحاسبات الآلية الصادر عام 1990 (The Computer Misuse Act) على الدخول غير المصرح به إلى المعلومات والبرامج التي يحتوي عليها أي حاسب آلي، وقد ورد العقاب على ثلاثة أشكال من الدخول وهي؛ الدخول غير المشروع بدون قصد ارتكاب الجريمة، الدخول غير المشروع بقصد إرتكاب الجريمة، التعديل غير المشروع في مكونات الحاسب الآلي[2].

هذا وقد جرمت المادة 1030/ أ من القانون الفيدرالي الأمريكي الخاص بإساءة إستخدام الحاسبات الآلية الحصول على المعلومات بطريق الدخول غير المصرح به إلى الحاسبات الآلية، كما وجرم بموجب الفقرة 03 من ذات المادة على الدخول إلى الحاسبات الآلية التابعة للحكومة الفيدرالية، خاصة إذا ما ترتب عن الدخول إليها المساس بأعمال تتعلق بالحكومة[3].

إلى جانب التشريع الفرنسي والأمريكي والانجليزي عاقبت بعض التشريعات المقارنة على الدخول غير المشروع إلى المعلومات والبيانات المخزنة بواسطة نظم المعالجة الآلية للمعلومات، دون الإشارة إلى أنظمة الحاسب الآلي أو شبكات المعلومات كمحلين للدخول، ومن هذه التشريعات القانون السويدي والذي عاقب بموجب المادة 21 من قانون المعلوماتية لعام 1973 والمعدل سنتي 1986 و1990 على فعل الدخول غير المصرح به إلى أية معلومة مسجلة يتم إستخدامها من خلال نظم المعالجة الآلية للمعلومات.

---

[1]- علي عبد القادر القهوجي، الحماية الجنائية لبرامج لبرامج الحاسب الآلي، المرجع السابق، ص.54.

[2]- ظهرت عدة مشكلات في انجلترا من جراء تطبيق القانون المذكور وأهمها المشكلة الخاصة بتطبيق مفهوم الدخول الذهني "intellectual Access" فقد اشترط القانون الانجليزي أن يتم الدخول إلى أي من المعطيات أو البرامج التي يحتوي عليها الحاسب الآلي عن طريق نشاط ما استجابة لنشاط الفاعل، ذلك أن مجرد قراءة المعطيات على الشاشة غير كاف لتحقق الركن المادي. مشار اليه من طرف، أحمد عاصم عجيلة، المرجع السابق، ص. 315.

[3]- رشدي محمد علي عيد، المرجع السابق، ص. 307؛ أحمد عاصم عجيلة، المرجع السابق، ص، ص. 316- 317 .

وبمقتضى هذا النص فإن كل معلومة يتم تسجيلها على أي وسيط لتخزين المعلومات كالشرائط الممغنطة التي تشكل جزءاً من الحاسب الآلي ولا يمكن الوصول إليها إلا من خلال نظم المعالجة الآلية للمعلومات تعد محلاً يمكن أن ينصب عليه فعل الدخول غير المصرح به[1].

هذا ويجرم قانون العقوبات الفنلندي كل من يقوم باستخدام شفرة غير صحيحة أو يقوم بإختراق الإجراءات الأمنية للدخول إلى نظام معلوماتي يحتوي على معلومات تمت معالجتها أو تخزينها أو نقلها إلكترونياً أو بأية وسيلة تقنية أخرى، هذا وقد أضاف المشرع الفنلندي سنة 1995 عند مراجعته لأحكام قانون العقوبات نصاً يتعلق بالعقاب على الدخول غير المصرح به إلى المعلومات المبرمجة باستخدام وسائل تقنية خاصة، ولو لم يترتب على ذلك دخول الفاعل إلى النظام الذي يحتوي عليها[2].

أما عن موقف المشرع الجزائري من هذه الجريمة، فيلاحظ أنه عمد إلى مواكبة التشريعات الغربية، بحيث إستحدث بموجب القانون 04-15 المعدل والمتمم لقانون العقوبات قسم سابع مكرر سماه بالمساس بأنظمة المعالجة الآلية للمعطيات[3]، وبموجب نص المادة 394 مكرر من هذا القانون عاقب على جريمة الدخول غير المشروع إلى منظومة المعالجة الآلية للمعطيات، حيث نصت المادة على أنه: «يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50.000 دج إلى 100.000 دج كل من يدخل عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك».

هذا وقد شدد المشرع في الفقرة الثانية من المادة آنفة الذكر العقاب على هذه الجريمة حيث ضاعف العقوبة إذا ما ترتب على الدخول بطريق الغش حذف أو تغيير لمعطيات المنظومة، كما قرر في الفقرة 03 من ذات المادة تطبيق عقوبة الحبس من ستة (6) أشهر

[1]- أحمد عاصم عجيلة، المرجع السابق، ص. 311.
[2]- رشدي محمد علي عيد، المرجع السابق،ص. 308؛ أحمد عاصم عجيلة، المرجع السابق، ص. 312.
[3]- قانون 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم بالقانون رقم 06-23 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون العقوبات الجزائري، سابق الإشارة إليه.

إلى سنتين والغرامة من 50.000 دج إلى 150.000 دج، إذا ما ترتب على فعل الدخول تخريب نظام إشتغال المنظومة [1].

ما يلاحظ على نص المادة 394 مكرر من قانون العقوبات أن المشرع الجزائري قد جرم فعل الدخول غير المشروع إلى النظام المعلوماتي كله أو لجزء منه دون أن يذكر بصريح العبارة المستندات الإلكترونية، وهو ذات ما انتهجه المشرع الفرنسي في المادة 323 فقرة 02 من قانون العقوبات، هذا ويلاحظ أن المشرع قد اعتبر في المادة 394 مكرر أن فعل الدخول غير المشروع يعد في حد ذاته جريمة، بحيث يعتبر اختراق جهاز الكمبيوتر بقصد الوصول إلى البيانات لمجرد التسلية انتهاكاً للنظام المعلوماتي[2]، وللإشارة فإن الجريمة تتحقق بالصور التالية:

- من خلال وصول الجاني إلى النظام المعلوماتي بطريق الغش، ذلك أن الجريمة عمدية تقوم بتوافر القصد الجنائي العام .
- كما وتقوم إذا كان الجاني عالما بدخوله إلى منظومة معلومات لا تخصه، وللإشارة فإنه يتضح من نص المادة 394 مكرر من قانون العقوبات أن جريمة الدخول غير المشروع تقوم ولو لم يترتب على ذلك الدخول إضرار بالمعلومات، كما وتقوم الجريمة في حالة الدخول لفترة قصيرة وبصفة غير دائمة، ذلك أن جريمة الدخول غير المشروع جريمة وقتية[3].

---

[1]- المادة 394 مكرر ف 02-03 من القانون رقم 04-15 المعدل والمتمم بالقانون رقم 06-23 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون العقوبات الجزائري.

[2]- يكاد نص المادة 394 مكرر من ق.ع.ج. يشبه نص المادة 323 فقرة 01 من ق.ع. الفرنسي الذي لم يشترط بدوره نية خاصة في جريمة الدخول غير المصرح به إلى أنظمة المعالجة الآلية للمعطيات، وفي هذا يرى البعض من الفقه الفرنسي أن لفظ "بطريق الغش" "Frauduleusement" الواردة بالمادة 323 فقرة 01 من قانون العقوبات الفرنسي، والذي تضمنته المادة 394 مكرر من ق.ع.ج يختلف عن مصطلحي عمدي وإرادي ويدل على أن جريمة الدخول غير المصرح به لا تقوم بمجرد القصد العام، وإنما لا بد لذلك من قصد خاص هو الغش، وبالمقابل فإن جانب من الفقه يرى أن قصد الإضرار بالغير غير متطلب هنا بحيث يفسر مصطلح الغش على أنه الدخول والبقاء غير المصرح بهما بدون رضا صاحب النظام، ذلك أن القصد الخاص هو علم وإرادة ينصرفان إلى وقائع خارجة عن أركان الجريمة، أي وقائع لا تدخل ضمن عناصرها، ولفظ الغش لا يدل على أن المشرع تطلب انحراف القصد إلى وقائع معينة غير أركان الجريمة، وعليع إن حمل هذا اللفظ معنى الاحتيال، إلا أنه لا يدل إلا على معنى واحد، وهو أن الجريمة عمدية يكفي لقيامها توافر القصد الجنائي العام فحسب. مشار إليه من طرف، خليفي مريم، المرجع السابق، ص. 183.

[3]- الجريمة الوقتية أو الآنية أو الفورية هي الجريمة التي ترتكب في فترة قصيرة محودة من الزمن. لتفاصيل أكثر يراجع، زيبحة زيدان، المرجع السابق، ص.49؛ علي عبد القادر القهوجي، قانون العقوبات، القسم العام، المكتبة القانونية، الدار الجامعية، 1994، ص.65؛ منصور رحماني، الوجيز في القانون الجنائي العام، فقه- قضايا، دار العلوم للنشر، عنابة، 2006، ص.86.

يبقى أن نضيف أن المشرع الجزائري إلى جانب العقوبات الواردة في نص المادة 394 مكرر والتي تطبق في حالة إرتكاب الجريمة سواء في صورتها البسيطة أو المشددة، فإنه قد رصد في المادة 394 مكرر 06[1] عقوبات أخرى تكميلية تطبق على الشخص الطبيعي، كما رصد في المادة 394 مكرر 4[2] عقوبات تطبق إذا كان مرتكب الفعل شخصاً معنوياً، وأكثر من ذلك يلاحظ أنه قد عاقب في المادة 394 مكرر 7[3] على فعل الشروع في جريمة الدخول غير المشروع، وفرض لمرتكبه نفس العقوبة المقررة للجنحة في حد ذاتها.

الفرع الثاني: جريمة البقاء غير المشروع داخل نظام معلوماتي يحتوي على مستندات إلكترونية.

لاشك في أن الجاني قد يتجاوز بدخوله غير المشروع إلى معطيات المستند الإلكتروني المخزنة بواسطة نظم المعالجة الآلية للمعطيات إلى درجة بقاءه داخل النظام المعلوماتي، وذلك بغية البحث والتلاعب في المعطيات والبيانات الإلكترونية المدرجة في هذه المستندات، أو بغية تحقيق أهداف إجرامية أخرى، ومن ثم فإن جريمة البقاء غير المشروع (أو غير المصرح به) مرتبطة بجريمة الدخول غير المشروع من الناحية الفنية، لا سيما وأن الجاني لا يمكنه البقاء داخل النظام المعلوماتي، إلا إذا كان قد سبق هذا البقاء دخول غير مشروع إلى نظام معالجة آلية يحتوي على مستندات إلكترونية، أو كان هذا الدخول مشروعاً ولكن تجاوز الجاني مدة البقاء المسموح له بها قانوناً[4].

ودراسة كل جريمة على حدا رغم إرتباطهما من الناحية التقنية يجد تبريره في أن أغلب التشريعات التي جرمت الدخول غير المصرح به إلى النظم المعلوماتية عاقبت على

---

[1]- تتمثل العقوبات التكميلية حسب نص المادة 394 مكرر 6 من قانون العقوبات في المصادرة وإغلاق الموقع فيما يتعلق بالمواقع التي تكون محلاً لجريمة ماسة بالمعلوماتية، وإغلاق المحل أو مكان الاستغلال حيث نصت المادة على أنه: «مع الاحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلاً لجريمة من الجرائم المعاقب عليها وفقاً لهذا القسم، علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها».

[2]- تنص المادة 394 مكرر4 من ق.ع.ج المعدل والمتمم: «يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس (5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي ».

[3]- تنص المادة 394 مكرر 7 من ق.ع.ج المعدل والمتمم: «يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها».

[4]- فائزة يونس الباشا، المرجع السابق، ص.23؛ أحمد عاصم عجيلة، المرجع السابق، ص. 304.

فعل الدخول المجرد ولو لم يرتب على الدخول ضرر، وكذا لو لم تتحقق فائدة من جراء هذا الدخول غير المشروع، وهو ما انتهجه المشرع الجزائري -كما سبق بيانه- إذ جرم مجرد الدخول إلى نظام المعالجة الآلية للمعطيات دون إشتراط الوصول إلى المعلومات.

وإذا كان الدخول غير المشروع يتطلب من الفاعل نشاطاً إيجابياً وهو فعل الدخول، فإن جريمة البقاء غير المصرح به داخل النظام المعلوماتي تتطلب هي الأخرى من الفاعل نشاطاً إيجابياً، كما قد تقوم بنشاط سلبي من الفاعل والمتمثل في فعل البقاء في حد ذاته[1]، وفي هذا يلاحظ أن معظم التشريعات التي تناولت هذه الجريمة ألقت على عاتق مرتكب الفعل واجب عدم البقاء داخل النظام المعلوماتي والخروج منه، خاصة إذا كان دخوله غير مصرح به، وعليه ينبغي على الجاني القيام بفعل إيجابي وهو قطع الاتصال وعدم الإبقاء عليه[2].

من خلال ما سبق، يتبين أن تسليط الضوء على هذه الجريمة لا يتم إلا ببيان ركنها المادي أو السلوك الإجرامي المكوّن لها **(البند الأول)**، ثم تحديد ركنها المعنوي **(البند الثاني)**، على أن يتم بعد ذلك التطرق للعقوبات المقررة لها سواء في التشريعات الأجنبية أو في التشريع الجزائري **(البند الثالث)**.

البند الأول: الركن المادي للجريمة.

يعرف الفقه فعل البقاء غير المشروع بأنه: «التواجد داخل نظام المعالجة الآلية للمعطيات، أو داخل نظام معلوماتي يحتوي على مستندات إلكترونية، رغما عن إرادة من له الحق في السيطرة على هذا النظام»[3]، هذا ويعرف جانب آخر البقاء غير المشروع بأنه:

---

[1]- Cf. Thierry Fossier, droit pénal spécial, T2, affaires, entreprises, et institution publiques, bibliothèque nationale de paris, 2013, p.p. 208-209.

[2]- خليفي مريم، المرجع السابق، ص. 169؛

Thierry Garé, droit pénal spécial, tome1, personnes et bien, 2eme ed, bibliothèque nationale de paris, 2013, p.176.

[3]- نهلا عبد القادر المومني، الجرائم المعلوماتية، ط1، دار الثقافة، الأردن، 2008، ص. 161؛ عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، المرجع السابق، ص. 360؛

Frédéric-Jérome Pensier et Emmanuel Jez, op. cit, p.114.

«عدم وضع حد للتشعب داخل النظام المعلوماتي رغم الإعتقاد بأن ذلك الأمر يشكل خطأ»، وعليه يمكن القول أن البقاء هو عدم قطع الفاعل للإتصال بالنظام المعلوماتي، رغم إدراكه أن وجوده فيه غير مشروع[1].

إستناداً لهذه التعاريف، فإن صور البقاء المعاقب عليه، يشمل البقاء داخل النظام المعلوماتي رغم انتهاء العقد وعدم تجديده، إستمرار وجود الجاني داخل النظام بعد المدة المحددة له، أي المصرح له بالمكوث خلالها داخل النظام[2]، كما ويعد من صور البقاء الحالة التي يجد فيها الجاني نفسه داخل نظام المعالجة الآلية للمعطيات بدون قصد منه، ليظل فيه بعد إكتشاف تواجده داخل النظام، وفي مثل هذه الحالة يبدأ البقاء منذ اللحظة التي يعلم الجاني فيها أنه داخل نظام غير مصرح له بدخوله ورغم ذلك لا يخرج منه، بهذا يمكن القول أن هذه الجريمة تستوجب من مرتكب الفعل الخروج من البرنامج أو النظام المعلوماتي وقطع الإتصال فور تحقق الإتصال غير المشروع[3].

إنطلاقا مما تقدم، يتضح أن الركن المادي لجريمة البقاء غير المصرح تبدأ لحظة إدراك الفاعل حقيقة الاتصال الحاصل وبقاءه ضمن نظام المعلوماتية دون حق يجيز إجراء اتصال أو الإبقاء عليه[4]، وللإشارة فإنه لا يشترط لتحقق الركن المادي في هذه الجريمة أن يقوم الجاني بارتكاب جريمة أخرى، ولكن يكفي لقيامها إستمرار الجاني بالبقاء في النظام ودون القيام بأي نشاط، ولا شك أن البقاء داخل النظام لا يعني قيام المخترق بالتعديل أو الإتلاف أو التخريب في النظام المعلوماتي وما يحتويه من مستندات إلكترونية، بل يعني

---

[1]- محمد خليفة، المرجع السابق، ص. 154.

[2]- أحمد عاصم عجيلة، المرجع السابق، ص، ص 304- 305؛ عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، المرجع السابق، ص. 360.

[3]- يرى البعض أن البقاء غير المصرح به داخل نظام الحاسب الآلية لا يقتصر فقط على حالة الدخول إلى نظام غير مصرح بالدخول إليه على سبيل الخطأ والبقاء داخل النظام على الرغم من العلم بذلك، إنما ينطبق أيضا على حالة الدخول إلى نظام الحاسب الآلي بموافقة المسؤول عن النظام إذا كانت هذه الموافقة مشروطة بزمن محدد وحدث تجاوز لهذا الزمن، فإن البقاء داخل النظام في هذه الحالة يعد غير مصرح به. مشار إليه من طرف، محمد عبيد الكعبي، المرجع السابق، ص. 354؛ محمد خليفة، المرجع السابق، ص. 155.

[4]- نجاة عباوي، جرائم المعلوماتية في التشريع الجزائي الجزائري، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة بشار، 2008، ص. 233؛

Thierry Fossier,droit pénal spécial, affaires, op. cit, p,p.208-209.

[4]- خليفي مريم، المرجع السابق، ص. 169.

إمكانية التحكم في نظام المعالجة الآلية للبيانات، وبهذا يبدو أن وصف جريمة البقاء يمكن أن يتغير إلى وصف جريمة أخرى إذا قام الجاني بارتكاب ما من شأنه أن يغير في وصف هذه الجريمة، كما لو قام بانتهاك الحق في الخصوصية والمساس بسرية البيانات[1].

هذا وتعتبر جريمة البقاء غير المشروع داخل النظم المعلوماتية بشكل عام من الجرائم التي يصعب تقديم دليل على إثباتها، حيث يزعم المتهم في حالة القبض عليه أنه كان على وشك الانفصال عن النظام المعتدى عليه، فضلا عن ذلك فإن هذه الجريمة تعتبر من الجرائم الشكلية التي لا يشترط فيها حدوث نتيجة جرمية معينة، إذ يكفي لقيام الركن المادي تحقق فعل البقاء غير المشروع داخل نظام معلوماتي يحوي مستندات إلكترونية[2].

مما سبق يتضح أن طبيعة جريمة البقاء هي ذاتها طبيعة جريمة الدخول، بحيث ينطبق عليها ذات الأمر كون أن الفعلين يجتمعان في العديد من النقاط، وإن كان يختلفان في نقاط أخرى، ولعل ما يميز فعل البقاء عن فعل الدخول أن فعل البقاء جريمة مستمرة، ذلك أن السلوك الإجرامي في البقاء يستمر ويستمر معه الاعتداء على المصلحة القانونية، بينما يعد الدخول سواء كان مجرداً أو مُرتباً لآثار معينة جريمة وقتية، ذلك أن الجريمة تكتمل في اللحظة التي يتم فيها الدخول إلى النظام، هذا و ينبغي الذكر أن ما يجمع بين حالة البقاء بعد دخول مصرح به، والبقاء بعد دخول عن طريق الصدفة أو الخطأ أن الدخول في كل هذه الحالات كان مشروعاً، وعليه لا يمكن تطبيق أحكام جريمة الدخول غير المشروع في هذه الحالة، بل تطبق أحكام جريمة البقاء غير المشروع[3].

البند الثاني: الركن المعنوي لجريمة البقاء غير المشروع.

تعتبر جريمة البقاء غير المشروع داخل نظام معلوماتي يحتوي على مستندات إلكترونية من الجرائم العمدية، التي تستلزم لقيامها توافر القصد الجنائي العام والمتمثل في عنصري العلم والإرادة، وهو ما أقرته جميع التشريعات الجنائية التي تناولت هذه الجريمة

[1]- أحمد عاصم عجيلة، المرجع السابق، ص. 305.
[2]- نهلا عبد القادر المومني، المرجع السابق، ص. 161.
[3]- محمد خليفة، المرجع السابق، ص، ص .155- 156.

بما فيها المشرع الجزائري، وإن كانت النصوص القانونية قد جاءت على اختلاف فيما بينها في العبارات المستخدمة لهذا الغرض[1].

الحقيقة أن ضرورة الموازنة بين حماية خصوصية الأنظمة المعلوماتية، وبين حماية الأفراد في إستخدام الإنترنت[2] إستلزم أن تكون جريمة البقاء غير المشروع جريمة عمدية، تتطلب لقيامها القصد الجنائي، بحيث ينبغي أن ينصرف علم الجاني بأنه يقوم بالتجول داخل نظام معلوماتي يحتوي على مستندات إلكترونية من غير حق يجيز له البقاء فيه، أو من غير وجود رخصة أو عقد يسمح له بذلك.

وعن عنصر العلم، فإنه يجب أن يشمل هذا الأخير علم الجاني بكل واقعة تدخل في تكوين جريمة البقاء غير المصرح به، وأول ما يجب أن ينصرف إلى علمه هو موضوع الحق المعتدى عليه، فلا بد أن يعلم الجاني بأن فعله ينصب على نظام المعالجة الآلية الذي يحتوي على المستندات الإلكترونية وليس على شيء آخر[3]، كما يجب أن يعلم بأن بقاءه داخل النظام المعلوماتي هو بقاء غير مصرح به أي غير مشروع، أو أن بقاءه قد تجاوز المدة القانونية المسموح بها، وعليه إذا كان الجاني يعتقد أن له تصريحاً بالبقاء داخل النظام المعلوماتي أو أن الزمن المخصص للبقاء لم ينته بعد، فإن ذلك يحول دون قيام القصد الجنائي.

وللتذكير فإنه إذا ما حصل ووقع فعل البقاء داخل النظام المعلوماتي بسبب الدخول خطأ، أو بطريق الصدفة، فإنه يتوجب على الجاني الخروج فورا من النظام لمجرد علمه أن بقاءه أصبح غير مشروع، فإن لم يفعل ذلك توافر القصد الجنائي لديه منذ اللحظة التي تحقق فيها علمه بذلك، وعُد من ثم مرتكبا لجريمة بقاء غير مشروع[4].

---

[1]- محمد عبيد الكعبي، المرجع السابق، ص. 370.

[2]- إن المنطق يحتم أن تكون هذه الجريمة عمدية لأن عمليات الدخول إلى أنظمة الحاسبات الآلية والبقاء فيها هي عمليات تتكرر بشكل مذهل في اليوم الواحد وتقع من عدد هائل من المستخدمين، لا سيما مع ارتفاع عدد مرتادي شبكة الإنترنت، وليس مستبعد في ظل كل هذه الحركة دخولاً وخروجاً أن تكون هناك عمليات دخول أو بقاء غير مصرح بهما لكنها غير عمدية، ولو كانت جريمة الدخول والبقاء غير عمدية لوقع الكثير من مستعملي هذه الشبكة والحاسب الآلي تحت طائلة العقاب، وعلى هذا كان من اللازم أن تكون هذه الجريمة عمدية. محمد خليفة، المرجع السابق، ص، ص. 162- 163.

[3]- نائلة عادل محمد فريد قورة، المرجع السابق، ص. 365؛ محمد خليفة، المرجع السابق، ص. 164.

[4]- محمد خليفة، المرجع السابق، ص. 165؛ نهلا عبد القادر المومني، المرجع السابق، ص. 162.

زيادة على ذلك لا بد أن يعلم الجاني بخطورة الفعل الذي يقوم به على المصلحة التي يحميها القانون، كأن يعلم أنه ينتهك سرية هذا النظام، وأن فعله قد يؤدي إلى تخريب هذا النظام أو الإضرار بالمستندات والمعطيات الموجودة فيه.

إضافة إلى وجوب توافر العلم لقيام القصد الجنائي للجريمة محل الدراسة، لا بد من توافر عنصر الإرادة، ذلك أنها هي التي تبين الموقف النفسي للفاعل من سلوكه ومن النتيجة المترتبة عليه، وبما أن جريمة البقاء غير المصرح به جريمة شكلية لا يتطلب لقيامها تحقق نتيجة معينة، فإن الإرادة فيها تقتصر على السلوك الإجرامي فتستغرقه بكل مقوماته، ولا تمتد إلى أي نتيجة لأن هذه الأخيرة لا يعتد بها القانون في قيام الجريمة[1].

وعليه يكفي لقيام هذه الجريمة أن تتجه إرادة الجاني إلى البقاء أو المكوث داخل النظام وعدم قطع الاتصال به مع علمه بعدم مشروعية الاتصال، هذا ولا يعتد القانون عادة بالغاية التي يرمي إليها الجاني، كما لا يعتد بالبواعث التي دفعت الجاني إلى المكوث داخل النظام المعلوماتي[2].

إلى جانب القصد العام الواجب توافره لقيام الركن المعنوي للجريمة محل الدراسة، تتطلب بعض التشريعات توافر القصد الخاص لقيام جريمة البقاء غير المصرح به[3]، ومن ذلك قانون إساءة استخدام الحاسبات الآلية لعام 1990 في المملكة المتحدة، والقانون البرتغالي لجرائم المعلوماتية لعام 1991، والقانون الدنماركي وغيره من القوانين التي سبق بيانها سابقاً عند دراسة الركن المعنوي لجريمة الدخول غير المشروع[4].

---

[1]- محمد خليفة، المرجع السابق، ص. 166؛ محمد عبيد الكعبي، المرجع السابق، ص ص .371- 372.

[2]- محمد عبيد الكعبي، المرجع السابق، ص. 375؛

Thierry Garé, op. cit, p.177.

[3]- محمد عبيد الكعبي، المرجع السابق، ص. 376.

[4]- يراجع في ذلك، ص. ص 256- 257 من هذه الأطروحة.

البند الثالث: العقوبة المقررة لجريمة البقاء غير المشروع.

نظراً لإرتباط جريمة البقاء غير المشروع مع فعل الدخول إلى الأنظمة المعلوماتية من الناحية الفنية سواء أكان هذا الدخول مشروعاً أو غير مشروع، عمدت غالبية التشريعات المقارنة إلى الجمع بين الفعلين في نص واحد، كما قررت لهما نفس العقوبة .

ولأهمية الجزاء في عقاب الجاني، وردع الغير عن إقتراف ذات الفعل سيتم تحديد العقوبات المقررة لفعل البقاء غير المشروع داخل نظام معلوماتي،على أن يتم الإحالة إلى العقوبات المقررة لجريمة الدخول غير المشروع كلما إقتضت الضرورة ذلك.

وفي هذا يلاحظ أن إتفاقية بودابست الخاصة بمكافحة الإجرام المعلوماتي، قد تطرقت إلى فعل الولوج غير القانوني دون أن تشير إلى فعل البقاء غير المشروع، وذلك ما يتضح من نص المادة الثانية من هذه الإتفاقية ولتأكيد هذا الأمر ينبغي الرجوع إلى المذكرة التفسيرية لإتفاقية بودابست، والتي أوضحت أن المقصود بالولوج غير القانوني كل فعل ينطوي على تدخل غير مصرح به، كما ويشمل أفعال السطو،القرصنة، و لدخول غير المشروع إلى الأنظمة المعلوماتية، دون أن تشير إلى فعل البقاء داخل النظام[1].

وفي هذا يرى جانب من الفقه ضرورة إشارة هذه الإتفاقية إلى جريمة البقاء غير المشروع بصريح العبارة، وذلك نظراً لأهميتها و لإرتباطها بفعل الولوج غير القانوني، لا سيما وأنها جاءت لتوفير السلامة والأمن للنظم والبيانات المعلوماتية.

على عكس إتفاقية بودابست يلاحظ أن الإتفاقية العربية لمكافحة جرائم تقنية المعلومات قد تطرقت في المادة 6 منها إلى فعل البقاء غير المشروع داخل الأنظمة المعلوماتية، وعبرت عنه بمصطلح الإستمرار بعد الإتصال غير المشروع مع كل أو جزء من تقنية المعلومات، هذا وقد إقترحت في الفقرة الثانية من المادة ذاتها ظرفين مشددين للجريمة تشدد على أثرهما العقوبة، ويشمل الظرف الأول حالة ما إذا نجم عن الإستمرار

[1]- لتفاصيل أكثر تراجع المذكرة التفسيرية لاتفاقية بودابست. مشار إليه من طرف، هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقاً عليها، المرجع السابق، ص. 49 وما يليها.

بهذا الاتصال محو، تعديل، تشويه، نسخ، نقل أو تدمير للبيانات المحفوظة وللأجهزة والأنظمة الإلكترونية وشبكات الاتصال، في حين يشمل الظرف المشدد الثاني حالة ما إذا نجم عن البقاء حصول على معلومات حكومية سرية[1].

ولئن كان هذا موقف الإتفاقيات الدولية، فإنه ينبغي الذكر أن التشريعات الوطنية جرمت فعل البقاء غير المشروع، بحيث تطرق المشرع الفرنسي لجريمة البقاء غير المشروع في كل أو جزء من نظام المعالجة الآلية للمعطيات بموجب نص المادة 323-1 من قانون العقوبات الفرنسي لسنة 1994 المعدل والمتمم، وهو ما يستفاد من سياق هذا النص الذي ورد كالآتي:

"Se maintenir frauduleusement dans tout ou partie d'un système de traitement automatisé de données".

ما يمكن ملاحظته على هذه المادة أن المشرع الفرنسي قد جمع بين جريمتي الدخول والبقاء غير المشروع في نص واحد، كما فرض على مرتكب فعل البقاء غير المشروع نفس العقوبة المقررة لجريمة الدخول غير المصرح به، والتي سبق الإشارة إليها عند دراسة هذه الجريمة، وتكمن العقوبة في الحبس لمدة سنتين وبغرامة قدرها 30.000 أورو[2].

هذا ويرى الفقه الجنائي أن الجزء الخاص بالبقاء غير المصرح به الوارد في نص المادة 323-1 من قانون العقوبات الفرنسي، قد تم إدراجه في النص الفرنسي أثناء القراءة الأولى للقانون داخل مجلس الشيوخ الفرنسي على إثر التقرير الذي تقدم به أحد الأعضاء[3]، لصعوبة النص في صياغته الأولى، والذي كان ينص فقط على الدخول غير المصرح به في

[1]- نص المادة 06 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، سابق الإشارة إليها.

[2]- ينظر في ذلك العقوبات المقررة لجريمة الدخول غير المشروع الواردة في نص المادة 323-1 من قانون العقوبات الفرنسي المعدلة بموجب القانون رقم 410-2012 الصادر في 27 مارس 2012 لا سيما النص باللغة الفرنسية. مشار إليه، هامش ص. 263 من هذه الأطروحة.

[3]- تقدم بهذا الاقتراح عضو مجلس الشيوخ الفرنسي « Thyraud » ، وقد تم الأخذ به عند الصياغة النهائية للقانون.

حالة الدخول إلى النظام عن طريق الصدفة، ثم البقاء داخل النظام على الرغم من عدم مشروعيته[1].

ولقد طبق القضاء الفرنسي نص المادة 323-1 في شأن حالة البقاء غير المصرح به داخل نظام الحاسب الآلي، حيث قضت محكمة استئناف باريس في حكم لها صادر بتاريخ 05 أفريل 1994 إلى أن القانون يجرم البقاء غير المصرح به داخل نظام الحاسب سواءً كان الدخول قد تم بطريق الخطأ أو تم بطريق مشروع، طالما أن الفعل قد إكتسب بعد ذلك صفة عدم المشروعية ، ومن ذلك حالة ما إذا فقد الفاعل حقه في البقاء بسبب خطأ من جانبه[2].

إلى جانب التشريع الفرنسي نلاحظ أن القانون الفيدرالي لجرائم الحاسب الآلي، جرم في المادة 1030/أ/6 الدخول غير المصرح به إلى نظام الحاسب الآلي، وإقتصر التجاوز المجرم على دخول الجاني إلى الحاسب الآلي المصرح له بالدخول إليه، والحصول على معلومات غير مصرح له بها أو تعديلها دون وجود إذن له بذلك، بهذا يتبين أن النص الأمريكي يكتفي بتجريم الحالات التي يكون فيها الدخول مصرحا به إبتداءا في حين يقوم الجاني بتجاوز الحدود الممنوحة له، بحيث يبقى في النظام رغم عدم أحقيته بذلك، ولا يتعرض لحالات بقاء الجاني داخل النظام بعد دخوله إليه بطريق الخطأ[3].

هذا عن موقف التشريعات الغربية، أما عن التشريعات العربية فيتبين أن المشرع الجزائري قد حذا حذو نظيره الفرنسي بحيث نص على جريمة البقاء غير المشروع في المادة 394 مكرر من قانون العقوبات التي جرمت فعل الدخول غير المشروع، وذلك بسبب الإرتباط الفني بين فعلي الدخول و البقاء غير المشروعين إلى الأنظمة المعلوماتية.

---

[1]- محمد عبيد الكعبي، المرجع السابق، ص. 353؛
Michael Véron, Droit pénal spécial, 14eme ed, édition dalloz, paris, 2012, p,p. 232-233.

[2]- C.A de paris, 05/04/1994, D, 1994, I.R., p 130. « … La loi incrimine également le maintien frauduleux dans un système de la part de celui qui y ayant régulièrement pénétré, se serait maintenu frauduleusement, lorsque l'accès a été régulier, le maintien sur un système automatisé de données peut devenir frauduleux, lorsque par une sorte d'intervention de titres, l'auteur du maintien se trouve privé de toute habilitation ».
مشار إليه من طرف، أحمد عاصم عجيلة، المرجع السابق، ص. 314.

[3]- محمد عبيد الكعبي، المرجع السابق، ص، ص. 353- 354؛ مدحت عبد الحليم رمضان، المرجع السابق، ص. 41.

بهذا يكون المشرع الجزائري قد قرر للجريمة محل الدراسة ذات العقوبة المقررة لجريمة الدخول غير المشروع بصورتيها البسيطة والمشددة، بحيث قرر كأصل عام عقوبة الحبس من 3 أشهر إلى سنة، وغرامة من (50.000) خمسين ألف دينار إلى (100.000) مئة ألف دينار، على أن تضاعف العقوبة إذا ما ترتب عن البقاء غير المشروع حذف أو تغيير لمعطيات المنظومة، أما إذا ترتب على فعل البقاء تخريب نظام إشتغال المنظومة فتكون العقوبة الحبس من ستة أشهر إلى سنتين وغرامة من (50.000) خمسين ألف إلى (150.000) مئة وخمسين ألف دينار[1]، ولتطبيق العقوبات المقررة يكفي أن يكون البقاء غير المشروع قد تم في كل أو في جزء فقط من نظام المعالجة الآلية للمعطيات[2].

إلى جانب هذه العقوبة الأصلية رصد المشرع الجزائري في المادة 394 مكرر6 لجريمة البقاء غير المشروع عقوبات تكميلية، وتشمل هذه الأخيرة مصادرة الأجهزة والوسائل المستخدمة في إرتكاب الجريمة، و غلق المواقع التي تكون محلاً للجريمة مع غلق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها.

هذا وتجدر الإشارة إلى أن المشرع الجزائري قد عاقب في المادة 394 مكرر4 من قانون العقوبات الشخص المعنوي الذي يرتكب هذه الجريمة بغرامة تعادل خمس مرات الغرامة المقررة للشخص الطبيعي[3]، كما عاقب في المادة 394 مكرر7 من ذات القانون على

---

[1]- المادة 394 مكرر من القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004المعدل والمتمم لقانون العقوبات الجزائري، سابق الإشارة إليه.

[2]- يتضح من خلال هذا أن الحرص على حماية النظم المعلوماتية لم يتوقف عند تجريم فعل الدخول أو البقاء فيه، بل اتجه إلى مواجهة ما هو أخطر من هذه الأفعال، وما قد يترتب عنها من نتائج ومنها:

1- حذف البيانات أو المعطيات أو تغييرها.

2- تخريب نظام اشتغال المنظومة.

ذلك أن حصول عملية التحريف والتغيير أو التخريب في المنظومة تعد أبرز صور الجريمة، لكونها تجسد الركن المادي للجريمة وتعطي انطباعا على بلوغ المجرم مبتغاه، ويتجسد الركن المادي هنا بإحداث تغيير في البيانات، وذلك بمحوها كلياً أو جزئياً أو تشويهها بحيث تصبح غير صالحة للاستعمال، في ذات الوقت قد يتحقق الركن المعنوي لهذه الجريمة بتوافر العلم بأن تتجه إرادة الجاني لتحقيق نتيجة تصرفه، من ثم فإن جريمة الإتلاف والتخريب جريمة عمدية وهي لا تقتصر على تغيير في البيانات، بل قد تصل إلى تخريب نظام اشتغال المنظومة كلية كما تصورها نص المادة 394 مكرر من ق.ع.ج. وبصدد ذلك ضاعف المشرع العقوبة. مشار اليه من طرف، زيبحة زيدان، المرجع السابق، ص، ص. 51-52 .

[3]- المادة 394 مكرر 4 من قانون رقم 04-15 المؤرخ في 10 نوفمبر 2004المعدل والمتمم لقانون العقوبات الجزائري، سابق الإشارة إليه.

الشروع في ارتكاب جريمة البقاء غير المشروع، بحيث فرض على مرتكبه العقوبة المقررة للجنحة ذاتها[1].

المطلب الثاني: الأعمال الماسة بسرية المستند الإلكتروني.

قد تتضمن المستندات الإلكترونية المخزنة في الحاسب الآلي بيانات ومعلومات بالغة الأهمية لا يجوز الاطلاع عليها من قبل أشخاص غير مرخص لهم بذلك، كما لا يجوز نشرها أو إفشاءها، وذلك لما تتضمنه من قيمة وخصوصية، ويستوي في هذه البيانات أن تكون شخصية، تجارية، صناعية، متعلقة بأسرار الدولة، أو غيرها من البيانات التي يؤدي المساس بها أو التعامل فيها بصورة غير مشروعة إلى الإضرار بمصالح أصحابها.

ولتكريس مبدأ الخصوصية في التعاملات الإلكترونية لا بد من إحاطة المستند الإلكتروني، وما يحويه من بيانات ذات طابع خاص بنوع من السرية، وذلك تأمينا للمعاملات الإلكترونية التي أصبحت تتم في وسط افتراضي وبين أشخاص لا يجمعهم مكان واحد.

وفي هذا السياق أشار السكرتير العام للأمم المتحدة، في أحد تقاريره إلى أن الحاسبات الإلكترونية تُمثل أكبر تهديد للحياة الخاصة والحرية الشخصية، ذلك أنها تُعد من أدوات المراقبة وأجهزة التطفل الحديثة، إذ من خلال بعض الأجهزة الموجودة بها يتم تسجيل أسماء وعناوين وأرقام هواتف من يقوم بالاتصال بهاتف معين، كما ويقوم قلم التسجيل الإلكتروني بالدور ذاته[2].

والمقصود بالسرية هنا حصر المعلومات أو البيانات الخاصة في نطاق محدود، بحيث إذا انعدم هذا الحصر، وأصبحت البيانات قابلة للتداول أصبحت بذات المعنى غير سرية.

---

[1]- تنص المادة 397 مكرر 7 من قانون رقم 04-15 المؤرخ في 10 نوفمبر 2004المعدل والمتمم لقانون العقوبات الجزائري، سابق الإشارة إليه على أنه: «يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها»، بل والأكثر من ذلك فإنه في نص المادة 394 مكرر من ق.ع. استعمل المشرع الجزائري عبارة "أو يحاول ذلك" وهذا تأكيداً على أن المشرع يعاقب على الشروع في ارتكاب جريمة الدخول أو البقاء غير المشروعين داخل نظام معلوماتي يحتوي على مستندات إلكترونية.

[2]- أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دراسة مقارنة في القانون الفرنسي والأمريكي والمصري وفقا لآخر التعديلات التشريعية، دار النهضة العربية، القاهرة، 1428هـ-2008م، ص.129.

ونظراً لأهمية ما تحويه المستندات الإلكترونية من بيانات ومعلومات، فإن كل تجميع لهذه البيانات بصورة غير مشروعة وكل توفير لها أو الاتجار فيها يعد من قبيل الأفعال المحظورة، التي حاولت التشريعات المقارنة الدولية والداخلية التصدي لها والعقاب عليها في نصوصها الجزائية المختلفة.

لخطورة الأفعال الماسة بسرية المستند الإلكتروني سيتم التطرق إلى جريمة إفشاء الأسرار المعلوماتية **(الفرع الأول)**، وبعدها لجريمة تجميع أو توفير بيانات إلكترونية مخزنة أو معالجة آلياً **(الفرع الثاني)**.

الفرع الأول: جريمة إفشاء سرية البيانات الإلكترونية.

لا شك أن التشريعات العقابية التقليدية[1] في الدول المختلفة تتضمن نصوصا قانونية تحمي المعلومات الواردة بالمستندات الورقية من الإفشاء، وذلك لما تحويه تلك المعلومات من أسرار خطيرة قد تمس بحياة الفرد، وقد تمس باقتصاد الدولة، أو استقرار المجتمع واستتباب الأمن فيه[2].

ولئن كانت التشريعات سعت إلى حماية المعلومات الواردة بالمحررات الورقية بتجريم المساس بها ومعاقبة الجاني على الأفعال التي يأتيها رغم أن الوصول إلى بعض تلك المعلومات، وخاصة منها تلك المتعلقة بأسرار الدولة تستلزم تسرب شخص معين إلى القطاع المعني، فإن حماية المعلومات الواردة بالمستندات الإلكترونية أضحى من المسائل الهامة، وذلك لسهولة الوصول إليها والكشف عنها.

إن أهمية هذه المسألة دفع التشريعات على المستويين الدولي والوطني إلى التصدي لها بطريقة مباشرة أو غير مباشرة، فعلى المستوى الدولي يلاحظ أن اتفاقية بودابست لسنة 2001 لم تتضمن أي نص يجرّم إفشاء الأسرار المعلوماتية، بل اقتصرت على حماية

[1]- من ذلك م 301 ق.ع ج. المعدل والمتمم.

[2]- عبد الرحمن محمد خلف، نظرة حول المشكلات القانونية والعملية لمواجهة الجريمة المعلوماتية، مجلة كلية الدراسات العليا، متخصصة في علوم الشرطة، مجلة علمية –نصف سنوية- محكمة ، تصدر عن كلية الدراسات العليا بأكاديمية مبارك للأمن، القاهرة، ع الحادي والعشرون، يوليه 2009- شعبان 1430، ص.20.

المعلومات وسريتها من خلال تجريم الدخول بدون تصريح وذلك وفقا للمادة 2 منها، وهو ما أكدت عليه المذكرة التفسيرية حينما فسرت معنى يترتب على الولوج غير المشروع، الوصول إلى بيانات سرية ككلمات المرور أو معلومات عن النظام، وكذا الأسرار التي تسمح باستخدام النظام مجاناً[1].

هذا على المستوى الدولي، أما على المستوى الوطني فقد تطرقت العديد من التشريعات إلى معاقبة الجاني على عملية إفشاء الأسرار، ومن ذلك ما ورد على الصعيد الفيدرالي، حيث جرم المشرع الأمريكي المنظم لحماية أسرار الدفاع إفشاء المعلومات المحظورة وذلك بموجب المادة 798منه[2].

كما أصدر المشرع الأمريكي قانون الخصوصية الذي يتعلق بحماية المعلومات المسجلة عن مواطني الولايات المتحدة الأمريكية والأجانب المقيمين فيها بشكل مشروع، طالما كانت تلك المعلومات محفوظة في السجلات الحكومية (الاتحادية أو الإقليمية الخاصة بالولايات)، وتتعرض لنشأتهم، ظروفهم المالية، تاريخهم الطبي، سجلهم الوظيفي وكافة المعلومات الشخصية الأخرى الخاصة بهم، بحيث حظرت المادة 1 من القسم B من ذلك القانون كشف أي سجل أو تقديم أية معلومات محفوظة في هذه السجلات لأي شخص أو جهة، ما لم يتم الحصول على الموافقة الخطية من الشخص المطلوب كشف المعلومات عنه.

إلى جانب هذه التشريعات أصدر المشرع الأمريكي قانون حماية السرية لسنة 1980، وقانون سياسة الاتصالات السلكية لسنة 1984، كما وأصدر سنة 1986 قانون خصوصية الاتصالات الإلكترونية.

هذا عن المشرع الأمريكي، أما المشرع الفرنسي فقد جرم المساس بالمحررات الإلكترونية السرية من خلال المواد 226-16 إلى 226-24 من قانون العقوبات الفرنسي التي تجرم سرية المعلومات المخزنة إلكترونيا، بحيث تطرق في المادة 226-16-1من قانون

[1]- مدحت محمد عبد العزيز إبراهيم، المرجع السابق، ص. 156.
[2]- مجدي محبوب محب حافظ، موسوعة جرائم الخيانة والتجسس، دراسة في التشريع المصري والتشريعات العربية والأجنبية والشريعة الإسلامية، ط1، المركز القومي للإصدارات القانونية، القاهرة، 2007، ص. 442 وما يليها.

العقوبات المعدل بالقانون رقم 801-2004 لجريمة الإنحراف عن الغرض أو الغاية من المعالجة الإلكترونية للبيانات الإسمية، كما وعالج في المادة 226-19من ذات القانون جريمة التسجيل والحفظ غير المشروع للبيانات الإسمية، كما وتعرض في المادة 226-22 من القانون ذاته لجريمة الإفشاء غير المشروع للبيانات الإسمية[1].

وعلى مستوى التشريعات العربية يلاحظ أن المشرع في دولة الإمارات العربية المتحدة جرم إفشاء المعاملات المعالجة آليا من خلال القانون الاتحادي للمعاملات والتجارة الإلكترونية لدولة الإمارات رقم 1 لسنة 2006 في المادة 28 منه[2].

في حين جرم المشرع في المملكة العربية السعودية إفشاء المعلومات بموجب نظام المعاملات والتواقيع الإلكترونية لسنة 2008، وقصر التجريم بموجب المادة 23 من القانون آنف الذكر على تلك المعلومات.

من خلال ما تقدم، يلاحظ أن التشريعات اختلفت في طريقة تنظيمها لجريمة إفشاء المعلومات الواردة بالمستندات الإلكترونية، إذ أن منها ما نص عليها بطريقة مباشرة، في حين أن هناك تشريعات لم تتطرق لها بطريقة مباشرة، بل إن من التشريعات من قصّرت الحماية على طائفة معينة من المعلومات، وهي تلك الخاصة بالتواقيع الإلكترونية، بل إن منها من وسعت من نطاق الحماية لتشمل المسائل المتعلقة بأسرار الدولة وحياة الأفراد الخاصة.

ولئن كان ذلك هو موقف التشريعات المقارنة، فما هو موقف المشرع الجزائري؟ هذا ما سيتم بيانه بالتطرق إلى أركان جريمة إفشاء الأسرار المعلوماتية **(البند الأول)** ثم العقوبات المقررة لها **(البند الثاني)**.

---

[1]- أسامة عبد الله قايد، المرجع السابق، ص ص.135-156.

[2]- تنص المادة 28 /1 من القانون الاتحادي رقم (1) لسنة 2006 في شأن المعاملات والتجارة الإلكترونية لدولة الإمارات سابق الإشارة إليه على: "يعاقب بالحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن عشرين ألفا ولا تزيد على مائتي ألف درهم أو بإحدى هاتين العقوبتين كل شخص تمكن بموجب أية سلطات ممنوحة له في هذا القانون من الإطلاع على معلومات في سجلات أو مستندات أو مراسلات إلكترونية وأفشى أيا من هذه المعلومات".

البند الأول: أركان جريمة إفشاء الأسرار المعلوماتية.

يتطلب قيام جريمة إفشاء الأسرار الواردة بالمستندات الإلكترونية توافر ركنين ركن مادي وآخر معنوي، ولتشابه الركن المعنوي في كافة الأفعال المكونة لهذه الجريمة سيتم التطرق إليه **(ثانياً)** على أن يخصص **(أولاً)** لتحليل الأفعال المكونة للإفشاء، خاصة وأن المشرع الجزائري لم يقتصر عند تجريمه لهذا الفعل على ما ورد عند تعديل قانون العقوبات بموجب قانون 04-15 المتعلق بأنظمة المعالجة الآلية للمعطيات، بل عمد إلى إصدار نصوص قانونية أخرى تتضمن تجريم إفشاء الأسرار المعلوماتية، ومن ذلك ما ورد في قوانين خاصة كقانون التوقيع والتصديق الإلكترونيين لسنة 2015.

أولاً: الركن المادي.

هناك مجموعة من الأفعال التي تكون الركن المادي لجريمة إفشاء المعلومات بعضها وارد في قانون العقوبات، وبعضها وارد في قوانين تكميلية أهمها قانون التوقيع والتصديق الإلكترونيين، وقانون التجارة الإلكترونية[1].

1- الركن المادي لجريمة إفشاء الأسرار المعلوماتية الوارد بقانون العقوبات.

بداية ينبغي الإشارة إلى أن المشرع الجزائري تطرق لأول مرة لجريمة إفشاء الأسرار المعلوماتية في القسم السابع مكرر من قانون 04-15 المعنون بالمساس بأنظمة المعالجة الآلية للمعطيات، بحيث خصها بالمادة 394 مكرر 2/2، وهي مسألة تحسب له إذا ما تمت مقارنته بغيره من التشريعات العربية التي لم تتطرق إلى تجريم ذلك الفعل إلا منذ سنة 2007.[2]

بالرجوع للمادة 394 مكرر 2 نجدها تعاقب كل من يقوم عمدا أو عن طريق الغش بإفشاء المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في القسم الوارد تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، وعليه فإن كل من يعمد إلى إخبار الغير

[1]- قانون 18-05 المؤرخ في 10مايو سنة 2018 المتعلق بالتجارة الإلكترونية، سابق الإشارة إليه.
[2]- يراجع في ذلك، ص. 280 من هذه الأطروحة.

بالمعلومات التي وصل إليها بسبب دخوله غير المشروع، أو بسبب بقاءه غير المشروع في كل أو جزء من منظومة المعالجة الآلية للمعطيات يكون قد ارتكب جريمة إفشاء معلومات سرية، ذلك أن المعلومات التي يعلم بها الجاني أثناء أو بمناسبة عملية الدخول أو البقاء غير المصرح به في أنظمة المعالجة الآلية للمعطيات تشكل سراً، ويترتب على إفشاءه حرج للغير.

بهذا يتضح أن المشرع استخدم كلمة إفشاء، والتي ينصرف مدلولها إلى اطلاع الغير على المعلومة الواردة بالمستند، وذلك بأي طريقة كانت، سواء بالكتابة، شفاهة أو بالإشارة[1].

ولا يشترط لقيام الجريمة أن يتم الإفشاء بكل المعطيات، بل يكفي أن يتم الإفشاء بجزء منها، كما لا يشترط أن يكون الإفشاء للكافة، بل يكفي أن يكون لشخص واحد فحسب.

ولعل مما ينبغي التنويه إليه في هذا الإطار أن المشرع استخدم في المادة 394 مكرر 2 مصطلح المعطيات المتحصل عليها، ولم يستخدم مصطلح "السر" وهي الكلمة التي ورد ذكرها في المادة 301 من قانون العقوبات[2]، ذلك أنه يعتبر كافة المعطيات التي يتم الحصول عليها بسبب الدخول غير المشروع أو البقاء غير المشروع في أنظمة المعالجة الآلية للمعطيات تعد سراً، كون أن المتحصل عليها غير مصرح له بالدخول إلى النظام.

2- الركن المادي لجريمة إفشاء البيانات الإلكترونية الواردة في قوانين خاصة.

لقد سبق الذكر أن المشرع الجزائري جرم إفشاء سرية البيانات الإلكترونية في نصوص خاصة، ومن ذلك ما قرره في قانون التوقيع والتصديق الإلكترونيين، حينما أناط لمؤدي خدمات التصديق الإلكتروني التزامات متعددة أهمها الالتزام بالحفاظ على سرية

[1]- أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، ج1، الجرائم ضد الأشخاص والجرائم ضد الأموال، طبعة منقحة ومتممة في ضوء النصوص الجديدة، ط 6، دار هومة- الجزائر، 2007، ص. 248.

[2]- تنص المادة 301 من ق.ع.ج المعدل والمتمم:" يعاقب بالحبس من شهر إلى ستة أشهر و بغرامة من 500 إلى 5000 دج الأطباء والجراحون و الصيادلة و القابلات و جميع المؤتمنين بحكم الواقع أو المهنة أو الوظيفة الدائمة أو المؤقتة على أسرار أدلي بها إليهم و أفشوها في غير الحالات التي يوجب عليهم فيها القانون إفشاءها ويصرح لهم بذلك.
ومع ذلك فلا يعاقب الأشخاص المبينون أعلاه، رغم عدم إلتزامهم بالإبلاغ عن حالات الإجهاض التي تصل إلى علمهم بمناسبة ممارستهم مهنتهم ، بالعقوبات المنصوص عليها في الفقرة السابقة إذا أبلغو بها ، فإذا دعوا للمثول أمام القضاء في قضية إجهاض يجب عليهم الإدلاء بشهادتهم دون التقيد بالسر المهني".

البيانات والمعلومات المتعلقة بشهادة التصديق الإلكتروني، وكرس في سبيل حماية هذه البيانات تجريم عملية الإفشاء التي تصدر منهم، وعاقب عليها بموجب نص المادة 70 التي تنص: «يعاقب... كل مؤدي خدمات التصديق الذي أخل بأحكام المادة 42 من هذا القانون»، وهي المادة التي تعالج الالتزام الآنف ذكره.

من خلال هذا يتبين أنه لقيام الركن المادي لا بد أن يقوم مزود خدمات التصديق بإتيان السلوك المعاقب عليه بموجب المادة 70 من القانون 15-04 والمتمثل في إفشاء المعلومات والبيانات التي تم تزويده بها لغرض إصدار شهادات التصديق الإلكتروني.

ولئن كان المشرع الجزائري جرم عملية إفشاء مزود خدمات التصديق للبيانات المقدمة له لإصدار شهادة التصديق الإلكتروني، فإن المشرع المصري جرم هو الآخر إنتهاك سرية البيانات، بحيث قرر في المادة 21 من قانون تنظيم التوقيع الالكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات أن الجهة المرخص لها بإصدار شهادات التصديق الإلكتروني ملزمة بالحفاظ على سرية بيانات التوقيع الالكتروني، الوسائط الإلكترونية والمعلومات، بحيث لا يجوز لمن قدمت إليه تلك المعلومات أو اتصل بها بحكم عمله إفشاؤها للغير[1].

استنادا لما تقدم، يتضح أن الجاني في هذه الجريمة شخص له صفة في تدوين البيانات التي تمت معالجتها وله علاقة مشروعة بالمعلومات، وهو من قام بإفشائها للغير في غير الغرض الذي خصصت له[2].

وإذا كان المشرع الجزائري قصر الالتزام بالحفاظ على سرية البيانات والمعلومات المتعلقة بشهادات التصديق الإلكتروني على مؤدي خدمات التصديق الإلكتروني، فإن المشرع المصري جرم انتهاك السرية الصادر من مزود الخدمة ولكل من اتصل بها بحكم

[1]- تنص المادة 21 من القانون رقم 15 لسنة 2004 بشأن تنظيم التوقيع الالكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات، سابق الإشارة إليه:" بيانات التوقيع الإلكتروني والوسائط الإلكترونية والمعلومات التي تقدم إلى الجهة المرخص لها بإصدار شهادات التصديق الإلكتروني سرية، ولا يجوز لمن قدمت إليه أو اتصل بها بحكم عمله إفشاؤها للغير أو استخدامها في غير الغرض الذي قدمت من أجله."

[2]- عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، المرجع السابق، ص.551.

عمله، وهو يقصد بذلك معاونيه اللذين توصلو إليها عند قيامهم بعملهم في معالجة تلك البيانات أو عند استخراجهم لشهادة التصديق الالكتروني بمناسبة إحدى عمليات التجارة الالكترونية[1].

هذا ويتضح أن المقصود بإفشاء المعلومات يشمل إذاعتها، نقلها أو إطلاع الغير عليها، ذلك أن هذه المسألة يترتب عليها خروجها من حيز الكتمان والسرية، بعد أن كان العلم بها قاصراً على أصحابها أو الذين ائتمنوا عليها بحكم وظيفتهم، وهم في هذه الجريمة مزودي خدمة المصادقة الإلكترونية، ومعاونيهم الذين يقومون بدون علم ورضاء صاحبها بإفشاء السر.

ويستوي في المعلومات التي يتم إفشاؤها أن تكون مكتوبة في أوراق، أو مسجلة على دعامة إلكترونية على شريط مرن أو قرص مدمج، أو تكون مخزنة ضمن برنامج معلوماتي في جهاز حاسب آلي واطلع عيها مزود الخدمة أومعاونوه عند القيام بعملهم..

وللإشارة فإن المشرع التونسي تبنى في الفصل 52 من قانون المبادلات والتجارة الالكترونية الطرح ذاته الذي عول عليه المشرع المصري، غير أنه كان أكثر دقة منه، بحيث جرم إفشاء المعلومات التي عهد بها إلى مزود خدمات المصادقة الإلكترونية وأعوانه، باستثناء الحالة التي يرخص لهم صاحب الشأن فيها وبمقتضى شهادة كتابية أو إلكترونية بنشرها أو الإعلام بها[2].

إن ما ينبغي الإشارة إليه كذلك أن المشرع الجزائري عاقب المكلف بالتدقيق[3] عن إفشاء المعلومات السرية التي اطلع عليها أثناء قيامه بالتدقيق، وذلك بموجب المادة 73 من

---

[1]- عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، المرجع السابق، ص.552.

[2]- تنص المادة 52 من قانون رقم 83 لسنة 2000 المتعلق بالمبادلات والتجارة الإلكترونية، سابق الإشارة إليه : "يعاقب طبقا لأحكام الفصل 254 من المجلة الجنائية مزود خدمات المصادقة الإلكترونية وأعوانه الذين يفشون أو يحثون أو يشاركون في إفشاء المعلومات التي عهدت إليهم في إطار تعاطي نشاطاتهم بإستثناء تلك التي رخص صاحب الشهادة كتابيا في نشرها أو الاعلام بها وفي الحالات المنصوص عليها في التشريع الجاري بع العمل."

[3]- إن أهمية المعلومات الواردة لكل من مؤدي خدمات التصديق، الطرف الثالث الموثوق دفعت بالمشرع الجزائري إلى منح جهة مختصة القيام بعملية التدقيق، وتتمثل هذه الجهة في الهيئة الحكومية على مستوى الطرف الثالث الموثوق الذي يتولى متابعة ومراقبة نشاط السلطة الحكومية للتصديق الإلكتروني، وذلك حسب المادة 28 من ق. 15-04، في حين تقوم السلطة الاقتصادية بمهمة التدقيق أو تعهد بها إلى مكاتب تدقيق معتمدة إذا كانت المعلومات المطلوبة من مزود خدمات التصديق،=

قانون 15-04، ويشمل المكلف بالتدقيق السلطة الاقتصادية أو مكاتب التدقيق المعتمدة إذا كانت المعلومات مقدمة إلى مزود خدمة التصديق، أما إذا كانت المعلومات مقدمة للطرف الثالث الموثوق، فإن الهيئة الحكومية هي المكلفة بالتدقيق، على أن يقوم بتدقيق المعلومات المقدمة لكل من السلطتين الحكومية والاقتصادية الهيئة الحكومية المكلفة بالتدقيق المتواجدة على مستوى السلطة الوطنية.

انطلاقا مما تقدم، يلاحظ أن الأمين على السر في قانون التوقيع والتصديق الإلكترونيين، إما يكون مؤدي خدمات التصديق وفقا لما ورد في المادة 70 من قانون 15-04، أو المكلف بالتدقيق وفقا لما ورد في المادة 73 من ذات القانون.

هذا وقد ألقى المشرع الجزائري في المادة 26 من قانون 18-05 المتعلق بالتجارة الإلكترونية على عاتق المورد الإلكتروني الذي يقوم بجمع المعطيات ذات الطابع الشخصي للزبائن إلتزاما بالإقتصار على جمع البيانات الضرورية دون غيرها، وذلك بعد حصوله على موافقة المستهلكين الإلكترونيين، وتعهده بضمان أمن نظم المعلومات وسرية البيانات[1]، ووفقا لهذا النص يتضح أن المشرع الجزائري يلزم المورد الإلكتروني وهو كل شخص طبيعي أو معنوي يقوم بتسويق أو إقتراح توفير السلع أو الخدمات عن طريق الإتصالات الإلكترونية[2] بالحفاظ على سرية البيانات، وذلك بتوفيره لأنظمة حماية على أعلى المستويات، وذلك لمنع الغير من الكشف عن أسرار المستهلكين الإلكترونيين[3].

=وذلك ما قررته المادة 8/30 من قانون 15-04، على أن تقوم الهيئة االوطنية المكلفة بالتدقيق بالقيام بعمليات التدقيق على مستوى السلطتين الحكومية والاقتصادية، وذلك ما تم التأكيد عليه بموجب المادة 5/18 من قانون 15-04.
ونظرا لعدم تفعيل هذه الهيئات على أرض الواقع، فقد أوكلت مهام التدقيق إلى مصالح مختصة في هذا المجال، والمفروض أن تحدد هذه المصالح عن طريق التنظيم، غير أن هذا ألأخير لم يصدر لحد الآن.

[1]- تنص المادة 26 من قانون 18-05 المتعلق بالتجارة الإلكترونية، سابق الإشارة إليه بأنه: "ينبغي للمورد الإلكتروني الذي يقوم بجمع المعطيات ذات الطابع الشخصي ويشكل ملفات الزبائن و الزبائن المحتملين، ألا يجمع إلا البيانات الضرورية لإبرام المعاملة التجارية، كما يجب عليه:
- الحصول على موافقة المستهلكين الإلكترونيين قبل جمع البيانات
- ضمان أمن نظم المعلومات وسرية البيانات،...."

[2]- المادة 4/6 من قانون 18-05 المتعلق بالتجارة الإلكترونية، سابق الإشارة إليه.

[3]- تعرف المادة 3/6 من قانون 18-05 المتعلق بالتجارة الإلكترونية، سابق الإشارة إليه المستهلك الإلكتروني بأنه: " كل شخص طبيعي أو معنوي يقتني بعوض أو بصفة مجانية سلعة أو خدمة عن طريق الإتصالات الإلكترونية من المورد الالكتروني بغرض الإستخدام النهائي".

ثانياً: الركن المعنوي لجريمة إفشاء البيانات الإلكترونية.

تقتضي مساءلة الجاني عن جريمة إفشاء الأسرار الواردة بالمستند الإلكتروني توافر القصد الجنائي العام بعنصريه العلم والإرادة، إذ لا بد أن يكون الفاعل عالماً بالفعل المكون للجريمة، ومع ذلك تتجه إرادته إلى قبول النتيجة المترتبة عنه، والمتمثلة في الاعتداء على الحق الذي يحميه القانون، أي المساس بالمعلومات المخزنة إلكترونيا أو المحررات الإلكترونية السرية، الأمنية أو الاقتصادية أو حتى التي تحوي بيانات اسمية[1].

فالجاني يسعى بإرادته إلى إفشاء المحررات الإلكترونية السرية مع علمه التام بماديات الواقعة المجرمة قانونا، وبأن تلك المحررات سرية لا يباح إطلاع الغير عليها، ورغم ذلك تتجه إرادته إلى التعدي عليها.

بهذا يتبين أن تطبيق المبادئ العامة على الركن المعنوي لجريمة انتهاك سرية المستندات الإلكترونية يقتضي علم الجاني بأنه يدخل إلى مستندات إلكترونية سرية بالمعنى المحدد سلفا، وأنه لا يجوز له الدخول إليها.

بهذا يبدو أن جريمة إفشاء السر المعلوماتي جريمة شكلية، وعليه فإنه لا ينبغي لتحققها توفر نية الإضرار بصاحب السر، ذلك أن الالتزام بكتمان السر يعود إلى رغبة المشرع في حماية المصلحة العامة لا حماية صاحب السر فحسب، وعليه لا يشترط المشرع نية خاصة أو نية الإضرار بالغير لقيام جريمة إفشاء السر، ذلك أن إفشاء السر في حد ذاته من الأفعال الشائنة التي لا تحتاج إلى قصد خاص يؤكدها[2].

كما ينبغي الذكر أن متابعة الجاني بجريمة انتهاك السر لا تستلزم الإعتداد بالباعث الذي دفع الجاني لإرتكاب الجريمة، فالبواعث والأغراض ليست من عناصر القصد الجنائي، ولا تؤثر في قيام هذه الجريمة، إلا إذا نص القانون على خلاف ذلك.

[1]- محمد نجيب حسني، المرجع السابق، ص، ص. 36- 37.
[2]- أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، ج1، المرجع السابق، ص. 249.

مما تقدم، يُلاحظ أن توافر القصد الجنائي من عدمه مسألة موضوعية، وعليه فإن تقديرها يظل متروكاً لسلطة محكمة الموضوع، التي تملك صلاحية تقديرها بحسب ما يتوافر لديها من أدلة طبقا لوقائع الدعوى وظروفها.

البند الثاني: العقوبة المقررة لجريمة إفشاء المعلومات الإلكترونية.

يترتب على تحقق أركان جريمة إفشاء سرية البيانات الإلكترونية معاقبة مرتكب الفعل، وفي هذا الإطار ينبغي الذكر بداية أن المشرع خص جريمة إفشاء المعلومات السرية الواردة بالمادة 394 مكرر 2 من قانون العقوبات بالحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج، على أن تضاعف هذه العقوبات إذا استهدفت الجريمة الدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام، وذلك وفق ما تقرره المادة 394 مكرر 3.

في حين تكون العقوبة رفع الحد الأقصى للغرامة بخمس مرات إذا كان مقترف الجريمة شخصا معنويا، وعليه فإن مقدار الغرامة يكون 25.000.000 دج.

للإشارة فإن المشرع عاقب بموجب المادة 394 مكرر 5 كل من شارك في مجموعة أو اتفاق مؤلف بغية الإعداد لهذه الجريمة متى كان التحضير للجريمة مجسدا في فعل أو عدة أفعال مادية، وقرر لهذا الفعل العقوبات المقررة للجريمة ذاتها[1]، كما عاقب المشرع بموجب المادة 394 مكرر 7 على الشروع بذات العقوبات المقررة للجريمة[2].

هذا عن العقوبات الأصلية، أما بخصوص العقوبات التكميلية، فقد ورد ذكرها في المادة 394 مكرر6[3] وتتمثل في مصادرة الأجهزة والوسائل المستخدمة، إغلاق المواقع التي

---

[1]- تنص المادة 394 مكرر5 من قانون 04-15 المعدل والمتمم لقانون العقوبات الجزائري، سابق الإشارة إليه على أنه: "كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية بالعقوبات المقررة للجريمة ذاتها."

[2]- تنص المادة 394 مكرر7 من قانون 04-15 المعدل والمتمم لقانون العقوبات الجزائري، سابق الإشارة إليه على أنه: "يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها."

[3]- تنص المادة 394 مكرر6 من قانون 04-15 المعدل والمتمم لقانون العقوبات الجزائري، سابق الإشارة إليه على أنه: "مع الإحتفاظ بحقوق الغير حسن النية، يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على إغلاق المحل أو مكان الإستعلال إذا كانت الجريمة قد ارتكبت بعلم مالكها."

كانت محلا للجريمة، إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة ارتكبت بعلم مالكها.

هذا عن العقوبات المقررة لجريمة إفشاء سرية البيانات الواردة في أحكام قانون العقوبات، أما إذا كانت الجريمة من الجرائم الواردة في قانون التوقيع والتصديق الإلكترونيين، فإن العقوبة ستكون حسب المادة 70 من القانون آنف الذكر بالحكم على مؤدي خدمات التصديق بالحبس من ثلاث (3) أشهر إلى سنتين (2)، وغرامة من مائتي ألف دينار (200.000) إلى مليون دينار (1000.000 دج)، أو إحدى هاتين العقوبتين فقط.

أما إذا كان مقترف الفعل من المكلفين بالتدقيق، فإن العقوبة حسب المادة 73 من قانون 15-04 هي الحبس من ثلاثة أشهر (03) إلى سنتين (2) وبغرامة من عشرين ألف دينار (20.000 دج) إلى مائتي ألف دينار (200.000 دج)، أو بإحدى هاتين العقوبتين.

أما إذا كان مقترف الجرائم الواردة بالمادتين 70 و73 من القانون المذكور شخصا معنويا، فإن العقوبة هي الغرامة المقدرة بـ 5 مرات الحد الأقصى المقرر للغرامة المنصوص عليها بالنسبة للشخص الطبيعي، وعليه تكون الغرامة بالنسبة لمؤدي خدمات التصديق هي 5 مليون دينار (5000.0000 دج) في حين تكون بالنسبة للمكلف بالتدقيق مليون دينار (1000.000 دج).

الفرع الثاني: جريمة تجميع أو توفير بيانات مخزنة أو معالجة آلياً.

في إطار ضمان سرية البيانات الإلكترونية، ولغرض توفير الثقة لدى المتعاملين في المجال الإلكتروني عملت التشريعات المقارنة على توسيع الحماية الجنائية لما أسمته بنظم المعالجة الآلية للمعطيات، بحيث بسطت هذه الحماية لتشمل المجال المتصل بالبيانات أو المعلومات، ففضلاً عن تجريمها لفعل الدخول غير المشروع في كامل المنظومة أو في جزء منها، وكذا تجريمها لفعل البقاء فيها اعتبرت أن عملية التجميع أو التقاط البيانات أو استغلالها أو نشرها أو الاتجار فيها من الجرائم المعاقب عليها قانونا[1].

[1]- زيبحة زيدان، المرجع السابق، ص. 62.

لأهمية هذه الجريمة يتوجب التعرض لأركانها **(البند الأول)** والعقوبات المقررة لها **(البند الثاني)**.

البند الأول: أركان الجريمة.

يتطلب لقيام جريمة تجميع أو توفير بيانات مخزنة أو معالجة آليا أو إستغلالها أو نشرها أو الإتجار فيها توافر ركنين أحدهما مادي والثاني معنوي، وهو ما سيتم التطرق إليه.

أولاً: الركن المادي للجريمة.

لا ريب في أن الركن المادي لهذه الجريمة يتمثل في إتيان الجاني سلوكات قد تكون إيجابية وقد تكون سلبية، وفي الجريمة محل الدراسة يلاحظ أن الركن المادي يتخذ صوراً متعددة تشمل فعل التجميع أي تجميع البيانات بطريقة غير مشروعة، وكذا فعل التوفير غير المشروع للبيانات الإلكترونية، فأما عن فعل التجميع فيقصد به جمع البيانات الإلكترونية الواردة في المستندات المخزنة في الحاسب الآلي، وذلك باستعمال طرق احتيالية مضللة ودون حق يُجيز جمعها والحصول عليها، على أن يتم استعمالها دفعة واحدة لأغراض غير مشروعة[1].

هذا عن فعل التجميع أما عن فعل توفير البيانات الإلكترونية وإلتقاطها بصورة غير مشروعة، فيقصد به حسب القانون العربي الموحد: «الالتقاط البصري أي الاستحواذ البصري للبيانات، بمعنى حيازتها والتقاطها ذهنيا وبصريا من الشاشة»[2].

حسب هذا التعريف يتجه جانب من الفقه إلى أن المقصود بالالتقاط هو الالتقاط البصري، أي إدراك البيانات من وسيط إلكتروني بالبصر، كأن تكون معروضة على شاشة الحاسب الآلي ومخزنة فيه، أو معروضة على شاشة الحاسب من خلال تفحص أحد مواقع

[1]- في عملية تجميع البيانات الإلكترونية من أجل استعمالها لغرض غير مشروع يستوي أن يتم جمع هذه البيانات عن طريق أخذها من قاعدة التخزين أو أثناء تبادلها عبر شبكة الإنترنت. مشار إليه من طرف، زيبحة زيدان، المرجع السابق، ص.62.

[2]- عبد الفتاح بيومي حجازي، التزوير في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص. 78.

شبكة الإنترنت أو معروضة على شاشة الهاتف المحمول الذي تتوافر فيه خاصية الاتصال بشبكة الإنترنت، أو الهاتف العادي ذو الشاشة المرئية الذي يمكن من خلاله للمتحدث أن يرى الطرف الآخر، أو أن تكون البيانات معروضة في جهاز التلفاز العادي من خلال اتصاله بشبكة الإنترنت.

لا ريب في أن هذا الإتجاه الفقهي يتبنى المفهوم الضيق للإلتقاط، في حين يتبنى إتجاه فقهي آخر المعنى الموسع له ومفاد ذلك، أن أنصار الإتجاه الأخير يرون أن الإتجاه الأول إقتصر في تعريفه للإلتقاط على الشطر الأول من التعريف الوارد بالقانون العربي الموحد، دون الشطر الثاني الذي ورد فيه عبارة أشمل كالحيازة والإلتقاط الذهني والبصري من الشاشة .

وبهذا فإن فعل الالتقاط يستلزم الحيازة بمعنى حيازة البيانات الإلكترونية قبل التقاطها بصرياً أو ذهنياً[1].

وفي الجريمة محل الدراسة يشترط أن يكون تجميع وتوفير، وكذا إلتقاط البيانات المخزنة والمعالجة آلياً قد تم بطريق غير مشروع، وأنه تم إستغلالها أو نشرها، أو الإتجار فيها، ويستوي أن يكون الجاني مالكا للنظام المعلوماتي أو مستأجراً له أو منتفعاً به ، ويستوي لتحقق هذه الجريمة أن يتم إلتقاط المعلومات والدخول إليها عن طريق التجسس المعلوماتي أو بطريق الاحتيال.

وللإشارة فإن قيام هذه الجريمة لا يقتصر على كون المعلومات أو المعطيات الإلكترونية مخزنة داخل النظام المعلوماتي ذاته، بل يمتد ليشمل المعلومات المعالجة آليا والمخزنة بواسطة الأشرطة والأقراص الممغنطة[2].

[1]- عبد الفتاح بيومي حجازي، التزوير في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص، ص. 76- 77.
[2]- زيبحة زيدان، المرجع السابق، ص، ص. 62- 63.

ثانياً: الركن المعنوي للجريمة.

لاشك في أن الجريمة تشمل إلى جانب ركنها المادي ركنا نفسيا، ويمثل الركن المعنوي الأحوال النفسية لماديات الجريمة والسيطرة النفسية عليها، وعليه ينبغي لقيام الركن المعنوي علم الجاني بماديات الجريمة واتجاه إرادته إلى تحقيقها[1]، وبالرجوع للجريمة محل الدراسة فإنه يتوجب الإشارة إلى أن توافر الركن المعنوي فيها أي القصد الجنائي يتطلب علم الجاني بجميع عناصر الجريمة أي ماديات الجريمة الواردة بالنص القانوني والسالف ذكرها، وهذا العلم في الواقع مفترض، ذلك أنه لا يعتد بجهل القاعدة القانونية، ولايكفي لتحقق الركن المعنوي توفر عنصر العلم بل لابد أن تتجه إرادة الجاني إلى إتيان ذلك السلوك.

وللإشارة فإن الإرادة عبارة عن قوة نفسية أو نشاط نفسي يوجهها الجاني إلى تحقيق غرض غير مشروع، ولا بد أن تنصرف الإرادة للسلوك والنتيجة معاً[2]، ويشمل هذا الغرض في الجريمة محل الدراسة تجميع والتقاط البيانات الإلكترونية، والتي تتخذ دعامة لها المستند الإلكتروني أو استغلالها أو نشرها أو الاتجار فيها.

ويستوي في ذلك أن يحقق الجاني من وراء فعله هدفاً شخصياً أو مصلحة للغير، والمقصود بالغير في هذه الحالة مالك أو صاحب النظام المعلوماتي نفسه، أو أي شخص مستأجر أو منتفع به، بمعنى أعم وأشمل كل من له مصلحة في تلك البيانات والمعلومات.

وبما أن الجريمة محل الدراسة من الجرائم العمدية، فإنه يستوي لتحققها أن يتم إلتقاط المعلومات والوصول إليها عن طريق التجسس المعلوماتي أو بطرق الاحتيال، لا سيما إذا تم ارتكاب هذه الأفعال بغرض استهداف بيانات سرية تجارية، عسكرية أو غيرها، أو إذا تعلق الأمر بجمع معلومات يمنع جمعها كما تقتضيه طبيعتها كتلك المتعلقة بالأسرة أو بالمعتقدات الدينية أو السياسية، أو بمعلومات إحصائية تختص بها الهيئات الرسمية[3].

---

[1]- جلال محمد الزعبي، أسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية، دراسة مقارنة، ط1، دار الثقافة، الأردن، 2010، ص ،ص. 55- 56.

[2]- جلال محمد الزعبي، أسامة أحمد المناعسة، المرجع السابق، ص، ص. 56- 57.

[3]- زيبحة زيدان، المرجع السابق، ص ص. 62.- 63.

إلى جانب القصد العام المشار إليه سابقاً، فإن هناك بعض التشريعات المقارنة التي تتطلب لقيام الركن المعنوي تحقق القصد الخاص، وهو ما عبرت عنه بنية الغش أو بمصطلح "عن طريق الغش"، وعليه لا يكفي عند تطلب القصد الخاص أن يكون الجاني قد تصرف بطريقة عمدية، بل يجب أن تكون لديه نية الغش، ذلك أن عملية تجميع البيانات أو الاتجار غير المشروع فيها يعد من صميم الإجرام المعلوماتي، ولعل من التشريعات التي تطلبت توفر القصد الخاص إتفاقية بودابست لمكافحة الإجرام المعلوماتي، والتشريع الجزائري في القانون المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات[1].

ولعل ما يميز نية الغش كقصد خاص يختلف عن القصد الخاص الذي كانت تتطلبه نصوص الجرائم السابق دراستها عنصر تجاهل حقوق الغير، وهو ما يُفسر في أن الغش يتضمن معنى العلم وإرادة إحداث ضرر للغير.

البند الثاني: العقوبة المقررة للجريمة.

نظراً لخطورة الجريمة محل الدراسة على المعاملات الإلكترونية، ولضمان حرية أكبر لسرية وخصوصية البيانات الإلكترونية، فقد حظيت هذه الجريمة باهتمام التشريعات المقارنة الدولية والداخلية، بحيث حاولت هذه الأخيرة جاهدة التصدي لهذه الأفعال، وذلك بفرض عقوبات جزائية في نصوصها العقابية.

فعلى الصعيد الدولي أشارت إتفاقية بودابست لمكافحة الإجرام المعلوماتي في المادة الثالثة منها لهذه الأفعال تحت مصطلح الإعتراض غير القانوني للبيانات الإلكترونية، و جاء نصها كالتالي: «يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من أجل اعتبارها جريمة جنائية، واقعة الاعتراض العمدي وبدون حق، من خلال وسائل فنية للإرسال غير العلني لبيانات الحاسب في مكان الوصول، في المنشأ، أو في داخل النظام المعلوماتي، بما في ذلك انبعاثات كهرومغناطيسية من جهاز حاسب يحمل

[1]- قانون 04-15 المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات المعدل والمتمم لقانون العقوبات الجزائري، سابق الإشارة إليه.

هذه البيانات، كما يجب لأي طرف أن يستوجب أن ترتكب الجريمة بنية إجرامية (بقصد الغش)، أو أن تُرتكب الجريمة في حاسب آلي يكون متصلاً عن بعد بحاسب آخر»[1].

حسب المذكرة التفسيرية لهذه الاتفاقية يكمن الهدف من المادة الثالثة في حماية الحق في إحترام السرية والخصوصية في نقل البيانات، ذلك أن هذه الجريمة تمثل انتهاكاً للحق في إحترام الاتصالات، والتي يمتد مفهومها حسب الاتفاقية ليشمل وسائل نقل بيانات الحاسب، وكذلك انبعاثات الإشعاع الكهرومغناطيسي، لا سيما إذا كانت تلك البيانات سرية ومهمة[2].

هذا عن موقف إتفاقية بودابست، أما عن موقف التشريعات الأجنبية والوطنية من هذه الجريمة، فيلاحظ أن المشرع الفرنسي على الرغم من أنه خصص المادة 323 من قانون العقوبات الفرنسي بفقراتها السبعة لتجريم الاعتداء على سلامة أنظمة المعالجة الآلية للمعطيات، إلا أنه لم يخصص فقرة تتطرق لفعل تجميع وتوفير البيانات الإلكترونية أو الإتجار غير المشروع فيها، وذلك على خلاف المشرع الجزائري الذي جرم في المادة 394 مكرر2 من قانون العقوبات هذا الفعل وقرر له عقوبة الحبس والغرامة، والتي جاء فيها بأنه: «يعاقب بالحبس من شهرين إلى ثلاث سنوات وبغرامة من 1000.000 دج إلى5.000.000 دج كل من يقوم عمداً أو عن طريق الغش بما يأتي:

1 - بتصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أو يرتكب بها الجرائم المنصوص عليها في هذا القسم»، هذا وقد ضاعف المشرع العقوبة المقررة في المادة المذكورة سابقاً إذا إستهدفت

[1]- Article 3 du convention sur la cybercriminalité dispose que : «Chaque partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne l'accès intentionnel et sans droit, effectuée par des moyens techniques de données informatiques, lors de transmission non publique, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques, une partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique.»

[2]- هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة الجرائم المعلوماتية معلقاً عليها، المرجع السابق، ص. 59.

هذه الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام[1]، كما وعاقب المشرع الجزائري على الشروع في إرتكاب هذه الجريمة وقرر لمرتكبها العقوبة المقررة لمرتكب الجنحة ذاتها[2].

إلى جانب العقوبات الأصلية التي فرضها المشرع الجزائري على مرتكب الجريمة محل الدراسة، يلاحظ أن المشرع فرض عقوبات تكميلية أوردها في نص المادة 394 مكرر 6 من القانون رقم 04-15المعدل والمتمم لقانون العقوبات الجزائري، هذا إذا كان مرتكب الفعل شخصاً طبيعياً، أما إذا كان مرتكب الجريمة محل الدراسة شخصاً معنويا فقد قرر المشرع الجزائري له في المادة 394 مكرر4 من قانون العقوبات الغرامة التي تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي .

إن تقرير العقوبات السابق ذكرها الغرض منه ضمان سلامة وسرية المعطيات المخزنة بالنظام المعلوماتي، وكذا تعزيز الثقة والائتمان في التعاملات الإلكترونية التي أصبحت سمة هذا العصر وعلامة دالة عليه.

المطلب الثالث:الأعمال الماسة بالتوقيع الالكتروني على المستند.

نظرا لما للتوقيع الالكتروني من أهمية بالغة في مجال توثيق إرادة المتعاقدين، وكذا التعرف على أطراف المعاملة الالكترونية، عمد المشرع الجزائري إلى سن نصوص قانونية تجرم المساس به، وذلك من خلال القانون 15-04 المتضمن التوقيع والتصديق الإلكترونيين، وبتصفح مواد هذا القانون في شقها الجزائي يتبين أن المشرع الجزائري حدد بعض الجرائم المتعلقة بالتوقيع دون أن يدرج تقسيما لها، ولكن يمكن من خلال الرجوع إلى هذا القانون تقسيم الأحكام الجزائية الضابطة للاعتداء على التوقيع الالكتروني الى ثلاث أنواع: جرائم مرتكبة من طرف مؤدي خدمات التصديق **(الفرع الأول)**، جرائم مرتكبة من طرف المستفيد **(الفرع الثاني)**، وجرائم واقعة على التوقيع الالكتروني يرتكبها الغير **(الفرع الثالث).**

[1]- المادة 394 مكرر 3 من قانون 04-15 المعدل والمتمم لقانون العقوبات الجزائري، سابق الإشارة إليه.
[2]- المادة 394 مكرر 7 من القانون رقم 04-15المعدل والمتمم لقانون العقوبات الجزائري، سابق الإشارة إليه.

الفرع الأول: الجرائم المرتكبة من طرف مؤدي خدمات التصديق.

الجرائم المرتكبة من طرف مؤدي خدمات التصديق هي الجرائم التي تطرق إليها المشرع الجزائري بموجب القانون 15-04 المتعلق بالتوقيع والتصديق الالكترونيين، وإشترط في مرتكبها تحقق صفة محددة وهي صفة مؤدي خدمات التصديق، و تتمثل هذه الأفعال في كل من جريمة عدم إعلام السلطة الإقتصادية بالتوقف عن النشاط **(البند الأول)**، جريمة الإخلال بإلتزام تحديد هوية طالب شهادة التصديق الإلكتروني **(البند الثاني)**، جريمة جمع البيانات الشخصية للمعني دون موافقته الصريحة وإستعمالها إستعمالا غير مشروع **(البند الثالث)**، جريمة مزاولة النشاط بدون ترخيص **(البند الرابع)**.

البند الأول: جريمة عدم إعلام السلطة الاقتصادية بالتوقف عن النشاط.

خول المشرع الجزائري للسلطة الاقتصادية للتصديق الالكتروني مهمة متابعة ومراقبة مؤدي خدمات التصديق الذين يقدمون خدمات التوقيع والتصديق الالكتروني لصالح الجمهور، وعليه تتولى هذه السلطة منح التراخيص لمؤدي خدمات التصديق وتعمل على مراقبتهم، وبالمثل فإنه يقع على عاتق مقدمي خدمات التصديق إلتزام إتجاه السلطة الإقتصادية، وهو إعلامها خلال ميعاد معين حدده القانون بتوقفهم عن النشاط، وبهذا يتضح أن كل سلوك سلبي بعدم الإعلام عن التوقف عن النشاط يشكل جريمة يقتضي لتطبيق العقوبة على مقترفيها **(ثانيا)**، تحقق أركانها **(أولا)**.

أولا: أركان الجريمة.

إن قيام جريمة عدم إعلام السلطة الاقتصادية بالتوقف عن النشاط في الآجال المحددة بموجب المادتين 58 و59 من قانون التوقيع والتصديق الالكترونيين يستلزم تحقق ركنين، ركن مادي وآخر معنوي، يتمثل الركن المادي لها في عدم إعلام مؤدي خدمة التصديق للسلطة الاقتصادية بالتوقف الإرادي حسب المادة 58 من قانون 15-04، أو التوقف اللاإرادي عن مزاولة نشاطه حسب المادة 59 من ذات القانون.

من خلال ما سبق، يلاحظ أن المشرع الجزائري تطرق في المادة 58 من القانون آنف الذكر لحالة التوقف الإرادي، بحيث ألزم مؤدي خدمة التصديق بإعلام السلطة الاقتصادية ضمن الآجال المحددة في سياسة التصديق -باعتبارها المكلفة بمتابعة ومراقبة عمله[1]، ولكونها المكلفة بمنح الترخيص لمؤدي خدمة التصديق لمزاولة نشاطه[2]- عن رغبته في التوقف عن ممارسة نشاطاته المتعلقة بتأدية خدمات التصديق الإلكتروني، ذلك أن مقدم خدمة التصديق ملزم بضمان ديمومة واستمرارية الخدمات المقدمة من طرفه طيلة مدة مباشرة النشاط، ما لم يسحب ترخيصه منه[3].

ولئن كانت المادة 58 تعالج حالة التوقف الإرادي، فإن المادة 59 من القانون آنف الذكر تعالج حالة التوقف اللاإرادي[4]، وتلزم مؤدي خدمة التصديق الراغب في التوقف عن ممارسة نشاطه لأسباب خارجة عن إرادته إعلام السلطة الاقتصادية بذلك فورا لتقوم هذه الأخيرة بإلغاء شهادة التصديق الإلكتروني الخاصة به بعد تقديرها للأسباب المقدمة، مع إلزام مؤدي خدمات التصديق باتخاذ التدابير اللازمة والواردة في سياسة التصديق الإلكتروني للسلطة الاقتصادية من أجل حفظ المعلومات المرتبطة بشهادة التصديق الإلكتروني الموصوفة الممنوحة له.

انطلاقا مما تقدم، يلاحظ أن الركن المادي لقيام هذه الجريمة يتمثل في عدم إبلاغ السلطة الاقتصادية بالتوقف عن ممارسة النشاط في الآجال المحددة، وعليه يتضح أن النشاط الإجرامي يتمثل في عدم الإبلاغ ، دون أن يتطلب تحقق نتيجة معينة وهو الأمر الذي يجعل هذه الجريمة تصنف ضمن جرائم الخطر لا جرائم الضرر.

---

[1]- يراجع في ذلك المادة 30 من قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، سابق الإشارة إليه.

[2]- تنص المادة 33 من قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، سابق الإشارة إليه: "يخضع نشاط تأدية خدمات التصديق الإلكتروني إلى ترخيص تمنحه السلطة الاقتصادية للتصديق الإلكتروني."

[3]- تنص المادة 3/58 من قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، سابق الإشارة إليه: "يترتب على وقف النشاط سحب الترخيص."

[4]- تنص المادة 59 من قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، سابق الإشارة إليه على أنه: "يجب على مؤدي خدمات التصديق الإلكتروني الذي يوقف نشاطه لأسباب خارجة عن إرادته أن يعلم السلطة الإقتصادية للتصديق الإلكتروني بذلك فورا، وتقوم هذه الأخيرة بإلغاء شهادته للتصديق الإلكتروني الموصوفة بعد تقدير الأسباب المقدمة.
وفي هذه الحالة، يتخذ مؤدي الخدمات التدابير اللازمة، والمنصوص عليها في سياسة التصديق الإلكتروني للسلطة الإقتصادية، من أجل حفظ المعلومات المرتبطة بشهادة التصديق الإلكتروني الموصوفة الممنوحة له."

هذا عن الركن المادي، أما بخصوص الركن المعنوي فيمكن القول أن هذه الجريمة عمدية تقتضي توافر القصد الجنائي العام بعنصريه العلم والإرادة، ولا ريب في أن عنصر العلم متوافر إذ أن الشخص الذي يمارس هذا النشاط يعلم أن توقفه يقتضي إبلاغه للسلطة الاقتصادية ضمن آجال محددة، ورغم ذلك لا يحترمها، بل وتتجه إرادته إلى إقتراف السلوك المجرم.

ثانيا: العقوبة المقررة.

إن تحقق الركنين المادي والمعنوي، يجعل مؤدي خدمة التصديق مرتكبا لجريمة عدم إعلام السلطة الاقتصادية بالتوقف عن النشاط، وهو ما يجعله خاضعا للعقوبات الواردة بالمادة 67 من قانون 15-04 والمتمثلة في الحبس من شهرين (2) إلى سنة (1) واحدة، وبغرامة من مائتي ألف دينار (200.000دج) إلى مليون دينار(1.000.000دج)، أو بإحدى هاتين العقوبتين.

وتطبيق العقوبات السابقة يخص الشخص الطبيعي، فإن ارتكبت الجريمة من شخص معنوي، فالعقوبة هي الغرامة التي تعادل خمس (5) مرات الحد الأقصى للغرامة المنصوص عليها في المادة 67، وعليه تكون الغرامة حسب المادة 75 من القانون الآنف ذكره هي خمس مليون (5.000.000دج) .

البند الثاني: جريمة الإخلال بالتزام تحديد هوية طالب شهادة التصديق الإلكتروني.

فرض المشرع الجزائري على مقدم خدمات التصديق بموجب القانون رقم 15-04 مجموعة من الالتزامات، وذلك في إطار ممارسته لمهمته و المتمثلة في التحقق من صحة التوقيع الالكتروني عن طريق شهادة التصديق الالكتروني التي يصدرها، ولعل أهم هده الالتزامات الالتزام بتحديد هوية طالب شهادة التصديق، ومن ثم فإن الإخلال بهذا الالتزام يعتبر جريمة معاقبا عليها **(ثانيا)**، متى تحققت أركانها **(أولا)**.

أولا: أركان الجريمة.

لقد حدد المشرع الجزائري بموجب المادة 69 من قانون التوقيع والتصديق الإلكترونيين[1] أركان جريمة الإخلال بالتزام تحديد هوية طالب شهادة التصديق الإلكتروني، والتي تشمل ركنين ركن المادي، وركن المعنوي، يتمثل الركن المادي في إخلال مزود خدمة التصديق الالكتروني -باعتباره المكلف بإصدار هذه الشهادات لطالبها- بإلتزامه بتحديد هوية طالب شهادة التصديق الالكترونية الموصوفة، كون أنه المعني والملتزم بالتحقق من بيانات الشهادة، في حين يتمثل الركن المعنوي في القصد الجنائي العام، إذ ينبغي أن يعلم الجاني بما يقوم به، أي بإخلاله بالتزامه المتمثل في تحديد هوية طالب شهادة التصديق، ورغم ذلك تنصرف إرادته إلى إتيان هذا السلوك.

ثانيا: العقوبة المقررة.

يترتب على تحقق الركنين السالف ذكرهما قيام جريمة الإخلال بالتزام تحديد هوية طالب شهادة التصديق الإلكتروني، والتي تكون عقوبتها حسب المادة 69 من قانون التوقيع والتصديق الإلكترونيين الحبس من شهرين (2) إلى ثلاث (3) سنوات، وغرامة من عشرين ألف دينار (20.000دج) إلى مائتي ألف دينار (200.000دج) أو إحدى هاتين العقوبتين، على أن تطبيق هذه العقوبات يتقرر إذا ما كان الجاني شخصا طبيعيا، أما إن كان شخصا معنويا فإن العقوبة ستكون الغرامة المقدرة بمليون دينار (1.000.000دج) حسبما تقرره المادة 75 من القانون آنف ذكره[2].

البند الثالث: جريمة جمع البيانات الشخصية للمعني دون موافقته الصريحة واستعمالها استعمالا غير مشروع.

فرض المشرع الجزائري على مؤدي خدمات التصديق بموجب المادة 43 من القانون 15-04 التزاما مفاده عدم جمع البيانات الشخصية للمعني، إلا بعد موافقته الصريحة، كما

[1]- تنص المادة 69 من قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، سابق الإشارة إليه: "يعاقب بالحبس من شهرين إلى ثلاث سنوات و بغرامة من عشرين ألف دينار إلى مائتي ألف دينار أو بإحدى هاتين العقوبتين فقط، كل من يخل عمدا بالتزام تحديد هوية طالب شهادة تصديق إلكترونية موصوفة".

[2]- تنص المادة 75 من قانون15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، سابق الإشارة إليه: "يعاقب الشخص المعنوي الذي إرتكب إحدى الجرائم المنصوص عليها في هذا الفصل بغرامة تعادل خمس مرات الحد الأقصى للغرامة المنصوص عليها بالنسبة للشخص الطبيعي".

فرض عليه بموجب المادة المذكورة أن لا يستعمل هذه البيانات استعمالا غير مشروع، وعليه فإن كل إخلال بهده الالتزامات يشكل جريمة يعاقب عليها قانونا **(ثانيا)**، إذا ما توفرت أركانها **(أولا)**.

أولا: أركان الجريمة.

من المعلوم أن البيانات الشخصية تسمح بتحديد هوية الشخص بطريقة مباشرة أو غير مباشرة، ولارتباط هذه البيانات بخصوصية الشخص عمدت التشريعات إلى إحاطتها بسياج من الحماية ، إذ كرست هذه الحماية في النصوص القانونية الكلاسيكية في أكثر من موضع.

بهذا يبدوا أن سياسة المشرع الجزائري تتجه إلى حماية البيانات الشخصية في مجال معاملات البيئة المادية، وذلك لخطورة الوضع من جهة، ولارتباط الموضوع بالتزاماتها الدولية نتيجة لمصادقتها على العديد من المواثيق الدولية الرامية إلى احترام البيانات الشخصية.

وعليه يظهر أن المشرع الجزائري اشترط لقيام هده الجريمة توافر صفة معينة في الجاني وهي أن يكون مؤدي خدمات التصديق أو أحد العاملين لديه، كما اشترط توافر الركنين المادي والمعنوي.

أما الركن المادي في هذه الجريمة فيتحقق بإتيان الجاني فعلا إيجابيا متمثلا في جمع البيانات الشخصية للموقع دون الحصول على موافقته التي يجب أن تكون صريحة، مع استعمال تلك البيانات إستعمالا غير مشروع، أما الركن المعنوي لهذه الجريمة فيقوم بتوافر القصد الجنائي العام بعنصريه العلم والإرادة.

ثانيا: العقوبة المقررة.

عاقب المشرع الجزائري على هذا الفعل في نص المادة 71 من القانون15-04[1] والتي جاء فيها أنه:" يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات، وبغرامة من مائتي

[1]- تنص المادة 71 من قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، سابق الإشارة إليه : "يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات، وبغرامة من مائتي ألف إلى مليون دينار أو بإحدى هاتين العقوبتين فقط، كل مؤدي خدمات التصديق الإلكتروني أخل بأحكام المادة 43 من هذا القانون".

ألف دينار 200.000 دج إلى مليون دينار 1.000.000 دج، أو بإحدى هاتين العقوبتين فقط كل مؤدي خدمات التصديق الإلكتروني أخل بأحكام المادة 43 من هذا القانون".

تطبيق هذه العقوبات يتقرر إذا كان مقترف الفعل شخصا طبيعيا، أما إذا كان هذا الأخير شخصا معنويا فإن العقوبة ستكون الغرامة المقدرة بخمس مرات الحد الأقصى لغرامة الشخص الطبيعي، بمعنى تكون العقوبة الغرامة المقدرة بخمس ملايين دينار جزائري، وفقا لما تقضي به المادة 75 من القانون آنف الذكر.

البند الرابع: جريمة مزاولة النشاط بدون ترخيص.

من المتعارف عليه أنه لا يجوز لمؤدي خدمات التصديق سواء كان شخصا طبيعيا أو معنويا أن يزاول نشاطه دون أن يكون قد حصل مسبقا على ترخيص بمزاولة هذا النشاط ، وإلا عد مرتكبا لجريمة يعاقب عليها القانون، وللإشارة فإن الأهمية من تجريم هذا الفعل تكمن في أنه يشكل الإطار الرادع الذي يضمن إصدار الشهادات دون ترخيص، وذلك بسبب الآثار الخطيرة التي ترتبها هذه الشهادة في حق الغير، حيث يكون مضمونها تسليم بيانات التوقيع أو بيانات المعاملة المطلوب صدور شهادة التصديق عنها، ونظرا لأن هذا السلوك يشكك في الثقة التي يجب توافرها في المعاملات الالكترونية، فإنه سيتم بيان أركان هذه الجريمة **(أولا)**، وكذا العقوبة المقررة لها **(ثانيا)**.

أولا: أركان الجريمة.

لقد ترتب على ازدياد استخدام الأشخاص للحاسبات الآلية لإبرام معاملاتهم المختلفة اللجوء إلى مزودي خدمات التصديق للحصول على شهادة التصديق التي يتم من خلالها إثبات وجود الصلة بين الموقع وبين بيانات التحقق من التوقيع الالكتروني.

لأهمية عمل مزود خدمة التصديق، فرض المشرع الجزائري لممارسة هذه المهنة الحصول على ترخيص لمزاولة النشاط، بحيث يترتب على مخالفة ذلك، أي على مزاولة النشاط دون ترخيص ارتكاب جريمة معاقب عليها بمقتضى المادة 1/72 من قانون 15-04 المتعلق بالتوقيع والتصديق الالكترونيين والتي تقضي: "يعاقب...كل من يؤدي خدمات

التصديق الالكتروني للجمهور دون ترخيص أوكل مؤدي خدمات التصديق يستأنف أو يواصل نشاطه بالرغم من سحب ترخيصه".

إنطلاقا من هذه المادة يتبين أن اقتراف هذه الجريمة يقتضي تحقق ركنين ركن مادي وآخر معنوي، ويتمثل السلوك المكون للركن المادي للجريمة في إصدار الشخص الطبيعي أو المعنوي لشهادة تصديق إلكتروني دون حصوله على ترخيص بإصدارها، إذ ينتحل الجاني صفة مؤدي خدمات التصديق الإلكتروني، وللإشارة فإن المشرع المصري نص على هذه الجريمة بموجب المادة 23/أ من قانون 15 لسنة 2004[1]، وكررها بموجب المادة 23/د من ذات القانون[2]، وعليه يعيب البعض على مسلك المشرع المصري الذي جرم جريمة واحدة بنصين قانونيين.

في حين يتجه جانب آخر[3] إلى عدم قبول الفرضية السالفة الذكر، ذلك أن المشرع المصري واجه بموجب نص المادة 23/أ فرضية عدم حصول مزود الخدمة على ترخيص من الهيئة المختصة والذي يسمح له بممارسة نشاط التصديق الإلكتروني، في حين واجه بمقتضى المادة 23/د فرضية توقف مزود خدمات التصديق الإلكتروني عن نشاطه المرخص له به دون الحصول على موافقة كتابية من الهيئة المعنية تأذن له بالتوقف عن ممارسة النشاط.

ولئن كان المشرع المصري تعرض إلى هذه الصور، فإن المشرع الجزائري أضاف صورة أخرى وتتمثل حسب المادة 1/72 من قانون 04/15 في استئناف أو مواصلة النشاط بعد سحب الترخيص، وهي الصورة التي لم يتعرض لها المشرع المصري، وفي هذا يناشد البعض موقف المشرع المصري، ذلك أن مزاولة النشاط من مزود خدمة التصديق الذي

---

[1]- تنص المادة 23/أ من قانون 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني، سابق الإشارة إليه:" مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون آخر، يعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين كل من أ- أصدر شهادة تصديق إلكتروني دون الحصول على ترخيص بمزاولة النشاط من الهيئة."

[2]- تنص المادة 23/د من قانون 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني، سابق الإشارة إليه: "د/ خالف أيا من أحكام المادتين (19)، (21) من هذا القانون."

هذا وتنص المادة 19من ذات القانون:" لا يجوز مزاولة نشاط إصدار شهادة التصديق الإلكتروني إلا بترخيص من الهيئة... ولا يجوز التوقف عن مزاولة النشاط المرخص به ....إلا بعد الحصول على موافقة كتابية مسبقة من الهيئة ."

[3]- عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، المرجع السابق، ص.550.

سحب منه الترخيص يندرج ضمن جريمة مزاولة المهنة دون ترخيص، ما لم يكن غير عالم بسحب الترخيص منه.

وعليه لا تقوم الجريمة إلا بقيام المؤسسة أو الفرد بإصدار شهادة تصديق إلكتروني دون ترخيص، ومن ثم يستلزم هذا السلوك مزاولة عملية الإصدار فعلا ، إذ لا تقوم الجريمة بمجرد إعلان الشخص عن نيته في إصدار شهادة التصديق الالكتروني، وبهذا يجب أن تكون الشهادة قد صدرت من الجاني حقا، ذلك أنها الدليل على مباشرته إصدار شهادة تصديق إلكتروني دون ترخيص.

هذا عن الركن المادي، أما الركن المعنوي فيشمل القصد الجنائي العام المتمثل في العلم والإرادة، إذ ينبغي أن يعلم الجاني أن سلوكه المتمثل في إصدار الشهادة دون الحصول على ترخيص يخوله ذلك وفقا للقانون سلوك مجرم، ورغم ذلك تتجه إرادته للقيام به.

كما يعلم أن الشطر المفترض في الجريمة أن يكون مصدر الترخيص متمتع بصفة مؤدي خدمة التصديق، كذلك يعلم أو يتوقع على الأقل النتيجة الإجرامية.

ثانيا: العقوبة المقررة.

إن توفر الركنيين المادي والمعنوي يترتب عليه قيام جريمة إصدار شهادة تصديق إلكتروني دون ترخيص المعاقب عليها بموجب المادة 1/72 من قانون 04/15 المتعلق بالتوقيع والتصديق الإلكترونيين، والتي قررت لهما عقوبة الحبس من سنة إلى ثلاث (3) سنوات، وبغرامة من مائتي ألف دينار (200.000دج) إلى مليوني دينار (2.000.000دج)، أو بإحدى العقوبتين فقط.

وإذا كانت العقوبات السابقة تخص الشخص الطبيعي، فإن عقوبة الشخص المعنوي تكون الغرامة المقدرة ب عشر ملايين دينار (10.000.000دج) حسب المادة 75 من قانون 15-04 التي تقضي برفع الحد الأقصى للغرامة المقررة للشخص الطبيعي إلى 5 مرات.

الفرع الثاني: الجرائم المرتكبة من المستفيد.

الجرائم المرتكبة من المستفيد هي أفعال يرتكبها الشخص الموقع أو المستفيد من خدمة التصديق على التوقيع الالكتروني، وقد تطرق إليها المشرع الجزائري في نصوص المواد 66 و74 من القانون 15-04 المتعلق بالتوقيع والتصديق الالكترونيين، وبالرجوع لهذه المواد يتبين أن هذه الجرائم تكمن في جريمة الإدلاء بتصاريح وإقرارات كاذبة **(البند الأول)**، جريمة استعمال شهادة تصديق الكتروني لغير الغرض الذي منحت لأجله **(البند الثاني)** .

البند الأول: جريمة الإدلاء بتصاريح وإقرارات كاذبة.

تكمن أهمية تجريم هدا الفعل في أنه قد يهدد مبدأ الثقة والأمان في التعاملات الالكترونية، خاصة وأن هذه التعاملات أصبحت تتم بين أشخاص لا يجمعهما مجلس عقد حقيقي، وكذا بين أشخاص قد لا يعرف بعضهم البعض الآخر، وعليه فان كل تصريح أو إقرار أو إدلاء ببيانات أو معلومات كاذبة بغية الحصول على شهادة تصديق الكتروني موصوفة يعد جريمة معاقب عليها. ولا تطبق العقوبات المقررة على مقترف هذه الجريمة **(ثانيا)**، إلا إذا تحققت أركانها **(أولا)**.

أولا: أركان الجريمة.

نظرا لأن البيانات المتعلقة بالعمليات التي تتم عبر الانترنت تتوقف على ما تقدمه الأطراف المتعاقدة، فقد عمد المشرع إلى تجريم كل تصريح أو إقرار كاذب من المعني بالأمر لمزود خدمة التصديق الالكتروني للحصول على شهادة تصديق إلكتروني، وقد ورد هذا التجريم بموجب المادة 66 من قانون15-04 المتعلق بالتوقيع والتصديق الإلكترونيين التي نصت على: "يعاقب....كل من أدلى بإقرارات كاذبة للحصول على شهادة تصديق إلكتروني موصوفة."

إن علة التجريم واضحة في هذا النص، فهو يرمي إلى زيادة الثقة لدى المتعاملين في هذا النوع من المعاملات والحفاظ على حقوقهم من خلال تأمين صحة البيانات الواردة بشهادة التصديق الإلكتروني، التي يعتمد عليها الغير للدخول في العملية التعاقدية لما تتضمنه

هذه الأخيرة من بيانات دقيقة تسمح له بمعرفة المتعامل معه كون أنها تشمل على إسم الموقع أو الإسم المستعار الذي يسمح بتحديد هويته، الصفات الخاصة بالموقع، حدود إستعمال شهادة التصديق، حدود قيمة المعاملات التي قد تستعمل من أجلها شهادة التصديق الإلكتروني، الوثيقة التي تثبت تمثيل شخص طبيعي أو معنوي آخر[1]، وعليه فإن التصريح الخاطئ بهذه البيانات يؤدي إلى المساس بالعملية التعاقدية.

إن قيام هذه الجريمة يتطلب تحقق الركنين المادي والمعنوي، ويتمثل الركن المادي في الإدلاء بالمعلومات الكاذبة، ويستوي أن تكون هذه المعلومات قد دخلت نظام معلوماتية أم لم تدخل بعد، كما لم يحدد المشرع موضوع هذه الإقرارات، وسواء تعلقت بهوية صاحب الشهادة أو نشاطه أو غيرها، ويستوي أن يُقدم هذا الإدلاء إلى مزود خدمة التصديق، أو إلى أطراف التعاقد ويكون الغرض من ذلك استصدار شهادة تصديق الكتروني موصوفة.

ولئن كان هذا شأن الركن المادي، فإن الركن المعنوي يتمثل في القصد الجنائي العام بعنصريه العلم والإرادة، والمقصود بالعلم علم الجاني بكافة وقائع الجريمة، أي يعلم بأنه يدلي بمعلومات ينبغي عليه تقديمها صحيحة، ورغم ذلك يخالف الالتزام الملقى على عاتقه بحيث تنصرف إرادته إلى السلوك الإجرامي المتمثل في الإدلاء بالمعطيات الكاذبة مع قبوله النتيجة المترتبة على فعله بوصفه مخالفا للقانون.

---

[1]- تنص المادة 15 /3 من قانون 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين، سابق الإشارة إليه: "شهادة التصديق الإلكتروني الموصوفة هي شهادة تصديق إلكتروني تتوفر فيها المتطلبات الآتية:
3- يجب أن تتضمن على الخصوص:
أ- إشارة تدل على أنه تم منح هذه الشهادة على أساس أنها شهادة تصديق إلكتروني موصوفة،
ب- تحديد هوية الطرف الثالث الموثوق أو مؤدي خدمات التصديق الإلكتروني المرخص له بلشهادة التصديق الإلكتروني وكذا البلد الذي يقيم فيه،
ج- إسم الموقع أو الإسم المستعار الذي يسمح بتحديد هويته،
د- إمكانية إدراج صفة خاصة للموقع عند الإقتضاء، وذلك حسب الغرض من استعمال شهادة التصديق الإلكتروني،
ه- بيانات تتعلق بالتحقق من التوقيع الإلكتروني، وتكون موافقة لبيانات إنشاء التوقيع الإلكتروني،
و- الإشارة إلى بداية ونهاية مدة صلاحية شهادة التصديق الإلكتروني
ز- رمز تعريف شهادة التصديق الإلكتروني،
ح- التوقيع الإلكتروني الموصوف لمؤدي خدمات التصديق الإلكتروني أو للطرف الثالث الموثوق الذي يمنح شهادة التصديق الإلكتروني،
ط- حدود استعمال شهادة التصديق الإلكتروني، عند الإقتضاء،
ي- حدود قيمة المعاملات التي قد تستعمل من أجلها شهادة التصديق الإلكتروني، عند الإقتضاء،
ك- الإشارة إلى الوثيقة التي تثبت تمثيل شخص طبيعي أو معنوي آخر، عند الإقتضاء."

ثانيا: العقوبة المقررة.

يترتب على تحقق أركان جريمة الإدلاء بتصريحات وإقرارات كاذبة معاقبة الجاني بتطبيق العقوبات المقررة في المادة 66 من قانون التوقيع والتصديق الالكترونيين، والمتمثلة في الحبس من ثلاثة (3) أشهر إلى ثلاث (3) سنوات، وبغرامة من عشرين ألف دينار (20.000دج) إلى مائتي ألف دينار (200.000دج) أو بإحدى هاتين العقوبتين فقط.

للإشارة فإن العقوبات السابقة تطبق إذا ما كان الجاني شخصا طبيعيا، أما إذا كان شخصا معنويا فإن العقوبة تتمثل حسب المادة 75 من القانون آنف الذكر في الغرامة المقدرة بخمس مرات الحد الأقصى للغرامة المنصوص عليها بالنسبة للشخص الطبيعي، وعليه تكون العقوبة الغرامة المقدرة 1.000.000دج.

البند الثاني: جريمة استعمال شهادة تصديق إلكتروني لغير الغرض الذي منحت لأجله.

لقد عاقب المشرع الجزائري بموجب المادة 74 من قانون 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين كل من يستعمل شهادة تصديق إلكتروني موصوفة خاصة به، ولكن لغير الأغراض التي منحت لأجلها، ولكن لعقاب مقترف الفعل **(ثانيا)**، ينبغي تحقق أركان هذه الجريمة **(أولا)**.

أولا:أركان الجريمة.

يستلزم قيام جريمة استعمال شهادة تصديق إلكتروني لغير الغرض الذي منحت لأجله، تحقق الركنين المادي والمعنوي، ويتحقق الركن المادي عند استعمال صاحب شهادة التصديق الالكتروني هذه الشهادة في غير الغرض الذي منحت لأجله وفقا لما تقرره المادة3/15/ط من قانون التوقيع والتصديق الإلكترونيين التي بينت أن هناك حدود لإستعمال شهادة التصديق[1]، غير أنها لم توضح هذه الحدود، ذلك أن هذه الأخيرة تختلف باختلاف نوع

[1]- تنص المادة 15 /3 من قانون 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين، سابق الإشارة إليه:" شهادة التصديق الإلكتروني الموصوفة هي شهادة تصديق إلكتروني تتوفر فيها المتطلبات الآتية:
3- يجب أن تتضمن على الخصوص:
ط- حدود استعمال شهادة التصديق الإلكتروني، عند الإقتضاء "

الشهادة بحيث تتمثل حدود شهادة توثيق التاريخ في توثق تاريخ، ووقت إصدار التوقيع الرقمي حيث يقوم صاحب الرسالة بعد التوقيع عليها بإرسالها إلى جهة التوثيق التي تقوم بتسجيل التاريخ عليها وتوقيعها من جهتها ثم تعيدها إلى مرسلها[1]، في حين تتمثل حدود شهادة الإذن في تقديم بيانات عن صاحب التوقيع، كمؤهلاته ومحل إقامته[2]، أما شهادة البيان فيتم من خلالها تأكيد صحة واقعة معينة ووقت وقوعها[3].

من خلال المادة 74 من قانون التوقيع والتصديق الالكترونيين يتبين أن قيام هذه الجريمة يقتضي استعمال الشهادة من طرف صاحبها، وعليه لا يتحقق الركن المادي في حالة ما إذا تم استعمال الشهادة من غير صاحبها، وذلك استنادا لمبدأ شرعية الجريمة المقرر بموجب المادة الأولى من قانون العقوبات التي تقضي بأن لا جريمة ولا عقوبة ولا تدبير أمن بغير قانون.

ولئن كان هذا هو مضمون الركن المادي، فإن مضمون الركن المعنوي يتمثل في إرتكاب الجاني ذلك السلوك الإجرامي عن قصد ، والمراد بالقصد هنا القصد العام الذي يشمل كل من العلم والإرادة، وعليه حتى تقوم هذه الجريمة لابد أن يعلم الجاني بمخالفته لنص قانوني، وهي مسألة لا خلاف بشأنها كون أن الفعل منصوص عليه في قانون التوقيع والتصديق الالكترونيين، ولا يكفي العلم فحسب بل لابد أن تنصرف إرادة الجاني إلى إتيان ذلك السلوك الإجرامي.

ثانيا: العقوبة المقررة.

يترتب على تحقق الركنين السالف ذكرهما قيام جريمة استعمال شهادة التصديق الالكتروني لغير الغرض الذي منحت لأجله، ومعاقبة الجاني بغرامة من ألفي دينار (2.000دج) إلى مائتي ألف دينار (200.000دج)، وتطبيق هذه العقوبة يتقرر إذا كان

[1]- لزهر بن سعيد، المرجع السابق، ص.184.
[2]- إيمان مأمون أحمد سليمان، المرجع السابق، ص.325.
[3]- لزهر بن سعيد، المرجع السابق، ص.184.

الجاني شخصا طبيعيا، أما إذا كان مقترفها شخصا معنويا، فإن العقوبة تكون الغرامة المقدرة بـ 1.000.000دج حسبما تقرره المادة 75 من قانون التوقيع والتصديق الإلكترونيين.

الفرع الثالث: الجرائم المرتكبة من الغير.

بالرجوع إلى قانون التوقيع والتصديق الإلكترونيين يلاحظ أن المشرع الجزائري جرم عددا من الأفعال المقترفة من قبل مزودي خدمات التصديق الالكتروني، وكذا المستفيد من هذه الخدمات، غير أنه أفرد مادة واحدة بالنسبة للأعمال المرتكبة من طرف الغير، ولكن بالتدقيق فيها يلاحظ أنها تتضمن جرائم متعددة وتشمل كل من حيازة بيانات إنشاء توقيع إلكتروني خاصة بالغير، إفشاءها، إستعمالها.

ورغم اختلاف هذه الجرائم، إلا أن المشرع أوردها ضمن مادة واحدة، وذلك لاشتراكها في صفة الفاعل –وهو الغير-، الذي لا يشمل مزود خدمة التصديق ولا المستفيد، وكذا لاشتراكها في العقوبة.

وعليه سيتم تبني ذات النهج الذي عول عليه المشرع الجزائري، وذلك بالتطرق للأركان المقررة لقيام هذه الجريمة **(البند الأول)**، وكذا للعقوبة المقررة بشأنها **(البند الثاني).**

البند الأول: الأركان المقررة لقيام الجرائم المرتكبة من الغير.

نظرا لّإمكانية تعدد الأشخاص المطلعة على المستند الإلكتروني، قرر المشرع الجزائري بموجب المادة 68 من قانون التوقيع والتصديق الالكترونيين، معاقبة كل من يقوم بحيازة، إفشاء، إستعمال بيانات إنشاء توقيع إلكتروني موصوفة خاصة بالغير.

إن إعمال المادة 68 آنفة الذكر يستلزم توفر ركنيين ركن مادي **(أولا)**، وآخر معنوي **(ثانيا)**، ولأهميتهما سيتم التطرق لهما.

أولا: الركن المادي.

يتمثل الركن المادي في قيام الشخص بحيازة، إفشاء، إستعمال بيانات إنشاء توقيع إلكتروني موصوفة خاصة بالغير، وعليه تتمثل الصورة الأولى في حيازة بيانات إنشاء توقيع إلكتروني موصوفة خاصة بالغير، ومدلول الشخص لا ينصرف للموقع لأن المادة كانت صريحة، حيث استخدمت مصطلح بيانات إنشاء توقيع إلكتروني خاصة بالغير، سيما وأن المادة 2/2 من قانون التوقيع والتصديق الإلكترونيين[1] تمنح للموقع، أي لكل شخص طبيعي حق حيازة بيانات إنشاء التوقيع الالكتروني، سواء كان هذا الشخص يتصرف لحسابه الخاص أو لحساب الشخص الطبيعي أو المعنوي الذي يمثله.

كما أنه يعاقب كل من يقوم بإفشاء بيانات إنشاء توقيع إلكتروني موصوفة خاصة بالغير، ويقصد بالإفشاء إطلاع الغير على بيانات إنشاء التوقيع الإلكتروني الخاص بالغير[2]، أي إطلاعه على تلك البيانات الفريدة كالرموز، أو مفاتيح التشفير الخاصة التي يستعملها الموقع لإنشاء التوقيع الإلكتروني[3].

إذا كان المشرع الجزائري جرم عملية إفشاء مفاتيح التشفير الخاصة، فالملاحظ أن المشرع المصري أورد في مشروع قانون التجارة الالكترونية ما يسمى بفض مفاتيح التشفير المودعة بمكتب التشفير المعني بالحفظ ومراقبة عملية التشفير، ويقصد بفض مفاتيح التشفير كشف البرامج الخاصة بتشفير التوقيع الالكتروني، وذلك بنقل التوقيع من صورة مكتوبة إلى صورة رقمية، أي نقله من صورة ذات دلالة معينة ومضمون معين، ليكون مجرد إشارة أو رمز[4].

---

[1]- تنص المادة 2/2 من قانون رقم 04/15 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، سابق الإشارة إليه. "الموقع: شخص طبيعي يحوز بيانات إنشاء التوقيع الإلكتروني ويتصرف لحسابه الخاص أو لحساب الشخص الطبيعي أو المعنوي الذي يمثله."

[2]- أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، ج1، المرجع السابق، ص.248.

[3]- تنص المادة 3/2 من قانون رقم 04/15 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، سابق الإشارة إليه: "بيانات إنشاء التوقيع الإلكتروني: بيانات فريدة، مثل الرموز أو مفاتيح التشفير الخاصة، التي يستعملها الموقع لإنشاء التوقيع الإلكتروني."

[4]- أيمن رمضان محمد أحمد، المرجع السابق، ص.148.

لتتحقق هذه الجريمة يتم تسليم برنامج الشفرة لمن ليس له حق في ذلك، ويعتبر مرتكبا لهذه الجريمة من يقوم بتسليم الرموز الهندسية المعقدة لغير صاحبها في حالة تشفير التوقيع بواسطة النظام السيمتري، أو من خلال تسليم المواصفات الشخصية المتعلقة بصاحب التوقيع ذاته في حالة تشفير التوقيع بواسطة النظام البيومتري[1].

ونظرا لأن هذه الجريمة من جرائم الخطر، فإن قيامها لا يتطلب حصول نتيجة معينة، بل يكفي أن يكون الجاني فيها قد قام بفض مفاتيح التشفير المتعلقة بالتوقيع الإلكتروني، دون نظر لما إذا كان فض الشفرة تم لمصلحته أو لمصلحة شخص ثالث، بمعنى آخر يكفي لتحقق هذه الجريمة كشف مفاتيح التشفير، بحيث لا يشترط لقيامها تحقق ضرر بالنسبة للمجني عليه من عملية فض الشفرة .

ولعل السبب في ذلك يكمن في أن حظر استعمال تلك الشفرة يظل قائم في المستقبل، وهذا هو السبب وراء استخدام المشروع مصطلح "كل من يقوم بكشف مفاتيح التشفير".

ولئن كانت هذه هي الصورة الثانية المكونة للركن المادي، فإن الصورة الثالثة تشمل إستعمال بيانات إنشاء توقيع إلكتروني موصوفة خاصة بالغير.

ويُقصد بالإستعمال إستخدام الشيء فيما أعد له، أي استخدام بيانات إنشاء توقيع إلكتروني موصوفة خاصة بالغير، وبمعنى أدق إستخدام الرموز أو مفاتيح التشفير الخاصة التي من المفترض أن يستعملها الموقع لإنشاء التوقيع الإلكتروني، أي التي يستخدمها الشخص الطبيعي الذي يحوز بيانات إنشاء التوقيع الإلكتروني سواء كان هذا الأخير يتصرف لحسابه الخاص أو لحساب الشخص الطبيعي أو المعنوي الذي يمثله.

ثانيا: الركن المعنوي.

تعد جريمة حيازة، إفشاء، استعمال بيانات التوقيع الالكتروني الموصوف الخاص بالغير من الجرائم العمدية التي ينبغي لقيامها تحقق القصد الجنائي العام بعنصريه العلم

[1]- عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، المرجع السابق، ص.586.

والإرادة، إذ لابد أن ينصرف علم الجاني إلى أنه يفشي، يستعمل، أو يحوز بيانات إنشاء التوقيع الإلكتروني الخاصة بالغير، ورغم ذلك تتجه إرادته إلى القيام بتلك الأعمال وتحقيق النتيجة الجرمية.

بعد أن تم تحديد أركان جريمة حيازة إفشاء إستعمال بيانات توقيع إلكتروني موصوفة خاصة بالغير، وجب التعرض للعقوبات المقررة لها.

البند الثاني: العقوبة المقررة.

لقد أوردت المادة 68 من قانون 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين العقوبات المقررة لجريمة حيازة، إفشاء أو إستعمال بيانات إنشاء توقيع إلكتروني موصوفة خاصة بالغير إذ نصت: " يعاقب بالحبس من ثلاثة (3) أشهر إلى ثلاث (3) سنوات وبغرامة من مليون دينار (1.000.000دج) إلى خمسة ملايين دينار (5.000.000دج)، أو بإحدى هاتين العقوبتين فقط...".

من خلال هذه المادة، يتبين أن الجزاء المقرر في حالة توفر أركان هذه الجريمة يتمثل في الحبس من ثلاثة أشهر إلى ثلاث سنوات، وغرامة من مليون دينار إلى خمسة ملايين دينار، كما يكون للقاضي توقيع إحدى هاتين العقوبتين، وتوقيع هذه العقوبات يتقرر إذا ما كان الفعل المقترف مرتكبا من قبل الشخص الطبيعي، أما إذا ما تمت هذه الجريمة من شخص معنوي فإن العقوبة تكون الغرامة والتي تقدر حسب المادة 75 من قانون التوقيع والتصديق الالكترونيين بخمس مرات الحد الأقصى المقرر للغرامة المنصوص عليها للشخص الطبيعي، وعليه تكون الغرامة خمسة وعشرون مليون دينار (25.000.000 دج).

الفصل الثاني:

الأحكام الإجرائية للمستند الالكتروني من الناحية الجزائية بين التنظيمين الداخلي والدولي

لا يقتصر البحث في موضوع الحماية الجزائية للمستندات الإلكترونية على الجانب الموضوعي الذي يتعلق بقواعد التجريم والعقاب، ولكنه يمتد ليشمل الجانب الإجرائي الذي يهتم بالبحث في مدى توافر شرط التجريم من أجل تطبيق العقاب، وعليه يُعتبر الجانب الإجرائي الوجه العملي لاتحاد شقي التجريم والعقاب في القاعدة الجنائية، فهو المحرك الفعال لقانون العقوبات، ذلك أنه ينتقل به من دائرة التجريم إلى دائرة التطبيق العملي، بمعنى أنه ينقله من حالة السكون إلى حالة الحركة.

بهذا يبدو أنه مهما سعت التشريعات في نصوصها العقابية لتوفير الحماية الموضوعية للمصالح الاجتماعية، فإن نجاحها في الحفاظ على تلك المصالح سيظل مرتهنا بمدى فاعلية التنظيم الإجرائي الذي يضمن تحقيق الهدف من العقاب.

وفي سبيل تحقيق المسعى السالف ذكره، عمدت التشريعات إلى إيجاد أحكام إجرائية إلى جانب الأحكام الموضوعية التي ينظمها قانون العقوبات، وقد قُسمت الأحكام الإجرائية الرامية إلى إلقاء القبض على المتهم، التحقيق معه، محاكمته إلى قسمين أحدهما داخلي بمعنى وطني، والآخر خارجي بمعنى دولي، ولا ريب في أن التنظيم الإجرائي الداخلي يهدف إلى تنظيم إجراءات ضبط مرتكب الفعل على المستوى الوطني، في حين يهدف التنظيم الإجرائي الدولي إلى بيان الإجراءات المتبعة إذا كان مرتكب الفعل موجودا خارج الحدود الوطنية، والحقيقة أن أهمية هذا الشق تبدو بوضوح في مجال المعلوماتية، كون أن الجرائم المرتكبة جرائم دولية عابرة للحدود الوطنية[1].

[1]- عادل عبد الله خميس المعمري، المرجع السابق، ص.251 ؛ ذياب البداينة، المرجع السابق ، ص.22؛ خالد حامد أحمد مصطفى، المعلوماتية والمسؤولية الجزائية، الفكر الشرطي، دورية ربع سنوية علمية محكمة ومفهرسة تعنى بالأبحاث الشرطية، تصدر عن مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، الإمارات العربية المتحدة، مج العشرون، ع الرابع، العدد رقم (79)، أكتوبر 2011، ص.159.

استنادا لما تقدم، يبدوا أن الشق الإجرائي في مجال الجريمة المعلوماتية عموما، وفي مجال الجرائم الواقعة على المستندات الإلكترونية خاصة لها من الأهمية بمكان، كونه موضوعا جديدا يحتاج إلى تشريع يتعامل معه، لا سيما على ضوء التطورات التكنولوجية والتقنية المتطورة باستمرار.

ولئن كان هذا الموضوع حديث وتقني ويتطور باستمرار، فما مدى كفاية النصوص الإجرائية التقليدية لمواجهة الجرائم الواقعة على المستندات الإلكترونية، خاصة أن المجرم المعلوماتي يتعامل بذكاء لإخفاء دليل إدانته؟ وهل استحدثت التشريعات نصوصا إجرائية تتماشى والبيئة الرقمية، وتساهم في إلقاء القبض على المجرم المعلوماتي؟.

هذا وغيره سيتم تحديده بالتطرق إلى التنظيم الإجرائي الداخلي لمتابعة الجرائم الماسة بالمستندات الإلكترونية **(المبحث الأول)**، وبعدها إلى التنظيم الإجرائي الدولي المقرر للغرض ذاته **(المبحث الثاني)**.

المبحث الأول: التنظيم الإجرائي الداخلي لمتابعة الجرائم الماسة بالمستند الإلكتروني.

تعتبر مسألة التنظيم الإجرائي الداخلي لمواجهة الإجرام الإلكتروني من المواضيع المهمة التي تحتاج إلى رجال قانون مؤهلين ومختصين ينظمونها، كما أنها تعد من المقدمات الضرورية التي تستظهر مدى كفاءة الدول في التعامل مع تكنولوجيات المعلومات، ومدى إمكانية تواصلها مع معادلة التطوير والتطبيق على السواء.

وبما أن الجرائم الإلكترونية من الجرائم المستحدثة التي تستعمل فيها التقنية العالية، وتستخدم بوسائل وتقنيات تختلف تماما عن وسائل ارتكاب الجرائم التقليدية، فإن محاولة تطبيق المسائل الجزائية الإجرائية التقليدية لمتابعة مرتكب الفعل قد أظهرت جملة من المشاكل والصعوبات العملية، كصعوبة اكتشافها وتحديد مصدرها خاصة وأنها جرائم قد ترتكب عن بعد، صعوبة ايقافها لسرعة انتشار المعلومات وتسجيلها أوتوماتيكيا من حاسب إلى آخر، ناهيك عن صعوبة إثباتها كون أن الدليل فيها يتصف بعدم المرئية، سهولة المحو

والتدمير في زمن قصير جدا هذا من جهة[1]، ومن جهة أخرى فإن التعامل مع هذه الجرائم يستلزم أن تكون الجهة المختصة بالمتابعة والتحري مكونة علميا وتكنولوجياً، وذلك حتى تتمكن من فهمها وتستطيع الكشف عنها وملاحقة مرتكبيها[2].

كل هذه المعطيات دفعت التشريعات المقارنة بما فيها المشرع الجزائري إلى إعادة النظر في الكثير من المسائل الإجرائية من الناحية الجزائية بخصوص متابعة مرتكبي هذه الجرائم، وذلك حتى لا تقف هذه الصعوبات والمشاكل العملية كحجر عائق أمام أجهزة العدالة في ضبط مرتكب الفعل، محاكمته والحكم عليه.

استنادا للمشاكل الإجرائية التي تُثيرها الجرائم الماسة بالمستندات الإلكترونية، فإنه ينبغي تحديد الإجراءات التي تتناسب والطبيعة الخاصة لهذه الجرائم، وذلك بغية مكافحتها، تعقب مرتكبيها، وفي هذا يُلاحظ أن خصوصية الجرائم الإلكترونية عامة، والجرائم الماسة بالمستند الإلكتروني خاصة جعلت المشرع يستحدث إلى جانب الإجراءات التقليدية، إجراءات حديثة للتحقيق وجمع الأدلة الإلكترونية.

إن التعرض للمسائل السالف ذكرها يستلزم بيان إجراءات التحقيق التقليدية في الجرائم الماسة بالمستند الإلكتروني **(المطلب الأول)**، وبعدها الإجراءات المستحدثة للتحقيق في هذه الجرائم **(المطلب الثاني)**.

---

[1]- تركي بن محمد العطيان، المرجع السابق، ص.332؛ محمد حسن السراء، الأساليب الحديثة والمهارات المتقدمة في تحقيق الجرائم الإلكترونية ، الفكر الشرطي، دورية ربع سنوية- علمية محكمة ومفهرسة تعنى بالأبحاث الشرطية، تصدر عن مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، الإمارات العربية المتحدة، مج الحادي والعشرون، ع الثاني، العدد رقم (81)، أبريل 2012، ص.41؛ هشام محمد فريد رستم، الجرائم المعلوماتية أصول التحقيق الجنائي الفني وآلية التدريب التخصصي للمحققين، دراسات أمنية، مجلة الأمن والقانون، تصدرها كلية شرطة دبي، القيادة العامة لشرطة دبي، ع 2، س السابعة، ربيع الأول، 1430هـ- يوليو 1999، ص.86.

[2]- سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت (الجرائم الواقعة في مجال تكنولوجيا المعلومات)، ط1، دار النهضة العربية، القاهرة، 1999، ص.95؛ سرحان حسن المعيني، التحقيق في جرائم تقنية المعلومات، الفكر الشرطي، دورية ربع سنوية علمية محكمة ومفهرسة تعني بالأبحاث الشرطية، تصدر عن مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، الإمارات العربية المتحدة، مج العشرون، ع الرابع، العدد رقم(97)، أكتوبر 2011، ص، ص. 31- 32؛ عادل عبد الله خميس المعمري، المرجع السابق، ص.253؛ ذياب البداينة، المرجع السابق، ص.22.

المطلب الأول: إجراءات التحقيق التقليدية في الجرائم الماسة بالمستند الإلكتروني.

يقصد بإجراء التحقيق الإجراء الذي يهدف إلى معرفة الحقيقة التي تتمثل عناصرها في مدى وقوع الجريمة ونسبتها إلى المتهم، وهو بهذا يُؤدي إلى تحضير الدعوى وتحديد مدى قابليتها للنظر أمام القضاء[1].

ولقد جرى منطق أغلب الفقه إلى تقسيم إجراءات التحقيق إلى نوعين؛ إجراءات تستهدف التنقيب عن الأدلة، وإجراءات تستهدف الاحتياط لاحتمال فرار المتهم وإفساد الأدلة[2].

ومن ثم فإن الدراسة في هذا سوف تقتصر على البحث في الإجراءات العامة للتحقيق، وسميت كذلك لأنها إجراءات عامة وتقليدية في نطاق الكشف عن الجرائم التقليدية والوصول إلى الأدلة فيها، ولا ريب في أن لهذه الإجراءات ذات الأهمية في مجال الجرائم الإلكترونية. ولأهميتها تلك فإنه سيتم التركيز على إجراءات جمع الأدلة المادية في الجرائم الماسة بالمستندات الإلكترونية، لا سيما وأن الأدلة المادية تنطلق من عناصر مادية ناطقة بنفسها، بحيث تسمح للقاضي الجنائي بأن يُكَون اقتناعه تلقائيا مستندا في ذلك للعقل والمنطق، وذلك بخلاف الأدلة القولية (الشهادة- الاستجواب) التي تنطلق من عناصر شخصية تتمثل فيما قد يصدر عن الغير من أقوال تُؤثر في اقتناع القاضي بطريق غير مباشر، بحيث يتوجب عليه التأكد من صدق أقوالهم[3].

فضلا عن ذلك فإن الفقه يرى بأن إجراءات جمع الدليل القولي في البيئة المعلوماتية لها دور ضئيل في الكشف عن الحقيقة مقارنة بتلك المتعلقة بجمع الدليل المادي، فالشهادة على سبيل المثال لا يبدو متصورا ورودها على السلوك المكون للجريمة الإلكترونية بحكم كونها تلاعباً في البيانات والأنظمة غير القابلة من حيث المبدأ لأن تشاهد أو تدرك من جانب الغير حتى يمكن أن يشهد بها أمام القضاء شهادة مباشرة[4].

---

[1]- أحمد عاصم عجيلة، المرجع السابق، ص. 392.

[2]- فوزية عبد الستار، شرح قانون الإجراءات الجنائية، ط2، دار النهضة العربية، القاهرة، 2011، ص. 332.

[3]- عبد الرؤوف مهدي، شرح القواعد العامة للإجراءات الجنائية، دار النهضة العربية، القاهرة، 2013، ص. 1746؛ أحمد عاصم عجيلة، المرجع السابق، ص. 393.

[4]- بوعناد فاطمة زهرة، المرجع السابق، ص. 98.

ومن ثم فإن إجراءات التحقيق التقليدية التي سيتم التطرق إليها هي تلك التي بينها القانون وتشمل كل من المعاينة، التفتيش، ضبط الأشياء، ندب الخبراء وكذا اجراء التسرب، وذلك لاعتبار أن هذه الإجراءات وإن كانت تمتد لتُطبق في مجال البيئة الرقمية، إلا أنها تُثير الكثير من التساؤلات في مجال الجرائم الواقعة على المستندات الإلكترونية.

الفرع الأول: المعاينة.

يعتبر المكان الذي ارتكبت فيه الجريمة الوعاء الأساسي الذي يحتوي على أخطر الأدلة الجنائية التي يخلفها الجاني وراءه في أعقاب ارتكابه الجريمة، ولذلك كان من الواجب على ضباط الشرطة القضائية الانتقال إلى ذلك المكان لمعاينة وإثبات حالة الآثار المادية للجريمة والمحافظة عليها، وإثبات حالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة[1].

وعلية تُعتبر المعاينة إجراء من إجراءات التحقيق ويُطلق عليها عادة إثبات الحالة، والمراد بها إثبات حالة الأشخاص والأمكنة والأشياء ذات الصلة بالحادث.

هذا وتُعرف المعاينة لغة بأنها نظر الشيء ومشاهدته، أما في الاصطلاح الجنائي فتُعرف على أنها: "رؤية محل ارتكاب الوقائع الجنائية وإثبات حالتها بالشكل الذي تركها به الجاني عقب ارتكابه الجريمة"[2]، فالمعاينة في علم التحقيق الجنائي هي مشاهدة المكان الذي ارتكبت فيه الجريمة وعمل وصف شامل له سواء بالكتابة أو بالرسم التخطيطي أو التصوير وذلك لإثبات حالته بالكيفية التي تركها بها الجاني، كما تشمل فحص جسم المجني عليه والمتهم، وبيان ما يوجد بهما من آثار خلفتها الجريمة[3].

---

[1]- نبيلة هبة مولاي علي هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، رسالة مقدمة للحصول على درجة ماجستير في العلوم الجنائية، كلية الحقوق، جامعة الإسكندرية، مصر، السنة الجامعية2005- 2006 ، ص.75؛ عبد الرحمن خلفي، القانون الجنائي العام (دراسة مقارنة)، دار بلقيس، دار البيضاء-الجزائر، 2017، ص.239.

[2]- سامح أحمد بلتاجي موسى، الجوانب الإجرائية للحماية الجنائية لجرائم الإنترنت، رسالة دكتوراه في الحقوق، كلية الحقوق، جامعة الإسكندرية، سنة 2010، ص. 232.

[3]- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، ط1، دار الفكر الجامعي، الإسكندرية، مصر، 2009، ص. 149.

ويُعرف جانب من الفقه المعاينة بأنها: "إجراء بمقتضاه ينتقل المحقق إلى مكان وقوع الجريمة ليشاهد بنفسه ويجمع الآثار المتعلقة بالجريمة، كيفية وقوعها، الأشياء الأخرى التي تفيد في كشف الحقيقة"[1].

هذا وقد تطرق المشرع الجزائري إلى هذا الإجراء في نصي المادتين 79 و80 من قانون الإجراءات الجزائية.

ما يُستفاد من هذه المفاهيم السالف ذكرها أن المعاينة تُشكل عصب التحقيق الجنائي ودعامته وعماده، وتبرز أهميتها في تعبيرها عن الوقائع والحقيقة تعبيراً صادقاً خالياً من اللبس والخداع، بحيث تُعطي للمحقق صورة صحيحة وواقعية لمكان الجريمة، وما يتصل به من ماديات وآثار.

هذا عن المعاينة عموما، أما معاينة مسرح الجريمة الإلكترونية فيُقصد بها معاينة وفحص الآثار التي يتركها مستخدم الحاسب الآلي والإنترنت، ويشمل الفحص الرسائل المرسلة منه وكذا تلك المستقبلة، وكافة الاتصالات التي تمت من خلال الحاسوب وعبر شبكة الإنترنت، هذا وتُعد الآثار الرقمية المستخلصة من أجهزة الحاسوب مفيدة للغاية لما تحتويه من معلومات.

ولعل من الوسائل والأدوات والوسائط التي تحتوي على أدلة تفيد كثيرا في كشف الحقيقة محل التحقيق نجد كل من صفحات المواقع (web page)، البريد الإلكتروني (e.mail)، الفيديو الرقمي (Digital video)، غرف الدردشة والمحادثة والملفات المخزنة في الحاسب الشخصي، الصور المرئية، كما ويسمح الدخول للخدمة والاتصال بالإنترنت والشبكة عن طريق مزود الخدمات في الوصول إلى المعلومات التي تُساهم في معرفة الحقيقة[2].

[1]- على عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، دراسة مقارنة، المكتب الجامعي الحديث، د. ب.ن، 2012، ص. 32؛ حطاب كمال، المرجع السابق، ص. 30.
[2]- سامح أحمد بلتاجي موسى، المرجع السابق، ص. 234.

وما ينبغي الإشارة إليه في هذا المقام، أن المعاينة في مجال كشف غموض الجريمة الإلكترونية لا تتمتع بنفس الدرجة من الأهمية كنظيرتها في مجال الجريمة التقليدية، ومرد ذلك في أن الجرائم التي تقع على نظم المعلومات والشبكات قلما يخلف ارتكابها آثار مادية، فضلا عن ذلك فإن عدداً كبيراً من الأشخاص قد يترددون على المكان أو مسرح الجريمة خلال الفترة الزمنية التي تتوسط عادة بين زمن ارتكاب الجريمة وبين اكتشافها، وهو الأمر الذي قد يُؤدي إلى حدوث تغيير أو تلفيق أو عبث بآثار الجريمة، كما وأنه قد يؤدي إلى زوال بعضها، وهذه الأمور كلها تُلقي ظلالاً من الشك على الدليل المستمد من المعاينة[1].

زيادة على ذلك فإن ما يجعل من المعاينة إجراء ضئيل الأهمية إمكانية التلاعب في البيانات عن بعد، أو محوها عن طريق التدخل من خلال وحدة طرفية من قبل المجرم المعلوماتي[2].

هذا وتتخذ المعاينة في الجرائم الإلكترونية عدة أشكال وذلك حسب نوعية الجريمة المرتكبة، ففي جرائم العدوان على الملكية الفكرية مثلاً يتم إنزال نسخة من المصنف المعتدى عليه أو التحفظ على نسخة منه، وذلك بطباعتها واستخراجها في هيئة ورقية أو صلبة، كأن يتم استخراجها على خشب أو بلاستيك خاص عن طريق الطابعة، وإلى جانب هذه الطرق هناك طرق عامة تتوافق مع طبيعة النظام المعلوماتي، كأن يتم حفظ الموقع باستخدام خاصية الحفظ المتوفرة في نظام التشغيل، أو من خلال تصوير شاشة الحاسوب (Impression de capture d'écran) بواسطة آلة تصويرية تقليدية، أو عن طريق استخدام برمجية حاسوب متخصصة في أخذ صور لما يظهر على الشاشة، وهو ما يُصطَلح عليه بتجميد مخرجات الشاشة[3].

أما عن كيفية إجراء المعاينة والضوابط الفنية الواجب على المحقق مراعاتها فيها فيتسم بيانه فيما يلي:

[1]- محمد حسن السراء، المرجع السابق، ص.51؛ هشام محمد فريد رستم، المرجع السابق، ص.93؛ سرحان حسن المعيني، المرجع السابق، ص.41.

[2]- علي عدنان الفيل، نفس المرجع، ص، ص. 32- 33؛ نبيلة هبة مولاي علي هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص. 76؛ سامح أحمد بلتاجي موسى، المرجع السابق، ص. 235.

[3]- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص. 154.

البند الأول: كيفية إجراء المعاينة في البيئة الإلكترونية.

تتم المعاينة في الجرائم الواقعة على المستندات الإلكترونية كأي جريمة أخرى عن طريق الانتقال إلى محل الواقعة الإجرامية، إلا أن الانتقال هنا لا يكون إلى العالم المادي وإنما إلى العالم الافتراضي أو عالم الفضاء الإلكتروني[1]، وإن كان بعض الفقه يرى بأنه ينبغي التعامل مع مسرح الجريمة الإلكترونية على أنه مسرحان؛ مسرح تقليدي، ويقع خارج بيئة الحاسوب والإنترنت، ويتكون بشكل رئيسي من المكونات المادية المحسوسة للمكان الذي وقت فيه الجريمة، وهو أقرب ما يكون إلى مسرح أي جريمة تقليدية قد يترك فيها الجاني آثار مادية عدة كالبصمات أو وسائط تخزين رقمية، ومسرح افتراضي، يقع داخل البيئة الإلكترونية، ويتكون من البيانات الرقمية التي توجد داخل الحاسب الآلي وشبكة الإنترنت في ذاكرة الأقراص الصلبة الموجودة بداخله[2].

ولما كانت المعاينة تتم في وسط افتراضي، فإن ضابط الشرطة القضائية أو العضو المكلف بالتحقيق يستطيع القيام بها وهو جالس في مكتبه من خلال الحاسوب الموضوع على مكتبه، كما يمكنه أن ينتقل إلى عالم الفضاء الإلكتروني لمعاينته عن طريق اللجوء إلى مقهى الإنترنت (Cyber café)، أو اللجوء إلى مقر عمل مزود خدمة الإنترنت، والذي يعتبر حسب الفقه أفضل مكان يمكن من خلاله إجراء المعاينة[3]، هذا ويمكنه الاستعانة كذلك بخبير متخصص في الحاسب الآلي، غير أنه يجب على المحقق الجنائي قبل الانتقال لإجراء معاينة لمسرح الجريمة الإلكتروني إتباع الخطوات الآتية:

1- توفير معلومات مسبقة عن مكان وقوع الجريمة وعن المالك لهذا المكان، وعن نوع وعدد أجهزة الكمبيوتر المتوقع مداهمتها وشبكاتها، وتحديد كيفيات التعامل معها فنياً من حيث الضبط، التأمين وكذا حفظ المعلومات والمستندات.

---

[1]- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص. 156.

[2]- بوعناد فاطمة زهرة، المرجع السابق، ص. 101.

[3]- أحمد عاصم عجيلة، المرجع السابق، ص. 438؛ خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص. 156.

2- الحصول على الاحتياجات الضرورية من الأجهزة والبرامج للاستعانة بها في الفحص والتشغيل.

3- وضع خريطة توضح الموقع الذي ستتم معاينته، وتفاصيل المبنى أو الطابق موضوع البلاغ، وعدد الأجهزة والخزائن والملفات.

4- تأمين الأجهزة والمعدات التي يستعان بها في عملية المعاينة، سواء كانت أجهزة أو برامج صلبة أو لينة.

5- إعداد الفريق المتخصص الذي يتولى المعاينة من الخبراء ورجال الضبطية القضائية والأمن.

6- تحديد البيانات والمهام والاختصاصات المطلوبة من كل عضو في فريق المعاينة، وذلك حتى تتكامل الاختصاصات ولا تتداخل.

7- إعداد خطة المعاينة موضحة بالرسومات مع تمام المراجعة التي تكلف تنفيذها على الوجه الأكمل.

8- تأمين عدم انقطاع التيار الكهربائي، لأن انقطاعه يُؤدي إلى التوقف غير العادي لجهاز الحاسب الآلي، وهو ما قد يُسبب محو المعلومات من الذاكرة، وفقدان كافة العمليات التي كان يتم تشغيلها، اتصالات الشبكة، وأنظمة الملفات الثابتة[1].

9- السعي لإتمام مختلف الإجراءات وفقا لمبدأ المشروعية، وفي إطار ما تنص عليه القوانين[2].

[1]- نبيلة هبة مولاي هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص. 77؛ خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص، ص. 156- 157.
[2]- سامح أحمد بلتاجي موسى، المرجع السابق، ص. 236.

البند الثاني: ضوابط معاينة مسرح الجريمة الإلكترونية.

نظراً لاختلاف مسرح الجريمة في جرائم التعدي على المستندات الإلكترونية عن غيره من الجرائم، لوجود الأدلة الإلكترونية ذات الطبيعة غير المرئية، يقترح الفقه الجنائي[1] ليكون معاينة مسرح الجريمة ذو فائدة عملية في الكشف عن الحقيقة، وتحديد مرتكبها ضرورة أن يراعي المحقق وهو يقوم بإجراء المعاينة مجموعة الضوابط والقواعد وكذا الاستشارات الفنية، ولعل أبرزها ما يلي:

1- تحديد نقطة البدء في المعاينة ونقطة الانتهاء منها، بحيث يجب أن تجري المعاينة بصورة مرئية يُلِمُ فيها المحقق بكافة الجوانب التي يريد الوصول إليها من المعاينة.

2- أخذ صورة شمسية لشاشة الحاسب الآلي والأجهزة الطرفية المتصلة به والمحتويات مع التركيز بوجه خاص على تصوير الأجزاء الخلفية للحاسب، وملحقاته لكي تظهر المعلومات أو الصور المطلوب معاينتها[2].

3- ملاحظة وإثبات حالة الكابلات والتوصيلات المتصلة بكل مكونات النظام، وذلك حتى يمكن إجراء عمليات المقارنة والتحليل حين عرض الأمر فيما بعد على المحكمة[3].

4- العناية البالغة بملاحظة الطريقة التي تم بها إعداد النظم، والآثار الإلكترونية التي يُخلفها ولوج النظام أو التردد على المواقع بشبكة المعلومات، وبوجه خاص السجلات الإلكترونية التي تزود بها شبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز الذي تم عن طريقه الدخول إلى النظام أو الموقع[4].

---

[1]- أحمد عاصم عجيلة، المرجع السابق، ص. 438.

[2]- جميل عبد الباقي الصغير، جرائم الإنترنت، الأحكام الموضوعية والجوانب الإجرائية، دار النهضة، القاهرة، 2010، ص. 26؛ نبيلة هبه مولاي هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص.77.

[3]- سرحان حسن المعيني، المرجع السابق، ص.43؛ خالد حامد أحمد مصطفى، المرجع السابق، ص.159.

[4]- عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، ط1، دار الفكر الجامعي، الإسكندرية، 2006، ص. 104.

5- وجوب التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالمستندات الإلكترونية محل الجريمة، وذلك لرفع ومضاهاة ما قد يوجد عليها من بصمات.

6- التحفظ على محتويات سلة المهملات من الأوراق الملقاة أو الممزقة القريبة من الحاسب والشرائط والأقراص الممغنطة غير السليمة أو المحطمة، وفحصها ورفع البصمات التي قد تؤدي إلى التعرف على المتهم مرتكب الواقعة[1].

7- حصر مباشرة المعاينة على فئة معينة من الخبراء والباحثين والمحققين الذين تتوافر لديهم الكفاءة العلمية والخبرة الفنية في مجال الحاسبات الإلكترونية والشبكات ونظم المعلومات، واسترجاع المعلومات، والذين تلقوا تدريباً كافيا على التعامل مع نوعية الآثار والأدلة التي يحويها مسرح الجريمة المعلوماتية، ففي فرنسا مثلا يقوم فريق مكون من 13 شرطي بالإشراف على تنفيذ المهمات التي يعهد بها إلى وكلاء النيابة والمحققين، وجميعهم تلقوا تدريبا متخصصا إلى جانب اختصاصهم الأساسي في مجال التقنية الحديثة، كما يقومون بمرافقة المحققين أثناء المعاينة والتفتيش، حيث يفحصون كل جهاز، وينقلون نسخة من الأسطوانة الصلبة، وبيانات البريد الإلكتروني، ثم يقومون بعمل تقرير يرسل إلى قاضي التحقيق وهم يستعينون لتحقيق مهامهم ببرامج تمكنهم من قراءة الحاسبات الآلية المحمولة[2].

8- عدم نقل أية مستندات إلكترونية أو أية معلومات مسجلة على الحاسب من مسرح الجريمة قبل إجراء اختبارات التأكد من خلو المحيط الخارجي لموقع الحاسب من أية مجالات لقوة مغناطيسية يمكن أن تتسبب في محو البيانات المسجلة على الوسيط المادي[3].

---

[1]- سامح أحمد بلتاجي موسى، المرجع السابق، ص. 237.

[2]- علي عدنان الفيل، المرجع السابق، ص. 35.

[3]- نبيلة هبة مولاي هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص. 77.

9- الحصول على الاحتياجات الضرورية من أجهزة وبرامج للاستعانة بها في الفحص والتشغيل مثل برنامج معالجة الملفات، والبرنامج الذي ينتج صوراً مطابقة من القرص الصلب، ويستخدم بصفة خاصة لأغراض التحقيقات الجنائية في المباحث الفيدرالية الأمريكية، والذي يسميه الخبراء بحقيبة الأدلة الرقمية.

10- وجوب السيطرة على الدائرة المحيطة بمكان المعاينة بوضع حراسات كافية لمراقبة التحركات داخل الدائرة، أو لإمكان العودة لإجراء معاينة أخرى فيما بعد حتى يتم الانتهاء من التحقيق[1].

فضلا عن هذه الضوابط الفنية الواجب مراعاتها فإن الإسراع في الانتقال وإجراء المعاينة يعد شرطا أساسيا في عملية المعاينة، كما يجب المحافظة على حالة الأمكنة قدر المستطاع والسعي لاستغلالها على الوجه الكامل وفق الطرق العلمية الحديثة، وهو ما حرص عليه قانون الإجراءات الجزائية حيث وضع نصوصاً تكفل أحسن الضمانات للتحري خلال هذه المرحلة، وذلك عن طريق توقيع عقوبات تصل إلى حد السجن في حالة عرقلة سير العدالة[2]، ونفس الموقف تم إتباعه من طرف المشرع الفرنسي[3].

---

[1]- أحمد عاصم عجيلة، المرجع السابق، ص. 440.

[2]- تطرق المشرع الجزائري إلى الأفعال المذكورة في المادة 43 من ق.إ.ج.ج حيث عاقب بموجب هذه المادة كل شخص لا صفة له يقوم بإجراء أو تغيير في حالة الأماكن التي وقعت فيها الجريمة ،أو ينزع منها أي شيء قبل الإجراءات الأولية للتحقيق القضائي، وإذا كان المقصود من لمس الآثار أو نزع الأشياء هو عرقلة سير العدالة، فعاقب على هذا الفعل بالحبس من ثلاثة أشهر إلى ثلاثة سنوات وبغرامة من 1000 إلى 10.000 دج... ق.إ.ج .الجزائري المعدل والمتمم.

[3]- كرس القانون الفرنسي في المادة 55 من قانون الإجراءات الجزائية الفرنسي الحماية الجزائية لمسرح الجريمة، وقد تعرضت هذه المادة لحالة إحداث تغيير في مسرح الجريمة دون قصد خاص، في حين عالجت المادة 434-4 من قانون العقوبات الفرنسي الفاعل الذي يهدف من وراء التغيير إلى عرقلة عمل العدالة وقد ورد نصها كالآتي:

Article 434-4 (C.P.F. modifié par ordonnance n°2000-916 du septembre 2000- Article 3 (v) JORF 22 septembre 2000 en vigueur le 1er janvier 2002) dispose que : «est puni de trois ans d'emprisonnement et de 45000 euros d'amende le fait, en vue de faire obstacle à la manifestation de la vérité.

1- De modifier l'état des lieux d'un crime ou d'un délit soit par l'altération, la falsification ou l'effacement des traces ou indices, soit par l'apport, le déplacement ou la suppression d'objet quelconques.

2- De détruire soustraire receler ou altérer un document public ou privé ou un objet de nature à faciliter la découverte d'un crime ou d'un délit, la recherche des preuves ou la condamnation des coupables.=

الفرع الثاني: التفتيش.

يعد التفتيش بصفة عامة إجراء من إجراءات التحقيق الابتدائي، يستهدف كشف الحقيقة، بشأن الجرم الواقع ومدى ثبوته في مواجهة المتهم[1]، وذلك عن طريق البحث في مستودع السر عن أشياء تفيد في الكشف عن الجريمة المرتكبة ونسبتها إلى فاعلها[2]، وفي معنى آخر هو الاطلاع على محل منحه القانون حرمة خاصة بإعتباره مستودع سر صاحبه لضبط ما يفيد في كشف الحقيقة عن جريمة معينة[3].

كما يعرف جانب آخر من الفقه[4] التفتيش بأنه: "إجراء من إجراءات التحقيق، يباشره موظف مختص بهدف البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة المسكن أو الشخص، وذلك وفقا للإجراءات القانونية المقررة"، هذا ويبدو أن التفتيش ليس غاية في حد ذاته، وإنما هو وسيلة لغاية تتمثل فيما يمكن الوصول من خلاله إلى أدلة مادية تساهم في بيان وظهور الحقيقة.

ويعد التفتيش كأصل عام من إختصاص سلطة التحقيق، والمتمثلة في قاضي التحقيق والنيابة العامة باختلاف التشريعات، بحيث يجوز لقاضي التحقيق اللجوء إلى التفتيش إما بنفسه، وإما أن يأذن بذلك لأحد ضباط الشرطة القضائية من خلال الإنابة القضائية[5].

=Lorsque les faits prévus au présent article sont commis par une personne qui, par ses fonctions, est appelée à concourir à la manifestation de la vérité, la peine est portée à cinq ans d'emprisonnement et à 75000 euro d'amende».

[1]- علي عدنان الفيل، المرجع السابق، ص. 38.

[2]- يعتبر تمسك الفرد بمستودع سره حق له باعتبار أن أسرار الإنسان تخصه وحده فقط، وهذه الأسرار جزء من حياته اليومية، ومن هذا المنطلق يحق للفرد التمسك بأسراره الشخصية وعدم انتهاكها سواء كان ذلك في مسكنه أو مراسلاته أو معلوماته المختزنة في جهاز الحاسب الآلي الخاص به، أو نظامه المعلوماتي، ولهذا فله الحق بالتمتع بحماية القانون لهذا الحق، الذي يعتبر من الحقوق الدستورية لهذا المواطن التي لا يحق انتهاكها دون سبب قانوني. مأخودة من، عادل عبد الله الخميس العمري، المرجع السابق، ص. 259.

[3]- علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والإنترنت، دراسة مقارنة، ط 01، عالم الكتب الحيث، د.ب.ن، سنة 2010، ص. 20

[4]- هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة، 2006، ص. 47.

[5]- تختلف التشريعات المقارنة في تحديد أعضاء السلطة المختصة بالتحقيق الابتدائي، ففي القانون الإجرائي الجزائري يلاحظ أن قاضي التحقيق هو سلطة التحقيق الأصلية واستثناءاً النيابة العامة، وهو ذات الأمر الذي يقرره القانون الإجرائي الفرنسي، على عكس المشرع المصري والذي يخول تلك السلطة للنيابة العامة باعتبار أنها الأصل والأجدر بذلك، واستثناءاً لقاضي التحقيق.=

وبما أن التفتيش قد يشمل الأشخاص والمساكن، فإن هذا يجعل منه من أخطر الحقوق التي قد تمنح للمحقق وذلك لمساسها بالحريات التي تكفلها الدساتير، ولهذا سعت التشريعات المختلفة إلى وضع ضوابط عديدة له سواء فيما يتعلق بالسلطة التي تباشره، أو تأذن بمباشرته والأحوال التي يجوز فيها ذلك، شروط إتخاذ هذا الإجراء بما يتلائم مع حريات الأفراد، حرمة المساكن وهذا كله لتعزيز مبدأ المشروعية[1].

هذا عن تعريف التفتيش عموماً، أما عن تعريفه في الجرائم الإلكترونية فيلاحظ أن المجلس الأوروبي قد تطرق له بحيث إعتبره: "الإجراء الذي يسمح بجمع الأدلة المخزنة أو المسجلة بشكل إلكتروني، وهو الإجراء الذي يسمح باستخدام الوسائل الإلكترونية للبحث في أي مكان عن البيانات والأدلة المطلوبة"[2].

هذا ويستلزم التفتيش عن البيانات المخزنة آلياً القيام بعملية ولوج للأنظمة المعلوماتية التي يتم تحديدها لضبط ما يفيد في الكشف عن الجريمة وإيجاد أدلة الإدانة، وهو الأمر الذي يستدعي من جهات التحقيق أن تكون على دراية كاملة حول إمكانية وكيفية التعامل مع البرامج، الملفات، البيانات المخزنة بالحاسب، وكذا كلمة السر اللازمة للدخول إلى النظام[3].

وينبني على القواعد السالف ذكرها أن تفتيش نظام الحاسب الآلي[4] يعد من أخطر وأصعب المراحل في حال إتخاذ الإجراءات الجنائية ضد مرتكب الجريمة المعلوماتية، لكون محل التفتيش - هو الحاسب والشبكات- كان مثارا لجدل فقهي، بسبب أن الكيان المعنوي

=أما التشريعات الأنجلوأمريكية فنجد أن جهاز الشرطة هو وحده من يضطلع بمهمة التحقيق الابتدائي، كما هو الحال في القانون الكندي والانجليزي. مشار اليه من طرف: نبيلة هبة مولاي على هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص. 38.

[1]- محمد فتحي، تفتيش شبكة الأنترنت لضبط جرائم الإعتداء على الأداب العامة، ط2، المركز القومي للإصدارات القانونية، مصر،2012 ،ص 353؛ خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص.180.

[2]- بوعناد فاطمة زهرة، المرجع السابق، ص 103؛ علي عدنان الفيل، المرجع السابق، ص. 39.

[3]- عفيفي كامل عفيفي، المرجع السابق، ص. 338.

[4]- يرى جانب من الفقه أن الإصطلاح الواجب إطلاقه على عملية البحث عن أدلة الجريمة المرتكبة في العالم الافتراضي هو "الولوج أو النفاذ"، باعتباره المصطلح الدقيق بالنسبة للمصطلحات المعلوماتية، بينما مصطلح التفتيش فيعني: البحث، القراءة، التخصص والتدقيق في البيانات وهو مصطلح تقليدي أكثر، غير أن هناك من يستخدم المصطلحين معاً بغرض التنظيم والتنسيق بين المفاهيم التقليدية والحديثة.مشار إليه من طرف، نبيلة هبة مولاي علي هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص. 39.

للحاسب يعد مجرد برامج وبيانات ومستندات إلكترونية ليس لها أي مظهر مادي محسوس، وهو ما يجعل من عملية التفتيش في البيئة الإلكترونية تتميز بنوع من الخصوصية.

لكل هذا يتم التساؤل حول مدى إمكانية إعتبار المستندات الإلكترونية محلاً يرد عليه التفتيش؟، وما هي الضوابط الواجب إتباعها لإتمام إجراء التفتيش في البيئة الرقمية؟، وماهي المعوقات الخاصة بتنفيذ الإذن بالتفتيش؟

كل هذه المسائل وغيرها سيتم بيانها بتحديد صلاحية التفتيش في البيئـــة الرقمية **(البند الأول)**، وكذا ضوابط التفتيش في الجرائم المعلوماتية **(البند الثاني)**.

البند الأول: صلاحية تفتيش المستند الإلكتروني في البيئة الرقمية.

للتفتيش محل يجب أن يرد عليه، ويختلف التفتيش كإجراء من إجراءات التحقيق من حيث طريقة إجراءه بحسب المحل الذي يرد عليه، لاسيما في الجرائم الواقعة على المستندات الإلكترونية، وبما أن الحاسب الآلي يتكون من مكونات مادية أو صلبة ومكونات منطقية، فإنه ينبغي تحديد مدى إمكانية خضوع تلك المكونات للتفتيش الجنائي التي تجريه جهة التحقيق بحثا عن دلائل تفيد في كشف الحقيقة ؟، ولايقتصر نطاق البحث على مكونات الحاسب الآلي، كون أن شبكات الحاسوب هي الأخرى ينبغي النظر في مدى قابليتها للتفتيش.

هذا ما سيتم بيانه بالتطرق لخضوع مكونات الحاسب الآلي المادية للتفتيش **(أولا)**، خضوع مكونات الحاسب الآلي المعنوية للتفتيش **(ثانيا)**، خضوع شبكات الحاسب الآلي للتفتيش **(ثالثا)** .

أولاً: مدى خضوع مكونات الحاسب الآلي المادية للتفتيش.

يتكون الحاسب الآلي من مكونات مادية، ومن هذه المكونات، وحدات الإخراج، وحدة الذاكرة الرئيسية، ووحدات الإدخال، وحدة الحساب والمنطق، وحدة التحكم، وكذا وحدات التخزين الثانوية، وللإشارة فإن كل وحدة من هذه الوحدات تشمل على مجموعة من المفردات المعلوماتية[1].

[1]- نبيلة هبة مولاي علي هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص.42؛ سامح أحمد بلتاجي موسى، المرجع السابق، ص، ص. 244- 245.

وبخصوص قابلية هذه المكونات للتفتيش في مجال الجرائم الواقعة على المستندات الإلكترونية، فإن الفقه يتفق على خضوع هذه المكونات للتفتيش متى تم ذلك وفقا للإجراءات القانونية[1]، بحيث لا يثير تفتيش هذه المكونات أي مشاكل متى تم هذا الإجراء وفقا لقواعد التفتيش في الجرائم التقليدية[2]، وعليه يمكن ولوج المكونات المادية للحاسب الآلي بأوعيتها المختلفة للبحث عن الجرائم الماسة بالمستندات الإلكترونية، و التنقيب عن أي شيء يفيد في كشف حقيقتها، وكذا تحديد مرتكبيها.

ولئن كان تفتيش المكونات المادية للحاسب الآلي أمر معقول، إلا أنه ينبغي الإشارة إلى أن حكم التفتيش يتوقف على طبيعة المكان الذي توجد فيه تلك المكونات، ذلك أن صفة المكان لها أهمية خاصة في مجال التفتيش، بحيث إذا كانت المكونات المادية للحاسب الآلي متواجدة في مكان خاص كمسكن المتهم، أو أحد ملحقاته كان لها حكمه، فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه، وبنفس الضمانات والإجراءات المقررة قانوناً في التشريعات المختلفة[3]، وفي الأوقات المقررة للتفتيش، وهو ما أخذت به بعض التشريعات ومنها التشريع المصري[4].

والملاحظ أن المشرع الجزائري في نص المادة 64 من قانون الإجراءات الجزائية[5] خرج عن القاعدة العامة بحيث إستلزم لمباشرة إجراء التحقيق الحصول على رضاء صريح من الشخص الذي ستتخذ لديه الإجراءات، كما وأوجد جملة من الضمانات لإجراء التفتيش، لكنه في الوقت ذاته إستثنى بعض الجرائم من الخضوع لتلك الضمانات وذلك لخطورتها،

---

[1]- علي عدنان الفيل، المرجع السابق، ص. 41.

[2]- لا يختلف التفتيش في جرائم المعلومات عن التفتيش في الجرائم التقليدية، سوى أن هذا الإجراء الأول يهدف إلى الدخول إلى نظم المعالجة الآلية للبيانات بما تشمله من مدخلات وتخزين ومخرجات، لأجل البحث فيها عن أفعال غير مشروعة مرتكبة وتشكل جناية أو جنحة، والتوصل إلى أدلة تفيد إثبات الجريمة ونسبتها إلى المتهم بارتكابها. مشار إليه من طرف، سرحان حسن المعيني، المرجع السابق، ص 43؛ حطاب كمال، المرجع السابق، ص. 304.

[3]- هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص.73؛ عادل عبد الله خميس المعمري، المرجع السابق، ص.261.

[4]- أحمد عاصم عجيلة، المرجع السابق، ص. 410.

[5]- تنص المادة 1/64 من القانون رقم 06-22 المؤرخ في 20ديسمبر2006 ،المعدل و المتمم لقانون الإجراءات الجزائية الجزائري، سابق الإشارة إليه: "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 فبامكانه الإستعانة بشخص يختاره بنفسه، ويذكر ذلك في المحضر مع الإشارة صراحة إلى رضاه".

وهو ما تقرر في المادة 47 فقرة 03 من ذات القانون بحيث أجاز المشرع الجزائري في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات إجراء التفتيش في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل، شريطة الحصول على إذن مسبق من وكيل الجمهورية المختص (م 47 ق.إ.ج.)[1].

ولئن كان المشرع الجزائري منح لوكيل الجمهورية صلاحية منح الإذن المسبق لإجراء التفتيش في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، إلا أن من الفقه من يرى ضرورة منح هذه الصلاحية لقاضي التحقيق[2]، كون أن المشرع الجزائري يأخذ بنظام الفصل بين الإدعاء والتحقيق.

إذا كان الفقه يتفق على خضوع مكونات الحاسب الآلي المادية للتفتيش بمراعاة الأحكام الإجرائية التقليدية الخاصة بهذا الإجراء، فإنه ينبغي الذكر أن تفتيش المكونات المادية للحاسب الآلي الموجودة في الأماكن الخاصة يستلزم التفرقة بين ما إذا كانت المكونات المادية للحاسب الآلي منعزلة عن غيرها من الحاسبات، أم أنها متصلة بحاسب أو بنهاية طرفية في مكان آخر كمسكن غير مسكن المتهم مثلاً، فإذا كانت كذلك وكانت البيانات المخزنة في أوعية هذا النظام الأخير من شأنها كشف الحقيقة، تعين مراعاة القيود والضمانات التي يستلزمها المشرع لتفتيش هذه الأماكن[3].

هذا عن الأماكن الخاصة، أما بالنسبة للأماكن العامة، فسواء كانت من الأماكن العامة بطبيعتها كالطرق العامة والميادين والشوارع والمنتزهات العامة، أو من الأماكن العامة بالتخصيص كالمقاهي والمطاعم والسيارات العامة، فإن تفتيشها لا يتم بنفس الضمانات والقيود المنصوص عليها قانونا[4]، بحيث إذا وجد في هذه الأماكن من يحوز أو يحمل مكونات مادية للحاسب الآلي، فإن تفتيشها سيتم وفقا للأحكام الخاصة بالتفتيش.

---

[1]- تنص المادة 3/47 ق.إ.ج.ج: «عندما 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 أو المعاينة أو الحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل، وذلك بناءً على إذن مسبق من وكيل الجمهورية المختص».

[2]- حطاب كمال، المرجع السابق، ص. 304.

[3]- سامح أحمد بلتاجي موسى، المرجع السابق، ص. 245.

[4]- هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص. 74؛ علي عدنان الفيل، المرجع السابق، ص. 41.

ثانياً: مدى خضوع مكونات الحاسب الآلي المعنوية للتفتيش.

لقد أثار تفتيش المكونات المنطقية وهي المكونات المعنوية للحاسوب في مجال الجرائم الواقعة على المستندات الإلكترونية خلافاً فقهيا كبيراً بشأن مدى صلاحيتها لتكون محلاً يرد عليها التفتيش، وكذا بشأن مدى إمكانية تطبيق الأحكام التقليدية للتفتيش حين مباشرة البحث والولوج إلى نظم الحواسيب والمعلومات للتنقيب عن الأدلة التي تفيد في كشف حقيقة الجريمة التي وقعت، والتي كان محلها أحد المستندات الإلكترونية.

وفي هذا الشأن تتعد الإتجاهات الفقهية، بحيث يُجيز الإتجاه الأول تفتيش البيانات الإلكترونية بمختلف أشكالها، ويستند هذا الاتجاه الفقهي عند تبريره لموقفه على نصوص القوانين الإجرائية التي تستخدم عند تنظيمها لأحكام إصدار الإذن بالضبط مصطلح "ضبط أي شيء"، فمصطلح "أي شيء"، حسب هذا الإتجاه الفقهي يجب تفسيره بحيث يشمل بيانات الحاسب المحسوسة وغير المحسوسة، كون أن الغاية من التفتيش هي ضبط الأدلة المادية التي تفيد في كشف الحقيقة .

وعلى نقيض هذا الإتجاه الفقهي، ينادي إتجاه ثاني بعدم إمكانية تطبيق المفهوم المادي على بيانات الحاسوب غير المرئية أو غير الملموسة، وكذا على الأدلة الإلكترونية غير المادية كالمستندات الإلكترونية، ذلك أن النبضات الإلكترونية أو الإشارات الإلكترونية الممغنطة لا تعد من قبيل الأشياء الملموسة، ونظراً لأنها لا تعد شيئاً مادياً بالمعنى المألوف للكلمة، فإنه لا يمكن ضبطها[1].

ويقترح أنصار هذا الإتجاه لمواجهة هذا القصور التشريعي إيراد نص يخص تفتيش الحاسبات الإلكترونية، على أن ينصرف معنى التفتيش ليشمل صراحة المواد المعالجة عن طريق الحواسيب الإلكترونية، أو عن طريق بيانات هذه الحواسيب، وسبب إيراد هذا النص التطور التقني الذي حدث بسبب ثورة الإتصالات عن بعد، والذي جعل غاية التفتيش الجديدة تتركز في البحث عن الأدلة المادية، أو أي مادة معالجة بواسطة الحواسيب الإلكترونية[2].

[1]- أحمد عاصم عجيلة، المرجع السابق، ص. 413.
[2]- سامح أحمد بلتاجي موسى، المرجع السابق، ص. 249، عادل عبد الله خميس المعمري، المرجع السابق، ص.261.

الحقيقة أن بُعْد نظر هذا الإتجاه الفقهي دفع الإتفاقيات الدولية وكذا التشريعات الأجنبية والوطنية إلى تبنيه في نصوصها التشريعية المتعلقة بالجريمة المعلوماتية، بحيث نصت المادة 19 من القسم الرابع من إتفاقية بودابست لمكافحة الإجرام المعلوماتي: «يجب على كل طرف أن يتبنى الإجراءات التشريعية، أو أية إجراءات أخرى يرى أنها ضرورية من أجل تخويل سلطاته المختصة سلطة التفتيش أو الولوج بطريقة مباشرة:

1- لنظام معلوماتي أو لجزء منه، وكذلك للبيانات المعلوماتية المخزنة فيه، وعلى أرضه.
2- لدعامة تخزين معلوماتية تسمح بتخزين بيانات معلوماتية."

كما نصت على ذلك المادة 26 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 2010/12/21، والتي صادقت عليها الجزائر، والتي ورد بها: «بأن تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين سلطاتها المختصة من التفتيش أو الوصول إلى:

أ) تقنية معلومات أو جزء منها، والمعلومات المخزنة فيها أو المخزنة عليها،

ب) بيئة أو وسيط تخزين معلومات تقنية والذي قد تكون معلومات التقنية مخزنة فيه أو عليه»[1].

وعلى غرار الاتفاقيات الدولية يلاحظ أن التشريعات الأجنبية والوطنية هي الأخرى قد تأثرت بهذا الاتجاه، بحيث إستجاب المشرع الفرنسي للتطورات التكنولوجية وعدل من النصوص الخاصة بالتفتيش بمقتضى القانون رقم (54-2004) المؤرخ في 21 يونيه 2004، حيث قام بإضافة عبارة "المعطيات المعلوماتية" في المادة 94 من قانون الإجراءات الجزائية الفرنسي لتصبح المادة على النحو التالي: «يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء أو معطيات معلوماتية يكون كشفها مفيداً لإظهار الحقيقة»[2].

[1]- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، سابق الإشارة إليها.

[2]- Article 94 du c.p.p.f (modifié par loi n° 2004-575 du 21 Juin 2004-art .42 JORF22 juin 2004) dispose que : «Les perquisitions sont effectuées dans tous les lieux où peuvent se trouver des objets ou des données informatiques dont la découverte serait utile à la manifestation de la vérité».

هذا عن القانون الفرنسي، أما بخصوص المشرع الجزائري فيتبين أنه قد حذا حذو المشرع الفرنسي، وإستحدث نصوصاً عقابية تعاقب على الأفعال غير المشروعة الماسة بسلامة نظم المعالجة الآلية للمعطيات، وذلك بداية بموجب القانون رقم 15/04 المعدل والمتمم لقانون العقوبات، ورغبة منه في مسايرة التطورات المعاصرة أصدر القانون رقم 09-04 الصادر في 08 غشت 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، بحيث تطرق إلى تفتيش المنظومة المعلوماتية في نص المادة 05 منه والتي جاء فيها: « يجوز للسلطات القضائية المختصة، وكذا ضباط الشرطة القضائية... الدخول بغرض التفتيش ولو عن بعد إلى:

أ- منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزونة فيها.

ب- منظومة تخزين معلوماتية،

في الحالة المنصوص عليها في الفقرة أ، إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى، وأن هذه المعطيات يمكن الدخول إليها انطلاقاً من المنظومة الأولى يجوز تمديد التفتيش بسرعة إلى هذه المعلومة، أو جزء منها، بعد إعلام السلطة القضائية المختصة مسبقاً بذلك...»[1].

إلى جانب الاتجاهات الفقهية السابقة حول مدى قابلية مكونات الحاسب الآلي المنطقية لتكون محلاً للتفتيش، ظهر إتجاه فقهي ثالث وقد نادى هذا الإتجاه بضرورة النظر إلى الواقع العملي، الذي يقتضي ليقع التفتيش على بيانات الحاسب أن تكون قد إتخذت شكلاً مادياً، وعليه لاتعد البيانات المنفردة عن الدعامات من قبيل الأشياء، ولا يمكن ضبطها، ولكن إذا تم طبع هذه البيانات، فمطبوعاتها تعد من قبيل الأشياء الملموسة المحسوسة التي يجوز ضبطها[2].

[1]- قانون 09-04 مؤرخ في 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، سابق الإشارة إليه.

[2]- علي عدنان الفيل، المرجع السابق، ص 43؛ سامح أحمد بلتاجي موسى، المرجع السابق، ص. 249.

وعلى نقيض هذا الاتجاه ظهر اتجاه فقهي رابع يرى تحديد مدلول الشيء فيما يخص مكونات الحاسوب يتم بتحديد مدلول كلمة المادة في العلوم الطبيعية، فإذا كانت المادة تُعَرف بأنها: "كل ما له كتلة ويشغل حيزاً مادياً في فراغ معين، بحيث يمكن قياس ذلك الحيز والتحكم فيه"، فإن الكيانات المنطقية أو البرامج تشغل حيزاً مادياً في ذاكرة الحاسوب ويمكن قياسها بمقياس معين، كون أنها تأخذ شكل نبضات أو ذبذبات إلكترونية أو إشارات أو موجات كهرومغناطيسية قابلة لأن تسجل وتخزن في وسائط معينة، ويمكن نقلها وبثها وحجبها واستغلالها.

إستنادا لهذا التبرير فإن البيانات أو المكونات المنطقية بما فيها المستندات لا تعتبر شيئا معنويا فحسب، بل تعد كذلك كيان مادي تتشابه مع التيار الكهربائي الذي يعتبره الفقه والقضاء في كل من مصر وفرنسا من قبيل الأشياء المادية المحسوسة.

وفقا لهذا التبرير يرى هذا الإتجاه الفقهي أن المكونات المنطقية للحاسب الآلي لها في العالم الخارجي وجود مادي وهي تصلح بذلك لأن تكون محلاً للتفتيش[1]، وهو ذات ما قضت به محكمة باريس الابتدائية حينما قررت عدم وجود فوارق في الطبيعة بين مستخرجات البرامج وبين البرامج المستغلة، كما وأدرجت محكمة جنح بروكسل عند قيامها بتكييف بيانات الحاسب ومكوناته المنطقية ضمن الأشياء المادية المحسوسة التي لها وجود مادي[2].

من خلال الإتجاهات الفقهية السابقة يعتقد أن الرأي الراجح هو ذلك الذي يمنح لمكونات المنطقية للحاسوب وجود مادي فعلي، ويعتبرها منقولاً لإمكانية نقلها من مكان إلى آخر، فضلاً عن إمكان تملكها وحيازتها، والقول بخلاف ذلك خاطئ ومرده عدم الفهم الصحيح لطبيعة وماهية المنقول، إذ لا يمكن الإستناد لعدم إعتبار المكونات المنطقية جسما قابلا للوزن وفقا للنظريات الطبيعية لرفض منح صفة الشيء المادي عليها.

[1]- سامح أحمد بلتاجي موسى، المرجع السابق، ص 251؛ علي عدنان الفيل، المرجع السابق، ص. 43.
[2]- حطاب كمال، المرجع السابق، ص. 306.

بتطبيق الأحكام السابقة على النصوص التشريعية الوطنية، يلاحظ أن المشرع الجزائري وُفِق حين نص صراحة في المادة 05 من قانون 09-04 على جواز تفتيش المنظومة المعلوماتية، وهو بذلك يكون قد حسم الجدل الفقهي حول مدى إمكانية تفتيش المكونات المعنوية للحاسب الآلي من عدمه، كما أجاز المشرع في الفقرة الأخيرة من المادة ذاتها للسلطات المكلفة بالتفتيش إمكانية الإستعانة بكل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها[1].

ثالثاً: مدى خضوع شبكات الحاسب الآلي للتفتيش.

ترتبط أجهزة الحاسوب أحيانا ببعضها عن طريق شبكات، وتلك الشبكات قد تكون داخل الشركة أو المؤسسة أو فروعها داخل الحدود الإقليمية لنفس الدولة، ولئن كان هذا الأمر منطقي وتفرضه ضرورات العمل في البيئة الرقمية، إلا أنه يثير في مجال التفتيش قضايا متعددة، إذ قد يستتبع تفتيش جهاز حاسوب إحدى الشركات، المؤسسات، الفروع الدخول إلى جهاز حاسب آخر ينتمي لشخص آخر يوجد في مكان آخر، وهذا الأمر يعني إمتداد الدليل الإلكتروني في جرائم المستندات الإلكترونية لأجهزة أخرى، وأكثر من ذلك فقد تُظْهِر التحقيقات ضرورة تفتيش أجهزة الحاسوب المتواجدة خارج حدود تلك الدولة، وهو الأمر الذي يحدث حينما يتعلق الأمر بشركة رئيسية (الأم) وفروعها المنتشرة في الخارج، كون أن تلك الشركات تكون مرتبطة ببعضها البعض عن طريق شبكة الأنترنت، ولا يقتصر الأمر على ذلك فحسب، بل يتعداه لإمكانية إرتباط بعض أجهزة الحواسيب بقاعدة بيانات متواجدة خارج الدولة التي تجري سلطاتها التحقيق في شأن إحدى الجرائم الواقعة على المستندات الإلكترونية[2].

كل هذه المعطيات تقف أمام أعمال التفتيش والضبط، وتثير أسئلة متعددة أهمها: هل يمتد تفتيش حاسب معين إلى الأجهزة المرتبطة به سواء أكانت موجودة داخل البلاد أو

[1]- المادة 4/05 من قانون 09-04 مؤرخ في 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، سابق الإشارة إليه.

[2]- سامح أحمد بلتاجي موسى، المرجع السابق، ص. 251؛ أحمد عاصم عجيلة، المرجع السابق، ص. 418.

خارجها؟، ما أثر تفتيش الأنظمة المتصلة بالنظام المأذون بتفتيشه إذا تواجد في دوائر اختصاص مختلفة؟

إن تحديد هذا الأمر يقتضي التمييز بين إحتمالين، إحتمال إتصال حاسب المتهم بحاسب آخر أو نهاية طرفية موجودة في مكان آخر داخل الدولة، وإحتمال إتصال حاسب المتهم وهو الحاسوب محل التفتيش بحاسب آخر أو نهاية طرفية موجودة في مكان آخر خارج حدود الدولة.

إذ وبالنسبة للفرض الأول، والمتمثل في إتصال حاسب المتهم بحاسب آخر أو نهاية طرفية موجودة في مكان آخر داخل الدولة، يمكن القول أن إذن التفتيش في الجرائم التقليدية يستلزم تحديد مكان و محل التفتيش، وهو ما يقصد بهما في الجرائم الإلكترونية المقر الذي يتواجد به الحاسب المراد تفتيشه سواءً كان منزلاً أو مكتباً أو شركة مملوكة للمتهم[1].

وفي حالة اتصال جهاز الحاسوب المملوك للمتهم بنهاية طرفية أخرى، أو بحاسوب آخر داخل الدولة، فقد أجازت الاتفاقيات الدولية وكذا التشريعات المقارنة امتداد الإذن بالتفتيش إلى تلك النهاية الطرفية، أو الحاسوب الآخر المتصل بحاسوب المتهم.

بحيث سمحت إتفاقية بودابست لمكافحة الإجرام المعلوماتي لسنة 2001 في المادة 2/19[2] منها للدول الأعضاء أن تُمِدَ نطاق التفتيش الذي كان محله حاسب آلي معين إلى غيره من الأجهزة المرتبطة به في حالة الاستعجال، وذلك في حالة ما إذا كانت هناك معلومات يتم الدخول إليها في هذا الجهاز من خلال الجهاز محل التفتيش.

---

[1]- محل التفتيش يقصد به أجهزة الحواسيب ذاتها التي قد تحتوي على بيانات تحوي أدلة تفيد في كشف الحقيقة، أما مكان التفتيش فيقصد به المقر أو الحيز المكاني الذي يتواجد فيه الحاسب المراد تفتيشه. مشار إليه من طرف، سامح أحمد بلتاجي موسى، المرجع السابق، ص. 252.

[2]- Art 19 al 2 du convention sur la cybercriminalité 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 paragraphe1(a), et ont des raisons de penser que les données recherchées sont stockées dans un autre système informatiqueou dans une partie de celui-cisitué sur son territoire, et que ces données sont légalement accessibles à partir de système initial ou disponible pour ce système initial, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou d'un accès d'une façon similaire à l'autre système ».

إلى جانب هذه الاتفاقية نصت المادة2/26من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات على أن: «تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من التفتيش أو الوصول إلى تقنية معلومات معينة أو جزء منها... فيجوز توسيع نطاق التفتيش والوصول للتقنية الأخرى».

هذا على المستوى الدولي، أما على المستوى الداخلي فيلاحظ أن التشريعات المقارنة، ومنها القانون الألماني، القانون البلجيكي و كذا الأسترالي قد أجاز إمتداد التفتيش إلى سجلات البيانات التي تكون في موقع آخر من الدولة[1].

هذا وقد حسم القانون الفرنسي هذا الإشكال من خلال تعديله لقانون الإجراءات الجزائية الفرنسي بموجب القانون رقم 239 لسنة 2003 بشأن الأمن الداخلي، حيث أضاف المادة (17-1) من قانون الإجراءات الجنائية، والتي أجازت تفتيش النظام الرئيسي والأنظمة المتصلة به في الداخل، وللإشارة فقد تم الإحتفاظ بمضمون هذه المادة مع التعديل في رقمها بموجب القانون 731-2016 المتعلق بتعزيز مكافحة الجريمة المنظمة والإرهاب وتمويلها، وتحسين كفاءة وفعالية الإجراءات الجزائية[2] إذ نصت المادة 58 على أنه: «يجوز لرجال الضبط القضائي من درجة ضباط وغيرهم من رجال الضبط القضائي تحت مسؤولية الضباط، أن يدخلوا عن طريق الأنظمة المعلوماتية المثبتة في الأماكن التي يتم فيها التفتيش على البيانات التي تهم التحقيق، والمخزنة في النظام المذكور أو في أي نظام معلوماتي آخر، ما دامت هذه البيانات متصلة في شبكة واحدة مع النظام الرئيسي أو يتم الدخول إليها، أو تكون متاحة ابتداءً من النظام الرئيسي»[3].

---

[1]- حسين بن سعيد بن سيف الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، المرجع السابق، ص. 482.

[2] -Cf. Myriam Quéméner, les nouvelles disposition de lutte contre la cybercriminalité issues de la loi du 13 novenbre 2014 renforcant la lutte contre le térrorisme, Aj pénal, mensuel, Dalloz, n°3, janvier 2015 ,p.32.

[3]- Art 57/1/1/e.c.p.p.f (crée par la loi 2003-239 du 18 mars 2003 pour la sécurité intérieure en France, modifiée par loi n°2016-731 du 3 juin 2016 art. 58 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale) dispose que: «Les officiers de la 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=

وقد إنتهج المشرع الجزائري في المادة 05 من القانون 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتهما، النهج ذاته بحيث أجاز لجهات التحقيق إمتداد التفتيش إلى منظومة معلوماتية أخرى، إذا كان هناك إعتقاد بأن المعطيات المبحوث عنها مخزنة لديها، بشرط أن تكون هذه المعطيات يمكن الدخول إليها بدءا من المنظومة الأولى، ولكن إستلزم المشرع لنجاح الأمر ضرورة إخطار السلطة القضائية المختصة مسبقاً بذلك[1].

هذا إذا كانت الحاسبات الآلية أو النهايات الطرفية موجودة في أماكن خاصة، أما إذا كانت موجودة في أماكن عامة كالحاسبات الشخصية التي يحملها الشخص خارج منزله، أو الهواتف الذكية، فإن تفتيش أنظمتها لا يكون إلا في الأحوال التي يجيز فيها القانون تفتيش شخص صاحبها، بإعتبار أن تفتيش الشخص يشمل تفتيش ذاته وكل ما في حوزته وقت هذا التفتيش سواءً أكان ملكا له أو لغيره، أما في الحالة التي يكون فيها الجهاز المراد تفتيشه داخل منزل أحد الأشخاص، فإنه تسري عليه القيود التي ينص عليها القانون بالنسبة لتفتيش مسكن المتهم أو تفتيش منزل غير المتهم[2].

ولئن كانت هذه هي الأحكام الواجب تطبيقها عند اتصال حاسب المتهم بحاسب آخر أو نهاية طرفية موجودة داخل حدود الدولة، فإنه ينبغي الذكر أن تواجد حواسيب أو نهايات طرفية متصلة بحاسب المتهم خارج حدود الدولة يُثير مشاكل قانونية عويصة ينبغي على سلطات التحقيق وضباط الشرطة القضائية مواجهتها عند تنفيذ الإذن بالتفتيش، وذلك لأن الأدلة إلكترونية التي تُفيد في كشف الحقيقة تتواجد في الحاسبات الآلية والنهايات الطرفية

=implanté sur les lieux ou se déroule par la perquisition à des données intéressant l'enquête en cours et stockées dans ledit système ou dans un autre système informatique, dés lors que ces données sont accessibles à partir du système initial ou disponible pour le système initial ».

[1]- تنص المادة05/ 2 من قانون 09-04 مؤرخ في 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، سابق الإشارة إليه: "في الحالة المنصوص عليها في الفقرة "أ" من هذه المادة، إذا كانت هناك أسباب تدعو للإعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى، وأن هذه المعطيات يمكن الدخول إليها، انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك."

[2]- حسين بن سعيد بن سيف الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، المرجع السابق، ص، ص. 485-486.

الموجودة خارج الحدود، وتواجدها خارج الحدود يعرقل سير التحقيق، ويثير مسألة حق كل دولة في التمسك بسيادتها على إقليمها[1].

في هذا يرى جانب من الفقه[2] أن التفتيش الإلكتروني العابر للحدود ينبغي أن يتم في إطار اتفاقيات تعاون خاصة ثنائية أو دولية تجيز مثل هذا الإمتداد، بحيث لا يجوز القيام بالتفتيش (الولوج) بدون مثل هذه الاتفاقيات، أو على الأقل الحُصول على تصريح أو إذن من الدولة الأخرى غير مصدرة إذن التفتيش، وهذا الأمر يبرز أهمية التعاون الدولي في مجال إجراءات جمع الأدلة بصفة عامة، وفي مجال مكافحة الجريمة الإلكترونية بصفة خاصة.

وفي سبيل تجنب هذه العقبات الإجرائية وحتى لا يفسح المجال أمام المجرمين للإفلات من العقاب، سعى المجلس الأوروبي في التوصية رقم 17 لسنة 1995 إلى التأكيد على إمكانية إمتداد نطاق تفتيش الحاسوب إلى النظام المتواجد في الخارج، متى كانت هناك ضرورة لاتخاذ إجراءات عاجلة في هذا الأمر، ولكن يجب أن يتم الحصول على موافقة الدولة التي يمتد التفتيش إلى الأجهزة أو النظام المتواجد في إقليمها، وذلك حتى يكون هذا التفتيش ذو أساس قانوني، وكي لا يمثل انتهاكاً لسيادة تلك الدولة[3].

هذا وقد أجازت الاتفاقية الأوربية بشأن الجرائم المعلوماتية في المادة 32[4]منها إمكانية الولوج بغرض التفتيش والضبط في أجهزة، أو شبكات متواجدة داخل الحدود الإقليمية لدولة أخرى بدون إذن من تلك الدول وذلك في حالتين:

1- عندما تكون البيانات متاحة للجمهور ويمكن لأي أحد الدخول إليها.

---

[1]- أحمد عاصم عجيلة، المرجع السابق، ص، ص. 420- 421، عادل عبد الله خميس المعمري، المرجع السابق، ص.262.

[2]- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص، ص. 205- 206.

[3]- سامح أحمد بلتاجي موسى، المرجع السابق، ص. 254.

[4]- Art 32 du convention sur la cybercriminalité dispose que: «Une partie peut, sans l'autorisation d'une autre partie :

a: accéder à des données informatiques, stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données, ou

b: accéder à, ou recevoir au moyen d'un système informatique situé sur un territoire, des données informatiques stockées situées dans un autre état, si la partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique."

2- عندما يكون لدى الطرف الذي دخل، أو تسلم البيانات خارج الإقليم عبر نظام حاسوبي في إقليمه الحصول على رضاء قانوني وإرادي ممن يملك سلطة قانونية للكشف عن تلك البيانات عبر النظام الذي تم الولوج داخله (بمعنى رضاء صاحب أو حائز هذه البيانات بهذا التفتيش).

إن تحقق الصورة الثانية المذكورة في المادة 32 من الإتفاقية المذكورة يبرز حينما يكون البريد الإلكتروني للشخص مخزناً في دولة أخرى من قِبَل مزود خدمة متواجد في تلك الدولة، وكذا في حالة قيام الشخص بتخزين البيانات الخاصة به في دولة أخرى ونظرا لأن صاحب البيانات أو حائزها له سلطة قانونية عليها فإنه يمكن له بإرادته استرداد البيانات أو القيام بالكشف عنها إلى السلطات المسؤولة، أو السماح لهم بالدخول إلى البيانات، وذلك وفقا لما هو مقرر في المادة آنفة الذكر[1].

إلى جانب التشريعات الواردة على المستوى الدولي، يلاحظ أن التشريعات المقارنة هي الأخرى قد أجازت لجهات التحقيق وسلطات التفتيش مباشرة هذا الإجراء، ولو كانت الأجهزة المراد تفتيشها متواجدة داخل إقليم دولة أخرى بشرط أن تكون تلك الاجهزة متصلة بالحاسوب الصادر بشأنه إذن التفتيش، ومن هذه التشريعات التشريع الهولندي الذي أجاز بموجب المادة 125 من قانون الإجراءات الجنائية إمتداد تفتيش الأجهزة المتواجدة على إقليم الدولة إلى الأجهزة الأخرى المتصلة في دول أخرى، كما وسمح بموجب المادة ذاتها للقاضي أن يطلب من الشاهد أن يدلي بأقوال عن معلومات حدثت خارج البلاد[2].

وإلى جانب التشريع الهولندي تصدى التشريع الفرنسي لهذا الإشكال في قانون الإجراءات الجنائية، وذلك بموجب المادة 57 الفقرة 02 من قانون الأمن الداخلي رقم 239 لسنة 2003 المعدل والمتمم، بحيث أجاز لضباط الشرطة القضائية القيام بتفتيش الأنظمة المتصلة بالحاسب، حتى ولو تواجدت خارج الإقليم شريطة أن يتم مراعاة الشروط

[1]- سامح أحمد بلتاجي موسى، المرجع السابق، ص. 255.
[2]- أحمد عاصم عجيلة، المرجع السابق، ص. 421.

المنصوص عليها في المعاهدات الدولية[1]، وقد أضحت هذه الفقرة بعد تعديل 2016 الثالثة من المادة 57-1 من قانون الإجراءات الجزائية[2].

هذا عن التشريعات المقارنة، أما المشرع الجزائري فيلاحظ أنه هو الآخر إنتهج نهج التشريعات الدولية والمقارنة، بحيث أجاز إمتداد التفتيش عن المعطيات المبحوث عنها ولو كانت مخزنة في منظومة معلوماتية خارج إقليم الدولة، شريطة أن يتم ذلك بمساعدة السلطات الأجنبية ووفقا لمبدأ المعاملة بالمثل وكذا الإتفاقيات الدولية ذات الصلة، وهو ما ورد في المادة 05 الفقرة 03 من القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما، والتي نص فيها: «إذا تبين مسبقاً بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقاً للاتفاقيات الدولية ذات الصلة، ووفقا لمبدأ المعاملة بالمثل»[3].

البند الثاني: ضوابط التفتيش.

إن البحث عن الحقيقة القضائية في الجرائم الواقعة على المستندات الإلكترونية لا ينبغي أن يكون طليقا من كل قيد، بل لا بد أن يخضع لضوابط معينة، وذلك حتى لا يتعسف من يسعى للحصول عليها، خاصة وأن التفتيش إجراء يمس بالحياة الشخصية للأفراد.

[1]- Art 57-1/2 c.p.p.f (créé par loi n°2003-239 du 18 mars 2003, art 17, et modifié par la loi n° 2016-731 du juin 2013 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale) dispose que: « s'il est préalablement avéré que ces données, accessibles à partir du système initial ou disponible 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]- Art 57-1 al 3 modifier par Loi n°2016-7331 DU 33 JUIN 2016-art.58.

[3]- قانون 09-04 مؤرخ في 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، سابق الإشارة إليه.

هذا ويلاحظ أن ضرورة الموازنة بين البحث عن الحقيقة، و بين صيانة الحريات الشخصية من التعسف يقتضي إحاطة إجراء التفتيش بجملة من الشروط، وهذه الاخيرة قد تكون موضوعية **(أولا)**، وقد تكون شكلية **(ثانيا)** .

أولاً: الضوابط الموضوعية للتفتيش.

يقصد بالضوابط الموضوعية، الضوابط الواجب توافرها ليتم إجراء التفتيش بشكل صحيح، ويمكن حصر هذه الضوابط في ثلاث وهي: السبب، المحل، والسلطة المختصة بإجراء التفتيش.

فأما عن سبب التفتيش في البيئة الإلكترونية، فيكمن في السعي نحو الحصول على كشف الحقيقة شأنه في ذلك شأن التفتيش في الجرائم التقليدية التي يقوم فيها التفتيش عند وقوع جريمة سواء كانت جناية أو جنحة ويتم إتهام شخص أو أشخاص معينين بإرتكابها أو المشاركة فيها، كل هذا مع ضرورة توافر أمارات قوية أو قرائن تدل على وجود أشياء تفيد في كشف الحقيقة لدى المتهم أو غيره[1].

بهذا يمكن القول أن التفتيش حتى يكون مشروعا لابد أن تكون الجريمة الإلكترونية وقعت بالفعل، وأن يتم إتهام شخص أو أشخاص معينين بإرتكابها أو المشاركة فيها، كما ولابد أن تتوافر إمارات قوية أو قرائن تدل على وجود أشياء أو أجهزة أو معدات معلوماتية تفيد في كشف الحقيقة.

ففيما يخص وقوع الجريمة الإلكترونية، فإنه ينبغي الذكر أن التفتيش لا يكون صحيحا إلا إذا كانت إحدى الجرائم الماسة بالمستند الإلكتروني أو الواقعة على التعاملات الإلكترونية، -وهي كل فعل غير مشروع يتورط في إرتكابه الحاسب الآلي، ويتم إقترافه بإستخدام المعالجة الآلية للبيانات- وقعت فعلا، وأن تُشكل تلك الجرائم في نظر القانون جناية

[1]- محمد فتحي، المرجع السابق، ص.361؛ هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص. 104.

أو جنحة[1]، استنادا للمبدأ المعروف لا جريمة ولا عقوبة، أو تدابير أمن بغير قانون[2]. وعليه يُستبعد من نطاق التفتيش المخالفات[3].

للإشارة فإن شرط وقوع جريمة إلكترونية يقتضي وجود نشاط إجرامي يتمثل في عمل غير مشروع يقع على وسيلة من الوسائل التقنية التي تستخدم فيها المعلومات بطريقة مباشرة أو غير مباشرة، وينبغي أن تكون تلك الأفعال معاقبا عليها، بحيث لا يمكن تطبيق عقوبة غير محددة سلفا بمقتضى نص القانون[4].

لقد أخذ المشرع الجزائري بهذا الشرط، حيث تصدى بموجب القانون 04-15 المعدل والمتمم لقانون العقوبات لمجموعة من الأفعال الماسة بسلامة المعالجة الآلية للمعطيات، وفيه تطرق لفعل الدخول والبقاء غير المشروعين وإلى أفعال أخرى، كحذف أو تغيير المعطيات، أو تخريب نظام اشتغال المنظومة المعلوماتية وغيرها من الأفعال الماسة بالبيانات الإلكترونية، وذلك بدءا من المادة 394 مكرر إلى غاية المادة 394 مكرر 7، كما عزز هذه الحماية كذلك بموجب القانون رقم 09-04[5] الذي تضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما، وأصدر سنة 2005 قانون التوقيع والتصديق الإلكترونيين، والذي جرم فيه بعض الأفعال التي تطال التوقيع الالكتروني[6]، ورغم صدور هذه النصوص التجريمية ظلت بعض الجرائم الماسة بالتعاملات الإلكترونية خارجة من نطاق التجريم كجريمة تزوير المستندات الإلكترونية.

---

[1]- خالد ممدوح إبراهيم، فن التفتيش الجنائي في الجرائم الإلكترونية، المرجع السابق، ص. 210، عادل عبد الله خميس المعمري، المرجع السابق، ص.263.

[2]- المادة 01 من الأمر رقم 66-156 المؤرخ في 8 يونيو 1966، المتضمن ق.ع.ج. المعدل والمتمم، سابق الإشارة إليه.

[3]- إن إستبعاد المخالفات من نطاق التفتيش يفهم ضمنيا من نص المادة 44 من ق.إ.ج.ج التي قصرته على الجنايات و الجنح في فقرتيها الأولى و الثانية إذ نصت على: "لا يجوز لضباط الشرطة القضائية الإنتقال إلى مساكن الأشخاص الذين يظهر أنهم ساهموا في الجناية أو أنهم يحوزون أوراقا أو أشياء لها علاقة بالأفعال الجنائية المرتكبة لإجراء التفتيش إلا بإذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق مع وجوب الإستظهار بهذا الأمر قبل الدخول إلى المنزل و الشروع في التفتيش.

ويكون الأمر كذلك في حالة التحري في الجنحة المتلبس بها أو التحقيق في إحدى الجرائم المشار إليها في المادتين 37 و40 من هذا القانون" .

[4]- بوعناد فاطمة زهرة، المرجع السابق، ص. 115.

[5]- قانون 09-04 مؤرخ في 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، سابق الإشارة إليه.

[6]- قانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، سابق الإشارة إليه.

هذا عن المشرع الجزائري، أما بخصوص المشرع المصري فيُلاحظ أنه لم يجرم جميع صور العدوان على التعاملات الإلكترونية، بل اقتصر في الحماية على أنواع معينة منها، ومن قبيل ذلك التوقيع الإلكتروني والمستند الإلكتروني وذلك من خلال قانون التوقيع الإلكتروني المصري[1].

إذا كان التفتيش لا يكون مشروعا، إلا إذا وقعت الجريمة الإلكترونية فعلا، فإنه وبالمثل ينبغي أن يتم إتهام شخص أو أشخاص معينين بارتكاب تلك الجريمة أو المشاركة فيها، وحتى يتحقق هذا الشرط ينبغي أن يتوافر في الشخص المراد تفتيش شخصه أو مسكنه دلائل كافية تدعو للاعتقاد بأنه ساهم في ارتكاب جريمة من جرائم المستندات الإلكترونية، سواء بوصفه فاعلا أصليا أو شريكا، وعليه إذ لم تتوافر هذه الدلائل كان على قاضي التحقيق أن يصدر أمرا بأن لا وجه لإقامة الدعوى، وذلك وفقا لما تقرره المادة 163 من قانون الإجراءات الجزائية[2]، والتي يقابلها المادة 177 قانون الإجراءات الجزائية الفرنسي[3].

وعن المقصود بمصطلح الدلائل الكافية، فالمتمعن لنصوص قوانين الإجراءات الجزائية سواء في الجزائر أو في مصر أو فرنسا يجد أنها لم تعرف ما هي الدلائل الكافية، بل اكتفت بالنص على تطلب الدلائل القوية والمتوافقة على الاتهام، وفي هذا يتجه الفقه الجنائي إلى تعريف هذه الدلائل بأنها:" مجموعة من القرائن والأمارات المعينة التي تقوم على المضمون العقلي والمنطقي لملابسات الواقعة، وعلى خبرة القائم بالتفتيش التي تؤيد نسبة تلك الجريمة إلى ذلك الشخص بوصفه فاعلاً أو شريكاً"[4].

---

[1]- سامح أحمد بلتاجي موسى، المرجع السابق، ص. 256.

[2]- تنص المادة 163 من ق.إ.ج. ج: «إذا رأى قاضي التحقيق أن الوقائع لا تكون جناية أو جنحة أو مخالفة، أو أنه لا توجد دلائل كافية ضد المتهم، أو كان مقترف الجريمة لا يزال مجهولاً، أصدر القاضي أمرا بألا وجه لمتابعة المتهم».

[3]- Ar 177al1 (c.p.p.f modifié par la loi n°2004-575 du 21 juin 2011- art. 2 JORF 22 juin 2004) dispose que: « Si le juge d'instruction estime que les faits ne constituent ni crime, ni délit, ni contravention, ou si l'auteur est resté inconnu, ou s'il n'existe pas de charges suffisantes contre la personne mise en examen, il déclare, par une ordonnance, qu'il n'y a lieu à suivre ».

[4]- علي عدنان الفيل، المرجع السابق، ص. 50.

هذا وعرفها جانب آخر[1] بأنها: «أمارات معينة تستند إلى العقل، وتبدأ من ظروف أو وقائع يستنتج منها الفعل، توحي للوهلة الأولى بأن جريمة ما وقعت وأن شخصاً ما هو مرتكبها، وهذه الامارات لا يكفي في تقديرها مجرد المنطق بل لا بد في شأنها تدخل الخبرة والتعقل".

وفيما يتعلق بالجرائم الواقعة على المستندات الإلكترونية والتي يصدر الإذن بالتفتيش فيها لضبط أدلة تفيد في وقوعها، فإنه يقصد بالدلائل الكافية بالنسبة لها مجموعة المظاهر والأمارات التي تكفي وفقاً للسياق العقلي والمنطقي أن ترجح ارتكابها ونسبتها إلى شخص معين سواء بوصفه فاعلا لها أم شريكاً.

ولا يقتصر الأمر على الشرطين السابقين لصحة التفتيش، بل ينبغي أن تتوافر أمارات قوية أو قرائن على وجود أشياء أو أجهزة أو معدات معلوماتية تفيد في كشف الحقيقة، وعليه لا يتم التفتيش إلا إذا توافرت لدى المحقق أسباب كافية على أنه يوجد في المكان أو لدى الشخص المراد تفتيشه أدوات استعملت في الجريمة المعلوماتية أو أشياء متحصلة منها، أو أية مستندات إلكترونية يحتمل أن يكون لها فائدة في استجلاء الحقيقة لدى المتهم المعلوماتي أو غيره، وبالتالي فإن مجرد وقوع جريمة سواء أكانت جناية أو جنحة واتهام شخص معين بارتكابها أو المشاركة فيها لا يكفي لحث سلطة التحقيق على إصدار إذنها بالتفتيش ومباشرتها، بل ينبغي لإصدار هذا الإذن أن تكون الدلائل التي تجمعت حول الجريمة تدعو للاعتقاد المعقول بوقوعها سواء أكان من تجمعت حوله هذه الدلائل فاعلاً أصلياً، أم يقف دوره الإجرامي عند حدود المساهم في الجريمة أو الشريك فيها[2].

هذا عن سبب التفتيش في البيئة الإلكترونية، أما عن محلها فيمكن القول أنه إذا كان محل التفتيش في الجرائم التقليدية هو شخص المتهم أو مسكنه، فإن المحل الذي يقع عليه التفتيش من أجل الحصول على الأدلة في نطاق الجرائم الواقعة على المستندات الإلكترونية هو جهاز الحاسوب بكافة مكوناته المادية والمنطقية، وشبكات الاتصالات المرتبطة بها بما

[1]- سامح أحمد بلتاجي موسى، المرجع السابق، ص.258.

[2]- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص. 213؛ حسين بن سعيد بن سيف الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، المرجع السابق، ص. 381.

تشمله تلك الشبكات من خوادم ومزودات وملحقات تقنية والتي قد تتواجد بحوزة الشخص، أو تكون تحت تصرفه في مكان له حرمة يحميها القانون[1].

وبالرجوع لما تم التطرق إليه حول مدى جواز تفتيش نظم الحاسب الآلي فيما يتعلق بمكوناته المادية والمعنوية، وكذا ما يخص إمكانية تفتيش شبكات الحاسوب[2]، فإنه ينبغي التعرض للشخص كمحل للتفتيش في الجرائم الواقعة على المستندات الإلكترونية، وكذا للمسكن وما في حكمه كمحل للتفتيش في نظم وشبكات الحاسوب.

فبالنسبة للشخص بوصفه محلا للتفتيش في الجرائم الواقعة على المستندات الإلكترونية، فإنه ينبغي الذكر أن هذا الأخير قد يكون من مستغلي أو مستخدمي شبكة الإنترنت أو من الخبراء في مجال البرمجيات سواء كانت برامج نظام أو برامج تطبيقات، وقد يكون من المحللين أو من مهندسي الصيانة والاتصالات، أو من مديري النظم المعلوماتية أو من مزودي خدمات الإنترنت، أو من المسؤولين عنها أو من أشخاص آخرين يكون بحوزتهم أجهزة أو معدات معلوماتية، أو أجهزة أو حواسيب محمولة، أو هواتف متصلة بجهاز المودم أو مخرجات أو مستندات، أو غير ذلك مما يتعلق بالجرائم محل البحث، وفي جميع الأحوال يقصد بالشخص كمحل قابل للتفتيش كل ما يتعلق بكيانه المادي، وما يتصل به[3]، ويشمل ذلك جسم الإنسان، وملابسه وأمتعته التي في حوزته باعتبارها من توابع الشخص[4].

أما بالنسبة للمساكن وما في حكمها كمحل للتفتيش في نظم وشبكات الحاسوب والإنترنت، فيقصد بها محال الإقامة أو المأوى أو محل السكنى للإنسان، والذي يحفظ فيه أسراره، ويحرص على أن لا يقتحمه عليه أحد، متى ما وجد فيه مكونات الكمبيوتر سواء أكانت مكونات مادية أو منطقية أو شبكات اتصال خاصة[5]، كما يدخل في هذا المفهوم كذلك

[1]- سامح أحمد بلتاجي موسى، المرجع السابق، ص. 258؛ محمد فتحي، المرجع السابق، ص.365.
[2]- يراجع في ذلك، ص، ص. 325-338 من هذه الأطروحة.
[3]- عادل عبد الله خميس المعمري، المرجع السابق، ص.264.
[4]- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص، ص. 214- 215؛ هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص. 126.
[5]- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص. 215.

الملحقات المخصصة لمنافع هذا السكن كغرف الغسيل، وحظائر الدواجن والمخازن والإسطبلات وحديقة المنزل وأفنيته المغلقة طالما كانت تابعة للمسكن ومتصلة به، ويضمها معه سور واحد[1].

هذا وتجدر الإشارة أن المشرع الجزائري قد وسع من نطاق التفتيش بموجب قانون الإجراءات الجزائية، بحيث جعله يشمل الأماكن التي يشغلها شخص ملزم قانوناً بكتمان السر المهني، بما فيها المحلات المهنية كمكاتب أصحاب المهن الحرة، كالأطباء والمحامين والموثقين والمحضرين، غير أنه أحاط تفتيش هذه الأماكن بضرورة اتخاذ كافة التدابير اللازمة لضمان احترام ذلك السر، وهذا الأمر الذي أورده في المادة 4/45 من القانون رقم 06-22 المعدل والمتمم لقانون الإجراءات الجزائية [2].

وفي هذا يُجمع الفقه[3] على أنه إذا وجدت مكونات ونظم شبكات الحاسوب سواءً أكانت مكونات مادية أو منطقية أو شبكات اتصال مرتبطة بها، في أي مكان من الأماكن المذكورة، فإن تفتيش هذه المكونات يخضع لذات قواعد تفتيش المساكن أو المحل المتواجدة به.

ولئن كانت هذه الأحكام تطبق على محل التفتيش، فإنه ينبغي الذكر أن السلطة المختصة بالتفتيش باعتباره إجراء من إجراءات التحقيق، تتمثل كأصل عام في سلطة التحقيق وهي النيابة العامة (في مصر) وقاضي التحقيق في الجزائر، وهذا ما نصت عليه المادة 79 من قانون الإجراءات الجزائية، والتي أجازت لقاضي التحقيق الإنتقال إلى أماكن وقوع الجرائم لإجراء عملية التفتيش، على أن يخطر بذلك وكيل الجمهورية الذي له الحق في مرافقته.

---

[1]- سامح أحمد بلتاجي موسى، المرجع السابق، ص. 260؛ هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، نفس المرجع، ص. 132.

[2]- تنص المادة 45 فقرة 4 من القانون رقم 06-22 المؤرخ في29ذي القعدة عام 1427 الموافق 20 ديسمبر سنة 2006، يعدل ويتمم الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، ج.ر، ع. 84، س.2006: «... غير أنه يجب عند تفتيش أماكن يشغلها شخص ملزم قانوناً بكتمان السر المهني أن تتخذ مقدما جميع التدابير اللازمة لضمان احترام ذلك السر».

[3]- سامح أحمد بلتاجي موسى، المرجع السابق، ص. 260؛ هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص. 132.

كما أجاز له بموجب نص المادة 81 من ذات القانون أن يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء يكون كشفها مفيدا لإظهار الحقيقة، وإذا كان هذا هو الأصل العام، فإن الاستثناء يقضي بأن سلطة التحقيق الأصلية والمتمثلة في قاضي التحقيق أو النيابة العامة غير مطالبة بإجراء التفتيش بنفسها في كل الحالات، بل لها أن تلجأ إلى الإنابة في بعض الحالات، فتقوم بندب أحد ضباط الشرطة القضائية لإجرائه (بمعنى إن إجراء التفتيش أمر جوازي بالنسبة لقاضي التحقيق)، ويعتبر إجراء الندب تفويض يصدر من سلطة التحقيق المختصة إلى أحد ضباط الشرطة القضائية مخولاً إياه إجراء التفتيش الذي تختص به أصلاً تلك السلطة، وعليه ينبغي أن يُراعى في إصداره وتحريره جميع القيود الخاصة بالإنابة القضائية[1].

ونظراً لخطورة خصوصية إجراء التفتيش باعتباره إجراء قد يمس بحرمة المسكن وبمستودع أسرار الفرد، فإن التشريعات المقارنة بما فيها المشرع الجزائري قد نصت على بعض الضمانات وعلى بعض الإجراءات الواجب احترامها حتى تكون عملية التفتيش صحيحة، وأهم هذه الضمانات أن يتم تفتيش نظم الحاسب الآلي بناءً على إذن قضائي بإجرائه، ومن ثم إذا قام قاضي التحقيق بندب أحد ضباط الشرطة القضائية للقيام بعملية التفتيش فإنه ينبغي أن تكون هذه الإنابة متضمنة الإذن بالتفتيش، ساعة وتاريخ صدورها، إسم من أصدرها، اسم المأذون له بالتفتيش واسم المأذون بتفتيش مسكنه، وعنوان المسكن والمهمة المقصودة من وراء التفتيش، وكذا المهلة المحددة لإجرائه، والغرض من هذا التحديد تجنب ما يسمى بالتفتيش الاستكشافي، بحيث لا تكون للضابط المنتدب أية سلطة تقديرية في ذلك[2].

[1]- هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص. 138؛ سامح أحمد بلتاجي موسى، المرجع السابق، ص .268.
[2]- حطاب كمال، المرجع السابق، ص. 311.

هذا وقد أوجب المشرع الجزائري في المادة 3/44 من قانون الإجراءات الجزائية أن يتضمن الإذن المذكور بيان وصف الجرم موضوع البحث عن الدليل، وعنوان الأماكن التي يتم زيارتها وتفتيشها، وإجراء الحجز فيها وذلك تحت طائلة البطلان[1].

وينبغي أن تنجز عملية التفتيش والحجز تحت الإشراف المباشر للقاضي الذي أذن بها، بحيث يكون ضابط الشرطة القضائية مقيداً بالقيود التي تقيد قاضي التحقيق[2].

لاشك أن الجريمة الإلكترونية كغيرها من الجرائم يمكن أن تتوافر فيها شروط الجريمة المتلبس بها، وعليه إذا تحققت شروط التلبس فإنه ينبغي لصحة التفتيش أن تتوفر شروط محددة أوردها المشرع الجزائري في المادة 44 من قانون الإجراءات الجزائية، وتتمثل هذه الأخيرة في:

- أن تتوافر العلامات الدالة على حالة التلبس.
- أن يكون المسكن، أو مكان إجراء التفتيش تابعاً لشخص ساهم في الجريمة أو يحوز أوراقا أو أشياء لها علاقة بها، فإذا انتفت رابطة السببية فلا يجوز تفتيش محله.
- الحصول على إذن مكتوب من وكيل الجمهورية، أو قاضي التحقيق.
- إستظهار الإذن قبل الدخول إلى المسكن أو المكان وما إلى غير ذلك من البيانات السابق إيضاحها.

غير أن أبرز ما يتم التأكيد عليه في هذا الصدد هو أن يكون إذن التفتيش محدداً خصوصا في محله، والأشياء المراد البحث عنها وضبطها، ذلك أن بعض التشريعات المقارنة كالتشريع الأمريكي يتطلب التحديد كشرط لازم لصحة الإذن بالتفتيش، ولكن يرى جانب من الفقه[3] أن هناك صعوبة في احترام هذا التحديد عملياً، وذلك نظرا للطبيعة الخاصة لأجهزة الحاسب الآلي التي تحوي على عدد كبير من الملفات، ناهيك عن أن أسماء هذه

[1]- تنص المادة 3/44 من القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري، سابق الإشارة إليه: «يجب أن يتضمن الإذن المذكور أعلاه بيان وصف الجرم موضوع البحث عن الدليل، وعنوان الأماكن التي ستتم زيارتها وتفتيشها وإجراء الحجز فيها، وذلك تحت طائلة البطلان».

[2]- بوعناد فاطمة زهرة، المرجع السابق، ص. 124.

[3]- حطاب كمال، المرجع السابق، ص. 311.

الملفات قد لا تدل بالضرورة على مسمياتها، إذ من الوارد أن يعمد المتهم إلى وضع أسماء مستعارة لملفات تحوي مواد غير مشروعة.

وبخصوص تحديد الملفات محل التفتيش في الإذن فقد أثار الفقه إشكالية مدى إمكانية إعتبار كل ملف من ملفات الحاسب الآلي المراد تفتيشه صندوقاً مغلقاً يحتاج كل واحد منها إلى إذن قضائي خاص؟ أم أن إذناً واحدا يكفي لتفتيشها كلها؟.

لقد دفعت هذه التساؤلات الفقه إلى البحث في أحكام القضاء الأمريكي الذي تضاربت أحكامه القضائية بشأن هذه المسألة، حيث إعتبرت بعض الأحكام أن القرص الصلب بما فيه من ملفات وجهاز الحاسب الآلي بما يحويه من مستندات صندوقاً واحدا مغلقاً ، وعليه فإنه يجوز تفتيش الجهاز كله بما فيه من ملفات، بناء على إذن تفتيش واحد، وعلى خلاف ذلك إعتبرت أحكام أخرى أن كل ملف في جهاز الحاسب الآلي يتطلب إذناً خاصاً لتفتيشه، ذلك أن كل ملف يعتبر صندوقاً مغلقاً، وقد بررت هذه الهيئات أحكامها بإعتبار أن جهاز الحاسب الآلي يحوي الكثير من المعلومات المتعلقة بالحياة الخاصة لصاحبه، وينبغي صيانة هذه المعلومات من الاعتداء عليها[1].

الحقيقة أن إعتبار كل ملف من ملفات الحاسب الآلي صندوقاً مغلقاً يستوجب تفتيشه إذناً خاصاً أمر في غاية الصعوبة من الناحية العملية، خاصة مع التطور السريع لتقنيات الحاسب الآلي، وكذا السعة التي يمكن أن يحويها القرص الصلب، إذ بإمكان هذا الاخير أن يحوي عددا كبيرا من الملفات، وكل ملف يحوي ملفات عديدة بداخله، وإذا أُرِيدَ إحصاء عدد الملفات التي يمكن أن يحويها قرص صلب واحد سعته "واحد تيرا" فقط لوُجِدَت تفوق المائة ألف، وذلك إذا تم إفترض أن متوسط سعة الملف تقدر ب 10 ميجا، في حين أن سعة الملف الواحد لا تتعدى الواحد ميجا ويمكن أن تكون أقل بكثير، وبهذا قد يصل عدد الملفات إلى

---

[1]- كمثال نموذجي عن التحديد الفني لأوامر التفتيش الصادرة في جرائم الحاسبات يشير أكثر الفقه الأمريكي إلى أمر التفتيش الذي استخدم في قضية وورد ضد المحكمة العليا (Word v. Superior Court)، والذي حدد المطلوب تفتيشه بأنه بنك ذاكرة الحاسب والأدوات الأخرى لتخزين البيانات والمزودة مغناطيسيا حسب تصميم نظم المعلومات ببرامج حاسب الطباعة عن بعد.

"Computer memory bank or other storage devices, magnetically imprinted with information systems design (ISD) remote plotting computer programs".

مشار إليه من طرف، أحمد عاصم عجيلة، المرجع السابق، ص، ص. 417- 418؛ شيماء عبد الغني محمد عطا الله، المرجع السابق، ص. 290.

مئات الآلاف بل الملايين، ولهذه الأسباب يتساءل أنصار هذا الاتجاه عن مدى إمكانية إستصدار مائة ألف إذن أو أكثر لتفتيش جهاز حاسب آلي واحد؟

الواقع أنه لا يستساغ أن يمتد إذن التفتيش ليطال كل ملفات الحاسب، ذلك أن هذا الأمر فيه مساس بحياة الشخص الفردية، وعليه يجب أن يقيد التفتيش بالغرض الذي صدر الإذن لأجله، وهو الحصول على أدلة تفيد القضية محل التفتيش[1].

ومن أهم النتائج المترتبة على الإذن بتفتيش نظم الحاسب الآلي أن يصبح لضابط الشرطة القضائية الصادر له الإذن بالتفتيش نفس السلطات التي تملكها جهة التحقيق الأصلية، كما أنه يلتزم بنفس الالتزامات ويخضع لنفس القيود.

بناء على ذلك، يمكن لضابط الشرطة القضائية وهو يحقق في جرائم الاعتداء على المستندات الإلكترونية أن يخترق نظم المعالجة الآلية للمعطيات، ويبحث عن كل ما يفيد في كشف الحقيقة، فله أن يشاهد مثلا البيانات المخزنة في الحاسب سواء كانت في الذاكرة الرئيسية أو في وحدات التخزين الثانوية، وذلك بإحضارها على شاشة العرض أو استنساخ صورة منها مفهومة ومقروءة، أو ضبطها مع الدعامة المادية التي تحتويها مهما كان شكل هذه الدعامة، أي سواء كانت هذه الأخيرة من قبيل الشرائط المغناطيسية أو الأقراص، كما ويستوي أن تكون تلك الأقراص مرنة أو صلبة.

هذا ويكون بإمكان ضابط الشرطة القضائية ضبط أي برامج وكيانات منطقية، أو كتب تشغيل وإرشادات خاصة بالجهاز، أو أجهزة طباعة المخرجات، أو الأجهزة الطرفية أو المودم، وكل ما يكون له اتصال بالجريمة المعلوماتية، بل وحتى ضبط الحاسب الآلي بكل مكوناته وشبكاته باعتباره دليلاً، هذا ويمكن له كذلك استخدام كل إمكانات الحاسب بما في ذلك كلمة السر، ومفاتيح الدخول، ومفاتيح فك الشفرة[2].

[1]- حطاب كمال، المرجع السابق، ص. 312.
[2]- هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص.152.

ثانياً: الضوابط الشكلية للتفتيش.

بالإضافة إلى الضمانات الموضوعية لتفتيش نظم الحاسب الآلي[1]، توجد ضمانات أخرى ذات طابع شكلي يجب مراعاتها عند ممارسة هذا الإجراء، وذلك صوناً للحريات الفردية من التعسف أو الانحراف في استخدام السلطة.

والضوابط أو الشروط الشكلية لتفتيش نظم الحاسب الآلي منها ما يعتبر عنصراً من عناصر العمل الإجرائي كالحضور الضروري لبعض الأشخاص أثناء إجراء التفتيش، وتحرير محضر التفتيش وأسلوب تنفيذه، ومنها ما يعتبر ظرفاً له كالمقيات الزمني لإجراء التفتيش[2]، وهو الأمر الذي سيتم بيانه.

1- الحضور الضروري لبعض الأشخاص أثناء إجراء تفتيش نظم الحاسب الآلي:

من أهم الضمانات الشكلية التي يتطلبها القانون في الجرائم التقليدية حضور شخص أو أشخاص أثناء التفتيش، والهدف من ذلك ضمان الاطمئنان إلى سلامة الإجراء وصحة الضبط[3]، والمتأمل للتشريعات الإجرائية المختلفة يجد أن غالبيتها لا تُسوي بين تفتيش الشخص وتفتيش المنازل، وما في حكمها فيما يتعلق باستلزام هذا الإجراء، ومن هذه التشريعات التشريع الإجرائي المصري، الذي وإن كان قد عني بمسألة حضور المتهم أو من ينيبه أثناء تفتيش المنزل، فإنه لم يشترط لصحة تفتيش الأشخاص حضور شهود[4]، وهذا ما أورده في نص المادة 51 من قانون الإجراءات الجزائية المصري[5].

هذا ويلاحظ أن المشرع الجزائري والفرنسي قد نصا على ضرورة حضور شاهدين سواء تم التفتيش بمعرفة قاضي التحقيق أم ضابط الشرطة القضائية، إذ وحسب نص المادة

---

[1]- يراجع في ذلك، ص. ص. 339- 349 من هذه الأطروحة.

[2]- سامح أحمد بلتاجي موسى، المرجع السابق، ص. 262؛ هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص. 163.

[3]- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص. 220.

[4]- هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص. 164.

[5]- تنص المادة 51 قانون رقم 150 لسنة 1950 المتضمن ق.إ.ج.م معدل ومتمم :" يحصل التفتيش بحضور المتهم أو من ينيبه عنه كلما أمكن ذلك، وإلا فيجب أ يكون بحضور شاهدين، ويكون هذان الشاهدان بقدر الإمكان من أقاربه البالغين أو من القاطنين معه بالمنزل أو من الجيران، ويثبت ذلك في المحضر."

45 من قانون الإجراءات الجزائية الجزائري، والتي تقابلها المادة 56 من قانون الإجراءات الجزائية الفرنسي، فلا بد من حصول التفتيش بحضور المتهم، فإذا لم يستطع الحضور وقت إجراء التفتيش كان عليه تعيين ممثل له، فإن امتنع أو كان هارباً، أجرى ضابط الشرطة القضائية التفتيش بحضور شاهدين من غير الموظفين الخاضعين لسلطته[1].

هذا ويلاحظ أن المشرع الجزائري استثنى بموجب المادة 7/45 من قانون الإجراءات الجزائية حضور الأشخاص المذكورين آنفا إذا تعلق الأمر ببعض الجرائم[2]، منها جريمة المساس بأنظمة المعالجة الآلية للمعطيات، ومن ثم فإنه يجوز التفتيش في هذه الجرائم دون الحاجة لحضور الأشخاص المذكورين أعلاه، ولعل ذلك مرده الطبيعة الخاصة لهذه الجرائم التي تحتاج من أجل الكشف عن الأدلة المتعلقة بها السرعة في التنفيذ والسرية، حتى لا يقوم المجرمون بمحو أو طمس أدلة الإدانة.

وللإشارة فإن هذه الضمانة قد بدأت تتضاءل أهميتها في الدول التي تأخذ بإجراء التفتيش عن بعد ومنها الجزائر، بحيث أجاز القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها في مادته الخامسة الدخول بغرض التفتيش ولو عن بعد في منظومة معلوماتية أو جزء منها، وكذا في المعطيات المعلوماتية المخزنة فيها، إضافة إلى إمكانية الدخول لتفتيش منظومة التخزين المعلوماتية[3].

2- الميقات الزمني لإجراء تفتيش نظم الحاسب الآلي:

تحرص بعض التشريعات الإجرائية على حظر القيام بتفتيش المنازل وما في حكمها في وقت معين، وذلك حرصا على تضييق نطاق الاعتداء على الحرية الفردية وحرمة

---

[1]- تنص المادة 45 /1 من القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري ، سابق الإشارة إليه:" تتم عمليات التفتيش التي تجرى طبقا للمادة 44 أعلاه على الوجه الآتي:
1- إذا وقع التفتيش في مسكن شخص يشتبه في أنه ساهم في ارتكاب الجناية فإنه يجب أن يحصل التفتيش بحضوره، فإذا تعذر عليه الحضور وقت التفتيش فإن ضابط الشرطة القضائية ملزم بأن يكلفه بتعيين ممثل له، وإذا امتنع عن ذلك أو كان هاربا استدعى ضابط الشرطة الفضائية لحضور تلك العملية شاهدين من غير الموظفين الخاضعين لسلطته.".

[2]- نصت المادة 45 / 7 من قانون الإجراءات الجزائية الجزائري على الجرائم التي استثنى فيها المشرع الجزائري ضمانة حضور الأشخاص المذكورين في إجراء التفتيش وتشمل كل من جرائم المخدرات،الجريمة المنظمة عبر الحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات- جرائم تبييض الأموال والإرهاب- الجرائم المتعلقة بالتشريع الخاص بالصرف.

[3]- المادة 05 من قانون 09-04 المؤرخ في 5 غشت سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، سابق الإشارة إليه.

المساكن، ومن هذه التشريعات المشرع الجزائري وكذا المشرع الفرنسي، حيث حظر المشرع الجزائري بموجب المادة 47 من قانون الإجراءات الجزائية تفتيش المساكن قبل الساعة الخامسة صباحا وبعد الساعة الثامنة مساءاً (بمعنى أن التفتيش مسموح به من الساعة الخامسة صباحاً إلى غاية الثامنة مساءاً كقاعدة عامة) إلا إذا طلب صاحب المنزل ذلك، أو وجهت نداءات من الداخل أو في الأحوال الاستثنائية المقررة قانونا[1].

غير أن المشرع الجزائري قد استثنى من هذا الحظر حالات استثنائية حيث أجاز إجراء عملية التفتيش ليلاً ونهاراً، إذا تعلق الأمر ببعض الجرائم ومنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وهذا ما نص عليه في المادة 3/47 من قانون الإجراءات الجزائية[2]، ولعل الأمر راجع إلى خصوصية هذه الجرائم التي لا تحتمل تأخير التفتيش بصددها.

هذا عن التشريع الجزائري، أما بخصوص التشريع الفرنسي فقد حظر هو الآخر القيام بعملية التفتيش قبل الساعة السادسة صباحا وبعد الساعة التاسعة ليلاً فيما عدا حالات الاستغاثة الصادرة من داخل المنزل أو الاستثناءات المقررة بواسطة القانون، وهذا ما أورده في نص المادة 59 من قانون الإجراءات الجزائية الفرنسي[3].

وفي مقابل هذه التشريعات التي حدت ميعادا للتفتيش كأصل عام، توجد تشريعات أخرى لم تحدد وقتاً معيناً يتم فيه هذا الإجراء، بحيث تركت للقائم بالتفتيش تحديد الوقت المناسب للقيام به دون النظر إلى أي اعتبار آخر متعلق بالمحل المراد تفتيشه، ومن بين هذه

---

[1]- تنص المادة 01/47 من القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري، سابق الإشارة إليه: " لا يجوز البدء في تفتيش المساكن ومعاينتها قبل الساعة الخامسة (5) صباحا، ولا بعد الساعة الثامنة (8) مساء إلا إذا طلب صاحب المنزل ذلك أو وجهت نداءات من الداخل أو في الأحوال الإستثنائية المقررة قانونا."

[2]- تنص المادة 3/47 من القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري، سابق الإشارة إليه: «عندما يتعلق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وجرائم تبييض الأموال وتمويل الإرهاب وكذا الجرائم المتعلقة بالتشريع الخاص بالصرف، فإنه يجوز إجراء تفتيش أو المعاينة أو الحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات الليل أو النهار، وذلك بناءاً على إذن مسبق من وكيل الجمهورية المختص».

[3]- Article 59 (C.P.P.F modifié par la loi n°93-1013 du 24-08-1993 Art. 20 JORF 25 aout 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.
Les formalités mentionnées aux articles 56, 56-1, 57 et au présent article sont prescrites à peine de nullité ».

التشريعات على سبيل المثال التشريع المصري الذي لم يحدد في قانون الإجراءات الجنائية وقتاً معيناً للتفتيش، فحسبه فإنه يمكن إجراء عملية التفتيش في كل الأوقات وعلى مدار 24 ساعة في اليوم، هذا وقد تواترت أحكام محكمة النقض المصرية على هذا المعنى[1].

من خلال استقراء موقف التشريعات المقارنة، يلاحظ أن المشرع الجزائري كان أقرب للمنطق حين لم يقيد إجراء التفتيش في الجرائم المعلوماتية بميقات زمني، وذلك رغبة منه في عدم ضياع الأدلة المعلوماتية وعدم إفلات المجرم المعلوماتي من العقاب.

3- أسلوب تنفيذ التفتيش في نظم الحاسب الآلي:

الأصل أن ضابط الشرطة القضائية - كما يقول الفقيه الفرنسي لامبير (Lambert)- هو السيد في الفن الخاص به، فهو المتخصص في جمع الأدلة، وهو الذي يقدر اللحظة المناسبة لأداء العمل الحاسم المنوط به، وكيفية هذا الأداء وعوامل نجاحه أو فشله[2].

والأصل أن تنفيذ التفتيش ينبغي أن يتم بطريقة معقولة، وباللجوء إلى الوسائل التي تتفق مع المرونة الواجبة في تنفيذ القانون وتحقيق روح العدالة، لا سيما وأن الجرائم الواقعة على المستندات الإلكترونية لها طبيعة خاصة، فالتفتيش عن الملفات الموجودة في الحاسب الآلي يعد من الأمور المعقدة، لكونها تحوي في طياتها عمليات إلكترونية غاية في التعقيد حيث يمكن تخزينها في قرص مرن، أو في عناوين مخبأة في الحاسوب المتنقل الخاص بالمشتبه فيه أو على خادم بعيد جداً على بعد آلاف الأميال، كما يمكن تشفير الملفات مع وضع عناوين مضللة لها وتخزينها في شكل ملفات غير تقليدية، هذا ويمكن أن يتم خلطها مع ملايين الملفات التي ليس لها علاقة بالموضوع، أو ملفات غير سيئة أو ضارة وتكون

[1]- قضت محكمة النقض المصرية في هذا الشأن بأنه: «من المقرر قانونا أن لمأموري الضبط القضائي إذا ما صدر إليهم إذن من النيابة بإجراء التفتيش أن يتخذوا ما يرونه كفيلاً بتحقيق الغرض من دون أن يلتزموا في ذلك طريقة بعينها ما داموا لا يخرجون في إجراءاتهم على القانون، ويكون لهم تخير الظرف المناسب لإجرائه بطريقة مثمرة، وفي الوقت الذي يرونه ملائماً ما دام ذلك يتم خلال الفترة المحددة بالإذن. لما كان ذلك وكان التفتيش الذي قام به الضابط في هذه الدعوى مأذوناً به قانوناً، فإن له أن يجريه بالطريقة التي يراها محققة للغرض منه ما دام أنه قد التزم الحدود التي تضمنها إذن النيابة، ومن ثم فلا تثريب عليه إن هو إقتحم غرفة نوم المطعون ضده فجر يوم الحادث بعد أن تمكن أحد معاونيه من فتح باب المسكن الخارجي بواسطة التسور ما دام الضابط رأى ذلك، ويكون ما انتهى إليه الحكم المطعون فيه من بطلان إجراءات القبض والتفتيش لا يقوم على سند من القانون مما يعيبه بما يستوجب نقضه». مشار اليه من طرف، سامح أحمد بلتاجي موسى، المرجع السابق، ص 264؛ هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص، ص. 175- 176.

[2]- سامح أحمد بلتاجي موسى، المرجع السابق، ص. 262.

محمية، وهو الأمر الذي يُصَعِب على ضابط الشرطة القضائية الوصول إليها، لهذه الأسباب يعتبر تفتيش نظم الحاسب الآلي فناً أكثر مما هو علم.

هذا ويمكن لضباط الشرطة القضائية ورجال النيابة العامة توسيع احتمالية نجاح تفتيش الحاسبات الآلية بإتباع الخطوات الآتية:

أ- تجميع فريق عمل يتكون من ضباط الشرطة القضائية والنيابة العامة، وخبير فني قبل القيام بالتفتيش .

ب- التعرف قدر المستطاع على نظم الكمبيوتر المراد تفتيشها قبل وضع خطة التفتيش أو طلب الإذن.

ج- وضع خطة لتنفيذ التفتيش، وخطة بديلة تكون مبنية على المعلومات التي عرفت عن النظام المراد تفتيشه.

د- إعطاء مسودة إذن التفتيش عناية خاصة من حيث اشتمالها على وصف لمحل التفتيش، والملكية أو الأشياء المراد ضبطها بدقة وواقعية، مع شرح إستراتيجية التفتيش الممكنة[1].

كما أن تفتيش نظم الحاسب الآلي يمكن أن يتم بطرق عدة وقد أورد المرشد الفيدرالي الأمريكي أربع طرق أساسية وهي:

أ- تفتيش الحاسب الآلي وطبع نسخة ورقية من ملفات معينة في ذات الوقت.

ب- تفتيش الحاسب الآلي وعمل نسخة إلكترونية من ملفات معينة في ذات الوقت.

ج- عمل نسخة إلكترونية طبق الأصل من جهاز التخزين بالكامل في الموقع، وبعد ذلك يتم إعادة عمل النسخة لتعمل من جهاز التخزين خارج الموقع للمراجعة.

د- ضبط الجهاز وإزالة الملفات ومراجعة محتوياته خارج الموقع.

[1]- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص، ص. 225- 226.

هذا ويجب الأخذ بعين الاعتبار عند القيام بتفتيش نظم الحاسب الآلي دور القطع الصلبة الخاصة بالكمبيوتر في ارتكاب الجريمة، ذلك أن نجاح التفتيش غالباً ما يعتمد على دور تلك القطع[1].

4- تحرير محضر بتفتيش نظم الحاسب الآلي:

بما أن التفتيش يعد عملاً من أعمال التحقيق، فإنه ينبغي على الشخص القائم به أن يحرر محضرا به يثبت فيه كل ما تم من إجراءات، وما أسفر عنه التفتيش من أدلة، ورغم أهمية هذه المسألة لم يتطلب القانون شكلاً خاصاً لهذا المحضر، بحيث لا يُشترط لصحته سوى ما تستوجبه القواعد العامة في المحاضر عموما كأن يكون مكتوباً باللغة الرسمية، وأن يحمل تاريخ تحريره وتوقيع محرره وأن يحوي في طياته كافة الإجراءات التي أتخذت بشأن الوقائع التي بينها[2].

وبالنسبة لمحضر تفتيش نظم الحاسب الآلي فإنه ينبغي الذكر أن إيراد المعلومات الضرورية يستلزم من المحقق سواء ضابط الشرطة القضائية، أو قاضي التحقيق أن يكون محيطاً بتقنية المعلومات، وأن يكون على دراية بهذه التكنولوجيات الحديثة، كما و أن عليه الإستعانة بأحد المتخصصين في مجال الحاسوب والإنترنت، وذلك حتى يساعده في المسائل الفنية الضرورية، فوجود الخبير سوف يساعد في صيانة مسودة التحقيق بحيث يتم تغطية كل الجوانب الفنية في عملية التفتيش والضبط، بالإضافة إلى المحافظة على الأدلة المتحصل عليها من كل تلف أو مسح[3].

الفرع الثالث: ضبط البيانات الإلكترونية.

إن الغاية من التفتيش هو ضبط كل شيء يتعلق بالجريمة ويفيد في التحقيق الجاري بشأنها، ومن ثم فإن ضبط الأشياء هو النتيجة الطبيعية للتفتيش، سواءً كان هذا الشيء الذي

[1]- حسين بن سعيد بن سيف الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، المرجع السابق، ص، ص. 387-388.
[2]- المرجع نفسه، ص. 385.
[3]- علي حسن محمد الطوالبة، المرجع السابق، ص. 60.

تم ضبطه أدوات استعملت في ارتكاب الجريمة أو شيئا نتج عنها، أو غير ذلك مما يفيد في كشف الحقيقة.

ويقصد بإجراء الضبط وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبها، وهو من حيث طبيعته القانونية قد يكون من إجراءات الإستدلال أو التحقيق[1]، كما أن إجراء الضبط بطبيعته وبحسب تنظيمه القانوني وغايته لا يَرِدُ إلا على الأشياء، سواء كانت هذه الأشياء منقولات أم عقارات وسواءا كانت مملوكة للمتهم أو لغيره، وعليه لا يصلح الأشخاص ليكونوا محلاً للضبط بمعناه الدقيق[2].

وإذا كان ضبط ماديات الجريمة في الجرائم التقليدية لا يثير صعوبات، إلا أن الضبط في مجال الجرائم المعلوماتية عامة، والجرائم الواقعة على المستندات الإلكترونية خاصة قد يثير بعض الصعوبات المتعلقة بمفهوم المحل الذي يرد عليه الضبط، وأنواع الأدلة الإلكترونية التي يتم ضبطها، وكذا مدى إمكانية ضبط المستندات الإلكترونية داخل جهاز الحاسب الآلي، وكيفية وطريقة القيام بهذا الضبط، ذلك أن الأشياء المضبوطة قد تكون بيانات إلكترونية أو مستندات معلوماتية[3].

إن أهمية إجراء الضبط في مجال الجرائم الماسة بالمستندات الإلكترونية يقتضي التطرق إلى المحل الذي يرد عليه **(البند الأول)**، وإلى طرق وأساليب ضبط البيانات الإلكترونية والمستندات **(البند الثاني)**، وكذا الصعوبات التي يمكن أن تقف أمام القائم بهذا الإجراء **(البند الثالث)**.

---

[1]- تتحدد طبيعة الضبط بحسب الطريقة التي يتم بها وضع اليد على الشيء المضبوط، فإذا كان الشيء وقت ضبطه في حيازة شخص واقتضى الأمر تجريده من حيازته كان الضبط بمثابة إجراء تحقيق، أما إذا كان الاستيلاء عليها دون الاعتداء على حيازة قائمة، فإنه يكون بمثابة إجراء استدلال. مأخودة من، علي عدنان الفيل، المرجع السابق، ص. 54؛ محمد فتحي، المرجع السابق، ص.377.

[2]- يتحدث قانون الإجراءات الجزائية في بعض الحالات عن ضبط الأشخاص وإحضارهم، فهذا يعني القبض على الأشخاص وإحضارهم، والقبض نظام قانوني يختلف تماماً عن ضبط الأشياء. مشار إليه من طرف، علي عدنان الفيل، المرجع السابق، ص. 54.

[3]- أحمد عاصم عجيلة، المرجع السابق، ص. 424.

البند الأول: المحل الذي يرد عليه الضبط في الجرائم الواقعة على المستندات الإلكترونية.

يختلف إجراء الضبط في الجريمة الإلكترونية عن الضبط في غيرها من الجرائم من حيث المحل، ومن ثم فإن السؤال المطروح يكمن في ما هي أنواع الأدلة الإلكترونية التي يمكن ضبطها في الجرائم الواقعة على المستندات الإلكترونية؟

الإجابة على هذا السؤال تقتضي البحث فيما يمكن للمحقق ضبطه في هذا النوع من الجرائم وما لا يمكن ضبطه، وبما أن الجريمة الإلكترونية قد يكون محلها شيئا مادياً أو بيانات معالجة إلكترونياً بما فيها المستندات الإلكترونية، فإنه سيتم البحث عن أنواع الأدلة المادية التي يتم ضبطها والتحفظ عليها في هذا النوع من الجرائم **(أولا)**، وعن الأدلة المعنوية كالبيانات الإلكترونية، وكذا المستندات المعالجة آليا ومدى إمكانية أن تكون محلاً للضبط **(ثانياً)**.

أولاً: الأدلة المادية.

هناك أنواع من الأدلة المادية التي يتم ضبطها والتحفظ عليها في الجرائم المتعلقة بالمستندات الإلكترونية، والتي لها قيمة في إثبات تلك الجرائم ونسبتها إلى المتهم، ومن هذه الأدلة:

1- **الأوراق:** رغم أن وجود أجهزة الحاسب الآلي قلل من حجم الأوراق والملفات التقليدية المستخدمة، إلا أن الكثيرين ما زالوا يقومون بطباعة المعلومات لأغراض المراجعة أو التأكد من الشكل العام للمستند أو الرسالة أو الرسومات موضوع الجريمة، وبالتالي تعتبر الأوراق من الأدلة التي ينبغي الإهتمام بها في البحث عن الحقيقة، حيث قد تؤدي إلى الوصول إلى أدلة أخرى وكيفية ارتكاب الجريمة، والورق أربعة أنواع:

- أوراق تحضيرية يتم إعدادها بخط اليد كمسودة أو تصوير للعملية التي يتم برمجتها.
- أوراق تالفة تتم طباعتها للتأكد وبعدها يتم إلقاؤها في سلة المهملات.
- أوراق أصلية تتم طباعتها والاحتفاظ بها كمرجع، أو لأغراض تنفيذ الجريمة.

- أوراق أساسية وقانونية محفوظة في الملفات العادية أو دفاتر الحسابات وتكون لها علاقة بالجريمة خاصة عند تلقيها أو تزوير بياناتها لتنفيذ الجريمة الإلكترونية[1].

2- **جهاز الحاسب الآلي وملحقاته:** إن وجود هذا الجهاز أمر مهم للقول بأن الجريمة الواقعة هي جريمة معلوماتية، ولأجهزة الحاسب الآلي أشكال وأحكام وألوان مختلفة، وخبير الحاسب الآلي وحده الذي يستطيع أن يتعرف على الحاسب المستخدم في الجريمة ومواصفاته بسرعة فائقة، كما يستطيع تمييزه عن الأجهزة الإلكترونية الأخرى، وتحديد أسلوب التعامل معه في حالة الضبط والتحريز.

أما ملحقات الحاسب فيقصد بها لوحة المفاتيح، الشاشة، الفأرة، السماعات، الطابعات، وأدلة الاستعمال المصاحبة للحاسب الآلي[2].

3- **وسائط التخزين المتحركة:** يندرج ضمن وسائل التخزين المتحركة الأقراص المدمجة "أقراص الليزر"، الأقراص المرنة، الأشرطة المغناطيسية، مفاتيح التخزين (USB) وغيرها، وتعد هذه الوسائط جزءاً من الجريمة المعلوماتية متى كانت محتوياتها عنصرا للجريمة.

إلى جانب ما سبق ذكره، يمكن ضبط بطاقات الائتمان والبطاقات الممغنطة، وكذا جهاز المودم (Modem)[3]، حيث أن كل هذه الأدلة يمكن أن يتم الاستعانة بها في كشف الحقيقة، ومن ثم فإنه لا يثور بالنسبة لهذه المكونات المادية أي إشكال، إذ تطبق عليها القواعد العامة المتعلقة بضبط الأشياء، وعليه يمكن أن تكون الأدلة المادية المذكورة محلاً يرد عليه إجراء الضبط في الجرائم الواقعة على المستندات الإلكترونية.

---

[1]- علي عدنان الفيل، المرجع السابق، ص. 55.

[2]- أحمد محمود مصطفى، جرائم الحاسبات الآلية في التشريع المصري، دراسة مقارنة، ط1، دار النهضة العربية، القاهرة، 2010، ص، ص. 161-162؛ ضياء يحي السادات، المرجع السابق، ص، ص. 26- 27.

[3]- المودم: هو جهاز لنقل الإشارات الرقمية على خطوات الاتصالات بين الحاسبات بتحويل الإشارات الرقمية إلى إشارات يمكن نقلها على قناة اتصالات، وهو الوسيلة التي تمكن أجهزة الكمبيوتر من الاتصال ببعضها البعض عبر خطوط الهاتف، والمودم أشكال وهياكل تتطور مع تطور تقنية صناعة الحاسبات الإلكترونية. مشار إليه من طرف، أحمد محمود مصطفى، المرجع السابق، ص. 163.

ثانياً: الأدلة المعنوية.

قد يكون محل الضبط في الجرائم الواقعة على المستندات الإلكترونية بيانات معالجة إلكترونياً أو مستندات إلكترونية أو ملفات رقمية، وعندئذ يثار التساؤل عن مدى إمكانية ضبط البيانات والمستندات الإلكترونية، وفي هذا الصدد برز جدل فقهي واسع، بحيث إنقسم الفقه[1]إلى رأيين:

رأي أول يُقِر بإمكانية إمتداد عملية الضبط لتشمل البيانات المعالجة إلكترونيا والمستندات الإلكترونية، وهي المكونات المعنوية للحاسب الآلي، ذلك أن الغاية من التفتيش هي ضبط الأدلة المادية التي تفيد في كشف الحقيقة، وهو مفهوم ينبغي أن يمتد بإمتداد الغاية له ليشمل البيانات والمستندات الإلكترونية وقواعد البيانات بمشتملاتها من ملفات وسجلات، سواء إتخذت شكل برامج نظام أو برامج تطبيقات بنوعيها الأساسيين، وعليه حسب هذا الرأي لا مانع من أن يرد الضبط على المستندات الإلكترونية[2].

بخلاف هذا الرأي ، يتجه الرأي الثاني إلى عدم إمكانية إمتداد الضبط إلى المكونات المعنوية للحاسب الآلي ومنها المستندات الإلكترونية، وعليه لا يتصور حسب هذا الإتجاه أن يرد الضبط على المكونات المعنوية لإنتفاء صفة الكيان المادي عنها، ويظل الأمر كذلك إلى غاية أن يتم نقلها على كيان مادي ملموس، عن طريق التصوير الفوتوغرافي، أو بنقلها على دعامة أو غيرها من الوسائل المادية[3]، ويستند هذا الرأي لتبرير موقفه على النصوص التشريعية المتعلقة بالضبط والتي يكون محل تطبيقها الأشياء المادية الملموسة[4].

في الواقع، إذا كان الفقه قد انتهى في مجال التفتيش إلى شمولية هذا الإجراء للمكونات المعنوية للحاسب الآلي، فإنه ومن المنطقي كذلك أن يترتب على ذلك إباحة ضبطها، وعليه

---

[1]- علي عدنان الفيل، المرجع السابق، ص. 57.

[2]- أحمد عاصم عجيلة، المرجع السابق، ص. 427.

[3]- علي عدنان الفيل، المرجع السابق، ص ص. 57- 58.

[4]- قصر قانون الإجراءات الجنائية الألماني في المادة94 منه محل الضبط على الأشياء المادية المحسوسة، وفي هذا يتجه الفقه الألماني إلى عدم صلاحية البيانات المعالجة إلكترونيا والمستندات الإلكترونية المجردة من دعامتها المادية لأن تكون محلاً للضبط نظرا لافتقادها للصفة أو الكيان المادي، غير أنه في حالة ما إذا تم تجسيدها في دعامة مادية، كما لو تم طباعة مخرجات الحاسب، فإن ضبط الدعامة المادية يكون ممكنا. مشار إليه من طرف، أحمد عاصم عجيلة، المرجع السابق، ص، ص. 428- 429.

يجوز ضبط المستندات الإلكترونية المخزنة داخل الحاسب، ذلك أن هذه المستندات عبارة عن نبضات أو ذبذبات إلكترونية قابلة لأن تسجل وتخزن على وسائط مادية، وعلى هذا الأساس تصلح المكونات المعنوية للحاسب الآلي لأن تكون دليلا عند ضبطها على أقراص مدمجة أو قرص صلب أو أي دعامة مادية، خاصة أنها تعد شيئا ذو وجود في العالم الخارجي المحسوس غير مجحود ويفيد في كشف الحقيقة.

للأسباب السالف ذكرها، فإنه ليس هناك ما يحول دون إمكانية ضبط هذه البيانات الإلكترونية وكذا المستندات، وقد سارت على هذا الإتجاه التشريعات المقارنة بما فيها المشرع الجزائري بحيث تضمنت نصوصاً تسمح بضبط البيانات الإلكترونية، وكذا المعلومات الموجودة في جهاز الكمبيوتر، وفي هذا الصدد يلاحظ أن إتفاقية بودابست لعام 2001 بشأن الإجرام المعلوماتي كرست المادة 19 للتعرض لضبط المكونات المعنوية، بحيث نصت : «من سلطة كل دولة طرف أن تتخذ الإجراءات التالية: أن تضبط نظام الكمبيوتر أو جزء منه أو المعلومات المخزنة على أي وسيط من وسائط التخزين الخاصة بالكمبيوتر، وأن تحافظ على سلامة تلك المعلومات المخزنة»[1].

هذا وقد سمح المشرع الجزائري بموجب القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بضبط البيانات الإلكترونية، وأفرد لذلك المواد 06-07-08 من القانون المذكور تحت عنوان حجز المعطيات المعلوماتية.

البند الثاني: طرق وتقنيات ضبط الأدلة الإلكترونية.

إن طريقة ضبط البيانات المعالجة آلياً تختلف عما هو متبع عند ضبط الأشياء المادية المحسوسة كجهاز الحاسب الآلي وملحقاته المتمثلة في الأقراص المرنة والطابعات والماسحات الضوئية وغيرها، ولئن كانت هذه الأخيرة لا تثير أي إشكال ذلك أن ضبطها ينطبق عليه جميع القواعد التقليدية المنصوص عليها في القانون، فإنه في المقابل يلاحظ أن ضبط وإحراز المكونات المعنوية للحاسب من بيانات إلكترونية ومستندات لا يخضع لهذه

[1]- هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها، المرجع السابق، ص، ص. 239- 240.

القواعد التقليدية، وذلك بحكم طبيعتها غير الملموسة، إذ ينبغي لضبطها وإحرازها اللجوء إلى طرق ووسائل تقنية وفنية تتفق مع الطبيعة الإلكترونية لها، ومن بين هذه التقنيات على سبيل المثال لا الحصر تقنية نسخ البيانات الإلكترونية **(أولا)** وتقنية تحميل البيانات **(ثانياً).**

أولاً: تقنية نسخ البيانات الإلكترونية (Copy).

يتم إستخدام هذه التقنية لضبط البيانات المعالجة آليا المخزنة داخل الحاسب، وذلك عن طريق إستخدام برامج مخصصة في النسخ مثل برنامج (Lap Link)، حيث يتم أخذ نسخة من تلك البيانات، ثم نقلها إلى أقراص صلبة متعددة وممغنطة، وللإشارة فإن مثل هذا الإجراء يصلح أن يتخذ في مواجهة الحاسبات التي تحوي على ملفات فيروسية، كما يُطبق أيضا إذا كان القرص الصلب يحتوي مثلا على ملفات مشفرة تحتاج إلى فك شفرتها، ولاشك في أن هذا كله يسمح بالحصول على أدلة يمكن أن يُعتد بها أمام القضاء[1].

هذا ولقد نص المشرع الفرنسي على هذه التقنية كطريقة لضبط البيانات الإلكترونية بحيث خصص المادة 76-1 فقرة 03 من القانون رقم 239 لسنة 2003، للتعرض لها، وقد ورد في هذه المادة أن: «البيانات التي يتم الحصول عليها من جراء تفتيش النظام المعلوماتي يتعين نسخها على دعامات يتم تحريزها».

للإشارة فإن المشرع الجزائري هو الآخر تبنى ذات النهج، بحيث نص في المادة 06 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتهما بأنه: «عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو عن مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث، وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في إحراز، وفقا للقواعد المقررة في قانون الإجراءات الجزائية».

[1]- عمر محمد أبو بكر بن يونس، المرجع السابق، ص. 71 وما بعدها.

هذا وقد تطرق المشرع الجزائري من خلال المادة 3/6 من ذات القانون إلى جواز إستعمال الوسائل التقنية الضرورية لتشكيل وإعادة تشكيل المعطيات محل الضبط بغية جعلها قابلة للاستغلال لأغراض التحقيق، طالما أن مثل هذا الأمر لا يؤدي إلى المساس بسلامة ومحتوى المعطيات، على أنه إذا استحال إجراء الضبط أو الحجز كما سماه المشرع الجزائري في هذا القانون لأسباب تقنية، تعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية أو نسخها[1].

هذا وقد أجاز المشرع الجزائري في المادة 08 من القانون السالف ذكره للسلطة التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة، وذلك من خلال تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك، وتبني المشرع لهذا النص الغرض منه ضمان سلامة المعطيات وصحة إجراء الضبط.

ثانياً: تقنية تجميد البيانات الإلكترونية (FROZEN).

وفقا لهذه التقنية يتم تجميد التعامل بالكمبيوتر أو النظام المعلوماتي الذي تتواجد بداخله المضبوطات الإلكترونية، وذلك بالإستعانة ببرامج معدة خصيصاً لهذا الغرض، ويتم بعد ذلك ضغط الملفات أو المضبوطات الإلكترونية من خلال برامج الضغط، حيث تقوم هذه الأخيرة بتقليص حجم تلك الملفات والمضبوطات، وتعمل على ضغطها بداخل ملف أو عدة ملفات صغيرة الحجم، ومن دون أن يؤثر ذلك على سلامة تلك الملفات، بحيث تبقى محفوظة بكامل خواصها الأصلية ليتم حفظها على أقراص الليزر ويتم فتحها على أي كمبيوتر من خلال برامج خاصة، ولكن لإنجاح هذه التقنية يجب إتباع ما يلي:

1- ضبط الدعائم الأصلية للبيانات وعدم الاقتصار على ضبط نسخها.

[1]- المادة 07 من قانون 09-04 المؤرخ في 5 غشت سنة 2009، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال ومكافحتها، سابق الإشارة إليه.

2- عدم ثني القرص لأن ذلك قد يؤدي إلى تلفه أو فقدان البيانات المسجلة عليه.

3- عدم تعريض الأقراص والأشرطة الممغنطة لدرجات حرارة عالية ولا إلى الرطوبة، مع الإشارة إلى أن درجة الحرارة المسموح بها تتراوح بين (4- 32) درجة مئوية، أما عن نسبة الرطوبة المسموح بها فتتراوح ما بين 20 %إلى 80%، وبإحترام التعليمات السابقة يمكن أن تصل مدة تخزين هذه الأقراص والأشرطة إلى ثلاث سنوات.

4- عدم الضغط على الأقراص والأشرطة الممغنطة بوضع أشياء ثقيلة، وعدم كتابة بيانات اللاصقة الورقية المخصصة للمستخدم بعد لصقها على القرص، لأن الضغط بالقلم قد يفسد سطح القرص.

5- عدم تعريض الأقراص للمجالات المغناطيسية بعد وضعها على الأجهزة حتى لا تفقد ما عليها، لأن التسجيل على الأسطوانة أو القرص يتم مغناطيسياً[1].

للإشارة فإن المشرع الجزائري لم يتطرق صراحة إلى هذه التقنية في القانون 09-04 بقدر ما أشار إلى تقنية النسخ السابق بيانها.

البند الثالث: الصعوبات التي تواجه إجراء ضبط البيانات الإلكترونية.

يواجه إجراء ضبط البيانات المعالجة إلكترونياً عدة صعوبات وعقبات منها:

حجم الشبكة التي تحتوي على المعلومات المعالجة إلكترونيا والمطلوب ضبطها، من ذلك البحث في نظام إلكتروني لشركة متعددة الجنسيات، وجود البيانات الإلكترونية في بعض الحالات في شبكات أو أجهزة تابعة لدولة أجنبية، مما يستدعي تعاونها مع جهات الشرطة والتحقيق في عملية التفتيش والضبط و التحفظ.

هذا ويترتب على الضبط إعتداءاً على حقوق الغير، أو على حرمة حياته الخاصة وهو الأمر الذي يتطلب ضرورة إتخاذ الضمانات اللازمة لحماية هذه الحقوق والحريات[2].

[1]- بوعناد فاطمة زهرة، المرجع السابق، ص. 147؛ عائشة بن قارة، المرجع السابق، ص. 117.
[2]- علي عدنان الفيل، المرجع السابق، ص. 59.

إلى جانب هذه العقبات، يثير الفقه إشكالية أخرى وتتعلق هذه الأخيرة بمدى إمكانية إلزام المتهم بفلك شفرة المستندات الإلكترونية أثناء الضبط[1].

من المعلوم أن ضبط وتفتيش المستندات الإلكترونية قد يتطلب ولوج نظام المعالجة الآلية للبيانات والبحث في محتوياته، وإذا قام المتهم بتشفير هذا النظام بما فيه من مستندات إلكترونية مطلوب ضبطها، فهل يمكن إجباره على الإدلاء ببيانات شفرة الدخول؟.

الأصل أنه لا يجوز إجبار المتهم على الإجابة على أسئلة تؤدي إلى تجريم نفسه، ومعنى ذلك أنه يمكن للمتهم الامتناع عن الإجابة والالتزام بالصمت، وهو ما يعرف بحق المتهم في الصمت، وللإشارة فإن هذا الحق نشأ مع أفكار الثورة الفرنسية، وبمقتضاه يمكن للمتهم أن يمتنع عن الإجابة عن الأسئلة الموجهة إليه، كما وله أن يمتنع عن الإدلاء بأية معلومات قد تؤدي إلى إدانته، وهو الأمر الذي تحرص معظم التشريعات المقارنة على النص عليه[2].

هذا ويجمع الفقه المصري على عدم جواز إجبار المتهم على الإدلاء بأقواله، وعدم اعتبار مجرد سكوته أو امتناعه عن الإجابة بمثابة قرينة ضده، وفي هذا قضت محكمة النقض أن المتهم إذا شاء أن يمتنع عن الإجابة أو الإستمرار فيها فله ذلك، ولا يعتبر هذا الامتناع قرينة ضده، وإذا تكلم فإنما ليبدي دفاعه، ومن حقه دون غيره أن يختار الوقت والطريقة التي يبدي بها هذا الدفاع، وعليه لا يصح أن يُتخذ من إمتناع المتهم عن الإجابة قرينة على ثبوت التهمة[3].

هذا وقد إنتهى الفقه الأمريكي إلى ذات الرأي طبقا لتفسيره لحق المتهم في عدم الشهادة ضد نفسه المُقرر بمقتضى التعديل الخامس للدستور الأمريكي[4]، الذي يقضي بعدم جواز إجبار أي شخص في قضية جنائية على الشهادة ضد نفسه، كما ولا يجوز حرمانه من حريته أو ممتلكاته دون مراعاة الوسائل القانونية السليمة.

---

[1]- أحمد عاصم عجيلة، المرجع السابق، ص. 431.
[2]- المرجع نفسه، ص. 431.
[3]- المرجع نفسه، ص. 432.
[4]- المرجع نفسه، ص. 432.

إستنادا لما سبق، يمكن القول أنه لا يجوز قانوناً إجبار المتهم على فك شفرة الدخول إلى المستندات الإلكترونية وإلزامه بالإفصاح والكشف عن مفاتيح الدخول وكلمات السر، لأن ذلك يتنافى مع حقه في الصمت أو الامتناع عن الإجابة أو الاستمرار فيها وهو حق مقرر له بمقتضى القانون.

وتبقى الوسيلة الوحيدة أمام المحقق لفك شفرة تلك المستندات هي الوسائل العلمية الحديثة، وإستخدام البرامج التي قد تساعده في فك شفرة الدخول إلى هذه المستندات، كما له أن يستعين بالخبراء إذا لزم الأمر، ذلك أن الأدلة الإلكترونية تقتضي تطويع العلم من أجل استخراجها والبحث عنها.

الفرع الرابع: الخبرة الفنية.

قد يقوم المحقق القضائي في مجال الكشف عن غموض الجريمة، وفاعلها باتخاذ الكثير من الإجراءات والوسائل المتنوعة اللازمة لتحقيق هدفه المتمثل في الوصول إلى الحقيقة، غير أن تحقيق هذا الهدف قد تعترضه مسائل فنية لا يستطيع المحقق بنفسه الفصل فيها أو التغلب عليها، لأن الأمر يتطلب توافر مهارات وقدرات خاصة قد لا تتوافر لديه، وهو ما يدعوه للاستعانة بخبير أو أكثر لتوضيح مسألة معينة أو أكثر قد تواجهه خلال التحقيقات[1].

ويقصد بالخبرة بصفة عامة، المهارات المكتسبة في تخصص معين سواء بحكم العمل في ذلك التخصص لمدة زمنية طويلة، أو نتيجة دراسات خاصة تلقاها الشخص أو نتيجة الاثنين معاً، ومن هنا يطلق على ذوي المهارات بالخبراء[2].

أما الخبرة القضائية فتعرف بأنها إجراء للتحقيق يعهد به القاضي إلى شخص مختص يسمى بالخبير بحيث يخوله صلاحية إبداء رأيه العلمي أو الفني بخصوص واقعة أو وقائع

[1]- سامح أحمد بلتاجي موسى، المرجع السابق، ص. 297؛ بلعليات إبراهيم، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري، ط1، دار الخلدونية، الجزائر، 2009، ص.242.

[2]- الخبير هو شخص مختص فنياً في مجال من المجالات الفنية أو العلمية أو غيرها من المجالات الأخرى، ويستطيع بما له من معلومات وخبرة إبداء الرأي في أمر من الأمور المتعلقة بالقضية والتي تحتاج إلى خبرة فنية خاصة. مشار اليه من طرف، خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص. 285.

مادية يتم البحث فيها، ويقدم الخبير على إثر ذلك تقريرا يُضَمِنُ فيه رأيه الذي لا يمكن للمحقق وحده الوصول إليه[1].

بهذا يبدو أن الخبرة هي الوسيلة التي تتمكن من خلالها سلطة التحقيق والمحكمة تحديد التفسير الفني للأدلة بالاستعانة بالمعلومات العلمية، وهي في حقيقتها لا تعد دليلاً مستقلاً عن الدليل القولي أو المادي، وإنما هي تقييم فني لذلك الدليل، ومن خلالها يقوم الخبير بتقديم تقرير أو رأي فني في أمر من الأمور المتعلقة بالجريمة[2].

وتكتسب الخبرة أهمية بالغة في مجال الجرائم الإلكترونية، نظراً لأن الحواسيب الآلية وشبكات الإتصال متعددة الأنواع والنماذج، والعلوم والتقنيات المتصلة بها تنتمي إلى تخصصات علمية وفنية دقيقة ومتنوعة، كما أن التطورات في مجالها سريعة ومتلاحقة لدرجة قد يصعب معها على المتخصص تتبعها واستيعابها[3]، وكل هذه الأمور تقف حجر عثرة في وجه المختصين في مجال القانون، بحيث لا تمكنهم معرفتهم القانونية وحدها من فك لغز الجريمة التي يعتبر الحاسوب القائم على اللوغاريتمات أساسها.

لاشك أن ندب الخبير من سلطات المحقق أو القاضي، يلجأ إليه في المسائل الفنية البحتة كالجرائم الإلكترونية التي لا يمكنه أن يقطع فيها برأيه دون إستطلاع رأي أهل الخبرة، وعليه يعد اللجوء إلى إجراء الخبرة في هذه الحالة واجب، فإذا تصدى القاضي للقضية دون استطلاع أهل الخبرة كان حكمه معيباً مستوجبا للنقض، وهو الأمر الذي أقرته محكمة النقض المصرية[4].

ولعل العنصر المميز للخبرة عن غيرها من إجراءات الإثبات هو الرأي الفني للخبير في كشف الدلائل وتحديد قيمتها التدليلية في الإثبات، وللإشارة فإن رأي الخبير غير ملزم بالنسبة للقاضي أو المحقق، بحيث تكون لهذا الأخير الحرية في تقديره، وله أن يستبدل

[1]- مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، ط1، مطابع الشرطة، القاهرة، 2009، ص.221؛ أحمد محمود مصطفى، المرجع السابق، ص.150.

[2]- خالد ممدوح إبراهيم، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص، ص. 283- 284.

[3]- عبد الله حسين علي محمود، المرجع السابق، ص 392؛ علي عدنان الفيل، المرجع السابق، ص، ص. 26- 27.

[4]- سامح أحمد بلتاجي موسى، المرجع السابق، ص. 298؛ مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص. 225.

الخبير في الدعوى بغيره من الخبراء، كما وله أن يأمر بإجراء خبرة تكميلية أو مضادة أو مقابلة، خاصة في حال تعارض النتائج التي توصل إليها الخبير مع غيره من الخبراء، غير أنه لا يجوز للقاضي تفنيد النتائج الفنية التي توصل إليها الخبير إلا بأسانيد فنية، وهو أمر غير متصور بالنسبة للشاهد لأن دوره في الدعوى قاصر عليه وحده[1].

وعليه فإن الخبراء الفنيين هم عنصر مكمل للقضاء يُتِمُّون رسالته، وبغيرهم لا يستقيم العدل، وإذا شئنا أن نجد سندا للخبرة في الشريعة الإسلامية فنجد قوله تعالى: (وَلاَ يُنَبِئُكَ مِثْلُ خَبِير)[2].

ومن التشريعات الحديثة التي نظمت أعمال الخبرة في مجال الجرائم الإلكترونية القانون البلجيكي الصادر في 2000/11/23 المتعلق بالإجرام المعلوماتي، حيث نصت المادة 88 منه على أنه: «يجوز لقاضي التحقيق، وللشرطة القضائية أن يستعينا بخبير ليقدم وبطريقة مفهومة المعلومات اللازمة عن كيفية تشغيل النظام وكيفية الدخول فيه، أو الدخول للبيانات المخزونة أو المعالجة أو المنقولة بواسطته، ويعطي القانون كذلك لسلطة التحقيق أن تطلب من الخبير تشغيل النظام، أو البحث فيه أو عمل نسخة من البيانات المطلوبة للتحقيق، أو سحب البيانات المخزنة أو المحولة أو المنقولة، على أن يتم ذلك بالطريقة التي تريدها جهة التحقيق».

ووفقا للقانون البلجيكي المذكور سلفاً فإن الالتزام بتشغيل النظام واستخراج البيانات المطلوبة منه، يرجع إلى قاضي التحقيق بصفة أصلية، ويجوز ذلك للنيابة العامة على سبيل الاستثناء في حالة التلبس أو عند الرضاء بعملية التفتيش[3].

ولأهمية الخبرة في مجال الجرائم الإلكترونية، شرعت بعض الدول في إعداد أجهزة متخصصة للخبرة في جرائم الحاسوب، وعلى رأس تلك الدول الولايات المتحدة الأمريكية التي تجاوز نشاطها في هذا المجال الإطار الدولي المتمثل في منظمة الإنتربول، وكان آخر

[1]- أحمد عاصم عجيلة، المرجع السابق، ص. 441؛ حطاب كمال، المرجع السابق، ص. 320.
[2]- الآية 14 من سورة فاطر.
[3]- علي عدنان الفيل، المرجع السابق، ص، ص. 30- 31.

نشاط مؤسسي لها في هذا الإطار الفرع الجديد الذي تأسس في المباحث الفيدرالية الأمريكية FBI، والذي أطلق عليه المعمل الإقليمي الشرعي للحاسب، ومقره سان ديجو (San Diego) والذي تم افتتاحه في شهر نوفمبر لسنة 2000، لكي يكون بيت خبرة عام 2000 غرضه مكافحة التصعيد في الجريمة عبر الإنترنت، وذلك بتحليل وتصنيف الدليل الرقمي، بحيث يتم إعداد محللين شرعيين للحاسب الآلي مهمتهم العمل على تكثيف مواجهة الجريمة الإلكترونية.

تبرز أهمية النواحي التي يتعامل معها المعمل الشرعي الجديد في تعاون العديد من منظمات الضبط القضائي للكشف عن الجرائم الإلكترونية، ومن تلك المنظمات إدارة مكافحة المخدرات، وحدة التحقيقات لمكافحة المجرمين، وحدة الجمارك، مكتب النائب العام للمقاطعة، وكذا مكتب حاكم المقاطعة[1].

هذا بالنسبة للدول الغربية، أما بالنسبة للمشرع الجزائري فيلاحظ أنه حاول اللحاق بالركب التكنولوجي، من خلال إصداره للقانون رقم 09-04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[2]، حيث خصص الفصل الخامس منه للتعرض لجهاز يسمى بالهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها (م13)[3]، ومن المهام التي أوكلت لهذا الجهاز مساعدة السلطات القضائية، ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال، بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية، وهو ما تم النص عليه في المادة 14 فقرة 02 من القانون المذكور[4].

---

[1]- أحمد عاصم عجيلة، المرجع السابق، ص، ص. 442- 443.

[2]- قانون رقم 09-04 المؤرخ في 5 غشت سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، سابق الإشارة إليه.

[3]- تنص المادة 13 من قانون 09-04 المؤرخ في 5 غشت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، سابق الإشارة إليه : «تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، تحدد تشكيل الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم».

[4]- المادة 14 الفقرة ب من القانون رقم 09-04 المؤرخ في 5 غشت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، سابق الإشارة إليه.

للإشارة فإن المشرع الجزائري قد أحال بموجب المادة 2/13 من قانون 09-04 آنف الذكر إلى التنظيم لتحديد تشكيلة الهيئة وتنظيمها وكيفيات سيرها، وهو الأمر الذي تقرر فعلا بمقتضى المرسوم الرئاسي رقم 15-261 المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال[1]، بحيث تم تشكيل سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والإستقلال المالي، توضع لدى الوزير المكلف بالعدل، ويحدد مقرها بمدينة الجزائر، على أن تكلف بمهام عديدة منها مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، بما في ذلك جمع المعلومات والتزويد بها من خلال الخبرات القضائية[2].

هذا وقد تم تعديل هذا المرسوم بمقتضى المرسوم الرئاسي رقم 19-172[3]، بحيث تم تحويل صلاحية هذه الهيئة من الوزير المكلف بالعدل إلى وزير الدفاع الوطني.

مما سبق كله، يستفاد أن الخبرة في جرائم المستندات الإلكترونية تهدف إلى الكشف عن الدليل الرقمي ومصدره، وذلك حتى يمكن تقديمه لأجهزة إنفاذ وتطبيق القانون، وعمل نسخة أصلية منه للتأكد من عدم وجود بيانات مفقودة أثناء عملية استخلاص الدليل، ولا شك أن جل عمل المحقق في تلك الجرائم يتوقف إلى حد كبير على تقرير الخبير الذي يسمح بإستكمال عمل المحقق ويوجهه إلى سير التحقيقات في الاتجاه الصحيح الذي يستخلص منه إما أدلة الإدانة أو البراءة، غير أن تحقيق كل ما سبق ذكره يتطلب احترام القواعد والأصول

---

[1]- مرسوم رئاسي رقم 15-261 مؤرخ في 24 ذي الحجة عام 1436هـ الموافق لـ 8 أكتوبر سنة 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر، ع. 53، سنة 2015.

[2]- حددت المادة 4 من المرسوم الرئاسي المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، سابق الإشارة إليه. مهام هذه اللجنة والتي تشمل:
- إقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها.
- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها،
- ضمان المراقبة الوقائية للإتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة، تحت سلطة القاضي المختص وباستثناء أي هيئات وطنية أخرى.
- تطوير التعاون مع المؤسسات الهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيات الإعلام والإتصال.
- المساهمة في تحديث المعايير القانونية في مجال اختصاصها.
- المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكتووجيات الإعلام والإتصال.

[3]- مرسوم رئاسي رقم 19-172 مؤرخ في 3 شوال عام 1440 الموافق 6 يونيو سنة 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها وتنظيمها وكيفيات سيرها، ج.ر، ع.37، سنة 2019.

الفنية لإعمال الخبرة، لا سيما في الجرائم الواقعة على المستندات الإلكترونية لما تتميز به هذه الجرائم من طابع فني وتقني.

لأهمية هذا كله سيتم التطرق إلى وسائل الخبير المعلوماتي في اكتشاف الدليل الإلكتروني **(البند الأول)**، يليها بعد ذلك دور الخبير المعلوماتي في الكشف عن جرائم المستندات الإلكترونية **(البند الثاني)**.

البند الأول: وسائل الخبير المعلوماتي في اكتشاف الدليل الإلكتروني.

هناك وسائل قد تساعد الخبير المعلوماتي في الوصول إلى المجرم المعلوماتي في مجال الجرائم الواقعة على المستندات الإلكترونية، ومعرفة كيفية وقوع الجريمة، هذه الوسائل منها ما هو مادي **(أولا)**، ومنها ما هو إجرائي **(ثانيا)** .

أولاً: الوسائل المادية: هي الأدوات الفنية التي يستخدمها الخبير في بيئة نظام المعلومات، والتي يمكن باستخدامها تنفيذ إجراءات وأساليب التحقيق المختلفة التي تثبت وقوع الجريمة[1]، ومن أهمها :

1- عنوان بروتوكول الإنترنت IP والبريد الإلكتروني: يعتبر عنوان الإنترنت المسؤول عن تراسل حزم البيانات عبر شبكة الإنترنت وتوجيهها إلى أهدافها، وهو يشبه إلى حد كبير البريد العادي، حيث يتيح للشبكات المعنية نقل الرسالة، ويوجد بكل جهاز مرتبط بالإنترنت، وفي حالة وجود أي مشكلة أو أية أعمال تخريبية فإن أول ما يجب أن يقوم به المحقق هو البحث عن رقم الجهاز، وتحديد موقعه لمعرفة الجاني الذي قام بتلك الأعمال غير القانونية، هذا ويمكن لمزود خدمة الإنترنت أن يراقب المشترك، كما يمكن للشبكة التي تقدم خدمة الاتصال الهاتفي أن تراقبه إذا ما توافرت لديهم أجهزة، وبرامج خاصة لذلك.

كما وتوجد أكثر من طريقة لمعرفة العنوان الخاص بجهاز الكمبيوتر في حالة الاتصال المباشر، منها على سبيل المثال ما يستخدم في حالة العمل على نظام تشغيل

[1]- سامح أحمد بلتاجي موسى، المرجع السابق، ص. 320.

(windows)، حيث يتم كتابة رمز (Win PC FG) ليظهر مربع حوار يبين فيه عنوان بروتوكول الإنترنت (IP)، مع ملاحظة أن عنوان الإنترنت قد يتغير مع كل اتصال بشبكة الإنترنت[1].

2- **البروكسي:** وهو حاسب يقوم بدور الوكيل، وذلك لاختصار الوقت اللازم للوصول إلى موضع معين على شبكة الإنترنت عند تكرار الدخول على نفس الموقع، وهو وسيط يتيح الاتصال بالشبكات لتعزيز قدرتها لإدارة الشبكة، وضمان الأمن وتوفير خدمات الذاكرة الجاهزة، وتقوم فكرة البروكسي على تلقي مزود البروكسي طلبات من المستخدم للبحث عن صفحة ما ضمن الذاكرة المحلية المتوفرة، فيتحقق البروكسي فيما إذا كانت هذه الصفحة قد جرى تنزيلها من قبل، ليقوم بإرسالها إلى المستخدم بدون الحاجة إلى طلب ذلك من الشبكة العالمية، وفي هذه الحالة يعمل البروكسي كمزود زبون ويستخدم أحد عناوين (IP)، ومن أهم مزايا مزود البروكسي أن الذاكرة المتوفرة لديه يمكن أن تحتفظ بتلك العمليات التي تمت عليها مما يجعل دوره قويا وفعالا في الإثبات، عن طريق فحص تلك العمليات المحفوظ بها، والتي تخص المتهم والموجودة عند مزود الخدمة[2].

3- **برامج التتبع:** يستطيع الخبير أن يقتفي أثر مخترقي النظام المعلوماتي بواسطة برامج يمكنها التعرف على محاولات الاختراق التي تمت، بحيث تقدم تلك البرامج بياناً شاملاً لمستخدم الجهاز الذي تم اختراقه، و للإشارة فإن البيان يحتوي على اسم الحدث، تاريخه، عنوان بروتوكول الإنترنت (IP) الذي تمت من خلاله عمليات الاختراق، إسم الشركة المزودة لخدمة الإنترنت والمستضيفة للمخترق، أرقام مداخلها ومخارجها على شبكة الإنترنت، إلى جانب معلومات أخرى[3].

إلى جانب هذه الوسائل المادية هناك وسائل أخرى قد يعتمد عليها الخبير المعلوماتي في كشف خبايا الجريمة و منها: برامج كشف الاختراق، أدوات الضبط، وكذا أدوات مراقبة

[1]- حسين بن سعيد بن سيف الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، المرجع السابق، ص، ص. 398-399.

[2]- أحمد عاصم عجيلة، المرجع السابق، ص. 445؛ ضياء يحي السادات، المرجع السابق، ص. 211.

[3]- حسين بن سعيد بن سيف الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، المرجع السابق، ص، ص. 399-400؛ ضياء يحي السادات، المرجع السابق، ص، ص.212- 213.

وفحص الشبكات، وهي تقنيات تساعد على كشف الأدلة الإلكترونية وتعمل على المحافظة عليها وعلى مسرح الجريمة[1].

ثانياً: الوسائل الإجرائية.

يقصد بها الإجراءات التي يتم باستخدامها تنفيذ طرق التحقيق الثابتة والمتغيرة التي تثبت وقوع الجريمة، وتحدد شخصية مرتكبها، ومنها :

1- **اقتفاء الأثر:** من أخطر ما يخشاه مجرم نظم المعلومات هو تقصي أثره أثناء ارتكابه لجريمته وبعد ارتكابها، و لتفادي تحقق هذه المسألة يعمل على مسح آثاره، وللإشارة فإن هناك الكثير من الوثائق التي يتم نشرها عبر المواقع الخاصة بالمخترقين تحمل في طياتها العديد من النصائح، أهمها نصيحة "قم بمسح آثارك"، ذلك أنه لو لم يقم المخترق بمسح آثاره فإنه من المؤكد أن يتم التوصل إليه، حتى وإن كانت عملية الاختراق قد تمت بشكل سليم، هذا ويمكن للخبير المعلوماتي تقصي الأثر بطرق عدة سواء عن طريق البريد الإلكتروني الذي تم استقباله، أو عن طريق تتبع أثر الجهاز الذي تم استخدامه للقيام بعملية الاختراق[2].

2- **الاستعانة بالذكاء الاصطناعي:** أثبتت تجارب استخدام تقنيات الحاسوب نجاحها في جمع الأدلة الجنائية، تحليلها واستنتاج الحقائق منها، وعليه يمكن للخبير الإستعانة بالذكاء الاصطناعي[3] في حصر الحقائق، الاحتمالات، الأسباب والفرضيات، والوصول إلى نتائج محددة على ضوء معاملات حسابية يتم تحليلها بالحاسوب، وفق برامج صممت خصيصا لهذا الغرض.

---

[1]- ضياء يحي السادات، نفس المرجع السابق، ص. 211 وما يليها؛ سامح أحمد بلتاجي موسى، المرجع السابق، ص. 320 وما يليها.

[2]- حسين بن سعيدبن سيف الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، المرجع السابق، ص. 405.

[3]- الذكاء الاصطناعي هو ذكاء الآلات، وهو فرع من علوم الحاسوب التي تهدف إلى ابتكاره، وأغلب كتب الذكاء الاصطناعي تُعرف هذا المجال على أنه: دراسة أو تصميم كيانات ذكية، أما الكيان الذكي فهو نظام يستوعب بيئته ويتخذ المواقف التي تزيد من فرصته في النجاح. مشار اليه من طرف، سامح أحمد بلتاجي موسى، المرجع السابق، هامش ص324.

إلى جانب هذه الوسائل الإجرائية يمكن للخبير وهو يقوم بمهامه أن يطلع على عمليات النظام المعلوماتي، طريقة حمايته كقاعدة البيانات وإدارتها، خطة تأمينها ومعرفة مواد النظام والمستفيدين، الملفات، بالإضافة إلى معرفة نوعية حماية البرامج وأسلوب عملها، كما له أن يقوم بالإستفادة من التقارير التي تنتجها نظم أمن البيانات، وتقارير جدران الحماية[1].

البند الثاني: دور الخبير المعلوماتي في جرائم المستندات الإلكترونية.

يعتمد نجاح المحقق أو ضابط الشرطة القضائية في مهمته المتمثلة في الكشف عن الحقيقة في مجال الجرائم الواقعة على المستندات الإلكترونية على حسن اختيار الخبير، وعلى تحديد المهمة المنتدب بشأنها والتي عهد إليه بأدائها، ومن ثم فإن جرائم الاعتداء على المستندات الإلكترونية تقتضي من المحقق أو ضابط الشرطة القضائية أو القاضي أن يلتزم بقواعد وأصول فنية في إجراء الخبرة، وذلك حتى تكون هذه الأخيرة نافعة له في كشف الحقيقة ومن هذه القواعد:

أولاً: ضرورة مراعاة حسن إختيار الخبير الذي يستعين به في هذه النوعية من الجرائم، حيث يجب أن تتوفر لديه الإمكانيات والقدرات العلمية والفنية في مجال التخصص الدقيق الذي يقتضيه موضوع التحقيق أو الجريمة، بل إن حصول الخبير على درجة علمية في تخصص معين لا يكفي بذاته، بل لا بد من توافر خبرة عملية في ذات المجال، ذلك أن الجرائم المعلوماتية عامة وجرائم المستندات الإلكترونية خاصة تتطلب هذا النوع من الخبرة، لأن تقرير الخبير في تلك الجرائم يكون بمثابة مرآة للمحقق، وللقاضي أن يهتدي بها في وزن الدليل ورجحان إدانة المتهم من عدمه[2].

ثانياً: يجب أن تتضمن مهمة الخبير وصف كيفية إرتكاب المتهم للجريمة من حيث نوع الحاسب المستخدم، طرازه، نوع نظام التشغيل، الأجهزة الطرفية التي إستخدمها، نظام

[1]- حسين بن سعيد بن سيف الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، المرجع السابق، ص، ص. 405-406؛ سامح أحمد بلتاجي موسى، المرجع السابق، ص. 323.

[2]- فتحي محمد أنور عزت، الحماية الجنائية الموضوعية والإجرائية للاعتداء على المصنفات والحق في الخصوصية والكمبيوتر والإنترنت في نطاق التشريعات الوطنية والتعاون الدولي، ط1، دار النهضة العربية، القاهرة، 2007، ص.300.

التشفير، طبيعة بيئة الحاسب من حيث تنظيم وتوزيع عمل المعالجة الآلية، وتردد موجات البث وأمكنة إختزانها[1].

ثالثاً: ينبغي أن تتضمن مهمة الخبير في جرائم تزوير المستندات الإلكترونية بيان ما إذا تم تغيير الحقيقة في المستند الإلكتروني من عدمه، بيان كيفية ذلك، وسيلة ذلك التغيير وتأثيره، وما إذا كان يحوي توقيعاً إلكترونياً من عدمه، الشخص أو الجهة المنسوب إليها ذلك المستند[2].

رابعاً: تجسيد الدليل المادي في الجرائم الواقعة على المستندات الإلكترونية في صورة مادية ملموسة إذا أمكن، بأن يطلب المحقق أو القاضي من الخبير نقلها إلى أوعية ورقية يتاح لهم فهمها واستنباط الدليل منها، مع إثبات أن المسطور على الورق مطابق لما هو مسجل على الدعامة الممغنطة أو القرص الصلب[3].

للإشارة فإن التزام الخبير هو التزام ببذل عناية، فلا يسأل إذا لم يصل إلى النتيجة المطلوبة نتيجة ضعف خبرته، أو بسبب العقبات التي واجهته أثناء مباشرته لمهمته، غير أنه يمكن أن يسأل جنائياً إذا ما رفض القيام بالمهمة المكلف بها، أو إذا ما قام عمدا بإتلاف البيانات المطلوب منه التعامل معها وحفظها.

فضلا عن إلتزام الخبير بأداء مهمته التي حددتها له جهة التحقيق، فإنه يلتزم كذلك بالمحافظة على سر المهنة، ومخالفة هذا الالتزام يُعرضه لعقوبات جزائية رادعة[4].

الفرع الخامس: التسرب.

نظراً لخطورة وخصوصية الجرائم الواقعة على المستندات الإلكترونية بصفة خاصة والجرائم الإلكترونية بصفة عامة، عمل المشرع الجزائري على استحداث مجموعة من الأساليب الخاصة للبحث والتحري لمجابهة هذا النوع المستحدث من الإجرام، ومن هذه

[1]- مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص. 225؛ علي عدنان الفيل، المرجع السابق، ص. 29.
[2]- أحمد عاصم عجيلة، المرجع السابق، ص. 448.
[3]- مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص. 226.
[4]- علي عدنان الفيل، المرجع السابق، ص.31.

الأساليب أسلوب التسرب الذي نص عليه بموجب القانون رقم 06-22 المعدل والمتمم لقانون الإجراءات الجزائية، حيث أفرد له فصلاً خاصاً مكونا من ثمان مواد وهي المواد من 65 مكرر 11 إلى غاية المادة 65 مكرر 18، وسمح بإجرائه في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات[1].

وبغية إلقاء الضوء على هذا الإجراء فإنه سيتم التطرق إلى بيان مفهوم إجراء التسرب **(البند الأول)**، ثم إلى الضمانات القانونية التي قررها المشرع في قانون الإجراءات الجزائية **(البند الثاني)**.

البند الأول: مفهوم عملية التسرب.

يعرف إجراء التسرب[2] بأنه تقنية من تقنيات التحري والتحقيق الخاصة، تسمح لضابط الشرطة القضائية أو عون الشرطة القضائية وتحت مسؤولية ضابط شرطة قضائية آخر، بالتوغل داخل جماعة إجرامية، لمراقبة أشخاص مشتبه فيهم وكشف أنشطتهم الإجرامية، ويتم التوغل بإخفاء المتسرب لهويته الحقيقية وتقديم نفسه على أنه فاعل أو شريك[3].

ولئن كان هذا التعريف فقهي، فيلاحظ أن المشرع الجزائري عرفه في المادة 65 مكرر 12 من القانون رقم 06-22 المعدل والمتمم لقانون الإجراءات الجزائية بأنه: «قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف ».

[1]- نص المشرع الجزائري بموجب المادة 65 مكرر 5 من القانون رقم 06-22 المؤرخ في 20ديسمبر سنة 2006، المعدل والمتمم لقانون الإجراءات الجزائية الجزائري على بعض الجرائم التي يسمح فيها باتخاذ إجراءات التحقيق المستحدثة وهذه الجرائم هي: جرائم المخدرات، الجريمة المنظمة عبر الحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، جرائم تبييض الأموال أو الإرهاب، الجرائم المتعلقة بالتشريع الخاص بالصرف، جرائم الفساد.

[2]- يعني التسرب لغة الدخول خفية، والولوج بطريقة متخفية إلى مكان أو جماعة ما مما يجعلهم يعتقدون بأنه ليس غريبا عنهم وإشعارهم بأنه واحد منهم، ولكلمة التسرب كلمة مرادفة لها وهي: الاختراق، وهي مستخدمة في الكثير من الكتب والمؤلفات القانونية والإختراق من يخترق، اختراقا، بمعنى مشى وسطهم. مشار اليه من طرف، علي بن هادية، بلحسن البليش، الجيلاني بن الحاج يحي، القاموس الجديد للطلاب، المؤسسة الوطنية الجزائرية للكتاب، الجزائر، 1987، ص. 20.

[3]- عبد الرحمن خلفي، محاضرات في قانون الإجراءات الجزائية، دار الهدى، الجزائر، 2010، ص. 75.

استنادا لما تقدم، يمكن القول أن التسرب أو ما يطلق علية التسلل أو التوغل عملية يتم من خلالها إقحام شخص أجنبي عن الجماعة المراد اختراقها ليكون عيناً يراقب أعمالها ويرصد تصرفاتها. هذا ويُطلق على التسرب مصطلح الزرع ذلك أنه يؤدي إلى زرع أحد ضباط وأعوان الشرطة القضائية ممن تتوفر فيهم بعض المواصفات الخاصة وسط مجموعة إجرامية، بقصد مراقبتها من الداخل، ومعرفة الإمكانات المادية والبشرية والتنظيمية لها كأساليب عملها ووسائل اتصالها، وهذا كله بغية مكافحة إجرامهم والقبض عليهم[1].

وبما أن المشرع الجزائري قد سمح باتخاذ هذا الإجراء في بعض الجرائم الخطيرة والتي من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، فإن تجسيد عملية التسرب في الجرائم الإلكترونية يمكن أن يتم باشتراك ضابط أو عون الشرطة القضائية في محادثات غرف الدردشة أو مواقع التواصل الاجتماعي، وذلك لرصد أي معلومات حول قيام أحد الجناة باختراق الشبكات أو بث الفيروسات أو تخريب المستندات الإلكترونية، وللقيام بهذه المهمة يقوم المتسرب باستعمال أسماء مستعارة، والظهور بمظهر طبيعي كما لو كان فاعلا معهم، ويحاول بعد ذلك الاستفادة من معرفتهم حول كيفية اقتحام الهاكر لموقع ما[2]، أو الطريقة التي توغل بها إلى النظام المعلوماتي وألحق أضرار بالمعطيات والملفات الإلكترونية، وذلك على نحو يمكنه من اكتشاف وضبط هذه الجرائم والتوصل إلى هوية مرتكبيها.

البند الثاني: ضمانات عملية التسرب.

نظراً لخطورة عملية التسرب التي تتم خلسة في وسط إجرامي ودون علم الجماعة الإجرامية بذلك، ونظراً لأن هذا الإجراء قد يمس بحرمة الحياة الخاصة للغير، عمد المشرع الجزائري إلى إحاطته بجملة من الضمانات والإجراءات الوقائية والتنظيمية، وتتمثل هذه الضمانات فيما يلي:

[1]- عبد الرحمن خلفي، محاضرات في قانون الإجراءات الجزائية، المرجع السابق، ص.76.
[2]- بوعناد فاطمة زهرة، المرجع السابق، ص. 173؛ عائشة بن قارة، المرجع السابق، ص. 120.

- الحصول على إذن قضائي، وعليه لا يتم التسرب إلا بإذن قضائي ويستوي أن يصدر هذا الإذن عن وكيل الجمهورية أو قاضي التحقيق، كما وينبغي أن تتم العملية تحت مراقبة من أصدر الإذن، هذا وقد أعطى المشرع الجزائري للجهة القضائية مصدرة الإذن (قاضي التحقيق أو وكيل الجمهورية) السلطة التقديرية في اتخاذ إجراء التسرب من عدمه، وهو ما يظهر جليا من نص المادة 65 مكرر 11 من قانون الإجراءات الجزائية.[1]

- وجوب أن يكون الإذن القضائي بالتسرب مكتوباً ومسبباً، وذلك تحت طائلة البطلان، كما ويجب أن يذكر في الإذن الجريمة التي تبرر اللجوء إلى هذا الإجراء، وهوية ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته[2].

- وجوب تحديد مدة عملية التسرب في الإذن القضائي، والتي لا يمكن أن تتجاوز أربعة أشهر قابلة للتجديد بحسب مقتضيات التحري، أو التحقيق ضمن نفس الشروط الشكلية والزمنية، مع جواز أن يأمر القاضي الذي رخص بإجرائها بوقفها في أي وقت قبل انقضاء المدة المحددة، على أن يتم إيداع هذه الرخصة في ملف الإجراءات بعد الانتهاء من عملية التسرب[3].

- عدم إظهار الهوية الحقيقية لضباط وأعوان الشرطة القضائية الذين يباشرون عملية التسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات، وذلك كله لضمان

---

[1]- تنص المادة 65 مكرر 11 من قانون رقم 06-22 المؤرخ في 20 ديسمبر سنة 2006 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري، سابق الإشارة إليه: «عندنا تقتضي ضرورات التحري أو التحقيق في إحدى الجرائم المذكورة في المادة 65 مكرر 5 أعلاه يجوز لوكيل الجمهورية أو لقاضي التحقيق، بعد إخطار وكيل الجمهورية، أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب ضمن الشروط المبينة في المواد أدناه».

[2]- تنص المادة 65 مكرر 15 ف 01 -02 من القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري، سابق الإشارة إليه: " يجب أن يكون الإذم المسلم تطبيقا للمادة 65 مكرر 11 أعلاه مكتوبا ومسببا وذلك تحت طائلة البطلان
تذكر في الإذن الجريمة التي تبرر اللجوء إلى هذا الإجراء وهوية ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته."

[3]- تنص المادة 65/ مكرر 15 ف 3-4-5-6 من القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري، سابق الإشارة إليه:" ويحدد هذا الإذن مدة عملية التسرب التي لا يمكن أن تتجاوز أربعة (4) أشهر.
يمكن أن تجدد العملية حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية.
ويجوز للقاضي الذي رخص بإجرائها أن يأمر، في أي وقت، بوقفها قبل انقضاء المدة المحددة.
تودع الرخصة في ملف الإجراءات بعد الانتهاء من عملية التسرب."

سلامة وأمن القائم بالتسرب، ولتحقيق هذا الغرض رتب المشرع الجزائري عقوبات جزائية على كل شخص يخالف هذا الحظر[1].

- تخويل ضباط وأعوان الشرطة القضائية المرخص لهم بإجراء عملية التسرب والأشخاص الذين يسخرونهم لهذا الغرض، ودون أن يكونوا مسؤولين جزائيا القيام ببعض الأفعال الإيجابية، كاقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال، أو منتوجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو المستعملة في ارتكابها.

- تخويل مرتكبي هذه الجرائم الحق في إستعمال الوسائل ذات الطابع القانوني أو المالي، وكذا وسائل النقل أو التخزين أو الإيواء أو الحفظ أو الاتصال[2]، وهو الأمر الذي كرسته المادة 65 مكرر 14.

بهذا يتبين أن القانون أعفى القائم بإجراء التسرب من المسؤولية الجزائية بالرغم من أن الأفعال المذكورة أعلاه تستوجب من القائمين بها مشاركة إيجابية كحيازة متحصلات الجريمة أو وسائل ارتكابها، ذلك أن عمل هؤلاء الضباط يندرج ضمن أسباب الإباحة والتي ورد النص عليها في المادة 1/39 من قانون العقوبات[3] تحت عبارة "فيما أذن أو أمر به

---

[1]- تنص المادة 65 مكرر 16 /2-3-4 من القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري، سابق الإشارة إليه على أنه: «يعاقب كل من يكشف هوية ضابط أو أعوان الشرطة القضائية بالحبس من سنتين (2) إلى خمس (5) سنوات وبغرامة من 50.000 دج إلى 200.000 دج.
وإذا تسبب الكشف عن الهوية في أعمال عنف أو ضرب أو جرح على أحد هؤلاء الأشخاص أو أزواجهم أو أبنائهم أو أصولهم المباشرين، فتكون العقوبة الحبس من خمس (5) إلى عشر(10) سنوات، والغرامة من 200.000 دج إلى 500.000 دج.
وإذا تسبب هذا الكشف في وفاة أحد هؤلاء الأشخاص فتكون العقوبة بالحبس من عشر (10) سنوات إلى عشرين (20) سنة، والغرامة من 500.000 دج إلى 1000.000 دج، دون الإخلال عند الاقتضاء بتطبيق أحكام الفصل الأول من الباب الثاني من الكتاب الثالث من قانون العقوبات».

[2]- تنص المادة 65 مكرر 14 من القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري، سابق الإشارة إليه:" يمكن ضباط وأعوان الشرطة القضائية المرخص لهم بإجراء عملية التسرب والأشخاص الذين يسخرونهم لهذا الغرض، دون أن يكونوا مسؤولين جزائيا، القيام بما يأتي:
-اقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتوجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها.
- استعمال أو وضع تحت تصرف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل أو التخزين أو الإيواء أو الحفظ أو الإتصال."

[3]- تنص المادة 1/39 من الأمر 156/66 المؤرخ في 8 يونيو سنة 1966 المتضمن قانون العقوبات الجزائري، المعدل والمتمم، سابق الإشارة إليه:"لا جريمة إذا كان الفعل قد أمر أو أذن به القانون."

القانون"، وعليه فإن تجاوز الغرض المحدد من التسرب يترتب عليه المسؤولية الجزائية حسب القواعد العامة، هذا وقد قرر المشرع الجزائري بموجب المادة 65 مكرر 12 الفقرة 02 أنه لا يجوز تحت طائلة البطلان أن تشكل الأفعال المذكورة تحريضاً على ارتكاب الجرائم[1]، وفي هذا الإطار اعتبر الفقه أن هذه النقطة هي مفتاح الوصول إلى الحقائق وأهداف العملية في أسرع وقت ممكن، كما أنها لا تخلو حسب الفقه من المخاطر بالنسبة للشخص المتسرب، حيث أنه بمشاركة المتسرب في نشاطات الجماعة الإجرامية يتمكن من:

- كسب ثقة أكبر للجماعة الإجرامية.
- كشف خبايا وأسرار الجماعة الإجرامية، وذلك من خلال تعميق البحث والتحري داخل هذا الوسط، ومراقبة جميع الأشخاص المشتبه فيهم لارتكابهم جناية أو جنحة، وكذلك معرفة جميع الوسائل المستعملة من قبل الجماعة والمتعلقة بالنقل والإيصال والتخزين أو الحفظ أو غيرها، من خلال استعمال وسيلة الحيلة والتستر بغرض ضبط الفاعلين والمساهمة معهم حتى الوصول إلى معرفة الصورة الحقيقية للجماعة الإجرامية، أو الوسط الإجرامي[2].

هذا وقد أجاز المشرع الجزائري بموجب المادة 65 مكرر 18 من قانون الإجراءات الجزائية سماع ضابط الشرطة القضائية الذي تجري عملية التسرب تحت مسؤوليته دون سواه بوصفه شاهدا عن العملية.

المطلب الثاني: الإجراءات المستحدثة لمواجهة الجرائم الماسة بالمستند الإلكتروني.

رغم أهمية الدور الذي تلعبه إجراءات البحث والتحري التقليدية لمواجهة الجرائم الماسة بالمستندات الإلكترونية، وتحديد المجرم المعلوماتي، إلا أنها تظل إجراءات قاصرة لا

[1]- تنص المادة 65 مكرر 12 ف 02 من قانون 06- 22المؤرخ في 20ديسمبر 2006 المتعدل والمتمم لقانون الإجراءات الجزائية الجزائري، سابق الإشارة إليه على أنه : « يسمح لضابط أو عون الشرطة القضائية أن يستعمل لهذا الغرض هوية مستعارة، وأن يرتكب عند الضرورة الأفعال المذكورة في المادة 65 مكرر 14 أدناه، ولا يجوز تحت طائلة البطلان أن تشكل هذه الأفعال تحريضاً على ارتكاب الجرائم».

[2]- عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، ط 2 ، دار هومة، الجزائر، 2011، ص. 281.

تتماشى مع طبيعة البيئة الإلكترونية، تلك البيئة الافتراضية التي يمكن للمجرم فيها طمس آثار الجريمة، والإفلات من العقوبة المقررة لها.

أمام هذه الحقيقة المؤكدة وخشية إفلات المجرم المعلوماتي من قبضة العدالة، عمدت التشريعات على المستويين الدولي والوطني إلى استحداث إجراءات جديدة تتماشى مع البيئة الافتراضية، إجراءات يمكن فيها للهيئات المختصة من ملاحقة الجاني، وفك لغز الجريمة الإلكترونية، إجراءات لا يمكن القول عنها إلا أنها إجراءات إلكترونية قائمة على استخدام أحدث الوسائل العلمية التي ابتكرها العقل البشري لمواجهة هذا النوع المستحدث من الجرائم. ولا ريب في أن هذه الإجراءات قد تهدف إلى جمع البيانات الإلكترونية المخزنة **(الفرع الأول)**، التجميع في الوقت الفعلي لبيانات المرور **(الفرع الثاني)**، مراقبة الاتصالات الإلكترونية **(الفرع الثالث)**، ثم لاعتراض الاتصالات السلكية واللاسلكية **(الفرع الرابع)**.

الفرع الأول: إجراءات التحقيق المستحدثة الرامية إلى الاستفادة من البيانات الإلكترونية المخزنة.

بسبب عدم كفاية الإجراءات التقليدية في عمليات البحث والتقصي لمواجهة الجرائم الإلكترونية عامة، والجرائم الماسة بالمستند الإلكتروني خاصة، استحدثت إجراءات جديدة تتماشى والتقنيات المستخدمة لارتكاب هذه الجرائم، إجراءات تسمح بالوصول إلى مرتكبي الجرائم المعلوماتية، ولعل من بين أهم الإجراءات المستحدثة تلك التي يتم من خلالها الاستفادة من البيانات الإلكترونية المخزنة سواء كانت بيانات متعلقة بمحتوى الاتصالات أو ببيانات المرور، أو خاصة بتقديم بيانات معلوماتية.

لأهمية هذه المسألة سيتم التعرض لها بالتطرق لكل من التحفظ العاجل على محتوى البيانات المخزنة **(البند الأول)**، الحفظ العاجل لبيانات المرور **(البند الثاني)**، وكذا الأمر بتقديم بيانات معلوماتية محددة **(البند الثالث)**.

البند الأول: التحفظ[1] السريع على محتوى البيانات المخزنة.

لا ريب في أن التحفظ السريع لمحتوى البيانات المخزنة في النظام المعلوماتي إجراء أولي يرمي إلى الاحتفاظ بالبيانات المخزنة في النظام المعلوماتي خشية ضياعها، ويتم اللجوء إلى مثل هذا الإجراء، كلما وجدت أسباب تدعو إلى الاعتقاد بأن تلك البيانات قابلة للإتلاف والتعديل[2].

بهذا يبدو أن التحفظ العاجل لمحتوى البيانات المخزنة إلكترونيا إجراء قانوني جديد، وهو أداة مستحدثة للبحث عن الجرائم المعلوماتية، وبصفة خاصة الجرائم الماسة بالمستندات الإلكترونية، ولأهميته وذيوع استخدامه لمواجهة هذا النوع من الجرائم تم تنظيمه بمقتضى اتفاقيات دولية، ومن ذلك اتفاقية بودابست، إذ خصصت له هذه الأخيرة أحكام المادة 16 منها[3]، وفيها ألزمت الدولة الأطراف في الاتفاقية باتخاذ الإجراءات التشريعية أو أية إجراءات أخرى تراها ضرورية لتمكين سلطاتها المختصة بالأمر بالتحفظ العاجل على البيانات المخزنة بواسطة نظام معلوماتي، خاصة عندما تكون هناك أسباب تدعو للاعتقاد بأن تلك البيانات معرضة للفقد أو التغيير.

إنطلاقا من هذه الأحكام، يلاحظ أن التحفظ العاجل على البيانات المخزنة إلكترونيا يتم بطرق متعددة، والدليل على ذلك أن اتفاقية بودابست لم تحدد الطريقة التي يتم من خلالها

---

[1]- إنه من الأهمية بمكان التفرقة بين مصطلحي التحفظ على البيانات (conservation des données) والاحتفاظ أو أرشفة البيانات (L'archivage des données)، إذ وعلى الرغم من أن للكلمتين معنيين متجاورين في اللغة الشائعة، إلا أنهما يختلفان في لغة المعلوماتية، ذلك أن عبارة تحفظ على البيانات تنصرف إلى حفظ بيانات سبق وجودها في شكل مخزن وحمايتها من كل شي يمكن أن يؤدي إلى إتلافها أو تجريدها من صفتها أو حالتها الراهنة، وذلك بخلاف عبارة الاحتفاظ بالبيانات والذي يقصد به حفظ البيانات لدى حائزها بالنسبة لمستقبل البيانات التي هي في طور الإنتاج، فأرشفة البيانات تشير إلى تجميع البيانات في الوقت الحاضر وحفظها، وحيازتها في أرشيف أي وضعها في ترتيب معين والاحتفاظ بها في المستقبل، وعليه فإن عملية أرشفة البيانات هي عبارة عن عملية تخزين البيانات، وذلك على عكس التحفظ على البيانات الذي يعني النشاط الذي يضمن للبيانات سلامتها. مشار إليه من طرف: هلالي عبد اللاه أحمد، إتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها، المرجع السابق، ص، ص 192- 293.

[2]- بوعناد فاطمة زهرة، المرجع السابق، ص 176؛ حطاب كمال، المرجع السابق، ص. 325.

[3] -Art 16 al 1 du convention sur la cybercriminalité dispose que : « 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 raison de penser que celles-ci sont particulièrement susceptibles de perte ou de modification. »

التحفظ على البيانات، بل تركت لكل دولة طرف صلاحية تحديد النماذج الملائمة للتحفظ، وهو ما يستشف من العبارة الواردة في الفقرة 1 من المادة 16 والمتمثلة في: «يأمر أو تفرض بطريقة أخرى»، فهذه العبارة ترمي إلى الترخيص للدول بتطبيق وسائل قانونية أخرى للتحفظ غير الأمر القضائي أو الإداري أو تحقيق الشرطة أو النيابة، وهنا ينبغي التنويه إلى أن قوانين الإجراءات الجزائية لبعض الدول لا تنص على أوامر التحفظ، بحيث لا يتم التحفظ على البيانات إلا من خلال عمليات التفتيش والضبط الآمر بالإنتاج - أي إنتاج البيانات-، ولكن رغم الحظر الوارد في قانون الإجراءات الجزائية لبعض الدول إلا أنه تجدر الإشارة أن عبارة "تفرض بطريقة أخرى" الواردة في اتفاقية بودابست تسمح للدول الأطراف من الاتفاقية تطبيق هذه المادة، ووضع هذه الطرق موضع التنفيذ.

ورغم مرونة العبارة سالفة الذكر "تعرض بطريقة مشابهة" فإنه يوصى بالنسبة للدول الأطراف في الاتفاقية التي لم تنظم إجراء التحفظ العاجل على البيانات المعلوماتية المخزنة أن تقوم بتأسيس سلطات، وإجراءات تسمح بأمر المرسل إليه بالتحفظ على البيانات، سيما وأن سرعة تدخل هذا الشخص قد تؤدي في بعض الحالات إلى تطبيق التحفظ بسرعة أكبر[1].

وعليه يتبين أن الهدف المتوخى من هذا الإجراء هو تمكين السلطات المحلية المختصة بالتحقيق في جرائم الكمبيوتر من التعرف على مضمون البيانات التي أرسلها المشترك أو استقبلها عن طريق طلبها من مقدمي الخدمات[2].

للتنويه فإن المذكرة التفسيرية لاتفاقية بودابست تشير إلى أن الإجراءات الواردة في المادة 16 تنطبق على البيانات المخزنة التي سبق تحيينها والاحتفاظ بها عن طريق حائزي البيانات كمقدمي الخدمات، كما وتشير إلى شمولية البيانات المعلوماتية المخزنة التي تكون محلا للتحفظ، بحيث تشمل كل نوع من البيانات المحددة في الأمر بالتحفظ، وقد تكون تلك البيانات واردة في مستندات تجارية طبية أو شخصية، وعليه بخرج من نطاق تطبيق هذه

[1]- هلالي عبد اللاه أحمد، إتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها، المرجع السابق، ص. 206.
[2]- بوعناد فاطمة زهرة، المرجع السابق، ص. 176.

المادة التجميع في الوقت الفعلي، والتحفظ المستقبلي على البيانات المتعلقة بالمرور أو الولوج في الوقت الفعلي إلى محتوى الاتصالات[1].

الملاحظ أن الفقرة 01 من المادة 16 تشير صراحة إلى البيانات المتعلقة بالمرور، وتنوه بتطبيق هذا النص على هذا النوع من البيانات عندما يتم الاحتفاظ بها من طرف مقدم الخدمة، خاصة وأنه عندما يتم الاحتفاظ بها فإنه لا يكون بصفة خاصة متحفظا عليها إلا لفترة وجيزة، وبهذا يبدو أن الإشارة إلى البيانات المتعلقة بالمرور في المادة 16 رغم تنظيمها بموجب المادة 17 من اتفاقية بودابست، يقيم علاقة بين الإجراءات المشار إليه في المادتين 16 و17.[2]

إذا كانت هذه هي الأحكام التي تضمنتها الفقرة 1 من المادة 16 من الاتفاقية، فإن الفقرة 02 من ذات المادة[3] أشارت إلى أن تطبيق الدول الأطراف لإجراء الحفظ من خلال أمر التحفظ يتصل ببيانات مخزنة ومتواجدة إما في حوزة الشخص الذي أرسل إليه الأمر أو تحت إشرافه، وهكذا فإن البيانات المخزنة والتي تكون محلا لأمر التحفظ ممكن أن تكون في حيازة المعني، كما يمكن أن تكون مخزنة في مكان آخر ولكنها خاضعة لإشرافه، ولتحقيق هذه المسألة فإنه يجب على الدولة الطرف في الاتفاقية اتخاذ الإجراءات التشريعية والإجراءات الضرورية لإلزام المعني بالأمر على التحفظ على البيانات المعلوماتية المخزنة وسلامتها لمدة معينة، وتحدد هذه المدة حسب الضرورة على أن لا تتجاوز 90 يوما كحد أقصى، وتكون هذه المدة قابلة للتجديد كلما وجدت أسباب تدعو للإعتقاد بأن تلك البيانات معرضة للفقد أو التغيير.

---

[1]- هلالي عبد اللاه أحمد، إتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها، المرجع السابق، ص. 195.

[2]- المرجع نفسه، ص. 207.

[3]- Art 16 al 2 du convention sur la cybercriminalité dispose que : « Lorsqu'une partie fait application du paragraphe 1 ci –dessus , au moyen d'un 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 protéger l'intégrité desdits données pendant une durée aussi longue que nécessaire, jusqu'à maximum 90 jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Une Partie peut prévoir qu'une telle injonction soit renouvelée par la suite. »

وحتى يحقق أمر التحفظ الغاية المرجوة منه، فقد فرضت الفقرة 03 من المادة 16[1] التزام السرية بالنسبة لتطبيق إجراءات التحفظ على حارس البيانات، أو أي شخص آخر يكون ملزماً بالتحفظ على البيانات في إطار المدة المحددة في قانونه الداخلي.

واستلزام كتمان السر المتعلق بالحفظ على البيانات المعلوماتية المخزنة حسب المدة المقررة في التشريع الداخلي لكل دولة الغرض منه، من جهة عدم تمكين المشتبه فيه من اتخاذ الاحتياطات اللازمة بسبب علمه بأمر التحفظ، ومن جهة أخرى تكريس حق الأفراد في احترام حياتهم الخاصة، وعليه لا يمكن أن يكون أمر التحفظ مفتوحا إلى ما لا نهاية.

الواقع، لا تعد اتفاقية بودابست الوحيدة التي نظمت إجراء التحفظ العاجل لمحتوى البيانات المخزنة، إذ تعرضت للأمر ذاته الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، وذلك في المادة 23 منها، حيث دعت إلى إلزام كل من بحيازته أو سيطرته معلومات تقنية التعهد بحفظ وسلامة تلك المعلومات، وقد حددت هذه الاتفاقية شأن اتفاقية بودابست مدة الحفظ بفترة 90 يوما كحد أقصى، على أن تكون تلك المدة قابلة للتجديد، وهذا لتمكين السلطات المختصة من القيام بمهمتها في البحث والتقصي، ونظرا لأن السرية مهمة في إطار التنقيبات والتحريات الأولية، فقد عمدت المادة 3/23 من ذات الاتفاقية إلى إلزام الدول الأطراف فيها بتبني الإجراءات الضرورية لإلزام الشخص المسؤول عن حفظ المعطيات المعلوماتية بعدم إفشاء محتويات أمر التحفظ طوال الفترة القانونية المنصوص عليها في قانونه الداخلي[2].

---

[1]- Art 16al 3 du convention sur la cybercriminalité dispose que : « Chaque Partie adopte les mesures législatives et autre 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 sont droit interne. »

[2]- تنص المادة 23 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، سابق الإشارة إليها:"

1. تلتزم كل دولة طرف بتبني 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 معلومات وخصوصا إذا كان هناك اعتقاد أن تلك المعلومات عرضة للفقدان أو التعديل.
2. تلتزم كل دولة طرف بتبني الإجراءات الضرورية فيما يتعلق بالفقرة (1) بواسطة إصدار أمر إلى شخص من أجل حفظ معلومات تقنية المعلومات المخزنة، والموجودة بحيازته أو سيطرته ، ومن أجل إلزامه بحفظ وصيانة تلك المعلومات لمدة أقصاها 90 يوما قابلة للتجديد، من أجل تمكين السلطات المختصة من البحث والتقصي.
3. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لإلزام الشخص المسؤول عن حفظ تقنية المعلومات للإبقاء على سرية الإجراءات طوال الفترة القانونية المنصوص عليها في القانون الداخلي".

البند الثاني: التحفظ العاجل لبيانات المرور.

نظرا لعدم كفاية الإجراءات العادية لجمع وإفشاء البيانات المعلوماتية، وبسبب أهمية البيانات المتعلقة بالمرور في الكشف عن الجريمة المعلوماتية، وتحديد هوية المشتبه فيه والمساهمين معه، فقد تم استحداث إجراء قانوني جديد يعرف باسم التحفظ العاجل لبيانات المرور.

ويقصد ببيانات المرور حسب ما ورد في المادة 1/د من اتفاقية بودابست طائفة من البيانات المعلوماتية لنظام قانوني معين، وللإشارة فإن هذه البيانات والمتمثلة في كل من منشأ أو أصل الاتصال[1]، مكان الوصول[2]، خط السير، وقت أو ساعة الاتصال وفقا لتوقيت غرينيتش، طول أو حجم الاتصال، المدة أو الفترة، نوع الخدمة[3]، تنشأ عن طريق أجهزة الحاسب في سلسلة من الاتصال بغرض توجيه هذا الأخير من منبعه أو أصله إلى مكان وصوله.

وبهذا تعد هذه البيانات من ملحقات الاتصال في حد ذاته، وهي ضرورية لتحديد البيانات السالف الإشارة لها، ذلك أنها تعتبر نقطة بداية تسمح بتجميع أدلة أخرى، ناهيك عن أنها تعد جزءاً من دليل الجريمة.

إن أهمية هذا الإجراء دفع بواضعي اتفاقية بودابست إلى أخذه في الحسبان وتنظيمه بموجب المادة 17 منها التي تستلزم من أجل ضمان التحفظ على البيانات المتعلقة بالمرور إلزام كل الدول باتخاذ الإجراءات التشريعية، أو أية إجراءات أخرى تراها ضرورية لكفالة قيام مقدمي الخدمات بالتحفظ السريع للبيانات المتعلقة بخط سير البيانات، ولضمان قيام هؤلاء المقدمين في الوقت ذاته بالإفشاء السريع لتلك البيانات للسلطة المختصة، أو الشخص

[1]- يشير مصطلح منشأ أو أصل الاتصال إلى رقم التلفون وعنوان بروتوكول الإنترنت (address IP)، أو بطريقة مماثلة تحديد هوية جهاز الاتصال الذي يقوم مقدم الخدمة بتقديم خدماته من خلاله. مشار إليه من طرف، هلالي عبد اللاه أحمد، إتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها، المرجع السابق، ص. 28.

[2]- يقصد بمكان الوصول جهاز الاتصال الذي تتجه إليه الاتصالات المرسلة. مشار إليه من طرف، هلالي عبد اللاه أحمد، إتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها، المرجع السابق، ص.28.

[3]- يقصد بمصطلح نوع الخدمة المؤداة نوع الخدمة المستخدمة داخل الشبكة مثل نقل ملف، بريد إلكتروني، بريد آني أو لحظي. مشار إليه من طرف، هلالي عبد اللاه أحمد، إتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها، المرجع السابق، ص. 28.

المعين من قبل تلك السلطة من كمية بيانات المرور بما يسمح بتحديد هوية مقدمي الخدمات الذين ساهموا في نقل الاتصال، والطريق الذي تم الاتصال من خلاله.

بهذا يلاحظ أن المادة 17 من اتفاقية بودابست تنشئ التزامات محددة في حالة التحفظ العاجل على بيانات المرور، كما تقرر الإفشاء السريع للبعض منها، ذلك أن الحصول على بيانات المرور المخزنة والمتعلقة باتصالات سابقة يكون أمرا حتميا لتحديد مصدر أو مكان وصول هذه الاتصالات، التي تعد جوهرية للتعرف على الأشخاص الذين ارتكبوا أعمالا إجرامية، كأن يكونوا قد نشروا إعلانات كاذبة أو بثوا فيروسات معلوماتية ،أو شرعوا في الوصول بطريقة غير مشروعة لنظم معلوماتية، أو بدءوا في تنفيذ مخططهم الإجرامي ونجحوا في الوصول للنظام المعلوماتي، أو قاموا بنقل اتصالات لنظام معلوماتي، وكانت تلك الاتصالات تحمل اعتداءاً على بيانات النظام أو تعرقل حسن سيره[1].

ونظرا لأن عملية النقل قد يساهم فيها العديد من مقدمي الخدمات، فإن بيانات المرور قد تكون موزعة على أكثر من مقدم خدمة واحد لمساهمتهم جميعا في نقل الاتصال، كما قد تكون بيانات المرور، أو بعض من نماذج تلك البيانات مشتركة بين عدة مقدمي خدمات لمشاركتهم في نقل الاتصال لأغراض تجارية أو أمنية أو تقنية.

لاعتبار أن بيانات المرور قد لا تكون بحوزة مقدم خدمة واحد، فإن هذا الأخير لن يكون قادرا لوحده على حل لغز الجريمة، بل لا بد لتحقيق هذا الهدف تضافر جهود كل مقدمي الخدمات الذين ساهموا في عملية نقل الاتصال، وذلك للكشف عن مصدر ونهاية الاتصال، وكل المعلومات المتعلقة بالمرور.

وبشأن هذه المسألة تؤكد المادة 17 من اتفاقية بودابست أنه وفي حال مساهمة أكثر من مقدم خدمة واحد في نقل اتصال معين، فإن التحفظ العاجل على بيانات المرور ينبغي أن يتم من خلالهم جميعا.

[1]- هلالي عبد اللاه أحمد، إتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها المرجع السابق، ص. 214.

ولكن بالرغم من أن هذه المادة تعرضت لفرضية تعدد مقدمي الخدمات في نقل الاتصال، إلا أنها لم تحدد الوسائل التي يمكن بواسطتها تحقيق مثل ذلك التحفظ، تاركة بذلك الأمر للقوانين الداخلية للدول لبيان الطريقة التي تتماشى ونظامها القانوني والاقتصادي.

ولعل من بين وسائل التحفظ العاجل على البيانات في مثل هذه الحالات قيام السلطات المختصة بإصدار أمر عاجل منفصل لكل مقدم من مقدمي الخدمات.

ولكن بسبب الانتقادات التي وجهت لهذا الحل، وخاصة منها تلك المتعلقة بالفترة المستغرقة للحصول على أوامر منفصلة، يفضل جانب من الفقه[1] اللجوء إلى الحصول على أمر واحد، وينطبق هذا الأمر على كل مقدمي الخدمات الذين ساهموا في نقل الاتصال، على أن يبلغ ذلك الأمر العام لمقدمي الخدمات المعنيين بالتعاقب.

وإذا لم يتم الأمر بهذه الطريقة، يتجه ذات الاتجاه الفقهي إلى صدور أمر واحد بالتحفظ العاجل لبيانات المرور لكل مقدمي الخدمات، على أن يطلب من كل مقدم خدمة يصله الأمر إخطار مقدم الخدمة الذي يليه بوجود أمر التحفظ وبمضمونه.

انطلاقا مما تقدم، يتبين أن التحفظ العاجل لبيانات المرور يختلف عن التحفظ العاجل على مضمون البيانات الذي نصت عليه المادة 1/16 من ذات الاتفاقية، ذلك أن الإجراء الأول يقتصر فيه التحفظ على البيانات المتعلقة بالاتصال من حيث مصدرها، وقتها، مرسلها، مستقبلها، والمساهم في عملية نقلها، دون أن يشمل محتوى البيانات، وهو الغرض من الإجراء الثاني[2].

ولما كان التعرض لهذا الإجراء الحديث قد ورد بهذا الشكل في ظل اتفاقية بودابست، فالملاحظ أن المشرع الجزائري هو الآخر حاول اللحاق بمصاف الدول المتقدمة، واستحدث هذا الإجراء بموجب قانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، إذ خصص له المادة 11 التي وردت في إطار

[1]- هلالي عبد اللاه أحمد، إتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها المرجع السابق، ص. 216.
[2]- بوعناد فاطمة زهرة، المرجع السابق، ص. 178.

الفصل الرابع المتعلق بالتزامات مقدمي الخدمات، ولكن قبل التعرض للإجراء الخاص بالتحفظ العاجل للمعطيات المتعلقة بحركة السير، ينبغي الإشارة إلى أن المشرع الجزائري عرف في المادة 2/هـ من القانون آنف الذكر[1] المحل الذي يرد عليه الإجراء، وهو المعطيات المتعلقة بحركة السير، وبين طوائف المعطيات المتعلقة بالمرور حين ذكر أن المعطيات المتعلقة بحركة السير هي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا من حركة الاتصال توضح مصدر الاتصال، الوجهة المرسل إليها، الطريق الذي يسلكه، وقت وتاريخ وحجم ومدة الاتصال ونوع الخدمة.

بهذا يكون المشرع الجزائري قد اتبع منهجية منطقية إذ بعدما عرف ما يرد عليه إجراء التحفظ انتقل إليه كإجراء في المادة 11، فألزم مقدمي الخدمات بحفظ المعطيات التي تسمح بالتعرف على مستعملي الخدمة، المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال، الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال، المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها، المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال، وكذا عناوين المواقع المطلع عليها، وهذا كله مع مراعاة طبيعة ونوع الخدمات[2].

وقد اعتبر المشرع الجزائري أن مدة حفظ تلك المعطيات مقدر بسنة واحدة ابتداء من تاريخ التسجيل[3]، ولأهمية تلك البيانات رتب جزاءات على عدم احترام مقدم الخدمة

---

[1]- المادة 2/هـ من القانون 04/09 المؤرخ في 5 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، سالف الإشارة إليه.

[2]- تنص المادة 11 من القانون 09-04 المؤرخ في 5 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، سابق الإشارة إليه على ما يلي: «مع مراعاة طبيعة ونوعية الخدمات يلتزم مقدمو الخدمات بحفظ:

أ- المعطيات التي تسمح بالتعرف على مستعملي الخدمة،

ب- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال،

ج- الخصائص التقنية، وكذا تاريخ ووقت ومدة كل اتصال،

د- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها،

هـ -المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال، وكذا عناوين المواقع المطلع عليها.

بالنسبة لنشاطات الهاتف، يقوم الفاعل بحفظ المعطيات المذكورة في الفقرة "أ" من هذه، وكذا تلك التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه».

[3]- تنص المادة 3/11 من القانون 09-04 المؤرخ في 5 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، سابق الإشارة إليه: «تحدد مدة حفظ المعطيات المذكورة في هذه المادة بسنة واحدة ابتداء من تاريخ التسجيل».

الالتزامات الملقاة على عاتقه فقرر إلى جانب المسؤولية الإدارية له، مسؤولية جزائية، في حال ما ترتب على أعماله عرقلة حسن سير التحريات القضائية، وقد اختلفت العقوبات الجزائية بحسب ما إذا كان مقدم الخدمة شخصا طبيعيا أم معنويا، فإذا كان شخصا طبيعيا كانت العقوبة المسلطة عليه إلى جانب العقوبة السالبة للحرية، والمتراوحة بين حديها الأدنى ستة أشهر والأقصى خمس سنوات، وغرامة مالية متراوحة ما بين 50.000 دج إلى 500.000 دج، في حين إذا كان مقدم الخدمة شخصا معنويا فإن العقوبة المقررة له هي الغرامة المحددة، وفقا للقواعد العامة لقانون العقوبات[1].

البند الثالث: الأمر بتقديم بيانات معلوماتية.

الأمر بتقديم بيانات معلوماتية إجراء جديد استوجبته التشريعات الحديثة، وهو من وسائل البحث والتحري الأقل تطفلا وتدخلا للحصول على المعلومات الضرورية للتحقيقات والتحريات الجنائية، وهو إجراء يرمي إلى تجاوز الدول القيام بإلزام الطرف الثالث أو ما يعرف بالأغيار لتقديم المعلومات بطريقة إجبارية من خلال القيام بعمليات التفتيش، وضبط البيانات[2].

وعليه فالأمر بتقديم بيانات الحاسب أو البيانات المعلوماتية إجراء مرن يُسمح للسلطات الجبرية بأن تضعه موضع التنفيذ في الحالات التي لا يكون من الضروري فيها اللجوء لإجراءات أكثر جبرا أو أكثر كلفة، وهو إجراء يسمح لحائز البيانات بمساعدة السلطات لمكافحة الإجرام المعلوماتي ومد يد العون لهم.

[1]- تنص المادة 4/11 من القانون 09- 04المؤرخ في 5 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، سابق الإشارة إليه: «دون الإخلال بالعقوبات الإدارية المترتبة على عدم احترام الالتزامات المنصوص عليها في هذه المادة، تقوم المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية، ويعاقب الشخص الطبيعي بالحبس من ستة (6) أشهر إلى خمس (5) سنوات، وبغرامة من 50.000 دج إلى 500.000 دج.
يعاقب الشخص المعنوي بالغرامة وفقا للقواعد المقررة في قانون العقوبات».

[2]- هلالي عبد اللاه أحمد، إتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها، المرجع السابق، ص. 224.

بمقتضى هذا الميكانيزم الحديث يكون للسلطات المختصة في البلد إصدار أمر إلى أي شخص موجود داخل أراضيها لتقديم بيانات معلوماتية معينة مخزنة، ويمكن أن يصدر هذا الأمر إلى مقدم الخدمة المتواجد على أراضيها، ليلتزم هذا الأخير بإرسال بيانات المشترك[1].

لأهمية هذا الإجراء، نظمته المادة 18 من الاتفاقية الأوروبية بحيث ألزمت بمقتضى الفقرة الأولى منها الدول على القيام بمناشدة سلطاتها المختصة حتى تلزم شخصا داخل أراضيها بتقديم بيانات معلوماتية معينة مخزنة، أو أن تلزم مقدم خدمات موجود على أراضي الدول الأطراف بأن يرسل لها بيانات المشترك[2].

ويستوي في البيانات المطلوب تقديمها أن تكون بيانات متعلقة بالمحتوى أو بخط السير، المهم أن تكون بيانات مخزنة أو موجودة، وعليه لا ينصرف فحوى البيانات إلى تلك التي لم توجد بعد كبيانات المرور، أو المحتوى المرتبطة بالاتصالات المستقبلية[3].

بهذا يبدو أن إصدار الأمر بتقديم البيانات إجراء كغيره من الإجراءات السابقة يصدر عن سلطة مختصة في الدولة، وينفذ من قبل أشخاص يكون في حيازتهم أو تحت سيطرتهم بيانات مخزنة داخل منظومة الكمبيوتر، أو في دعامة تخزين المعلومات، وعليه يمكن القول أن الأمر يصدر لصاحب الحيازة المادية للبيانات ولصاحب السيطرة، ولو لم يحز البيانات حيازة مادية[4].

---

[1]- بوعناد فاطمة زهرة، المرجع السابق، ص. 182.

[2]- Art 18 al 1 du convention sur la cybercriminalité dispose que : « Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner :
a. à une personne présente sur son territoire de communiquer les donner informatiques spécifiées, en la possession ou sous le contrôle de cette personne, et stockées dans un systèème informatique ou un support de stockage informatique ; et
b. à un fournisseur de services offfrant des prestations sur le territoire de la Parties, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services . »

[3]- هلالي عبد اللاه أحمد، إتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها، المرجع السابق، ص. 224.

[4]- رامي متولي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق، ط1، دار النهضة العربية، القاهرة، مصر، 2011، ص. 128.

لتحقيق هذه الأغراض فإنه يتوجب بمقتضى البند (أ) من الفقرة الأولى من هذه المادة، على كل طرف أن يتأكد أن سلطاته الجبرية المختصة تملك سلطة إصدار الأمر بتقديم المعلومات لشخص موجود على أرضها، ليقوم هذا الأخير بإرسال بيانات إلكترونية معينة مخزنة في نظام معلوماتي يكون في حوزة هذا الشخص أو تحت سيطرته.

وللإشارة فإن مصطلح "في حيازة الشخص أو تحت سيطرته" ينصرف إلى الحيازة المادية للبيانات المعينة داخل حدود هذا البلد، كما أنه يشير إلى الحالات التي تكون فيها البيانات المراد إظهارها خارج الحيازة المادية للشخص، لكن بمقدوره السيطرة عليها بسبب مرورها داخل حدود ذلك البلد.

وعليه لا يندرج في مفهوم السيطرة الوارد في البند 1 من الفقرة أعلاه مجرد القدرة الفنية على الوصول للبيانات المخزنة عن بعد.

إلى جانب البند 1 من الفقرة 1 يتجه البند (ب) من ذات الفقرة إلى إلزام كل دولة لاستحداث سلطة تكون لها إمكانية إصدار أمر تقديم المعلومات لمقدم خدمات يقدم خدماته على أراضي تلك الدولة، وذلك من أجل إرسال البيانات المتعلقة بالمشترك، والتي تكون في حيازة أو تحت سيطرة مقدم الخدمات، وينصرف معنى الحيازة أو السيطرة في هذا البند ليشمل بيانات المشترك التي يحوزها مقدم الخدمات حيازة مادية، ناهيك عن بيانات المشترك المخزنة عن بعد، والتي تكون تحت سيطرة مقدم الخدمة.

ولئن كانت الفقرة 1 من المادة 18 أتاحت للسلطات المختصة في البلد صلاحية إصدار الأمر بتقديم البيانات، إلا أنها كرست في الفقرة 2 منها قدرة القانون الداخلي لكل دولة من أن يستبعد بيانات أو معلومات سرية، كما يمكن أن يتم منح هيئات معينة صلاحية إصدار مثل هذا الأمر، إذ يمكن لكل دولة أن تخول لرجال السلطة العامة صلاحية إصدار أمر تقديم البيانات على أن تكون صلاحياتهم مقتصرة على بيانات المشترك المعروفة للكافة، في حين إذا خرج الأمر عن تلك البيانات، فإن الأمر يستوجب منح إصدار هذا الأمر للمحكمة.

ويمكن في بعض الحالات للدولة المعنية أن تتطلب أو تفرض بمقتضى ضمانات حقوق الإنسان عدم صدور الأمر إلا عن طريق سلطة قضائية، وذلك للحصول على أنواع محددة من البيانات، ويمكن استبعاد هذه الإجراءات في القضايا ذات الخطورة المنعدمة، وذلك استنادا لمبدأ التناسب، أي تناسب الإجراءات المتخذة مع الجرائم المرتكبة[1].

بهذا يلاحظ أن تحديد شروط الأمر بالإنتاج يخضع للقانون الداخلي لكل دولة، وبالمثل يكون لكل منها تحديد نموذج أمر تقديم البيانات، كما يكون لها أن تضع تحديد البيانات الواردة في هذا الأمر، الفترة الزمنية التي يجب خلالها إفشاء البيانات، وكذا النص على وجوب تقديم البيانات التي تم إنشاؤها في شكل نص واحد على الهواء، أو مخرج مطبوع أو في شكل قرص.

استنادا لما تقدم، يمكن القول أن إلزام مقدمي الخدمات بتقديم البيانات المتعلقة بالمشتركين ينصرف حسب الفقرة 3 من ذات المادة[2] ليشمل كل المعلومات التي تتصل بالمشترك وخدماته، وتمت حيازتها بواسطة إدارة مقدم الخدمات على أن لفظ "المشترك" يشمل كل من الشخص الذي يدفع مقابل الخدمة، العميل الذي يدفع مقدما نظير الخدمات التي يستعملها الشخص الذي يستفيد من الخدمات مجانا، في حين ينصرف معنى المعلومات المتعلقة بالمشتركين إلى أنواع مختلفة من المعلومات، إذ قد تكون هذه الأخيرة مرتبطة باستخدام الخدمة، ومستخدم الخدمة.

---

[1]- هلالي عبد اللاه أحمد، إتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها، المرجع السابق، ص. 229.

[2]- Art 18 al 3 du convention sur la cybercriminalité dispose que :" Aux fins du present article, l'expression " données relatives au abonnés" désigne toute information, contenue sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de service et qui se rapport aux abonnés de ses services, autres que des données relatives au traffic ou au contenu, et permettant détablir:

a. le type de service de communication utilize, les dispositions techniques prises à cet égard et la période de service;

b. l'identité, l'adresse postale ou géographique et le numérode telephone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de service;

c. toute autre information relative à l'endroit ou se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de service."

ويندرج ضمن الطائفة الأولى والمتعلقة بالمعلومات الخاصة باستخدام الخدمة كل المعلومات التي يمكن من خلالها التعرف على نوع خدمة الاتصال المستعملة، والفترة التي من خلالها اشترك الفرد في الخدمة، والبنود الفنية المتصلة بها بمعنى الإجراءات المتخذة لتمكين المشترك من الاستفادة من خدمة الاتصال المقدمة، وتشمل هذه البنود على الأخص حفظ رقم أو عنوان تقني كرقم هاتف، عنوان موقع الويب، اسم النطاق، أو عنوان إلكتروني، ناهيك عن تقديم وتسجيل معدات الاتصال المستخدمة بواسطة المشترك كالأجهزة التلفونية، مراكز المكالمات أو الشبكات المحلية.

ولئن كانت هذه المعلومات تخص استخدام الخدمة، فإن المعلومات المتعلقة بمستخدم الخدمة، تشمل كل المعلومات التي يمكن من خلالها تحديد هوية المستخدم، كالعنوان البريدي أو الجغرافي الخاص به، رقم هاتفه أو أي رقم آخر للدخول، البيانات المتعلقة بالفاتورة المرسلة إليه، والمعلومات المتعلقة بطريقة الدفع، وأي معلومات أخرى تتعلق بأداء الخدمة أو بالاتفاق بين المشترك ومقدم الخدمة[1].

فضلا عن ذلك فإن معلومات المشتركين تمتد لتشمل كل المعلومات - ما عدا بيانات المرور والمحتوى- المتعلقة بالموقع أو بالمكان الذي تتواجد فيه تجهيزات الاتصال المتوفرة على أساس عقد أو اتفاقية الخدمة.

الواقع، لا تعد اتفاقية بودابست الاتفاقية الوحيدة التي تعرضت للأمر بإصدار بيانات معلوماتية، بل تعرضت لها كذلك المادة 25 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، وقد وردت أحكامها شبيهة لأحكام المادة 1/18 (أ، ب) من اتفاقية بودابست، حيث ألزمت كل دولة بتبني الإجراءات الضرورية لتمكين سلطاتها المختصة من إصدار الأوامر إلى أي شخص في إقليمها، ليسلم لها هذا الأخير معلومات موجودة في حيازته ومخزنة على تقنية معلومات أو وسيط تخزين معلومات، وقد أشارت هذه المادة كذلك إلى صدور الأمر إلى أي مزود خدمة يقدم خدماته في إقليم الدولة الطرف في الاتفاقية، ليقوم هو

[1]- بوعناد فاطمة زهرة، المرجع السابق، ص. 183.

الآخر بتسليم معلومات المشترك الموجودة بحوزته، أو تحت سيطرته للسلطات المختصة في الدولة[1].

لأهمية هذا الإجراء يلاحظ أن تشريعات بعض الدول عمدت إلى تنظيمه في نصوصها القانونية، وذلك هو شأن القانون الأمريكي المعروف بقانون خصوصية الاتصالات الإلكترونية "ECPA" حيث أجازت لرجال الضبط القضائي الاطلاع على البيانات الموجودة لدى مزودي الخدمات، من خلال تكليف هؤلاء المزودين بتقديم تلك المعلومات، وهو ذات الأمر الذي نص عليه القانون الفرنسي رقم 719 لسنة 2000 الخاص بحرية الاتصالات في المادة 9/43 منه[2].

الفرع الثاني: التجميع في الوقت الفعلي لبيانات المرور.

لا ريب في أن قدرة التكنولوجيا المعلوماتية على نقل كميات ضخمة من البيانات -نصوص مكتوبة، صور أو أصوات، صور مرئية- يخول للأشخاص إمكانية ارتكاب جرائم متعددة، وقد تصل هذه الأخيرة إلى غاية بث محتوى غير مشروع، ومن ذلك مثلا بث مواد إباحية طفولية (La panographie enfantine) .

ونظرا لأن علم المعلوماتية يرتكز على معالجة البيانات بوصفها منتجا نهائياً، أو باعتبارها أحد عناصر الوظيفة التشغيلية كتنفيذ البرامج المعلوماتية، فإن كل تدخل في تلك البيانات قد يكون له نتائج وخيمة على حسن وظيفة النظم المعلوماتية في حالة البث غير المشروع لمواد إباحية طفولية، وكذا في حالة الولوج غير القانوني للنظام المعلوماتي، وهو ما ينجر عنه عرقلة حسن سير وظيفة النظام المعلوماتي، أو الاعتداء على سلامة البيانات الموجودة فيه.

---

[1]- تنص المادة 25 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، سابق الإشارة لها: "تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى:

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 مقدم الخدمة أو تحت سيطرته."

[2]- عائشة بن قارة، المرجع السابق، ص 161؛ حطاب كمال، المرجع السابق، ص. 327.

بهذا يلاحظ أن تجميع بيانات المرور المتعلقة بالاتصالات المعلوماتية له أثر بالغ الأهمية في إجراءات البحث والتحري، بحيث أنه يسمح بتتبع مسار الاتصال بين فاعل الجريمة والضحية[1].

إذ يساهم هذا الإجراء في تسهيل مهمة الجهات القائمة بجمع الأدلة، ويسمح بعمل مقارنات بين ساعة وتاريخ ومصدر ومآل اتصال المشتبه فيه، وساعة التدخلات غير القانونية في نظم الضحايا، كما يمكن من تحديد هوية الضحايا الآخرين، وبيان الروابط الموجودة بين الشركاء الآخرين[2].

لأهمية هذا الإجراء تطرقت له الاتفاقية الأوروبية بمقتضى نص المادة 20، بحيث ألزمت الدول بأن تتيح للسلطات المختصة لديها استخدام الوسائل الفنية التي تسمح لها بجمع أو تسجيل بيانات المرور، كما أنها خولت للسلطات المختصة في الدول الأطراف سلطة إلزام مقدم الخدمة في إطار قدرته الفنية الموجودة على أرضه لجمع أو تسجيل بيانات المرور، أو على الأقل مد يد العون والمساعدة للسلطات المختصة من أجل تجميع البيانات المتعلقة بالمرور، على أن تكون هذه الأخيرة مصحوبة باتصالات معينة منقولة على أرضه عن طريق نظام معلوماتي.

الملاحظ على هذا النص أنه لم يحدد الطرق التكنولوجية الواجب استخدامها من أجل مباشرة عملية التجميع حينما تتم هذه العملية من طرف السلطات المختصة في الدولة، ناهيك عن أن الالتزام المفروض على مقدمي الخدمات لا يتم تطبيقه إلا في حدود عملية التجميع، التسجيل، التعاون، المساعدة، كما أن القيام بالمسائل سالفة الذكر ينبغي أن يكون في حدود الإمكانيات الفنية المتوفرة لدى مقدم الخدمات.

وعليه لا يلزم نص المادة آنفة الذكر مقدمي الخدمات بضمان حيازتهم لإمكانيات فنية لمباشرة عملية التجميع، التسجيل، منح العون والمساعدة، كما لا يفرض عليهم أن يحوزوا

[1]- هلالي عبد اللاه أحمد، إتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها، المرجع السابق، ص. 277.
[2]- بوعناد فاطمة زهرة، المرجع السابق، ص. 187؛ هلالي عبد اللاه أحمد، إتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها، المرجع السابق، ص. 287.

تجهيزات جديدة أو أن يعمدوا إلى الاستعانة بخبراء لمساعدتهم، ولا إلى صرف مبالغ باهظة لمباشرة هذا الإجراء، غير أنه إذا كانت نظمهم المعلوماتية تتوفر على الإمكانيات الفنية اللازمة وكانوا موظفيهم مؤهلين لمباشرة التجميع أو التسجيل في الوقت الفعلي فإنهم يكونون ملزمين باتخاذ الإجراءات الضرورية من أجل استخدام هذه الإمكانيات الفنية.

وعليه إذا كان النظام المعلوماتي لمقدم الخدمة مصمم بطريقة تسمح له بالتجميع أو التسجيل في الوقت الفعلي، أو إذا كانت بحوزته برامج معلوماتية تسمح له بمباشرة التجميع أو التسجيل لبيانات المرور في الوقت الفعلي، فإنه في هذه الحالة يكون ملزما بتشغيل هذه الأجهزة لمساعدة السلطات المعنية.

ما يلاحظ كذلك أن مباشرة هذا الإجراء يطبق على المستوى المحلي فقط، وعليه ينبغي أن تكون الإجراءات المطبقة على تجميع أو تسجيل الاتصالات موجودة على أرض الطرف المعني أو صاحب الشأن، كأن يكون مقدم الخدمة يقيم بعض البنى التحتية أو بعض التجهيزات على هذه الأرض، وتكون تلك البنى والتجهيزات قادرة على القيام بالتجميع أو التسجيل في الوقت الفعلي، ويمتد الأمر ليشمل حالة ما إذا كانت البنى التحتية أو التجهيزات مقامة في موقع آخر غير الموقع الذي يمارس فيه مقدم الخدمة نشاطه الرئيسي، أو مركز شركته، طالما أنها كانت موجودة في أرض الطرف المعني[1].

ولا ريب في أن هذه المادة لا تطبق إلا إذا كان الاتصال قد تم على أرض الدولة المعنية، ويتحقق هذا الأمر إذا كان أحد المتصلين -والذي يمكن أن يكون شخصا طبيعيا، ويمكن أن يكون وسيطا إلكترونيا مؤقتا- متواجدا على أرض الدولة المعنية، و يتحقق الأمر ذاته إذا كان الكيان المادي للحاسب أو معدات الاتصال عن بعد التي يتم من خلالها الاتصال متواجد على هذه الأرض.

باستقراء الأحكام السابق ذكرها، يتبين أن تجميع أو تسجيل بيانات المرور من طرف السلطات المختصة أو من طرف مقدمي الخدمات لا يتم على سبيل التناوب، وعليه إذا لم

[1]- هلالي عبد اللاه أحمد، إتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها، المرجع السابق، ص. 280.

يتوافر لدى مقدم الخدمة الإمكانيات الفنية لمباشرة عملية التجميع أو التسجيل، فإن السلطات المكلفة بتطبيق قانون الدولة صاحبة الشأن هي التي تأخذ على عاتقها القيام بهذه العملية.

ناهيك عن أن إجبار مقدم الخدمة على مساعدة السلطات المختصة بتجميع أو تسجيل بيانات المرور لن يكون له أي معنى، إذا لم يكن باستطاعة تلك السلطات أن تباشر بنفسها مهمة تجميع أو تسجيل تلك البيانات.

كما أنه في حالة الشبكات المحلية التي لا يوجد بها مقدم خدمة، فإن تجميع أو تسجيل البيانات يكون من خلال قيام السلطات المختصة نفسها بمباشرة هذه المهمة.

ما ينبغي الإشارة إليه أن هذا الالتزام المزدوج يثير صعوبات عملية بالنسبة لبعض الدول، ذلك أن السلطات المختصة بالقيام بهذه الإجراءات لا يمكنها اعتراض بيانات نظم الاتصال عن بعد، إلا من خلال مساعدة مقدم الخدمة، وبعلم مقدم الخدمة قد تنتفي السرية المحاطة بالعملية.

ولا شك في أن عملية التجميع في الوقت الفعلي لبيانات المرور لا تكون فعالة إلا إذا تمت دون علم الأشخاص محل التحقيق والتحري، وعليه فإنه يقع لزاما على عاتق مقدمي الخدمات الحفاظ على السرية، وذلك لضمان تمام الإجراء بصفة فعالة.

ولئن كانت الأحكام السابقة تحدد الملتزم بإجراء التجميع أو التسجيل في الوقت الفعلي لبيانات المرور، فإنه ينبغي الذكر أن الفقرة 3 من ذات المادة تنشئ التزاما على عاتق الدول المعنية بتبني الإجراءات التشريعية أو أية إجراءات أخرى يرون أنها ضرورية لإلزام مقدمي الخدمات على الحفاظ على بيانات المرور في الوقت الفعلي، وكل المعلومات المتعلقة بهذا الموضوع، وهذا الإجراء يضمن إلى جانب سرية التحري والتقصي إعفاء مقدم الخدمة من أي التزام عقدي أو قانوني بإعلام المشتركين بأن البيانات الخاصة بهم يتم تسجيلها.

بهذا الإجراء يتم ضمان سرية الأمر بتقديم بيانات المرور في الوقت الفعلي وفقا للأحكام القانونية الواردة بالقانون الداخلي، كما يسمح بتتبع الأشخاص الذين يساعدون الجناة

بإعلامهم بموضوع الإجراء ليتم بسبب هذا الإخطار محاكمتهم عن تهمة تعطيل حسن سير العدالة، ولعله من الأفضل أن يتم تقرير جزاء فعال يطبق في حالة انتهاك إفشاء قاعدة السرية هذه.

والجدير بالذكر أنه حينما يتم وضع الأحكام القانونية التي يتم من خلالها ضمان سرية إجراء التجميع أو التسجيل في الوقت الفعلي لبيانات المرور، فإنه لا بد أن يتم تحديد المدة القصوى المعقولة للالتزام الملقى على عاتق مقدم الخدمة حين القيام بإجراء التجميع أو التسجيل.

أمام حساسية إجراء التجميع أو التسجيل في الوقت الفعلي لبيانات المرور، ونظرا لمساس هذا الإجراء بحق الشخص في احترام حياته الخاصة، سيما إذا تجاوز تجميع بيانات المرور المتعلقة بساعة، مدة أو حجم الاتصال ليصل إلى مصدر ومآل الاتصال، تلزم الاتفاقية الدول عند تنظيمها لهذا الإجراء أن تضع في الحسبان كل الاعتبارات السابقة[1].

استنادا لما تقدم، يتبين أن إجراء التجميع الفوري لبيانات المرور المنظم بمقتضى أحكام المادة 20 من اتفاقية بودابست، يختلف عن إجراء التحفظ العاجل لبيانات المرور الوارد ذكره في المادة 17 من ذات اتفاقية، ذلك أن البيانات في حالة التحفظ تكون مخزنة لدى مقدم الخدمة بالنظام المعلوماتي للحاسب الآلي أو أحد ملحقاته، في حين لا تكون البيانات في حالة التجميع في الوقت الفعلي مخزنة بعد، إذ يسمح هذا الإجراء بجمعها وتخزينها مباشرة وقت الاتصال[2].

الفرع الثالث: مراقبة الاتصالات الإلكترونية.

إن قدرة تكنولوجيا المعلومات على نقل كميات ضخمة من البيانات، سمح لها بتقديم إمكانيات واسعة لارتكاب جرائم متعددة، وغالبا ما تأخذ هذه الأخيرة شكل بث محتوى غير قانوني.

[1]- هلالي عبد اللاه أحمد، إتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها، المرجع السابق، ص. 284.
[2]- حطاب كمال، المرجع السابق، ص. 328.

ونظرا لأن ارتكاب العديد من الجرائم المعلوماتية يفترض نقل البيانات أو الاتصال بها قصد الانضمام بطريقة غير قانونية لنظام معلوماتي أو بث فيروسات معلوماتية، فقد أضحى الكشف عن الطبيعة الضارة وغير القانونية لهذه الأفعال لا يتحقق إلا عن طريق مراقبة الاتصالات الإلكترونية[1].

ولا ريب من أن هذا الإجراء الحديث من الإجراءات التي كشف عنها التطور التكنولوجي، إذ أفرز هذا الأخير أجهزة مراقبة ذات تقنية عالية، وإمكانيات خارقة تلتقط حديث الشخص دون أن يشعر، ويستوي أن يكون الحديث قد تم بطريق وسائل الاتصال الكلاسيكية، أو بواسطة وسائل الاتصال الحديثة، والتي يتربع على عرشها شبكة الإنترنت[2].

إن هذه المعادلة الصعبة أدت إلى تداخل المفاهيم الراسخة، فمن ناحية نجد حق الشخص في الخصوصية والذي يكون محل تهديد بسبب تطور الوسائل التكنولوجية، خاصة وأن هذه الأخيرة قدمت وسائل تسمح بالتصنت على الأحاديث، ومن ناحية أخرى نجد ضرورات الحفاظ على المصلحة العامة واستتباب الأمن لاستقرار المجتمع، وهو الأمر الذي لا يمكن الوصول إليه في ظل التطور التكنولوجي الرهيب إلا عن طريق السماح باللجوء إلى إجراء المراقبة الإلكترونية الذي يساهم في الكشف عن الجرائم والوصول إلى الجاني.

بهذا يبدو أن إعمال التوازن بين حق المجتمع في كشف حقيقة الجرائم، وبين حق الشخص في الخصوصية لا يتحقق إلا عن طريق تقرير شرعية مراقبة الاتصالات الإلكترونية بصورة استثنائية، على أن يكون هذا الإجراء منظم بمقتضى قانون يعمل جاهدا على إقامة ذلك التوازن، من خلال تحديده للحالات التي تجوز فيها المراقبة مع تبيانه للضوابط الواجب احترامها للحيلولة دون التعسف في استعمال هذا الإجراء الجديد، فضلا عن تحديد الجزاءات المقررة في حالة مخالفة القواعد القانونية المنظمة للمراقبة الإلكترونية[3].

---

[1]- هلالي عبد اللاه أحمد، إتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها، المرجع السابق، ص.289.

[2]- بوعناد فاطمة زهرة، المرجع السابق، ص. 188.

[3]- ياسر الأمير فاروق، مراقبة الأحاديث الخاصة في الإجراءات الجنائية، ط1، دار المطبوعات الجامعية، الإسكندرية، مصر، 2009، ص. 22.

لأهمية هذه المسألة سيتم التعرض لها بالنظر إلى مفهوم الاتصالات الإلكترونية **(البند الأول)**، ثم تحديد الضوابط الواجب إعمالها لتقرير مشروعيتها **(البند الثاني)**.

البند الأول: مفهوم مراقبة الاتصالات الإلكترونية.

نظرا لحداثة الإجراء محل الدراسة، لم يتفق الفقهاء والباحثون بعد على تسمية محددة له، إذ يتجه بعض الفقه[1] إلى تسميته بمراقبة المحادثات وتسجيلها، في حين يطلق عليه البعض الآخر[2] مصطلح التصنت على المحادثات الخاصة وتسجيلها، واستخدم فقهاء آخرون تسمية التصنت والرقابة الإلكترونية، في حين عبر عنه البعض بمصطلح التصنت والتسجيل الإلكتروني، واتجه فقه آخر إلى التعبير عنه بمصطلح المراقبة الإلكترونية أو استراق السمع الإلكتروني.

والحقيقة أن كل هذه المصطلحات تعرضت للنقد، بحيث عيب على مصطلح مراقبة المحادثات وتسجيلها، ومصطلح التصنت على المحادثات الخاصة وتسجيلها عدم شموليتهما، كون أن كلمة المحادثات تعني في اللغة تبادل الحديث بين شخصين أو أكثر، وهو ما يجعل من التسمية قاصرة على هذا الحديث دون غيره من الحديث الفردي الذي يصدر من صاحبه ليسجله بنفسه، كما انتقد مصطلح التصنت والرقابة الإلكترونية، ومصطلح التصنت والتسجيل الإلكتروني لعدم قدرتهما على توضيح محل الإجراء[3].

إن تعدد المصطلحات الفقهية لهذا الإجراء انعكس على الناحية التشريعية، فبرزت تسميات متعددة للدلالة عليه، بحيث استعمل المشرع الأمريكي في المادة 4/2510 من قانون الجرائم والإجراءات الجنائية الأمريكي عبارة الاعتراض للتعبير عن عملية مراقبة الاتصالات الإلكترونية، وهو المصطلح ذاته الذي أوردته المادة 21 من الاتفاقية الأوربية

[1]- عوض محمد عوض، المبادئ العامة في قانون الإجراءات الجنائية، د.ط، دار المطبوعات الجامعية، القاهرة، 1999، ص 403. مشار إليه من طرف، بوعناد فاطمة زهرة، المرجع السابق، ص. 189.

[2]- أحمد عوض بلال، قاعدة استبعاد الأدلة المتحصلة بطريقة غير مشروعة، د.ط، دار النهضة العربية، القاهرة، مصر، سنة 1994، ص 311.

[3]- بوعناد فاطمة زهرة، المرجع السابق، ص. 189.

لمكافحة الجرائم الإلكترونية، وكذا المادة 29 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

وللإشارة فإن مصطلح اعتراض البيانات الإلكترونية المتعلقة بالمحتوى مصطلح لا يخلو من النقد، سواء من الناحية اللغوية أو العملية، فمن الناحية اللغوية ترد هذه العبارة بمعنى صار عارضا له أي مانعا له، وهو ما يعني من الناحية العملية أنه ينبغي أن يتم اعتراض المحادثة وقطع الطريق عنها، في حين أن أنظمة المراقبة لا تؤثر في محتوى ووجه الاتصال المراقب، وإنما تقوم فيه بالتصنت، وعليه فإن استعمال عبارة الالتقاط يكون أكثر اتفاقا مع الآلية المقدمة للمراقبة[1].

ويعرف الاعتراض بأنه معرفة محتوى اتصال قد يتم داخل نظام حاسب آلي واحد، أو بين نظامين مختلفين، أو بين عدة أنظمة ترتبط فيما بينها من خلال شبكة اتصالات، وذلك بالتقاط المعلومات التي يتضمنها هذا الاتصال، وتعتبر الموجات الكهربائية الصادرة عن الحاسب الآلي الوسيلة الأساسية للاعتراض، وتعرف في الولايات المتحدة الأمريكية باسم التقاط الموجات الكهربائية، وهي جمع معلومات يتم إرسالها من خلال نظام الحاسب الآلي داخل مبنى، وذلك باستعمال شاشة عرض يتم توصيلها بجهاز تسجيل خارج المبنى، لتقوم الشاشة بالتقاط الموجات الكهربائية التي تحيط بالحاسب الآلي، فتحولها إلى معلومات مقروءة على الشاشة من ناحية، كما يتم تسجيلها من ناحية أخرى[2].

ما يلاحظ أن المشرع الجزائري استحدث بموجب المادة 3 من قانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها مصطلح مراقبة الاتصالات الإلكترونية، واعتبرها إجراء يهدف إلى تجميع وتسجيل محتوى الاتصالات الإلكترونية في حينها.

[1]- بوعناد فاطمة زهرة، المرجع السابق، ص. 191.
[2]- المرجع نفسه، ص. 191.

وعلى هذا يبدو أن مراقبة الاتصالات الإلكترونية[1] إجراء يرد على الاتصالات الإلكترونية حال إجرائها، وهو بهذا إجراء خطير واستثنائي مقرر من أجل التعامل مع الطبيعة الحركية للبيانات التي لا يمكن تفتيشها وضبطها إلا من خلال هذا الإجراء، وذلك بخلاف الاتصالات الإلكترونية المخزنة التي يمكن تفتيشها وضبطها مباشرة إذا كانت مخزنة في الكمبيوتر الخاص بالمستخدم، كما يمكن أن تكون محلا للتحفظ المستعجل إذا كانت مخزنة في الخادم المعلوماتي لمقدم الخدمة.

وقد أكد هذا الطرح المجلس الأوروبي خلال توصياته التي طالبت بالتفرقة بين مراقبة البيانات الإلكترونية المتحركة، وبين تفتيش وضبط البيانات الإلكترونية الساكنة، وعليه لا تعد المراقبة الإلكترونية تفتيشا، بل هي إجراء خاص يبدأ من لحظة التقاط الاتصال الإلكتروني من خلال الأجهزة والتقنيات المعدة لهذا الغرض، وتنتهي بمجرد وصول المحادثة أو المراقبة إلى حيازة الجهة المراقبة[2].

ويرى جانب من الفقه أن المراقبة الإلكترونية عمل أمني أساسي له نظام معلومات إلكتروني، يقوم فيه المراقِب بمراقبة المراقَب بواسطة الأجهزة الإلكترونية، وعبر شبكة الإنترنت لتحقيق غرض محدد، وتحرير تقارير بالنتيجة المتوصل لها[3].

البند الثاني: الضوابط الواجب توفرها لإجراء مراقبة الاتصالات الإلكترونية.

لقد سبق الذكر أن مراقبة الاتصالات الإلكترونية إجراء حديث من إجراءات البحث والتحري، ومن خلاله يتم جمع البيانات المتعلقة بمحتوى الاتصالات وتحديد الطابع غير المشروع لها، وينصرف معنى البيانات المتعلقة بالمحتوى لكل محتوى إخباري بمعنى لكل اتصال أو رسالة أو معلومة منقولة بواسطة الاتصال غير بيانات المرور[4].

---

[1]- عرفت المادة 2/ و من قانون 09-04 المؤرخ في 5 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، سابق الإشارة إليه. الاتصالات الإلكترونية بأنها: «أي تراسل أو إرسال واستقبال علامات، أو إشارات وكتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية».

[2]- بوعناد فاطمة زهرة، المرجع السابق، ص. 192.

[3]- مصطفى محمود موسى، المراقبة الإلكترونية عبر شبكة الإنترنت (دراسة مقارنة)، سلسلة اللواء الأمنية في مكافحة الجريمة الإلكترونية، الكتاب الخامس، دار الكتب القانونية، القاهرة، 2005، ص. 192.

[4]- هلالي عبد اللاه أحمد، إتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها،المرجع السابق، ص. 290.

لأهمية هذا الإجراء نظمت أحكامه الاتفاقية الأوربية لمكافحة الجريمة المعلوماتية في المادة 21 منها[1]، حيث ألزمت كل دولة طرف في الاتفاقية أن تتبنى الإجراءات التشريعية أو أية إجراءات أخرى تراها ضرورية لتخويل سلطاتها المختصة استخدام وسائل فنية موجودة على أرضها لجمع أو تسجيل البيانات المتعلقة بالمحتويات، كما أنها خولت السلطات المختصة لديها صلاحية إلزام مقدم الخدمة في إطار إمكانياته الفنية المتوافرة استخدام وسائل فنية موجودة على أرضه لجمع أو تسجيل البيانات المتعلقة بالمحتوى، أو على الأقل مساعدة السلطات المختصة من أجل جمع أو تسجيل في الوقت الفعلي البيانات المتعلقة بالمرور مصحوبة باتصالات معينة منقولة على أرضه عن طريق نظام معلوماتي.

بهذا يلاحظ أن الهيئات المختصة بتجميع أو تسجيل البيانات المتعلقة بالمحتوى تكمن إما في السلطات المختصة في الدولة، وإما في مقدم الخدمة، وللإشارة فإن هذا الأخير يكون ملزما بتجميع أو تسجيل تلك البيانات، كما قد يكون مكلفا فقط بمد يد العون والمساعدة للسلطة المختصة.

استنادا لما تقدم، يتبين أنه لا يمكن تطبيق الالتزام المفروض على عاتق مقدمي الخدمات، سواء تعلق الأمر بعملية التجميع أو التسجيل أو التعاون والمساعدة، إلا في حدود الإمكانيات المتوفرة لديه.

وعليه فإن مقدم الخدمة لا يكون ملزما بحيازة إمكانيات فنية لمباشرة عملية التجميع أو التسجيل أو منح المساعدة والعون، كما أنه لا يكون ملزما بحيازة تجهيزات جديدة للقيام

[1]- Art 21 al 1 du convention sur la cybercriminalité dispose que : « Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes relativement à un éventail d'infractions graves à définir en droit interne,à :
a. collecter ou à enregistrer par l'application de moyens techniques existany sur son territoire ; et
b. obliger un fournisseur de services, dans le cadre de ses capacités téchniques existantes, à :
1. collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou
2. préter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer ;
En temps réel, les données relatives au contenu de communications spécifiques sur son territoire, transmises au moyen d'un système informatique. »

بالمسائل السالفة الذكر، فمقدم الخدمة يقدم خدماته في حدود الإمكانيات الفنية المتوفرة لديه، فإن كانت لديه الإمكانيات ساهم في عملية التجميع أو التسجيل أو مد يد العون والمساعدة، وإلا فإن القيام بعملية اعتراض البيانات المتعلقة بالمحتوى تبقى على عاتق السلطة المختصة في الدولة.

ولا ريب في أن هذا الإجراء يطبق على تجميع أو تسجيل الاتصالات المحددة على أرض الطرف المعني أو صاحب الشأن، بحيث ينبغي أن يقيم مقدم الخدمة بعض البنى التحتية أو بعض التجهيزات على هذه الأرض، كما يكون في الإمكان تطبيق تلك الإجراءات التشريعية ولو كانت البنى التحتية أو التجهيزات مقامة في موقع آخر غير الموقع الذي يمارس فيه مقدم الخدمة نشاطه الرئيسي أو مركز شركته، طالما أنها كانت موجودة في أرض الدولة الطرف في الاتفاقية.

إن هذا الالتزام المزدوج يثير صعوبات جمة، كون أن السلطات المكلفة بتطبيق القانون لا يمكنها اعتراض بيانات نظم الاتصال عن بعد إلا من خلال مد يد العون لها من طرف مزود الخدمة، وهو الأمر الذي يحتم معرفة هذا الأخير بإجراء المراقبة، أو كما سمته الاتفاقية إجراء الاعتراض.

في ظل هذا الوضع، فإنه ينبغي الإشارة إلى أنه إذا كان بإمكان أي دولة بسبب المبادئ المنصوص عليها في قانونها تمكنها بدلا من أن تلزم السلطات المختصة بالتجميع أو التسجيل أن تتبنى طريقة أخرى، كأن تلزم مقدم الخدمة بإعداد التجهيزات الفنية اللازمة لتقوم السلطات المكلفة بتطبيق القانون بعملية الاعتراض، وفي مثل هذه الحالة فإن كل القيود الأخرى المتعلقة بالأرض، بخصوصية الاتصالات، استعمال الطرق الفنية تظل قابلة للتطبيق.

ما ينبغي ذكره في هذا السياق أن إجراء الاعتراض في الوقت الفعلي للبيانات المتعلقة بالمحتوى لا يكون له أي فعالية، إلا إذا تم دون علم الأشخاص محل البحث والتحري، ونظرا لأن عملية الاعتراض سرية بطبيعتها، فإنه يتوجب على مقدمي الخدمات وموظفيهم الحفاظ

على السرية حتى يتم هذا الإجراء بطريقة فعالة، ولضمان سرية هذه العملية فإنه يكون لكل دولة طرف في الاتفاقية تبني الإجراءات التشريعية أو أية إجراءات أخرى تراها ضرورية من أجل إلزام مقدم الخدمات بالمحافظة على سرية العملية[1]، وهو الأمر الذي يضمن إلى جانب سرية البحث والتحري، إعفاء مقدم الخدمة من كل التزام تعاقدي أو قانوني بإعلام مشتركيه بأن الاتصالات الإلكترونية التي يجرونها محل مراقبة.

من جهة أخرى أشارت الاتفاقية إلى الإمكانية المخولة لكل دولة طرف لضمان إجراء المراقبة وفقا للأحكام القانونية في قانونها الداخلي، وذلك عن طريق سلطة تتبع الأشخاص الذين يساعدون الجناة بإعلامهم بإجراء المراقبة ومحاكمتهم بتهمة تعطيل حسن سير العدالة، أو عن طريق تقرير جزاء فعال لانتهاك سرية الإجراء.

بسبب خطورة هذا الإجراء، يلاحظ أن الاتفاقية قصرت إمكانية اللجوء إليه على الجرائم الخطيرة دون سواها.

وفي الواقع، لا تعد الاتفاقية الأوروبية لمكافحة الجرائم المعلوماتية الاتفاقية الوحيدة التي نظمت هذا الإجراء، بل تطرقت له كذلك الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في المادة 29 منها[2]، بحيث أوردت أحكاما مماثلة لسابقتها، فألزمت كل دولة طرف بتبني الإجراءات التشريعية والضرورية فيما يخص الجرائم المنصوص عليها في القانون الداخلي لديها لتمكين سلطاتها المختصة من جمع أو تسجيل المعلومات المتعلقة بالمحتوى، وذلك من خلال الوسائل الفنية المتوافرة لديها، كما وألزمت مقدمي الخدمات

[1]- Art 21 al 3 du convention sur la cybercriminalité dispose que : « Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaire pour obliger un fournisseur de services à garder secrets le fait que l'un quelque des pouvoirs prévus dans le présent article a été exécuté, ainsi que toute information à ce jujet. »

[2]- تنص المادة 1/29 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، سابق الإشارة لها:" تلتزم كل دولة طرف بتبني الإجراءات التشريعية والضرورية فيما يختص بسلسلة من الجرائم المنصوص عليها في القانون الداخلي، لتمكين السلطات المختصة من:

أ- الجمع أو التسجيل من خلال الوسائل الفنية على إقليم تلك الدولة الطرف، أو

ب- التعاون ومساعدة السلطات المختصة في جمع أو تسجيل معلومات المحتوى بشكل فوري للإتصالات المعنية في إقليمها والتي ثبت بواسطة تقنية المعلومات".

بالتعاون مع السلطات المختصة ومساعدتها لجمع أو تسجيل المعلومات المتعلقة بالمحتوى بشكل فوري للاتصالات المعنية في إقليمها، والتي تم بثها بواسطة تقنية المعلومات.

وأشارت المادة ذاتها في الفقرة الثانية منها إلى الإمكانية المخولة للدولة الطرف لتبني إجراءات أخرى ضرورية لضمان الجمع أو التسجيل الفوري لمعلومات المحتوى المرافقة للاتصالات، وذلك باستخدام الوسائل الفنية في ذلك الإقليم، وهذا كله يتقرر في حالة عدم قدرة الدولة الطرف في الاتفاقية على تبني الإجراءات المنصوص عليها في الفقرة 1- أ، وذلك بسبب النظام القانوني الداخلي لديها[1].

إلى جانب هذه المسائل، أكدت الفقرة 03 من ذات المادة على التزام كل دولة طرف باتخاذ الإجراءات الضرورية لإلزام مزود الخدمة بالاحتفاظ بسرية أية معلومة، وذلك عند تنفيذه للصلاحيات المنصوص عليها في هذه المادة[2].

إذا كانت هذه هي الأحكام التي استوجبتها الاتفاقية الأوروبية، وكذا الاتفاقية العربية لسلامة إجراء مراقبة الاتصالات الإلكترونية، فإنه يتوجب الذكر أن المشرع الجزائري هو الآخر عمد إلى تنظيم هذا الإجراء، بحيث سمح باللجوء إليه بمقتضى أحكام المادة 1/4 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها للوقاية من الأفعال الموصوفة بجرائم الإرهاب، التخريب أو الجرائم الماسة بأمن الدولة، وكذا في حالة توافر معلومات عن احتمال وقوع اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، وقد وسّع المشرع حالات اللجوء إلى إجراء المراقبة الإلكترونية كلما استلزمت مقتضيات التحريات والتحقيقات القضائية ذلك، كون أنه لا يمكن الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى هذا الإجراء.

---

[1]- تنص المادة 29 /2 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، سابق الإشارة لها: "إذا لم تستطع الدولة الطرف بسبب النظام القانوني الداخلي تبني الإجراءات المنصوص عليها في الفقرة (1- أ) فيمكنها تبني إجراءات أخرى بالشكل الضروري لضمان الجمع والتسجيل الفوري لمعلومات المحتوى المرافقة للاتصالات المعنية في إقليمها باستخدام الوسائل الفنية في ذلك الإقليم."

[2]- تنص المادة 29 /3 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، سابق الإشارة لها: "تلتزم كل دولة طرف باتخاذ الإجراءات الضرورية لإلزام مزود الخدمة بالإحتفاظ بسرية أية معلومة عند تنفيذ الصلاحيات المنصوص عليها في هذه المادة."

ولم يقتصر الأمر على ذلك، بل سمح باستخدام هذا الإجراء في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة[1].

لخطورة إجراء مراقبة الاتصالات الإلكترونية، منح المشرع الجزائري بمقتضى الفقرة 02 من المادة 04 من قانون 09-04 السالفة الذكر للسلطة القضائية المختصة صلاحية إصدار إذن مكتوب لمباشرة هذا الإجراء[2]، كما وخول للنائب العام المتواجد بمجلس قضاء الجزائر صلاحية منح ضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها لمباشرة إجراء المراقبة الإلكترونية، كما ويلاحظ أنه خول بموجب المادة 22 من المرسوم الرئاسي 15-261 المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال للللهيئة ذاتها إمكانية وضع وحدة مراقبة واحدة أو أكثر مزودة بالوسائل والتجهيزات التقنية

---

[1]- تنص المادة 1/4 من قانون 09-04 المؤرخ في 5 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال ومكافحتها، سابق الإشارة إليه: " يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 3 أعلاه في الحالات الآتية:
أ- للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة،
ب- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الإقتصاد الوطني،
ج- لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية،
د- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة."

[2]- إذا كان الأصل العام عدم جواز إجراء مراقبة الاتصالات الالكترونية إلا بإذن قضائي مسبق، إلا أن هناك حالات تجوز فيها المراقبة دون صدور إذن، وفي هذا يلاحظ أن بعض التشريعات ومنها القانون الأمريكي تسمح بوضع أجهزة لتسجيل الاتصالات الإلكترونية في حالة الضرورة إذا توافر خطر حال، وما دام قد توافر من الأسباب ما يدعو إلى الاعتقاد بأن الإذن سوف يصدر، فإن لم يصدر الإذن بعدها خلال مدة 48 ساعة وجب إنهاء المراقبة فورا.
ويجوز في نصوص القانون الأمريكي لمزودي الخدمات مراقبة الاتصالات الإلكترونية الخاصة بالمشتركين، وذلك في إطار المراقبة المعتادة لحماية أنظمتهم من إساءة استعمالها أو الإضرار بها أو الاستيلاء عليها، ويسمح القانون الأمريكي بالمراقبة بدون إذن لمزودي الخدمات فقط، كما يسمح لهؤلاء المزودين بتسجيل المداخلات والتبليغ عنها لرجال الضبط القضائي، غير أنه لا يجيز لرجال الضبط القضائي المبادرة بهذه المراقبة دون تبليغ من مزودي الخدمات أو حصولهم على إذن مسبق بذلك.
إلى جانب هذه الحالة تجوز المراقبة دون إذن بناء على شكوى المشترك، وهي الحالة التي نص عليها القانون الأمريكي، وتتعلق هذه الحالة بصدور طلب من صاحب الجهاز محل الاعتداء بوضع جهازه تحت المراقبة من قبل رجال الضبط القضائي أو وفق شروط معينة، وتشمل هذه الشروط سماح المالك لرجال الضبط بوضع الجهاز الخاص به تحت المراقبة، حصول ذلك في إطار تحقيق جنائي قائم، توافر دلائل كافية على تسجيل الاتصالات القادمة من الجهاز الصادر منه الاعتداء تفيد في كشف الحقيقة، سعي رجال الضبط على اعتراض الاتصالات الصادرة من وإلى الأجهزة محل التحقيق.
إلى جانب هذه الحالات، هناك حالة ثالثة تتمثل في مراقبة رب العمل للاتصالات الإلكترونية الخاصة بالعاملين لديه، وتتقرر صحة هذا الإجراء لكون الكمبيوتر إحدى أدوات العمل، ويكون لرئيس الإدارة حق مراقبته لما له من صلاحية متابعة أجهزة الموظفين. مشار إليه من طرف، حطاب كمال، المرجع السابق، ص.329 .

الضرورية لتنفيذ عملية مراقبة الإتصالات الإلكترونية، على أن تتكون تلك الوحدة من مستخدمين تقنيين يعملون تحت إدارة ومراقبة قاضي يساعده ضابط واحد من ضباط الشرطة القضائية أو أكثر ينتمي للهيئة، وتحرر الوحدة أشغالها في محضر طبقا للأحكام المعمول بها في قانون الإجراءات الجزائية، كما ويكون بمقتضى المادة 23 من المرسوم الرئاسي السالف الذكر لمسؤول الوحدة اتخاذ التدابير اللازمة أثناء سير العملية، بالإتصال مع المسؤولين المعنيين في الهيئة، وذلك كله لضمان سرية العملية وحماية المعلومات المستقاة من المراقبة.

رغم الأحكام السالفة الذكر يلاحظ أن المشرع الجزائري وبمقتضى قانون 09-04 قَصَرَ صلاحية إصدار الإذن على النائب العام لمجلس قضاء الجزائر في حالات محددة وتشمل الأفعال الموصوفة بجرائم الإرهاب، التخريب والجرائم الماسة بأمن الدولة، لتبقى صلاحية إصدار الإذن في الحالات الأخرى من اختصاص السلطات القضائية.

بهذا يكون المشرع الجزائري قد حدد النطاق الشخصي للمكلف بإصدار الإذن بحيث يترتب على مخالفة الأحكام السالفة الذكر عدم مشروعية إجراء المراقبة[1].

ونظرا لأن إجراء مراقبة الاتصالات الإلكترونية يستوجب صدور الإذن، فلا شك أن هذا الإذن يكون مكتوبا، واستلزام الكتابة أمر في غاية الأهمية، إذ لا يمكن بغير الإذن المكتوب إثبات حصول المراقبة، ناهيك عن أن كتابة الإذن تسمح ببقاء إجراء المراقبة حجة على الكافة، كما وتكون الكتابة أساسا صالحا للنتائج التي بني عليها الإجراء[2].

ما ينبغي الإشارة إليه أن المشرع الجزائري، وإن كان قد ألزم السلطات المكلفة بالتحريات القضائية بإجراء مراقبة الاتصالات الإلكترونية، إلا أنه جعل في الوقت ذاته مقدم الخدمة ملزم بتقديم المساعدة لهذه السلطات لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها، وذلك بحكم ارتباطه العملي بهذه الاتصالات.

[1]- بوعناد فاطمة زهرة، المرجع السابق، ص. 193.
[2]- المرجع نفسه، ص. 194.

ولضمان نجاح العملية ألزم مقدمي الخدمات بكتمان سرية المعلومات التي ينجزونها بطلب من المحققين، وكذا كتمان المعلومات المتصلة بها، وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق، وهو الأمر الذي ورد النص عليه في المادة 10 من قانون 09-04 السالف الذكر[1].

ونظرا لتعدي إجراء مراقبة الاتصالات الإلكترونية على سرية المراسلات والاتصالات، وهو الحق المكفول دستوريا لكل الأشخاص بما فيهم المشتركين في مجال الاتصالات الإلكترونية، عمد المشرع الجزائري بعد تقييده لحق الخصوصية بمقتضى نصوص القانون إلى تقييد إجراء المراقبة بمدة زمنية محددة، وهو الأمر الذي نص عليه بصفة صريحة في الفقرة 03 من المادة 04 حينما منح للنائب العام بمجلس قضاء الجزائر صلاحية إصدار إذن المراقبة لضباط الشرطة القضائية، وجعل الإذن صالحا لمدة ستة (06) أشهر قابلة للتجديد.

للإشارة، فإن المشرع أكد في ذات الفقرة على توجيه الترتيبات التقنية لتجميع وتسجيل المعطيات ذات الصلة للوقاية من الأفعال الإرهابية التخريبية، الأفعال الماسة بأمن الدولة، ورتب على استخدام الترتيبات التقنية لغير هذه الأغراض توقيع العقوبات المنصوص عليها في قانون العقوبات لخروج المكلفين عن نطاق الإذن الموضوعي الممنوح لهم، ولانتهاكهم حرمة الحياة الخاصة بالغير.

استنادا لما تقدم يلاحظ أن المشرع الجزائري لم ينظم كل المسائل المتعلقة بإجراء المراقبة الإلكترونية، وذلك بخلاف المشرع الفرنسي الذي استوجب من الهيئات المعنية بعد الانتهاء من مباشرة عملية المراقبة تحرير محضر ووضع التسجيلات الخاصة بالمراقبة في أحراز مغلقة مع ختمها بالأختام الرسمية المغلقة، كما أجاز إمكانية إتلاف تلك التسجيلات بعد انتهاء التحقيق والمحاكمة، على أن يتم ذلك بناء على طلب المدعي العام في المقاطعة أو

[1]- تنص المادة 3/10 من القانون 09- 04 المؤرخ في 5 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والإتصال ومكافحتها، سابق الإشارة إليه: "ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق."

النيابة العامة[1]، وعليه نهيب بالمشرع الجزائري لاستحداث نصوص قانونية تتعلق بمآل التسجيلات الإلكترونية بعد انتهاء مرحلتي التحقيق والمحاكمة.

الفرع الرابع: اعتراض الاتصالات السلكية واللاسلكية.

يعد اعتراض الاتصالات السلكية واللاسلكية من الإجراءات الحديثة التي نظمها المشرع الجزائري عند تعديله لقانون الإجراءات الجزائية بمقتضى القانون رقم 06-22، وإذا كان هذا الإجراء يتعلق بالمحادثات التي تتم عن طريق الهاتف، إلا أن المشرع الجزائري أجاز لوكيل الجمهورية المختص أن يقوم باللجوء إلى هذا الإجراء في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات[2].

لا ريب في أن استخدام هذا الأسلوب يستلزم تحقق جملة من الشروط، إذ لا يمكن اللجوء إليه إلا بناء على إذن صادر من جهة قضائية مختصة، وبخصوص هذا الشرط يلاحظ اختلاف التشريعات بشأن الجهة المناط إليها إصدار الإذن، إذ تعهد بعض التشريعات بهذه المهمة إلى النيابة العامة، في حين يمنحها البعض الآخر للقضاء، ويجعل البعض الآخر صدور الإذن من اختصاص كل من النيابة العامة والقضاء، في حين تخول قلة من التشريعات صلاحية إصدار الإذن لضباط الشرطة القضائية[3].

وفي هذا الإطار يلاحظ أن المشرع المصري منح صلاحية إصدار الإذن لقاضي التحقيق[4]، أو لرئيس المحكمة الابتدائية[5]، كما أجاز للنيابة العامة في حالة ما إذا كانت تتولى

---

[1]- بوعناد فاطمة زهرة، المرجع السابق، ص. 196.

[2]- تنص المادة 65 مكرر 5 /1 من قانون 06-22 المؤخ في 20 ديسمبر سنة 2006 المعدل ووالمتمم لقانون الإجراءات الجزائية الجزائري، سابق الإشارة إليه: «إذا اقتضت ضرورات التحري في الجرائم المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات... يجوز لوكيل الجمهورية المختص أن يأذن بما يأتي:
- اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية.

[3]- بوعناد فاطمة زهرة، المرجع السابق، ص. 197.

[4]- تنص المادة 95 من ق.إ.ج.م: «لقاضي التحقيق أن يأمر بضبط جميع الخطابات والرسائل والجرائد والمطبوعات والطرود لدى كاتب البريد، وجميع البرقيات لدى مكاتب البرق، وأن يأمر بمراقبة المحادثات السلكية واللاسلكية أو إجراء تسجيلات لأحاديث جرت في مكان خاص، متى كان لذلك فائدة في ظهور الحقيقة في جناية أو جنحة معاقب عليها بالحبس لمدة تزيد على ثلاثة أشهر».

[5]- تنص المادة 95 مكرر من ق. إ.ج.م: «لرئيس المحكمة الابتدائية المختصة في حالة قيام دلائل قوية على مرتكب إحدى الجرائم المنصوص عليها في المادتين 166 مكرر و207 مكرر من قانون العقوبات قد استعان في ارتكابها بجهاز تلفوني معين أمر بناء على تقرير مدير عام مصلحة التلغرافات والتليفونات، وشكوى المجني عليه في الجريمة المذكورة بوضع جهاز التلفون المذكور تحت الرقابة المعدة التي يحددها».

التحقيق بنفسها وتبين لها ضرورة اعتراض المحادثات الهاتفية للمتهم الحصول على إذن من القاضي الجزئي لمراقبة تلك المحادثات[1].

وقد خول المشرع الفرنسي لقاضي التحقيق صلاحية إصدار أمر الاعتراض[2]، بحيث لا يجوز للنيابة العامة أو رجال الضبط القضائي مباشرة إجراء الاعتراض إلا بعد الحصول على إذن من قاضي التحقيق[3].

أما بخصوص المشرع الجزائري، فقد سبق الذكر أنه خول صلاحية إصدار هذا الإذن لوكيل الجمهورية المختص، وذلك استنادا لنص المادة 65 مكرر 05 فقرة 01، وللإشارة فإنه من أجل القيام بالترتيبات التقنية يسمح الإذن المسلم بالدخول إلى المحلات السكنية أو غيرها ولو كان ذلك خارج المواعيد المحددة في المادة 47 من قانون الإجراءات الجزائية، ويستوي في ذلك عدم علم أو عدم رضاء الأشخاص الذين لهم الحق على تلك الأماكن، ولكن يشترط لصحة ما سبق أن تتم العمليات تحت المراقبة المباشرة لوكيل الجمهورية المختص، وهو الأمر الذي نص عليه المشرع صراحة بمقتضى المادة 65 مكرر05 فقرة 02-03.[4]

إن منح وكيل الجمهورية صلاحية إصدار إذن الاعتراض يكون معلقا على حالة عدم فتح تحقيق قضائي، إذ يترتب على فتح مثل هذا التحقيق منح صلاحية إصدار الإذن لقاضي

---

[1]- تنص المادة 206 من ق.إ.ج.م: «لا يجوز للنيابة العامة تفتيش المتهم أو منزل غير منزله إلا إذا اتضح من أمارات قوية أنه حائز لأشياء تتعلق بالجريمة، ويجوز لها أن تضبط لدى مكاتب البريد جميع الخطابات والرسائل والجرائد والمطبوعات والطرود لدى مكاتب البرق، جميع البرقيات، وأن تراقب المحادثات السلكية واللاسلكية، وأن تقوم بتسجيلات لمحادثات جرت في مكان خاص، متى كان لذلك فائدة في ظهور الحقيقة في جناية أو جنحة معاقب عليها بالحبس لمدة تزيد على ثلاثة أشه، ويشترط لاتخاذ أي إجراء من الإجراءات السابقة الحصول على أمر مسبب بذلك من القاضي الجزئي بعد اطلاعه على الأوراق».

[2]- Article 100 C.P.P.F (Modifier par loi n°2016-731 du 3 juin 2016-rt.57) dispose que : « En matière 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 télécommunications. Ces opérations sous autorité et son contrôle.
La décision d'interception est écrite. Elle n'a pas de caractère juridictionnel et n'est pas susceptible d'aucun recours ».

[3]- بوعناد فاطمة زهرة، المرجع السابق، ص. 24.

[4]- تنص المادة 65 مكرر 5 فقرة 2-3 من القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المتضمن قانون الإجراءات الجزائية الجزائري، سابق الإشارة إليه: «... يسمح الإذن المسلم بغرض وضع الترتيبات التقنية بالدخول إلى المحلات السكنية أو غيرها ولو خارج المواعيد المحددة في المادة 47 من هذا القانون، وبغير علم أو رضا الأشخاص الذين لهم حق على تلك الأماكن.
تنفذ العمليات المأذون بها على هذه الأماكن تحت المراقبة المباشرة لوكيل الجمهورية المختص...».

التحقيق، بحيث تتم كل العمليات المذكورة بناء على إذن منه، وتكون تحت مراقبته المباشرة، وذلك طبقا لما كرسته المادة 65 مكرر 05 فقرة 04 من قانون الإجراءات الجزائية[1].

لا شك في أن منح جهة معينة صلاحية إصدار إذن الاعتراض يعني أن هذا الإذن ينبغي أن يكون مكتوبا، وهذا هو الشرط الثاني الذي لا بد من تحققه، إذ لا يجوز أن يصدر الإذن بصورة شفوية، بل يتوجب أن يكون مكتوبا، وأن يكون مبنيا على أسباب معقولة خصوصا حينما يتعلق الأمر بعدم توافر وسائل أخرى يمكن اللجوء إليها لإثبات الجريمة، كما لا بد أن يكون الإذن متضمنا كافة المعلومات الضرورية التي تسمح بالتعرف على نوعية الاتصالات المطلوب التقاطها، الأماكن المقصودة سكنية أو غيرها، كما لا بد أن يتضمن الجريمة التي تبرر اللجوء إلى هذا الإجراء، ومدته، وهو الأمر الذي نظمته المادة 65 مكرر 07 من قانون الإجراءات الجزائية[2].

إن إصدار أمر اعتراض الاتصالات ينبغي أن يكون محددا بمدة زمنية معينة، وهو الشرط الثالث لصحة هذا الإجراء، وفي هذا يلاحظ اختلاف في المدد القانونية المقررة، إذ حددها المشرع المصري بثلاثين يوما قابلة للتجديد لمدة أو لمدد أخرى طبقا لأحكام المادتين 95[3] و206 من قانون الإجراءات الجنائية المصري[4]، في حين حددها المشرع الفرنسي بمدة أربعة (04) أشهر قابلة للتجديد طبقا لنص المادة 100-02 من قانون الإجراءات الجزائية الفرنسي[5]، أما المشرع الجزائري فقد تبنى ذات المدة التي أخذ بها المشرع الفرنسي، فأجاز اللجوء لهذا الإجراء لمدة أقصاها أربعة أشهر قابلة للتجديد، وذلك حسب مقتضيات التحري

---

[1]- تنص المادة 65 مكرر5 فقرة 04 من القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المتضمن قانون الإجراءات الجزائية الجزائري، سابق الإشارة إليه: «في حالة فتح تحقيق قضائي، تتم العمليات المذكورة بناء على إذن من قاضي التحقيق ،وتحت مراقبته المباشرة».

[2]- تنص المادة 65 مكرر 01/07 من القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المتضمن قانون الإجراءات الجزائية الجزائري، سابق الإشارة إليه : «يجب أن يتضمن الإذن المذكور في المادة 65 مكرر5 أعلاه، كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها، والأماكن المقصودة سكنية أو غيرها والجريمة التي تبرر اللجوء إلى هذه التدابير ومدتها».

[3]- تنص المادة 2/95 من ق.إج.م: «وفي جميع الأحوال يجب أن يكون الضبط أو الاطلاع أو المراقبة أو التسجيل بناء على أمر مسبب، ولمدة لا تزيد على ثلاثين يوما قابلة للتجديد لمدة أو مدد أخرى مماثلة».

[4]- تنص المادة 3/206 من ق.إ.ج.م: «وفي جميع الأحوال يجب أن يكون الأمر بالضبط أو الاطلاع أو المراقبة لمدة لا تزيد على ثلاثين يوما، ويجوز للقاضي الجزئي أن يحدد هذا الأمر مدة أو مددا أخرى مماثلة».

[5]- Article 100 - 2 c.p.p.f. (Modifier 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 durée …».

والتحقيق، وضمن نفس الشروط الشكلية والزمنية، وذلك طبقا لأحكام المادة 65 مكرر7 فقرة 02 من قانون الإجراءات الجزائية[1].

ولئن كانت هذه هي الشروط المتعلقة بإصدار إذن اعتراض المراسلات السلكية واللاسلكية، فإنه ينبغي التنويه إلى أن صدور هذا الإذن يمس طائفة معينة من الجرائم، ومنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وهو الأمر الذي تطرقت له المادة 65 مكرر 5 فقرة 01 السابق الإشارة لها.

نظرا لأن هذا الإجراء يمس الحريات الفردية بصفة فاضحة، ولاعتبار أن مكافحة هذا النوع من الجرائم لا يتقرر إلا باللجوء إلى مثل هذا الإجراء، فقد عمد المشرع إلى الموازنة بين الصالح العام في حماية المجتمع من الجريمة، والصالح الخاص في حماية حق الفرد في الخصوصية بوضع تدابير استثنائية، بحيث استوجب طبقا لأحكام المادة 65 مكرر 06 من قانون الإجراءات الجزائية أن تتم عمليات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور دون المساس بالسر المهني المنصوص عليه في المادة 45 من ذات القانون.

ونظرا لأن العملية تقنية محضة، فقد أجاز القانون لوكيل الجمهورية أو ضابط الشرطة القضائية أو قاضي التحقيق تسخير كل شخص مؤهل، سواء كان هذا الأخير متواجدا في مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية واللاسلكية، للتكفل بالجوانب التقنية المذكورة في المادة 65 ، وهو الأمر الذي تم النص عليه بمقتضى أحكام المادة 65 مكرر 8 من قانون الإجراءات الجزائية[2].

ولنجاح هذا الإجراء فقد خول لضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص صلاحية تحرير محضر عن كل عملية اعتراض وتسجيل للمراسلات، وكذا عن عملية وضع الترتيبات التقنية وعملية الالتقاط والتثبيت والتسجيل

[1]- تنص المادة 65 مكرر 7 فقرة 02 من القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المتضمن قانون الإجراءات الجزائية الجزائري، سابق الإشارة إليه: «يسلم الإذن مكتوبا لمدة أقصاها أربعة (4) أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية».

[2]- تنص المادة 65 مكرر 08 من القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المتضمن قانون الإجراءات الجزائية الجزائري، سابق الإشارة إليه : «يجوز لوكيل الجمهورية أو ضابط الشرطة القضائية الذي أذن له، ولقاضي التحقيق أو ضابط الشرطة القضائية الذي ينيبه أن يسخر كل عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية، أو خاصة مكلفة بالمواصلات السلكية واللاسلكية للتكفل بالجوانب التقنية للعمليات المذكورة في المادة 65 مكرر أعلاه».

الصوتي أو السمعي البصري، وينبغي أن يذكر في المحضر المحرر تاريخ وساعة بدء العملية والانتهاء منها، وهو الأمر الذي نظمت أحكامه المادة 65 مكرر09 من قانون الإجراءات الجزائية.

ما يلاحظ أن المشرع الجزائري نظم إجراء الأمر باعتراض المراسلات السلكية واللاسلكية بإحكام، غير أنه لم يتطرق لمصير التسجيلات بعد انتهاء الغرض المقصود منها، وعليه يتوجب عليه التدخل لإتمام أحكام هذا الإجراء.

المبحث الثاني: التنظيم الإجرائي الدولي لمتابعة الجرائم الماسة بالمستند الالكتروني

نظرا لأن الجرائم الماسة بالمستندات الإلكترونية جرائم عابرة للحدود، فإن الحماية الفعالة لهذه المستندات يتطلب تعاونا دوليا من الناحية الإجرائية ، وذلك لما لهذه المسألة من أهمية بالغة في إكتشاف الجرائم الإلكترونية وحل لغز الجريمة، ناهيك عن قدرة هذه الإجراءات على إنارة درب العدالة بتمكينهم من الحصول على شهادات السوابق العدلية، ونقل الإجراءات الجزائية في إطار ما يعرف بالإنابة القضائية الدولية، ولا يقتصر الأمر على ذلك، كون أن التطبيق الفعلي للإجراءات من الناحية الدولية يسمح بتسليم المجرمين من أجل محاكمتهم أو من أجل توقيع العقاب عليهم، وهذا كله حتى لا يتمكن مرتكبوا الجرائم المعلوماتية من التذرع بعدم إمكانية معاقبتهم لاعتبار الأفعال المجرمة ارتكبت في غير الدولة التي رتبت آثارها فيها.

لأهمية هذه المسائل، سعت التتشريعات على المستويين الدولي والداخلي جاهدة لوضع الأحكام القانونية الضابطة لهذا التعاون على مختلف المستويات، على المستوى الشرطي الدولي **(المطلب الأول)**، التعاون القضائي الدولي **(المطلب الثاني)**، ناهيك عن تنظيمها لمسألة التعاون في تنفيذ الأحكام القضائية المتعلقة بتسليم مجرمي المعلوماتية **(المطلب الثالث)**.

المطلب الأول: التعاون الشرطي الدولي.

أثبت الواقع العملي أن أي دولة لا تستطيع بجهودها المنفردة القضاء على الجريمة مع هذا التطور الملموس والمذهل في كافة ميادين الحياة لاسيما مع التطور الذي شهده مجال الاتصال وتكنولوجيات المعلومات وظهور الإنترنت والإنتشار الواسع والسريع لها أدى إلى ظهور أشكال وأنماط جديدة من الجرائم منها الجرائم المعلوماتية الواقعة على المستندات الإلكترونية، التي باتت تشكل دعرا لا على سرية النظم الحاسوبية أو سلامتها أو توافرها فحسب، بل تعدت إلى أمن البنى الأساسية الحرجة[1].

[1]- حسين بن سعيد بن سيف الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، المرجع السابق، ص.636.

ومع تميزها بالعالمية وبكونها عابرة للحدود فإن مكافحتها لا تتحقق إلا بوجود تعاون دولي على المستوى الإجرائي الجنائي، بحيث يسمح بالإتصال المباشر بين أجهزة الشرطة في الدول المختلفة، وذلك بإنشاء مكاتب متخصصة لجمع المعلومات عن مرتكبي الجرائم المتعلقة بالإنترنت وتعميمها.

أمام هذا كله، أضحت الحاجة ماسة إلى وجود كيان دولي يأخذ على عاتقه القيام بهذه المهمة وتتعاون من خلاله أجهزة الشرطة في الدول المختلفة، خاصة فيما يتعلق بتبادل المعلومات المتعلقة بالجريمة والمجرمين بأقصى سرعة ممكنة، بالإضافة إلى تعقب المجرمين الفارين من العدالة، ومن هذه الأجهزة المنظمة الدولية للشرطة الدولية **(الفرع الأول)**، جهاز الشرطة الأوروبية **(الفرع الثاني)**، ومجلس وزراء الداخلية العرب **(الفرع الثالث)**.

الفرع الأول: المنظمة الدولية للشرطة الجنائية.

تعرف المنظمة الدولية للشرطة الجنائية اختصاراً بـ "Interpol" وهي تعني بالانجليزية (Criminal Police International Organization)، ترجع البدايات الأولى للتعاون الدولي الشرطي إلى سنة 1904 عندما تم عقد اتفاقية دولية لمكافحة الرقيق الأبيض، وقد قررت هذه الاتفاقية في المادة الأولى منها تعيين سلطة لجمع المعلومات الخاصة بموضوع الاتفاقية، يكون لها الحق في مخاطبة الإدارة المماثلة في كل الدول الأطراف المتعاقدة.

إن أهمية ما ورد من مضمون في هذه الاتفاقية دفع سبعة من الدول المتعاقدة - وقبل مرور سنة واحدة من إبرامها- إلى إنشاء مثل تلك الأجهزة، وذلك حتى تتمكن من تبادل المعلومات والبيانات المتعلقة بموضوع الاتفاقية، وكذا للقضاء على الجريمة في أقاليمها[1].

إذا كان التاريخ السابق ذكره هو بداية بروز التعاون الدولي الشرطي، فإنه ينبغي الذكر أنه بعد هذا التاريخ أخذ التعاون الدولي الشرطي يأخذ صورة المؤتمرات الدولية، كان أولها مؤتمر موناكو سنة 1914، والذي ضم رجال الشرطة والقضاء والقانون من أربع

[1]- حسين بن سعيد بن سيف الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، المرجع السابق، ص. 638.

عشرة دولة لمناقشة بعض المسائل الشرطية منها مدى إمكانية إنشاء مكتب دولي للتسجيل الجنائي، تنسيق إجراءات المجرمين.

رغم نتائج هذا المؤتمر إلا أن حلم تحقيقه ضاع بسبب اندلاع الحرب العالمية الأولى، بعد أن وضعت الحرب الكونية الأولى أوزارها، حاول الكولونيل الهولندي "فان هوتين" سنة 1919 إحياء فكرة التعاون الدولي الشرطي، غير أنه لم يوفق في مسعاه[1].

ومع نهاية سنة 1923 نجح مدير شرطة فيينا "جوهانو سويرا" في عقد ثاني مؤتمر دولي للشرطة الجنائية، ضم مندوبي تسع عشرة دولة كان من نتائجه إنشاء اللجنة الدولية للشرطة الجنائية المعروفة اختصارا بـ (ICPO)، مقرها "فيينا" وتعمل على التنسيق بين أجهزة الشرطة من أجل التعاون في مكافحة الجريمة[2].

لكن مع اندلاع الحرب العالمية الثانية أوقفت اللجنة نشاطها إلى غاية 1946، حيث عقد بالعاصمة البلجيكية بروكسل مؤتمر دولي يهدف إلى بعث مبادئ التعاون الأمني من جديد ووضعها موضع التنفيذ، وأسفر المؤتمر عن إحياء اللجنة الدولية للشرطة الجنائية، ونقل مقرها إلى العاصمة الفرنسية باريس، وتغيير اسمها ليصبح المنظمة الدولية للشرطة الجنائية، وتم تشكيل لجنة تنفيذية من خمسة أعضاء برئاسة المفتش العام للشرطة البلجيكية في عام 1989، وأصبح مقر المنظمة الجديد رسميا في مدينة ليون الفرنسية[3]، وبلغ عدد أعضائها سنة 1998 حوالي 177 دولة، وهي ما تزال في تزايد مستمر[4].

ينحصر الغرض من هذه المنظمة حسب المادة الثانية من ميثاقها في تأكيد المعرفة المتبادلة، وتشجيعها في أوسع نطاق ممكن مع سلطات الشرطة الجنائية، وفي حدود القوانين

[1]- حطاب كمال، المرجع السابق، ص. 389.
[2]- حسين بن سعيد بن سيف الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، المرجع السابق، ص. 639.
[3]- رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة مقدمة لنيل شهادة الدكتوراه علوم في القانون الخاص، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، جامعة أبو بكر بلقايد، تلمسان، السنة الجامعية 2017-2018، ص.307.
[4]- إيهاب فوزي السقا، المرجع السابق، ص. 504.

القائمة في الدول المختلفة، وفي نطاق الإعلان العالمي لحقوق الإنسان، وهي تساهم بدور فعال في منع جرائم القانون العام ومكافحتها، وذلك بإقامة النظم التي تساعد على ذلك[1].

من خلال ما تقدم ذكره، يتبين أن هذه المنظمة تهدف إلى تأكيد تشجيع التعاون بين سلطات البوليس في الدول الأعضاء على نحو فعال بما يحقق مكافحة الجريمة، وذلك بتجميع البيانات والمعلومات المتعلقة بالمجرم والجريمة من خلال المكاتب المركزية الوطنية للشرطة الدولية الموجودة في أقاليم الدول المنظمة، وتبادل المعلومات والبيانات فيما بينها، والتعاون في ضبط المجرمين بمساعدة أجهزة الشرطة في الدول الأطراف ومدها بالمعلومات المتوفرة لديها على إقليمها.

وعليه فإن عضو الإنتربول لا يقوم بنفسه بإجراء القبض على المجرم، بل إن هذا العمل منوط بجهاز الشرطة الوطنية في الدولة التي يتواجد المجرم في إقليمها، الأمر الذي يؤكد على احترام السيادة الوطنية[2].

من أهم ما أصدرت الإنتربول نشرات باللغات الرسمية الأربع "عربية، فرنسية، انجليزية وإسبانية"، وقد بلغ عدد هذه النشرات حوالي ستة أنواع، نشرة حمراء لطلب توقيف المطلوبين بغية تسليمهم، نشرة صفراء لتحديد مكان وجود المفقودين، نشرة زرقاء لتحديد مكان إقامة الأشخاص وجمع المعلومات بخصوصهم، نشرة سوداء لتبيين الجثث المجهولة، ونشرة برتقالية لإعطاء إشعارات تحذيرية عن تهديدات إرهابية محتملة.

تتمثل نشاطات الإنتربول حسب أهميتها وأولويتها في حفظ الأمن العام في متابعة جرائم الإرهاب، والمنظمات الإجرامية، الجرائم المتعلقة بالمخدرات، الإجرام المالي، جرائم التكنولوجيا المتقدمة، جرائم تقنية المعلومات، جرائم الاتجار بالبشر وإنشاء التحقيق بشأن المجرمين الفارين.

[1]- حطاب كمال، المرجع السابق، ص. 388.

[2]- جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، 2001، ص.76 وما يليها.

للقيام بالمهام الموكلة لها أنشأت الإنتربول سنة 2004 وحدة خاصة لمكافحة جرائم التكنولوجيا، كما قامت بالتفاوض مع مجموعة الدول الثمانية الكبرى (G8) لوضع إستراتيجيات لمواجهة هذا النوع من الجرائم من خلال:

- إنشاء مركز اتصالات أمني عبر الشبكة يعمل دون توقف على مستوى مصالح الشرطة في الدول الأطراف.
- استخدام وسائل حديثة في المكافحة كاستخدام قاعدة البيانات المركزية للصور الإباحية المحولة من قبل الدول الأعضاء، والتي تستخدم برنامج (excalibum) للتحليل والمقارنة الأوتوماتيكية لتلك الصور.
- تزويد شرطة الدول الأطراف بكتيبات إرشادية حول الجرائم الإلكترونية، وكيفية التدريب على مكافحتها والتحقيق فيها، من ذلك الكتيب المسمى دليل جرائم الحاسب الآلي.

أول مؤتمر دولي نظمته الأمانة العامة للإنتربول كان سنة 1994 يخص الغش والاحتيال فيما يتعلق بالبطاقات الائتمانية التي تعد احد أهم وسائل الدفع، وقد نجم عن هذا المؤتمر توصيتين الأولى تتعلق بضرورة مراجعة الدول الأعضاء لتشريعاتها وقوانينها المتعلقة ببطاقة الائتمان بما يضمن تجريم تصنيع أو امتلاك البطاقة المزورة، أو امتلاك معلومات غير قانونية، أو تم الحصول عليها بطريقة غير مشروعة، واستخدامها في إدخال نظام بطاقات الائتمان.

إنشاء مجموعات عمل شرطية من خبراء في الاحتيال الدولي التابعين لشرطة هونغ كونغ والشرطة الكندية والخدمة السرية الأمريكية، وخدمة الاستخبارات الوطنية الجنائية لزيلاندا الجديدة، ومندوبين من منظمات بطاقات الائتمان لمكافحة هذا النوع من الجرائم، والتقوا جميعهم في شهر فبراير 1995، وتم وضع الأسس الخاصة بتبادل المعلومات بهدف الحد من هذه الجرائم[1].

[1]- حطاب كمال، المرجع السابق، ص. 390.

لتحقيق نتائج هذا المؤتمر وقعت منظمة الإنتربول خمس اتفاقيات مع المنظمات الراعية للبطاقات وهي "أمريكان إكسبريس"، "دسكفري"، "يروباي"، "انترناشيونال ماستركارد الدولية" و"الفيزا الدولية"[1].

من بين ما يمكن للإنتربول القيام به تنسيق الموارد الميدانية في التحقيقات الجارية في مجال تكنولوجيا المعلومات بالتعاون مع الدول الأعضاء، ومن أمثلة ذلك التعاون طلب دولة كولومبيا في مارس 2008 من الإنتربول إجراء فحوص أدلة جنائية مستقلة على أجهزة ومعدات حاسبات آلية تم ضبطها خلال عملية لمكافحة المخدرات نُفِذت ضد معسكر للقوات المسلحة الثورية الكولومبية (الفارك)، لتحديد ما إذا كان قد جرى التلاعب بمضمون أي من المعدات أو المستندات المخزنة على الحاسب الآلي لوزارة الدفاع، وما إذا كان قد تم المساس بحجيتها الإلكترونية، وبعد إجراء فريق من الخبراء بالإنتربول الدراسة الفنية تبين غياب أي دليل يشير إلى تعديل ملفات المستخدمين أو تحريفها أو الإضافة عليها[2].

ولئن كانت الإنتربول أحد مظاهر التعاون الشرطي على المستوى الدولي، إلا أنها لا تعد المنظمة الوحيدة في هذا المجال، إذ يوجد إلى جانب ذلك أجهزة أخرى.

الفرع الثاني: جهاز الشرطة الأوروبية.

جهاز الشرطة الأوروبية أو ما يعرف باليوروبول جهاز اقترحه المجلس الأوروبي في لكسمبورج عام 1991[3]، وتمت الموافقة على تأسيسه في معاهدة ماستريخت سنة 1992[4]، باشر بتاريخ 3 يناير 1994 القيام بعمليات محدودة، وفي سنة 1998 قامت دول

---

[1]- إيهاب فوزي السقا، المرجع السابق، ص. 508.

[2]- حطاب كمال، المرجع السابق، ص. 391.

[3]- حسين بن سعيد بن سيف الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، المرجع السابق، ص. 506.

[4]- معاهدة ماستريخت، أو ما يعرف أيضا بمعاهدة الاتحاد الأوروبي هي اتفاقية المؤسسة للاتحاد الأوروبي، تم الاتفاق عليها من قبل المجلس الأوروبي في ماسترخت الهولندية في ديسمبر 1991، دخلت هذه المعاهدة التي تم توقيعها في 7 فبراير 1992 في ماسترخت حيز التنفيذ في 1 نوفمبر 1993، يرجع تأخر تطبيقها إلى تأخر قبول الدانمركيين للمعاهدة وشروطها بسب قضية دستورية ضدها أقيمت في ألمانيا.
أدخلت هذه المعاهدة عدة تغيرات على قوانين المجموعة الأوروبية، وعلى قوانين المجموعة الأوروبية الذرية التي كانت تشكل نواة الاتحاد الأوروبي، هذا و شكلت أيضا المعاهدة أساس للدستور الأوروبي الذي تم الاتفاق عليه لاحقا في عام 2004.
http://or.wikipedia.org/wiki/معاهدة_ماستريخت. Date de consultation le site28/07/2018 à 16 :42.

الاتحاد الأوروبي بإجراء مراجعة طبيعية لعمله ليبدأ بمباشرة مهامه كاملة بتاريخ 1 يوليو 1998.[1]

يعد اليوروبول همزة وصل بين أجهزة الشرطة الوطنية في الدول المنظمة هدفها ملاحقة الجناة في الجرائم العابرة للحدود، ومنها بطبيعة الحال الجرائم المتعلقة بالإنترنت[2]، والتي يشغل الاعتداء على المستندات الإلكترونية حيزا كبيراً منها.

بهذا يبدو أن جهاز اليوروبول يسعى إلى تحسين سبيل التعاون الشرطي بين الدول الأعضاء في الاتحاد لمكافحة الأشكال الخطيرة للإجرام الدولي، وذلك من خلال مده للمحققين بمساعداته التقنية[3].

من بين التطبيقات العملية للتعاون الدولي في الجرائم الإلكترونية ما يسمى بعملية "أوديسوس" التي تمت في 2004/02/26، والتي قامت فيها قوات الشرطة بعمليات شملت عشر دول[4].

وإلى جانب هذه العملية، هناك عملية أخرى تسمى عملية محطم الجليد قامت بها اليوروبول في 2005/06/14، وتم خلالها مداهمة وتفتيش شبكات الحاسب الآلي في ثلاث عشرة دولة أوروبية، وفيها تم توقيف أفراد في بعض من هذه الدول[5].

إن مظاهر التعاون الدولي لا تقتصر على عمل اليوروبول بل تمتد لتشمل اليوروجست (Eurojust)، واليوروجست وكالة تابعة للاتحاد الأوروبي مقرها لاهاي بهولندا، يعمل هذا الجهاز على التعاون الشرطي في مجال مكافحة الجرائم، ومن بينها الجرائم الإلكترونية، حيث ينعقد الاختصاص لهذه الوكالة عندما يمس الإجرام دولتين على

---

[1]- http://or.wikipedia.org/wiki/يوروبول Date de consultation le site28/07/2018 à 16 :33.

[2]- حسين بن سعيد بن سيف الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، المرجع السابق، ص. 506؛ رابحي عزيزة، المرجع السابق، ص.308.

[3]- حطاب كمال، المرجع السابق، ص. 392.

[4]- من هذه الدول أستراليا، بلجيكا، كندا، ألمانيا، هولندا، النرويج، البيرو، إسبانيا، السويد، وبريطانيا. مشار إليه من طرف، حطاب كمال، المرجع السابق، ص. 392.

[5]- هذه الدول هي: النمسا، بلجيكا، فرنسا، ألمانيا، المجر، أيسلندا، إيطاليا، هولندا، بولندا، البرتغال، سلوفاكيا، السويد، بريطانيا. مشار اليه من طرف، حطاب كمال، المرجع السابق، ص. 392.

الأقل من أعضاء الاتحاد الأوروبي، أو إحدى دول الأعضاء مع دولة من دول العالم الثالث، أو دولة عضو مع الرابطة الأوروبية.

إن دور اليوروجست لا يقتصر على الأفراد، بل يمتد ليشمل المؤسسات، وهو ينسق عمله مع اليوروبول، بحيث يزوده بالتحليلات اللازمة للقيام بالتحقيقات في الجرائم المنظمة[1].

إذا كان اليورجست واليوروبول من الأجهزة التي تحقق التعاون الشرطي الدولي في المجال الأوروبي، فإن هناك نظيرا لهذه الأجهزة في المجال العربي، ويكمن هذا الجهاز في مجلس وزراء الداخلية العرب.

الفرع الثالث: مجلس وزراء الداخلية العرب.

برزت فكرة إنشاء مجلس وزراء الداخلية العرب لأول مرة سنة 1977 في المؤتمر الأول لاجتماع وزراء الداخلية العرب بالعاصمة المصرية، ثم تبلورت هذه الفكرة سنة 1980 في المؤتمر الثالث لهؤلاء الوزراء بمدينة الطائف السعودية، لينجم على أعقابها عقد مؤتمر استثنائي للوزراء العرب بالرياض سنة 1982 لوضع مشروع النظام الأساسي للمجلس.

في ديسمبر من نفس السنة أقر مجلس جامعة الدول العربية نظام مجلس وزراء الداخلية العرب، ليحل محل المنظمة التي كانت تسبقه، والتي كان يطلق عليها تسمية منظمة الدفاع الاجتماعي ضد الجريمة[2].

يهدف هذا المجلس إلى تأمين وتنمية التعاون بين أجهزة الشرطة في الدول الأعضاء في مجال مكافحة الجريمة، وملاحقة المجرمين في حدود القوانين والأنظمة المعمول بها في كل دولة، بالإضافة إلى تقديم المعرفة في مجال دعم وتطوير أجهزة الشرطة في الدول الأعضاء[3].

---

[1]- حطاب كمال، المرجع السابق، ص. 393.

[2]- المرجع نفسه، ص. 394.

[3]- حسين بن سعيد بن سيف الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، المرجع السابق، ص. 506؛ رابحي عزيزة، المرجع السابق، ص.308؛ فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية، رسالة دكتوراه، جامعة عين شمس، القاهرة، 2012، ص.519.

المطلب الثاني: التعاون القضائي الدولي.

لا ريب في أن التعاون القضائي الدولي يوفق بين استقلال كل دولة في ممارسة اختصاصها الجنائي على حدود إقليمها، وبين ضرورة ممارسة حقها في العقاب، وبدون هذا التعاون لا يمكن للدولة من الناحية العملية إقرار حقها في العقاب، وبهذا يبدو أن التعاون القضائي الدولي تفرضه الضرورة العملية لسببين، يكمن السبب الأول في تقييد سلطات الدولة بحدود إقليمها، إذ لا يمكن مباشرة الإجراءات الجزائية خارج حدود الإقليم الوطني لما في ذلك من مساس بسيادة الدولة الأجنبية الأخرى، في حين يكمن السبب الثاني في عدم إمكانية تطبيق قانون العقوبات بدون قانون الإجراءات الجنائية، بحيث يوجد تلازم بين حق الدولة في العقاب والدعوى الجنائية، وتعد الإجراءات الجزائية الوسيلة اللازمة لتطبيق أحكام قانون العقوبات، ونقله من حالة الجمود أو السكون إلى حالة الحركة.

وعليه إذا تطلب تطبيق قانون العقوبات مباشرة بعض الإجراءات الجزائية خارج حدود إقليم الدولة، فإنه يتوجب عدم الاصطدام بمشكلة الحدود الإقليمية بين الدول، والالتجاء إلى التعاون القضائي لتذليل تلك الصعوبات[1].

بناء على ما تقدم، يبدو أن دور التعاون القضائي الدولي يتضح جليا بالنسبة للجرائم العابرة للحدود، والتي تعد الجرائم الواقعة على المستندات الإلكتروني إحداها، ذلك أن آثارها قد تتعدى عدة دول، بحيث لا يمكن ملاحقة مرتكبيها وتقديمهم للمحاكمة، وتوقيع العقاب عليهم إلا من خلال القيام بأعمال إجرائية خارج حدود تلك الدولة التي ارتكبت الجريمة أو جزء منها فيها، ومن ذلك معاينة مواقع الإنترنت في الخارج، ضبط الأقراص الصلبة التي توجد عليها المعلومات غير المشروعة، تفتيش الوحدات الطرفية في حالة الاتصال عن بعد، سماع الشهود، اللجوء إلى الإنابة القضائية، تقديم المعلومات التي يمكن أن تساهم في التحقيق في هذه الجرائم، وهذه الأمور كلها لا تتحقق بدون مساعدة الدول الأخرى[2].

[1]- حسين بن سعيد بن سيف الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، المرجع السابق، ص. 420.
[2]- سليمان أحمد محمد فضل، المرجع السابق، ص. 421.

لأهمية هذه المسائل، سيتم التعرض للإنابة القضائية الدولية **(الفرع الأول)**، ونقل الإجراءات الجزائية **(الفرع الثاني)**، ثم نتطرق إلى تبادل المعلومات **(الفرع الثالث)**.

الفرع الأول: الإنابة القضائية الدولية.

لا ريب في أن الإنابة القضائية الدولية تعد إحدى أهم صور التعاون القضائي الدولي في المسائل الجزائية عامة، وفي المسائل المتعلقة بالمستندات الإلكترونية خاصة، ولأهميتها سيتم التطرق إلى تعريفها **(البند الأول)**، ثم لإجراءاتها **(البند الثاني)**.

البند الأول: تعريف الإنابة القضائية الدولية.

تعتبر الإنابة القضائية الدولية إحدى صور التعاون القضائي الدولي، وبمقتضى هذه الصورة تقوم دولة معينة نيابة عن دولة أخرى بمباشرة إجراء قضائي يتعلق بدعوى قيد النظر داخل الحدود الإقليمية لهذه الأخيرة، ويكون ذلك بناء على طلب الدولة المناب عنها.

بهذا يمكن القول أن الإنابة القضائية الدولية هي الطلب الذي تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها الإنابة لاتخاذ إجراء قضائي من إجراءات الدعوى الجنائية، وذلك لما تقتضيه ضرورة الفصل في مسألة معروضة على السلطة القضائية في الدولة الطالبة ويتعذر عليها القيام بها بنفسها[1].

استناداً لما تقدم، يعرف جانب من الفقه[2] الإنابة القضائية الدولية بأنها: «الطلب الذي تنتدب فيه المحكمة المرفوعة أمامها الدعوى محكمة وجود الشاهد أو الأوراق أو الشيء وتنيبها لعمل الإجراء اللازم وتحرير محضر بذلك وإرساله لها بعد تمامه».

وقد حددت المادة 14 من اتفاقية الرياض العربية للتعاون القضائي مجالاتها وحصرتها في مباشرة أي إجراء قضائي خاصة سماع الشهود، تلقي تقارير الخبراء ومناقشتهم وإجراء المعاينة، وطلب حلف اليمين.

[1]- حسين بن سعيد بن سيف الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، المرجع السابق، ص.511.
[2]- المرجع نفسه، ص 509.

بهذا يمكن القول أن الإنابة القضائية الدولية تهدف إلى تسهيل الإجراءات الجنائية بين الدول بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة، والتغلب على عقبة السيادة الإقليمية التي تمنع الدولة الأجنبية من ممارسة بعض الأعمال القضائية داخل إقليم الدول الأخرى كسماع الشهود، أو إجراء التفتيش والمعاينات إلى ما غير ذلك[1]، وهي بذلك تساعد على عدم ضياع الأدلة والآثار المتعلقة بالجريمة وإنجاز التحقيقات الجارية في الدولة الطالبة، كما أنها تحفظ حقوق المتهمين في الإسراع بمحاكمتهم، وعدم بقاءهم في الحبس المؤقت دون محاكمة انتظارا لإتمام تلك الإجراءات القانونية في دولة أخرى[2].

إن الإنابة القضائية الدولية وفقا للمفهوم السابق الذكر تتم بثلاث طرق، وتشمل كل من الطريق القضائي، الطريق الدبلوماسي والطريق القنصلي.

فبخصوص الطريق القضائي يمكن القول أن هذا الأسلوب يعرف كذلك بالأسلوب المباشر، وفيه تتولى المحكمة المختصة بالنزاع توجيه الإنابة القضائية مباشرة إلى المحكمة المراد منها تنفيذ الإنابة القضائية تطبيقا لمعاهدة دولية سابقة، أو وفقا لأحكام قانون الدولتين. ويتم اللجوء لهذا الطريق للحد من الروتين والتعقيد والبطء الذي تتميز به الإجراءات الدبلوماسية، بحيث تشترط المعاهدات والاتفاقيات الخاصة بتبادل المساعدة القضائية الدولية على الدول الأطراف تعيين سلطة مركزية، وهي عادة ما تكون وزارة العدل لترسل إليها الطلبات مباشرة بدلا من الولوج إلى القنوات الدبلوماسية التي من شأنها تسريع الإجراءات التي قد تأخذ وقتاً طويلا فيما لو تمت عبر تلك القنوات[3].

هذا عن الطريق القضائي، أما الطريق القنصلي، فيتحقق عندما ترسل المحكمة المختصة الإنابة القضائية مباشرة إلى قنصل دولتها في البلد الأجنبي المطلوب منه تنفيذ الإنابة، ليقوم هذا الأخير بتوجيهها إلى الجهة المختصة في الدولة القائمة بالتنفيذ.

---

[1]- حسين بن سعيد بن سيف الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، المرجع السابق، ص. 511؛ جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، المرجع السابق، ص.79.

[2]- حطاب كمال، المرجع السابق، ص. 368.

[3]- حسين بن سعيد بن سيف الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، المرجع السابق، ص. 512.

ولئن كانت الإنابة القضائية الدولية القنصلية، أو ما يعرف بالطريق السياسي تتقرر بهذه الطريقة، فإن الطريق الدبلوماسي يتم عندما تقوم المحكمة المختصة بإرسال الطلب إلى وزارة الخارجية لتقوم هذه الأخيرة بإرساله إلى ممثلها الدبلوماسي في الدولة المطالبة بتنفيذ طلب الإنابة، فمثلا طلب الحصول على دليل الإثبات والذي يكون عادة من شأن النيابة العامة يتم من المحكمة الوصية المختصة في الدولة الطالبة ليمرر بعد ذلك عن طريق وزارة الخارجية إلى سفارة الدولة متلقية الطلب، وما أن يتم تلبية الطلب ينعكس الاتجاه الوارد في سلسلة العمليات[1].

البند الثاني: إجراءات طلب الإنابة القضائية الدولية.

يقصد بإجراءات الإنابة القضائية الدولية الإجراءات الشكلية اللازمة لتنفيذ الإنابة، ويعبر عنها بطريق الإنابة بين جهتيها، وهما الجهة الطالبة، والجهة المطلوب منها الإنابة.

تنطلق إجراءات الإنابة القضائية الدولية من خلال طلب الإنابة الذي توجهه الدولة الطالبة إلى الدولة المطلوب منها التنفيذ، بحيث يتضمن طلب الإنابة القضائية نوع القضية، الجهة الصادر عنها الطلب، الجهة المطلوب منها التنفيذ، البيانات التفصيلية المتعلقة بالقضية، وخاصة ما تعلق منها بأسماء الشهود، محال إقامتهم، نوع الأسئلة المطلوب طرحها عليهم، وللإشارة فإن طلب الإنابة القضائية يحرر بلغة الجهة المطلوب منها التنفيذ أو يكون مصحوبا بترجمة للغة تلك الدولة حتى يتم تمكين القائم من التنفيذ من مباشرة عمله.

بعد وصول طلب الإنابة القضائية تبدأ الجهة المطلوب منها التنفيذ عملها وفقا للإجراءات القانونية المعمول بها في دولتها[2]، وفي حالة رغبة الدولة طالبة التنفيذ تنفيذ الإنابة القضائية وفق شكل خاص يتوجب عليها أن تصرح بذلك بناء على طلب صريح منها إلى الدولة المطلوب منها التنفيذ.

[1]- حسين بن سعيد بن سيف الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، المرجع السابق، ص. 511.
[2]- تنص المادة 1/18 من اتفاقية الرياض العربية للتعاون القضائي : «يتم تنفيذ الإنابة القضائية وفقا للإجراءات القانونية المعمول بها في قوانين الطرف المطلوب إليه ذلك».

تنفذ الإنابة وفق ذلك الشكل ويكون من الواجب على الطرف المتعاقد المطلوب إليه ذلك إجابة رغبته، ما لم يتعارض ذلك مع قانونه أو أنظمته.

الفرع الثاني: نقل الإجراءات الجزائية.

يقصد بنقل الإجراءات الجزائية قيام إحدى الدول بنقل الإجراء الجزائي المنوط بها القيام به إلى دولة أخرى بناء على طلبها، ويطلق على الدولة التي ينتقل إليها هذا الإجراء "الدولة المنقول إليها"، ويتم نقل الإجراءات الجزائية بين الدول في الحالة التي تبسط فيها أكثر من دولة ولايتها، واختصاصها على جريمة معينة[1].

إن تحقق هذه الصورة من صور التعاون القضائي الدولي يستلزم تحقق شروط معيّنة وتتمثل في التجريم المزدوج، بمعنى لا بد أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والدولة المطلوب إليها نقل الإجراءات، وذلك بغض النظر عن التكييف الذي يلحق الفعل في البلدين، إذ يجوز أن يكون الفعل جناية في الدولة الطالبة وجنحة في الدول المطلوب إليها نقل الإجراءات، وهو ما اشترطته المادة 5/32 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

كما يشترط أن تكون الإجراءات المطلوب اتخاذها مقررة في قانون الدولة المطلوب إليها نقل الإجراءات عن الجريمة ذاتها، وينبغي إلى جانب ذلك أن تكون الإجراءات المطلوب اتخاذها من الأهمية بمكان، حيث تؤدي دوراً مهماً في الوصول إلى الحقيقة، كأن تكون أدلة الجريمة موجودة بالدولة المطلوب إليها نقل الإجراءات[2].

لأهمية هذه الصورة اعترفت بها العديد من الاتفاقيات الدولية والإقليمية، ومن ذلك معاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية، اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية 2000 في المادة 21، كما نظمتها المادة 9 من معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي 1999، وكذا المادة 16 من

[1]- حطاب كمال، المرجع السابق، ص. 371.
[2]- حسين بن سعيد بن سيف الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، المرجع السابق، ص. 510؛ رابحي عزيزة، المرجع السابق، ص.311.

النموذج الاسترشادي لاتفاقية التعاون القانوني والقضائي عن مجلس التعاون الخليجي 2003.

كما وأقر المجلس الأوروبي اتفاقية نقل الإجراءات الجزائية، والتي بمقتضاها تم السماح للدول الأطراف بمحاكمة المتهمين طبقا لقوانينها، بناء على طلب دولة أخرى طرف في تلك الاتفاقية، شريطة أن يكون الفعل مجرما ومعاقبا عليه في كلتا الدولتين[1].

الفرع الثالث: تبادل المعلومات.

يشمل تبادل المعلومات تقديم البيانات والوثائق والمواد الاستدلالية، والمعلومات التي تطلبها سلطة قضائية أجنبية وهي بصدد النظر في جريمة ما عن الاتهامات التي وجهت إلى رعاياها في الخارج، والإجراءات التي اتخذت ضدهم، وقد يشمل التبادل السوابق القضائية للجناة[2].

لهذه الصورة من صور المساعدة القضائية الدولية صدى كبير في العديد من الاتفاقيات، ومن ذلك ما نصت عليه الفقرة الثانية من المادة الأولى في بنديها (و) و(ز) من معاهدة الأمم المتحدة النموذجية لتبادل المساعدة في المسائل الجنائية[3]، حيث قضت بضرورة اتفاق الأطراف على أن يقدم كل منهم للآخر أكبر قدر ممكن من المساعدة المتبادلة في التحقيقات، أو إجراءات المحاكمة المتعلقة بجرائم يكون العقاب عليها وقت طلب المساعدة داخلا في اختصاص السلطة القضائية في الدولة الطالبة للمساعدة.

ولا يقتصر الأمر على تلك الاتفاقية، إذ نص البند الأول من المادة الرابعة من معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي على ضرورة تبادل المعلومات[4].

---

[1]- حطاب كمال، المرجع السابق، ص. 371.

[2]- حسين بن سعيد بن سيف الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، المرجع السابق، ص. 509.

[3]- صدرت هذه المعاهدة في 1990/12/14 في الجلسة العامة 68 للجمعية العامة للأمم المتحدة، وتقضي باتفاق أطرافها على أن يقدم كل منهم للآخر أكبر قدر ممكن من المساعدة المتبادلة في التحقيقات، أو إجراءات المحاكمة المتعلقة بجرائم يكون العقاب عليها وقت طلب المساعدة داخلا في اختصاص السلطة القضائية في الدولة الطالبة للمساعدة. مأخوذة من، رابحي عزيزة، المرجع السابق، هامش ص.310.

[4]- صدرت هذه المعاهدة واعتمدت عام 1999 من قبل مؤتمر وزراء خارجية دول المنظمة في اجتماعهم المنعقد في واغادوغو في الفترة من 1999/6/28 إلى 1999/7/1.

والصورة ذاتها قررتها المادة الأولى من اتفاقية الرياض العربية للتعاون القضائي[1]، التي صادقت عليها الجزائر، حيث اقتضت أن تتبادل وزارات العدل لدى الأطراف المتعاقدة بصفة منتظمة نصوص التشريعات النافذة، والمطبوعات والنشرات والبحوث القانونية والقضائية والمجلات التي تنشر فيها الأحكام القضائية، كلما استلزمت ضرورة تبادل المعلومات المختلفة المتعلقة بالتنظيم القضائي، والعمل على اتخاذ الإجراءات الرامية إلى التوفيق بين النصوص التشريعية والتنسيق بين الأنظمة القضائية لدى الأطراف المتعاقدة، حسب ما تقتضيه الظروف الخاصة بكل منها.

والتبادل المذكور في الاتفاقية السالفة الذكر يمتد ليشمل صحف الحالة الجنائية، حيث منحت المادة 5 من ذات الاتفاقية لوزارتي العدل في أي من الدولتين المتعاقدتين إمكانية تبادل البيانات عن الأحكام النهائية الصادرة ضد مواطني إحدى الدولتين، أو ضد الأشخاص المولودين أو المقيمين في إقليمها والمقيدين في صحف الحالة الجنائية، لما تكشف عنه تلك البيانات من سوابق جنائية لهؤلاء الأشخاص.

إن التبادل الوارد في الاتفاقيات السالفة، نصت عليه كذلك اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية 2000 في بنودها 3، 4 من المادة الثانية.

وقد أخذت بالمسألة ذاتها المادة 32 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، حيث دعت الدول الأطراف إلى تبادل المساعدة فيما بينها بأقصى قدر ممكن[2]، وأكدت على ذلك المادة 33 من الاتفاقية سالفة الذكر، حيث أجازت للدولة الطرف في الاتفاقية إعطاء معلومات حصلت عليها خلال تحقيقها لدولة أخرى، ولو لم تطلب منها تلك الدولة ذلك بمقتضى طلب المساعدة متى رأت أن كشف مثل تلك المعلومات يمكن أن يساعد الدولة الطرف المرسلة إليها المعلومات في إجراء الشروع، أو القيام بتحقيقات في الجرائم

[1]- صدرت هذه الاتفاقية في 1993/04/06 بمدينة الرياض بالمملكة العربية السعودية.

[2]- تنص المادة 1/32 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، سابق الإشارة لها: "على جميع الدول الأطراف تبادل المساعدة فيما بينها بأقصى قدر ممكن لغايات التحقيقات أو الأجراءات المتعلقة بجرائم تقنية المعلومات أو لجمع الأدلة الإلكترونية في الجرائم."

المنصوص عليها في المعاهدة[1]، على أنه في كل الحالات يكون للدولة المزودة بالمعلومات قبل منح تلك المعلومات أن تطلب من الدولة الطرف المستقبلة الحفاظ على سرية المعلومات، وإذا لم تستطع الدولة الطرف المستقبلة الإلتزام بهذا الطلب فيتوجب عليها إعلام الدولة المزودة بذلك، ليكون لهذه الأخيرة تحديد مدى إمكانية تزويدها بالمعلومات من عدمه، على أنه وفي حالة ما إذا قبلت الدولة المستقبلة بمثل ذلك الإلتزام فعليها الحفاظ على سرية المعلومات المقدمة لها، وهو ذات الأمر الذي أكدت عليه المادة 18 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها[2]، إذ بعدما خولت المادة 17 من القانون آنف الذكر للدولة الجزائرية حق الاستجابة لطلبات المساعدة القضائية الدولية الرامية لتبادل المعلومات وذلك في حدود الاتفاقيات الدولية ذات الصلة ومبدأ المعاملة بالمثل[3]، عادت لتؤكد في المادة 18 على أن الإستجابة لطلبات المساعدة يكون مقيدا بشرط المحافظة على سرية المعلومات المبلغة وكذا بشرط عدم استعمالها في غير ما هو موضح في الطلب، ناهيك عن رفض تنفيذ طلبات المساعدة في حالة ما إذا كان من شأن ذلك المساس بالسيادة الوطنية أو النظام العام.

[1]- تنص المادة 33 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، سابق الإشارة لها: " 1. يجوز لأي دولة طرف -ضمن حدود قانونها الداخلي- وبدون طلب مسبق أن تعطي لدولة أخرى معلومات حصلت عليها من خلال تحقيقاتها إذا اعتبرت أن كشف مثل هذه المعلومات يمكن أن تساعد الدولة الطرف المرسلة إليها في إجراء الشروع أو القيام بتحقيقات في الجرائم المنصوص عليها في هذه الاتفاقية أو قد تؤدي إلى طلب التعاون من قبل تلك الدولة الطرف.
2. قبل إعطاء مثل هذه المعلومات يجوز للدولة الطرف المزودة أن تطلب الحفاظ على سرية المعلومات، وإذا لم تستطع الدولة الطرف المستقبلة الإلتزام بهذا الطلب يجب عليها إبلاغ الدولة الطرف المزودة بذلك والتي تقرر بدورها مدى إمكانية التزويد بالمعلومات، وإذا قبلت الدولة الطرف المستقبلة المعلومات مشروطة بالسرية فيجب أن تبقى المعلومات بين الطرفين."

[2]- تنص المادة 18 من القانون 09-04 المؤرخ في 5 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافختها، سابق الإشارة إليه: " يرفض تنفيذ طلبات المساعدة إذا كان من شأنها المساس بالسيادة الوطنية أو النظام العام.
يمكن أن تكون الإستجابة لطلبات المساعدة مقيدة بشرط المحافظة على سرية المعلومات المبلغة أو بشرط عدم استعمالها في غير ما هو موضح في الطلب".

[3]- تنص المادة 17 من القانون 09-04 المؤرخ في 5 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، سابق الإشارة إليه: "تتم الإستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظية وفقا للإتفاقيات الدولية ذات الصلة والاتفاقيات الدولية الثنائية ومبدأ المعاملة بالمثل."

هذا وأكد المرسوم الرئاسي رقم 15-261،[1] المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها على هذه المسألة بمقتضى المادة 4 منه بحيث خول للهيئة الوطنية مهمة تطوير تبادل المعلومات والتعاون على المستوى الدولي وذلك في إطار إختصاصاتها المحددة قانونا.

إن مسالة تبادل المعلومات وردت كذلك في اتفاقية بودابست حول الجرائم الافتراضية، وتحديدا في المادة 26[2] منها بحيث خولت لأي طرف وفي حدود قانونه الداخلي، ودون طلب مسبق، أن يرسل لأي طرف آخر معلومات يكون قد حصل عليها في نطاق التنقيبات الخاصة به، وذلك إذا كان يرى أن تلك المعلومات يمكن أن تساعد الطرف المرسل إليه في إستجلاء أو إجراء تنقيبات أو تحقيقات تتعلق بجرائم جنائية مقامة وفقا لهذه المعاهدة، أو عندما يمكن أن تؤدي تلك الجرائم إلى طلب المساعدة بواسطة الطرف الآخر.

وللإشارة فإنه وقبل إرسال تلك المعلومات، يمكن للطرف الذي يقوم بإعدادها أن يطلب بقاء تلك المعلومات سرية، أو أن تستخدم وفقا لشروط معينة، على أنه إذا لم يكن في إمكان الطرف المرسل إليه تلبية تلك الشروط، فإنه يتوجب عليه في هذه الحالة إخطار الطرف الآخر بذلك، ويبقى للطرف المرسل آنذاك تحديد مدى إمكانية تقديم تلك المعلومات

[1]- تنص المادة 4 من المرسوم الرئاسي رقم 15-261 المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، سابق الإشارة إليه: " تكلف الهيئة في ظل إحترام الأحكام التشريعية المبينة أعلاه على الخصوص، بما يأتي:
- السهر على تنفيذ.....وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها."

[2]- Art 26 du convention sur la cybercriminalité dispose que : « Une Partie peut , dans les limites de son droit interne et en l'absence de demande préalable, communiquer à une autre Partie des informations obtenues dans le cadre de ses propre enquetes lorsqu'elle estime que cela pourrait ader la Partie destinataire à engager ou à mener à bien des enquétes ou des procédures au sujet d'infractions pénales établies conformément à la présente convention, ou lorsque ces informations pourraient aboutir à une demande formulée par cette Partie au titre du présent chapitre.
2- Avant de communiquer de telles informations, la Partie qui les fournit peut demander qu'elles restent confidentielless ou ou ne soient utilisées que sous certaines conditions. Si la Partie destinataire ne peut faire droit à cette demande, elle doit en informer l'autre Partie, qui devra alors déterminer si les informations en question devraient néanmoins étre fourni. Si la Partie destinataire accepte les informations aux conditions prescrites, elle sera liée par ces dernières. »

من عدمه، على أنه متى قبل المرسل إليه المعلومات تحت شروط معينة، فإنه يصبح مقيدا بتلك الشروط.

المطلب الثالث: التعاون في تنفيذ الأحكام القضائية المتعلقة بتسليم المجرمين.

لقد أدى ارتكاب جرائم الإنترنت من خلال وحدة طرفيه في دولة أجنبية، وابتعاد المجرمين عن سلطات الدولة المتضررة من الجريمة وإفلاتهم في كثير من الأحيان من العقاب إلى بروز أهمية تسليم المجرمين لمكافحة الجرائم العابرة للحدود، والتي تعد جرائم الإنترنت إحداها، وذلك لما يترتب عن ذلك التسليم من ضمان توقيع العقاب على مرتكبي تلك الجرائم.

لأهمية ذلك سعت الدول إلى إبرام اتفاقيات دولية بشأن تسليم المجرمين، وذلك حتى تقوم الدولة المطلوب منها التسليم بتسليم أحد الأشخاص الموجودين على إقليمها إلى الدولة الطالبة لمحاكمته أو لتنفيذ عقوبة قضت بها عليه إحدى محاكمها[1].

بهذا يلاحظ أن موضوع تسليم المجرمين يقوم على أساس التزام الدولة التي يتواجد المتهم المرتكب لإحدى الجرائم عابرة للحدود -ومنها جرائم الإنترنت- على إقليمها، بمحاكمته إذا كانت تشريعاتها تسمح بذلك، أو تسليمه لمحاكمته بمعرفة دولة أخرى مختصة.

استنادا لما تقدم، يتبين أن التسليم يؤدي إلى المحافظة على العلاقات الدولية فيما بين الدول، وهو بذلك إجراء لا يقوم على أساس الالتزام القصري أيا كان نوع وطبيعة الجريمة المرتكبة، بقدر ما يهدف إلى تحقيق مصلحة المجتمع الدولي في عدم تمكين المجرم من الإفلات من عدالة الدولة الطالبة، وهو بذلك يعد ذا أثر مانع من ارتكاب الجريمة، وهو ما يتضح بجلاء في مجال جرائم الحاسب الآلي باعتبارها من الجرائم العابرة للحدود.

لعلّ ما ينبغي الإشارة إليه أن أهمية التسليم لا تقتصر على ما تقدم بل تتعداها لتشمل ضمانات المتهم، فمثول هذا الأخير أمام قاضي موقع الجريمة يسمح بحمايته خلال محاكمته،

[1]- جميل عبد الباقي صغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، المرجع السابق، ص. 82.

كما يسمح بإجراء التحقيقات بصورة أكثر فاعلية، فيما لو تمت تلك الإجراءات بعيدا عن موقع ارتكاب الجريمة محل التسليم[1].

بهذا يمكن القول أن احد مبررات التسليم يكمن في حق الدولة الطالبة في عقاب كل من ينتهك قوانينها، وذلك إعمالا لمبدأ الإقليمية، كما وأنه يرمي إلى عدم إتاحة الفرصة للمجرم من الإفلات من العقاب، وذلك حماية للمصلحة الخاصة، وكذا للمصلحة العامة لمنع الغير من ارتكاب جرائم عابرة للحدود[2].

انطلاقا مما تقدم، يتبين أن أهمية موضوع التسليم يستلزم التطرق إلى مختلف جوانبه بدءا من مفهومه **(الفرع الأول)**، وصولا إلى إجراءاته **(الفرع الثاني)**.

الفرع الأول: مفهوم تسليم المجرمين.

يقتضي دراسة مفهوم تسليم المجرمين تسليط الضوء على تعريفه **(البند الأول)**، ثم التعرض لشروطه **(البند الثاني)**.

البند الأول: تعريف تسليم المجرمين.

إن أهمية التسليم[3] وخطورة النتائج المترتبة عليه، دفع الفقه إلى تعريفه، وفي هذا عرّفه جانب من الفقه بأنه: «الإجراء الذي تسلم من خلاله دولة شخصاً موجوداً في إقليمها

---

[1]- طارق فوزي الفقي، المرجع السابق، ص. 269.

[2]- حطاب كمال، المرجع السابق، ص. 376.

[3]- يعتبر اصطلاح تسليم المجرمين ذو أصل لاتيني، حيث كان يعبر عنه إعادة الشخص المطلوب إلى الدولة ذات السيادة والسلطة لمحاكمته، وكان يطلق عليه آنذاك باللاتينية "Extrudere".
والمتتبع للدراسات الفقهية والتشريعات المعاصرة للتسليم يجد أن استخدامها يخرج من اصطلاح "Extradition" باللغة الانجليزية و"L'extradition" باللغة الفرنسية، ويعني المصطلحات الترحيل، أما في الأنظمة العربية فقد درج استخدام المصطلحين وهما إما الاسترداد وإما تسليم المجرمين، ويعاب على المصطلح الأخير عدم دقته، ذلك أنه يتحدث عن مجرم، وهو لفظ يفترض أن الشخص المطلوب تسليمه قد تمت إدانته مقدما، رغم أن التسليم قد ينصب على شخص لم تتم محاكمته بعد وما زال في طور الاتهام، وتعد هذه الحالة من حالات التسليم.
وهنا يمكن القول أن طلب تسليم شخص متهم بارتكاب جريمة لتوفر أدلتها لا يعني أن يضفي على هذا الأخير وصف المجرم، لأنه مهما تعاظمت الأدلة وقويت حجيتها فقد تؤدي المحاكمة إلى براءته، كأن يثبت المتهم أنه كان بحالة دفاع شرعي، أو أنه قد ارتكب الجريمة تحت ظروف نفسية أو إكراه يسمحان للقاضي بعدم توقيع العقوبة عليه أو إصدار حكم مخفف لا يخضع من خلاله للتسليم.
أما في حالة طلب تسليم شخص صدر ضده حكم جنائي بالإدانة، فإنه يمكن أيضا ألا يعتبر هذا الشخص مجرما، خاصة إذا كان الحكم الصادر غيابيا، إذ أنه يتيح للشخص المطلوب فرصة إعادة محاكمته من جديد، وقد يترتب على إعادة محاكمته براءته أو الحكم بعقوبة لا يتفق حدها الأقصى والجرائم التي يجوز فيها التسليم.=

إلى دولة أخرى بناء على طلبها، وذلك حتى تحاكمه عن جريمة يعاقب عليها قانونها أو حتى تنفذ عليه الحكم الصادر عن محاكمها».

كما عرّفه جانب آخر بأنه: «إجراء أو تفاوض دولي تقوم بمقتضاه دولة تسمى بالدولة المطلوب إليها التسليم، بتسليم شخص يوجد في إقليمها إلى دولة ثانية تسمى الدولة الطالبة بهدف ملاحقته عن جريمة اتهم بارتكابها، أو لأجل تنفيذ حكم جنائي صدر ضده».

وعرّفه اتجاه آخر بأنه: «الإجراء القانوني الذي تقوم به دولة (الدولة الطالبة)، ضد شخص موجود في إقليم دولة أخرى (الدولة المطلوب منها التسليم)، من أجل أن تحاكمه (تسليم لغاية المحاكمة)، أو من أجل تنفيذ العقوبة عليه (تسليم لغاية التنفيذ)»، إن التسليم المعروف على هذا المنوال هو وسيلة فعّالة للتعاون الردعي الدولي لأنه يؤدي إلى الاعتقال الجسدي للفرد الذي تم تسليمه[1].

ولعلّ من التعاريف الواردة في بيان المقصود بتسليم المجرمين، ذلك التعريف الذي يتجه إلى اعتباره: «قيام دولة موجود على إقليمها متهم بجريمة أو مدان فيها بحكم قضائي بتسليمه إلى الدولة التي وقعت الجريمة على إقليمها، أو التي صدر فيها الحكم القضائي بالإدانة، بهدف محاكمته أو تنفيذ الحكم عليه، وذلك بناء على طلب هذه الدولة تأسيسا على معاهدة تسليم المجرمين أو على مبدأ المعاملة بالمثل»[2].

انطلاقا من هذا التعريف يتبين أن التسليم يتم وفقا للمعاهدات المبرمة بين الدول سواء كانت معاهدات ثنائية أو متعددة، ومن بين تلك المعاهدات الاتفاقيات المتعلقة بتنفيذ الأحكام

=وعليه ينبغي القول أن الشخص الذي يكون محل إجراءات التسليم لا يمكن وصفه بالمجرم، وذلك لإمكانية دحض الأدلة التي تكون سببا في إقامة الدعوى ضده أو صدور حكم عليه، ولو فرضنا أنه في الحالة الأولى التي يكون فيها الشخص المطلوب للتسليم قد صدر حكم ضده يقضي بعقوبته وطلب تسليمه لتنفيذها، فإن ذلك لا يكفي لإطلاق اصطلاح تسليم المجرمين على هذه الصورة لأنه يمكن للشخص المطلوب أن يطعن في الحكم الصادر ضده بعد تسليمه للدولة الطالبة، وقد يغير ذلك الطعن في حالة الشخص المطلوب. مشار اليه من طرف، لحمر فافة، تسليم المجرمين في التشريع الجزائري على ضوء الاتفاقيات الدولية، مذكرة لنيل شهادة الماجستير في القانون العام، تخصص القوانين الإجرائية والتنظيم القضائي، كلية الحقوق والعلوم السياسية، جامعة وهران، السنة الجامعية 2013-2014، ص. 7.

[1]- Cf. André Huet et Renée Koering Joulin, Droit pénal international, 2ème éd., Puf, 1994, p.356.

[2]- منتصر سعيد حمودة، الإرهاب الدولي جوانبه القانونية ووسائل مكافحته في القانون الدولي العام والفقه الإسلامي، د.ط، دار الجامعة الجديدة، الإسكندرية، 2006، ص. 340.

وتسليم المجرمين المبرمة بين الجزائر وفرنسا، اتفاقية الرياض العربية، ناهيك عن الاتفاقيات التي سنت لمواجهة الجرائم الإلكترونية، ومنها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، غير أنه وفي حال انعدام المعاهدات بين الدول، فإن التسليم يتم وفقا لما استقر عليه العرف الدولي في هذا الصدد، مع اشتراط مبدأ المعاملة بالمثل، غير أن ما ينبغي الإشارة إليه أن بعض الدول تقبل التسليم دون إعمالها لمبدأ المعاملة بالمثل، وذلك لأسباب سياسية[1].

استناداً لما سبق، يتبين أن التعريف الذي حظي بتأييد الأغلبية هو الذي يعرّف التسليم بأنه: «الإجراء الذي تسلم من خلاله دولة شخص موجود في إقليمها إلى دولة أخرى بناء على طلبها لتحاكمه عن جريمة يعاقب عليها قانونها، أو لتنفيذ حكم صادر عليه من محاكمها».

من خلال التعاريف السابقة يتضح أن التسليم لا يتم إلا بناء على طلب الدولة طالبة التسليم، وعليه إذا تم تسليم متهم بدون طلب الدولة الأخرى، فإن ذلك الإجراء لا يندرج ضمن نظام التسليم، كما أن التسليم يتم بين دول ذات سيادة، فإذا تم إلى جهة قضائية دولية فلا يطلق عليه التسليم، بل مصطلح التقديم.

بهذا يمكن القول أن التسليم كنظام قائم بذاته يتميز عن غيره من الأنظمة القانونية التي تبدو مشابهة له، فهو يتميز عن الإبعاد، ذلك أن هذا الأخير هو تكليف الشخص بمغادرة الإقليم أو إخراجه منه بغير رضاه، ويستند حق الدولة في الإبعاد إلى حقها في البقاء وصيانة النفس، فكما أن للدولة أن تمنع أي شخص من دخول إقليمها إذا كان في ذلك ما يهدد أمنها وسلامتها، فإنها وبالمثل يكون لها كذلك أن تخرج أي أجنبي من إقليمها متى كان في وجوده خطر عليها، وعليه لا يخص الإبعاد غير الأجانب سواء كان وجودهم على إقليم الدولة دائما أو مؤقتا[2].

---

[1]- سامح أحمد بلتاجي موسى، المرجع السابق ، ص. 514.

[2]- علي صادق أبو هيف، القانون الدولي العام، الأصول والمبادئ العامة، أشخاص القانون الدولي العام، النطاق الدولي، العلاقات الدولية، التنظيم الدولي، المنازعات الدولية، الحرب والحياد، ط الحادية عشر، منشأة المعارف، الإسكندرية، د.س.ن، ص. 257.

وعليه يعدّ الإبعاد قرار إداري يضع حدا لإقامة أجنبي داخل البلاد، وكما يختلف التسليم عن الإبعاد، فهو يختلف كذلك عن المنع من دخول البلاد الذي يقصد به عدم تمكين شخص ما من اجتياز حدود بلد معين.

وبالمثل يتميز التسليم عن الإعادة إلى الوطن الذي يراد منه إعادة بعض الأشخاص إلى بلادهم دون أن تطلبهم دولتهم، وغالبا ما تتم الإعادة إلى الوطن في سياق غير جنائي، بمعنى لا ينبغي أن يكون الشخص الذي يتم إعادته إلى وطنه متهما أو محكوما عليه بخلاف ما هو عليه الوضع في التسليم.

ولئن كان هذا هو المقصود بالتسليم، فإنه يتوجب الإشارة إلى أن الفقه يفرّق في تسليم المجرمين بين نوعين من التسليم؛ تسليم إيجابي وتسليم سلبي، فالتسليم السلبي هو ذلك التسليم الذي يتضمن ضمانات قضائية ويتميز بالصبغة الإجرائية، ولا ينبغي أن يتم بناء على طلب الدولة الأجنبية، بل يجوز أن تحرك إجراءاته بناء على رغبة الدولة التي يوجد بها المتهم أو المحكوم عليه، ويمر هذا النوع من التسليم بمرحلتين الأولى قضائية، ويكون الهدف منها حماية الحقوق الشخصية للمتهم أو المحكوم عليه، ويتعلق بالفعل الذي من أجله تم طلب التسليم في حين تكون المرحلة الثانية إدارية، وفيها تعمل الدولة على التعبير عن قرارها بشأن التسليم معتمدة في ذلك على سيادتها[1].

وإذا كان هذا هو التسليم السلبي، فإن التسليم الإيجابي يبرز حينما تطلب دولة أجنبية تسليم المتهم أو المحكوم عليه، ويكون هذا التسليم ذو طبيعة إدارية، إذ غالبا ما يطلب من وزارة العدل عن طريق السلك الدبلوماسي ووزارة الخارجية، وتتم طلبات تسليم المجرمين وفقا لقوانين كل دولة، وذلك ما أكدت عليه المادة 5/31 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، حيث نصت على خضوع تسليم المجرمين للشروط المنصوص عليها في قانون الدولة الطرف التي يقدم إليها الطلب أو لمعاهدات التسليم المطبقة[2].

[1]- حطاب كمال، المرجع السابق، ص. 377.
[2]- المرجع نفسه، ص. 378.

وعليه يلاحظ أن عملية تسليم المجرمين غالبا ما تضبط بمقتضى معاهدات دولية، وقد تكون هذه المعاهدات ثنائية كما أنها قد تكون متعددة، ومن أهم الاتفاقيات الثنائية الاتفاقية الجزائرية الفرنسية المتعلقة بتنفيذ الأحكام وتسليم المجرمين.

ومن الاتفاقيات المتعددة، اتفاقية الرياض العربية، والاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

إلى جانب هذا التقسيم، يمكن أن تكون اتفاقيات التسليم دولية تتضمن أحكاما متعلقة بتسليم المجرمين دون أن تكون بحد ذاتها اتفاقية تسليم، ولعل ما تجدر الإشارة إليه، أنه وفي حال انعدام المعاهدات بين الدول، وانعدام التشريع الداخلي المنظم لمسألة التسليم، فإنه لا يكون أمام الدول حل غير القبول بنظام التسليم طبقا لما استقر عليه العرف الدولي، مع اشتراط المعاملة بالمثل، ولكن الملاحظ أن بعض الدول تطبق الأعراف الدولية دون استنادها للمبدأ السابق ذكره لأسباب سياسية.

من منطلق ما تقدم، يمكن القول أن التسليم يخص فئتين من الأشخاص، فئة المتهمين وفئة المحكومين، فأما الفئة الأولى، فيندرج ضمنها الحالة التي يقترف فيها الشخص جريمة في بلد ما، ثم قبل أن يلقى عليه القبض يهرب إلى بلد آخر فتطلب الحكومة التي وقعت على ترابها الجريمة استرداد ذلك المتهم لملاحقته ومحاكمته أمام القضاء.

هذا عن الفئة الأولى، أما الفئة الثانية فتبرز حين يقترف الشخص جرما ما فيلاحق وتصدر المحاكم التي وقعت على ترابها الجريمة قرارها، وحكمها عليه في الجريمة المنسوبة إليه، وقبل أن ينفذ الحكم القطعي البات يفر هاربا إلى بلد آخر، فتطلب الحكومة التي حكمت عليه من الدولة المتواجد عندها استرداده، وتسليمه لتنفيذ الحكم والعقوبة المحكوم عليه بها قبل هروبه إلى دولة أجنبية.

وقد أشارت لهذه المسألة المادة 696 قانون الإجراءات الجزائية الجزائري[1] حينما حددت حالتين لتسليم الشخص إلى حكومة أجنبية، وحصرتهما في التسليم لاتخاذ إجراءات

[1]- تنص المادة 1/696 من الأمر رقم 66-155 المؤرخ في 8 يونيو سنة 1966 المتضمن قانون الإجراءات الجزائية الجزائري المعدل والمتمم، سابق الإشارة إليه: " يجوز للحكومة الجزائرية أن تسلم شخصا غير جزائري إلى حكومة =

المتابعة ضده عن جريمة معينة باعتباره متهما، أو التسليم بسبب صدور حكم ضده باعتباره محكوما عليه.

لعل ما ينبغي التنويه إليه أن تسليم المحكوم عليه لا يعد بمثابة تنفيذ للحكم الجزائي الأجنبي، لأن تنفيذ هذا الأخير لا يكون إلا بتطبيق العقوبة التي يُقضى بها على الشخص المجرم، ولا يعد التسليم تنفيذا للعقوبة، بل هو مجرد وسيلة تجعل التنفيذ ممكنا، بحيث تظل مسؤولية التنفيذ من اختصاص الدولة طالبة التسليم[1].

هذا على المستوى الفقهي، أما على المستوى التشريعي، فيلاحظ أن مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC)[2] عرّف التسليم في دليل التعاون الدولي في المسائل الجنائية لمكافحة الإرهاب وذلك سنة 2009، واعتبره «قيام الدولة المطلوب منها التسليم بتسليم شخص يوجد في إقليمها إلى دولة أخرى وهي الدولة الطالبة، ذلك أن هذه الأخيرة كانت تبحث عنه إما بهدف محاكمته، أو بهدف تسليط العقوبة التي حكمت بها عليه محاكمها».

في حين عرّفته ذات الهيئة[3] في دليل المساعدة القانونية المتبادلة، وتسليم المجرمين بأنه: «العملية الإجرائية الرسمية، التي تطلب بواسطتها إحدى الولايات القضائية من ولاية قضائية أخرى إنفاذ إعادة شخص موجود في الولاية القضائية متلقية الطلب، متهم أو مدان بارتكاب جرم جنائي واحد أو أكثر انتهاكا لقانون الولاية القضائية الطالبة، وتلتمس الإعادة لكي يواجه ذلك الشخص المحاكمة في الولاية القضائية الطالبة، أو لكي توقع عليه العقوبة على ذلك الجرم أو الجرائم».

=أجنبية بناء على طلبها إذا وجد في أراضي الجمهورية وكانت قد اتخذت في شأنه إجراءات متابعة باسم الدولة الطالبة أو صدر حكم ضده من محاكمها."

[1]- لحمر فافة، المرجع السابق، ص. 10.

[2]- مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC)، دليل التعاون الدولي في المسائل الجنائية لمكافحة الإرهاب، مكتب الأمم المتحدة، فيينا، 2009، ص. 201.

[3]- مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC)، دليل المساعدة القانونية المتبادلة، تسليم المجرمين، مكتب الأمم المتحدة، فيينا 2013، ص. 41.

البند الثاني: شروط تسليم المجرمين.

يستلزم تسليم المجرمين تحقق جملة من الشروط منها ما يتعلق بالشخص المطلوب تسليمه، ومنها ما يتعلق بالجريمة المطلوب التسليم لأجلها، ولأهمية هذه الشروط سيتم التعرض لها مع بيان مدى إمكانية تحققها في الجرائم الماسة بالمستند الإلكتروني.

أولاً: الشروط المتعلقة بالشخص المطلوب تسليمه.

نظراً لأن الشخص المطلوب تسليمه هو محور موضوع إجراءات التسليم، فإنه لا بد من الإشارة إلى أن هناك شروطاً أساسية ينبغي التطرق لها حين التعرض لشروط التسليم، ومن هذه الشروط ما يكون وطيد الصلة بالجنسية، ومنها ما يكون شديد الارتباط بحالة الشخص المطلوب تسليمه.

فبخصوص الشروط المتعلقة بالجنسية يمكن القول أن الجنسية باعتبارها رابطة سياسية وقانونية بين الشخص والدولة[1]، تتحكم كثيراً في القيام بعملية التسليم، بحيث يكون من اللازم على دولة الملجأ تسليم الشخص إلى الدولة الطالبة، إذا كان ذلك الأخير يحمل جنسيتها طبعا متى توفرت باقي شروط التسليم الأخرى[2]، وذلك بخلاف ما إذا كان الشخص المطلوب تسليمه يحمل جنسية الدولة المطلوب منها التسليم، إذ لا يكون لهذه الأخيرة تسلمه لأنه يرتبط معها برابطة الولاء من جهة، أو لأن الدولة تكون ملزمة بتوفير الحماية لمواطنيها من جهة أخرى، وقد تبنت هذا الحل[3] معظم الاتفاقيات الدولية، وكذا التشريعات الوطنية، وقد كرس المشرع الجزائري هذا الحل بمقتضى المادة 1/698 من قانون الإجراءات الجزائية حيث قرر عدم قبول التسليم إذا كان الشخص المطلوب تسليمه جزائري الجنسية، والعبرة بتقدير تلك الصفة بوقت وقوع الجريمة المطلوب التسليم من أجلها[4]، وهو الأمر ذاته الذي

---

[1]- الطيب زروتي، الوسيط في الجنسية الجزائرية، دراسة تحليلية مقارنة بالقوانين العربية والقانون الفرنسي، مطبعة الكاهنة، الجزائر، 2002، ص. 19.

[2]- منتصر سعيد حمودة، المرجع السابق، ص، ص. 341- 342.

[3]- إن مبدأ امتناع تسليم المواطنين هو مبدأ قديم تعود جذوره التاريخية إلى ماضي بعيد استقر به عرفٌ يبرر حماية الدولة لرعاياها إعمالا لحقها في السيادة. مشار إليه من طرف، لحمر فافة، المرجع السابق، ص. 22.

[4]- تنص المادة 1/698 من الأمر رقم 66-155 المؤرخ في 8 يونيو سنة 1966 المتضمن قانون الإجراءات الجزائية الجزائري المعدل والمتمم، سابق الإشارة إليه: " لا يقبل التسليم في الحالات الآتية:=

تبنته غالبية الاتفاقيات المتعلقة بتسليم المجرمين، والتي أبرمتها الجزائر مع مختلف دول العالم، طبعا ما لم تقرر الاتفاقية الدولية خلاف ذلك، ومن ذلك ما قررته الاتفاقية الجزائرية البريطانية المتعلقة بتسليم المجرمين، والتي أشارت في نص المادة 1/3 منها على الإمكانية المخولة لكل طرف في أن يسلم مواطنيه للطرف الآخر شريطة أن يسمح تشريعه بذلك، وهو الأمر الذي لا يسمح به التشريع الجزائري[1].

استنادا لما تقدم، يتوجب الذكر أنه إذا ما تجنس الهارب بجنسية دولة الملجأ قبل ارتكابه الجريمة، فإنه لا يجوز تسليمه لأنه يعد من مواطني الدولة الجزائرية، وذلك استنادا لنص المادة 1/698 قانون الإجراءات الجزائية الجزائري التي لم تستلزم تمتع الشخص المطلوب تسليمه بالجنسية الجزائرية الأصلية، بل اكتفت بضرورة أن يكون الشخص المطلوب تسليمه جزائري الجنسية وقت وقوع الجريمة المطلوب التسليم لأجلها، وعليه إذا كان الشخص جزائري الجنسية قبل ارتكاب الجريمة وفقد الجنسية الجزائرية وقت ارتكاب الجريمة على إثر اكتسابه جنسية دولة أخرى، فهنا يتوجب تسليمه للدولة طالبة التسليم، لأنه لم يعد من مواطني الدولة الجزائرية.

وذات الأمر ينطبق على من اكتسب الجنسية الجزائرية بعد ارتكابه للجريمة، وقد قررت اتفاقية الرياض العربية المبدأ السالف ذكره في نص المادة 39 منها حيث استوجبت أن لا يكون الشخص المطلوب تسليمه يتمتع بجنسية الدولة المطلوب منها التسليم، وحدد ذلك بتاريخ وقوع الجريمة المطلوب التسليم لأجلها[2].

=1- إذا كان الشخص المطلوب تسليمه جزائري والعبرة في تقدير الصفة بوقت وقوع الجريمة المطلوب التسليم من أجلها."

[1]- لحمر فافة، المرجع السابق، ص. 22.

[2]- تنص المادة 39 من اتفاقية الرياض العربية للتعاون القضائي، سابق الإشارة لها: " يجوز لكل طرف من الأطراف المتعاقدة أن يمتنع عن تسليم مواطنيه ويتعهد في الحدود التي يمتد إليها اختصاصه، بتوجيه الإتهام ضد من يرتكب منهم لدى أي من الأطراف المتعاقدة الأخرى جرائم معاقب عليها في قانون كل من الدولتين بعقوبة سالبة حرية مدتها سنة أو بعقوبة أشد لدى أي من الطرفينالمتعاقدين وذلك إذا ما وجه إليه الطرف المتعاقد الآخر طلبا بالملاحقة مصحوبا بالملفات والوثائق والأشياء والمعلومات التي تكون في حيازته ويحاط الطرف المتعاقد الطالب علما بما تم في شأن طلبه.
وتحدد الجنسية في تاريخ وقوع الجريمة المطلوب من أجلها التسليم."

وبالمثل تتجه غالبية الاتفاقيات الدولية التي ترتبط بها الجزائر مع مختلف دول العالم إلى تحديد الجنسية بوقت وقوع الجريمة[1]، باستثناء البعض منها حيث يُقدر مدى تمتع الشخص بجنسية الدولة المطلوب منها التسليم بوقت وصول طلب التسليم، ومن ذلك اتفاقية التعاون القضائي والقانوني في المواد المدنية، والاتفاقية الجزائرية بين الجزائر ورومانيا[2]، وكذا تلك المبرمة مع الصين[3].

إن مبدأ عدم جواز تسليم المواطنين لا يعني إفلات الجاني من العقاب، وعليه فإذا رفضت الدولة الجزائرية تسليم أحد مواطنيها للحفاظ على سيادتها في حماية رعاياها لا يمنعها من متابعة الجاني أو محاكمته، وقد أكدت على ذلك صراحة المادة 39 من اتفاقية الرياض العربية، حيث خولت لكل طرف من الأطراف المتعاقدة إمكانية الامتناع عن تسليم مواطنيه على أن يتعهد في الحدود التي يمتد إليها اختصاصه بتوجيه الاتهام ضد من يرتكب منهم لدى أي من الأطراف المتعاقدة.

وهو ذات الحكم الذي قررته باقي الاتفاقيات التي أبرمتها الجزائر في مجال تسليم المجرمين، كالاتفاقية الجزائرية التونسية م2/27، الاتفاقية الجزائرية المصرية م 24، الاتفاقية الجزائرية البلجيكية م 31، الاتفاقية الجزائرية الليبية 31، الجزائرية الفرنسية 12، الجزائرية البريطانية 3، وكذا الاتفاقية الجزائرية البرتغالية 3، وكذا الاتفاقية الجزائرية الإيرانية م 3.

وعلى الخلاف من ذلك، إذا كان الهارب ينتمي لدولة ثالثة ليست هي دولة الملجأ، ولا هي الدولة طالب التسليم، فهنا يجوز حسب نص المادة 696 قانون الإجراءات الجزائية الجزائري على الحكومة الجزائرية أن تسلم الأجنبي الذي لا يعد من رعايا الدولة الطالبة، إذا ما ارتكبت الجريمة على أراضي الدولة الطالبة أو خارج أراضيها إذا كانت الجريمة من

[1]- من ذلك الاتفاقية الجزائرية المغربية (م 32)، الاتفاقية المبرمة بين الجزائر والإمارات العربية المتحدة (م 24)، تركيا (م 34)، تونس (27)، النيجر (28)، كوبا (30).
[2]- م 34 من الاتفاقية المبرمة بين الجزائر ورومانيا.
[3]- (م3/د) من إتفاقية تسليم المجرمين المبرمة بين الجزائر والصين

الجرائم التي يجيز القانون الجزائري المتابعة فيها في الجزائر، حتى ولو ارتكبت من طرف أجنبي في الخارج.

ويطبق الأمر ذاته في مجال الجرائم الماسة بالمحررات الإلكترونية، بحيث لا يجوز للدولة الجزائرية أن تسلم الشخص الذي يعمد إلى المساس بالمحررات الإلكترونية متى كان هذا الأخير جزائري الجنسية وقت ارتكاب الجريمة، بخلاف ذلك فإنه يتوجب عليها تسليمه لدولة الملجأ إذا كان يحمل جنسيتها، وتوفرت باقي شروط التسليم الأخرى.

أما إذا كان مرتكب الجريمة لا ينتمي لدولة الملجأ ولا للدولة الطالبة، فهنا يجوز للدولة المطلوب منها التسليم تسليمه، وهو ما تقرر في قضية "حمزة بن دلاج" الهاكر الجزائري الذي سلمته السلطات التايلاندية سنة 2013 بعد أن اعتقلته بالتعاون مع جهاز الإنتربول الدولي في العاصمة بانكوك بتهمة التورط في جرائم الإنترنت، بعد أن تم توقيفه أثناء عبوره المطار بكونه من الشخصيات المطلوب تسليمها من قبل مكتب التحقيقات الفيدرالي[1].

هذا عن الشروط الخاصة بالجنسية، أما بخصوص الشروط المتعلقة بحالة الشخص، فإنه يتوجب الذكر أنه وفي ظل عدم وجود نص في قانون الإجراءات الجزائية يكون للدولة المطلوب منها التسليم السلطة التقديرية في قبول أو رفض طلب التسليم مع مراعاة الاعتبارات الاستثنائية، طبعا ما لم توجد اتفاقية تقضي بخلاف ذلك، لأن وجود الاتفاقية يستلزم تطبيقها بالأولوية على النص القانوني تكريسا لمبدأ سمو المعاهدة على القانون المقرر في المادة 150 من الدستور الجزائري[2].

وفي هذا الصدد يتوجب الذكر أن من الاتفاقيات الواردة لمعالجة هذه المسألة الاتفاقية القضائية الخاصة بالتعاون القضائي في المجال الجزائي، وتسليم المجرمين بين الجزائر والصين والتي قررت في المادة 4 منها التي وردت تحت عنوان الأسباب التقديرية للرفض،

[1]- http://ar.m.wikipedia.org/wil. Date de consultation le site 12-12-2018 à 18:30.

[2]- تنص المادة 150 من قانون رقم 16-01 مؤرخ في 26 جمادى الأولى عام 1437 الموافق 6 مارس سنة 2016، يتضمن التعديل الدستوري، ج.ر، ع14، س.2016: "المعاهدات التي يصادق عليها رئيس الجمهورية، حسب الشروط المنصوص عليها في الدستور تسمو على القانون."

بجواز رفض التسليم، إذا كان يتنافى مع اعتبارات إنسانية بسبب سن الشخص أو حالته الصحية أو لظروف أخرى تتعلق بالشخص المطلوب، وهو ذات ما أكدت عليه المادة 5 من اتفاقية تسليم المجرمين بين الجزائر والبرتغال[1].

إن حظر التسليم لا يقتصر على الأشخاص السابق الإشارة لهم، بل يشمل إلى جانب ذلك اللاجئ السياسي، وهو الأجنبي الهارب الذي يحتاج إلى المساعدة المادية والحماية القانونية[2]، وذلك بسبب أن الشخص المستفيد من حق اللجوء السياسي لا يعتبر مجرماً بالمعنى الذي يحمله هذا الاصطلاح في علم الإجرام أو علم الاجتماع.

كما لا يجوز تسليم الأشخاص الذين تمت محاكمتهم عن ذات الجريمة المطلوب تسليمهم لأجلها، وعليه إذا كان الشخص المطلوب تسليمه قد سبقت محاكمته في الجريمة المطلوب تسليمه لأجلها فتمت تبرئته منها أو عوقب عنها فإنه لا يجوز تسليمه، ليس هذا فحسب، بل لا يجوز كذلك تسليم الشخص متى كان قيد التحقيق والمحاكمة عند ارتكابه فعلا ما هو ذاته المطلوب تسليمه لأجله، ويُعد هذا الشرط من الضمانات الأساسية عند محاكمة الشخص المطلوب تسليمه، وهو يرمي إلى توفير أكبر قدر من الحماية القضائية للشخص المطلوب تسليمه في الدولة الطالبة، وذلك حتى لا يتعرض هذا الشخص لعقوبة مزدوجة[3].

ثانياً: الشروط المتعلقة بالجريمة المطلوب التسليم لأجلها.

لا ريب في أن تسليم المجرمين عموما، وتسليم مجرمي الأنظمة المعلوماتية خاصة يستلزم إلى جانب توافر الشروط المتعلقة بالشخص المطلوب تسليمه، توفر شروط أخرى تتعلق بالجريمة المطلوب التسليم لأجلها، وعليه يعد تحديد طبيعة الجرائم التي تخضع لنطاق التسليم في غاية الأهمية، كون أنه يحدد ما إذا كان يجوز التسليم أو لا، وفي هذا تختلف الدول فيما بينها في تحديدها للجرائم التي يجوز التسليم لأجلها، ويتراوح الأمر بين ثلاث

[1]- لحمر فافة، المرجع السابق، ص. 26.
[2]- المرجع نفسه، ص. 27.
[3]- طارق فوزي الفقي، المرجع السابق، ص. 274.

اتجاهات[1]، فهناك أسلوب الحصر أو ما يطلق عليه تسمية نهج القائمة، وفي هذا الأسلوب تقوم الدولة بوضع قائمة في القانون أو في الاتفاقية، وتعمد فيها إلى إدراج مجموعة من الجرائم التي يتم التسليم لأجلها، ويكون تحديد تلك الجرائم وارد على سبيل الحصر.

للإشارة، فإن هذا الأسلوب يعد من أقل الأساليب شيوعاً وانتشاراً بين الدول، ذلك أنه يؤدي إلى إفلات بعض المجرمين من العقاب متى ما كانت الجريمة غير واردة في القائمة[2].

إلى جانب هذا الأسلوب، يوجد أسلوب آخر هو أسلوب جسامة الجريمة أو الحد الأدنى للعقوبة، ويعد هذا الأسلوب أكثر الأساليب شيوعاً في تحديد الجرائم التي يجوز التسليم فيها، إذ وبمقتضاه تحدد الدول تشريعاتها الداخلية أو في المعاهدات المنظمة لها سواء كانت ثنائية أو متعددة الأطراف، الحد الأدنى للعقوبة المقررة للجرائم التي يمكن أن يتم التسليم لأجلها.

ولا يقتصر الأمر على النظامين السالف ذكرهما، بل يوجد كذلك النظام المختلط، وهو من الأساليب الشائعة في تحديد الجرائم الجائز التسليم فيها، وما يميز هذا النظام أنه يحقق فائدتين فهو من جهة يضمن درجة معينة من جسامة الجريمة المعاقب عليها في البلدين ليتم التسليم وفقا لها، كما أنه يضمن من جهة أخرى خضوع جرائم محددة تمثل خطرا على الدول الأطراف للتسليم دون النظر لدرجة جسامتها أو العقوبة المقررة لها.

وقد أخذت بهذا الأسلوب الاتفاقية الأوروبية للإجرام المعلوماتي حيث ورد في المادة 24 منها أن مقتضيات هذه المادة: «تطبق على عملية تسليم المجرمين فيما بين الدول الأطراف بالنسبة للجرائم المنصوص عليها وفقا للمواد من 2- 11 -وتعالج هذه المواد كل من الدخول غير المشروع (2)، الاعتراض غير المشروع (3)، التدخل في البيانات (4)، التدخل غير المشروع في المنظومة (5)، إساءة استخدام الأجهزة (6)، جريمة التزوير المتعلقة بالكمبيوتر (7)، جريمة التدليس المتعلقة بالكمبيوتر (8)، الجرائم المتعلقة بالأعمال الإباحية وصور الأطفال الفاضحة (9)، الجرائم المتعلقة بالانتهاكات الخاصة بحقوق الطبع

[1]- طارق فوزي الفقي، المرجع السابق، ص. 275.

[2]- حسين بن سعيد بن سيف الغافري، الجهود الدولية في مواجهة جرائم الإنترنت، منشورة على موقع المنشاوي للدراسات والبحوث، ص .29.

www.minshawi.com. Date de consultation le site 14-12-2018 à18 :00

والنشر، والحقوق المتعلقة بها (10)، الشروع والمساعدة والتحريض (11)-، من هذه الاتفاقية بشرط أن يعاقب عليها بموجب القوانين بالدولتين المعنيتين طرفي الاتفاقية بالحرمان من الحرية لفترة لا تزيد عن سنة واحدة على الأقل، أو بعقوبة أشد».

وهو ذات الأسلوب الذي تبنته الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، والتي ورد في المادة 31 منها بأن تسليم المجرمين ينطبق على الجرائم المنصوص عليها في الفصل الثاني من الاتفاقية بشرط أن تكون تلك الجرائم يعاقب عليها في قوانين الدول الأطراف المعنية بسلب الحرية لفترة أدناها سنة واحدة أو بعقوبة أشد، وتشمل الجرائم المذكورة في الفصل الثاني من الاتفاقية كل من جريمة الدخول غير المشروع (6)، جريمة الاعتراض غير المشروع (7)، الاعتداء على سلامة البيانات (8)، جريمة إساءة استخدام وسائل تقنية المعلومات (8)، جريمة التزوير (10)، جريمة الاحتيال (11)، الجريمة الإباحية والجرائم المرتبطة بها (12- 13)، جريمة الاعتداء على حرمة الحياة الخاصة (14)، الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات (15)، الجرائم المتعلقة بالجرائم المنظمة والمرتكبة بواسطة تقنية المعلومات (16)، الجرائم المتعلقة بانتهاك حقوق المؤلف والحقوق المجاورة (17)، الاستخدام غير المشروع لأدوات الدفع الإلكترونية (18).

وقد تبنت ذات الأمر اتفاقية الرياض العربية لتعاون القضائي التي دخلت حيز النفاذ ابتداءا من 1985/10/30 في المادة 40/أ، و التي وردت تحت عنوان الأشخاص الواجب تسليمهم.

في سياق ما سبق ذكره ينبغي الإشارة إلى أنه يجوز القيام بعملية التسليم بشرط أنه لا تكون الدعوى العمومية أو الحكم القاضي بفرض عقوبة محددة قد انقضى بسبب من أسباب الانقضاء المحددة في تشريعات الدولة الطالبة، والدولة المطلوب منها التسليم أو الدولة التي ارتكبت الجريمة على أرضها.

إن الأمر لا يقتصر على الشروط السالف ذكرها، بل لا بد أن يكون الفعل المقترف يعد جريمة في تشريعات الدولة الطالبة، وكذا الدولة المطلوب منها التسليم، وهو ما يعبر عنه

بشرط التجريم المزدوج، إذ وبخصوص هذا الشرط ينبغي الذكر أنه لا بد أن يكون الفعل مجرّما أيا كانت الصورة التشريعية المعاقب عليها، إذ لا عبرة للوصف أو التكييف القانوني الذي يطلق على الفعل عند تقرير توافر هذه الشروط.

ولا ريب أن شرط التجريم المزدوج يجد أساسه في رغبة الدولة طالبة التسليم في محاكمة من نسب إليه ارتكاب السلوك الإجرامي أو تنفيذ العقوبة المحكوم بها عليه، بسبب أن السلوك مجرم في تشريعها، ذلك أنه إذا لم يكن مجرما فلا يتصور صدور حكم يقضي بعقوبة عليه.

هذا من جهة، ومن جهة أخرى لا يجوز أن تتم مطالبة الدولة المطلوب إليها التسليم بإيقاع عقوبة على ارتكاب سلوك ما هو في الأساس غير مجرم وفقا لقانونها.

لأهمية هذا الشرط عمد المشرع الجزائري إلى استلزامه في نص المادة 2/697 من قانون الإجراءات الجزائية، كما وتبنته العديد من الاتفاقيات والمعاهدات المتعلقة بتسليم المجرمين، ومن ذلك ما قضت به المادة 02 من المعاهدة النموذجية للأمم المتحدة بشأن تسليم المجرمين، والمادة 03 من اتفاقية جامعة الدول العربية بتسليم المجرمين، المادة 40 من اتفاقية الرياض العربية للتعاون القضائي، وكذا المادة 24 من الاتفاقية الأوروبية للإجرام المعلوماتي.

ولم يظل الأمر حبيس النصوص القانونية، بل تم إعمال هذا الشرط أمام الهيئات القضائية، وذلك خلال سنوات التسعينات على إثر الهجوم الذي شنه شاب روسي على مصرف (Sity Banc)، من خلال استخدام حاسوبه الموجود في روسيا للقيام بعملية اختراق دون إذن وحدات خدمة حواسيب المصرف في الولايات المتحدة، كما وقام بتجنيد عدد من المتواطئين لفتح حسابات مصرفية في شتى أنحاء العالم، ثم أصدر تعليمات إلى حاسوب (Sity Banc) لتحويل أموال إلى تلك الحسابات، غير أنه عند اكتشاف المخطط وتحديد هوية المتهم، صدر بحقه أمر اعتقال من محكمة اتحادية بالولايات المتحدة، ورغم ذلك لم يسر في حقه أمر الاعتقال.

غير أنه وبسبب خطئه الذي ارتكبه بزيارته لانجلترا لحضور معرض للحواسيب، سعت السلطات البريطانية إلى التعاون لتسليمه لمواجهة التهم الموجهة ضده في الولايات المتحدة، ذلك أنه وفقا لترتيبات تسليم المجرمين النافذة بين المملكة المتحدة والولايات المتحدة، يمكن لسلطات الملكة المتحدة أن تقوم بتقديم المساعدة ما دامت الجريمة موضع الاتهام لها ما يقابلها في قانون المملكة المتحدة.

على إثر ذلك طلب المتهم من المحكمة النظر في قانونية القبض عليه للطعن في تسليمه، وقدم لذلك حججا منها أن تحويل الأموال قد صدر في روسيا، حيث توجد لوحة مفاتيح حاسوبه لا في الولايات المتحدة.

وارتأت المحكمة أن الوجود المادي للمتهم في (سان بطرسبرخ) أقل أهمية من كونه باشر عملياته على أقراص ممغنطة موجودة في الولايات المتحدة، ناهيك عن أن الأفعال الموجهة للمتهم لها ما يقابلها في قانون إساءة استعمال الحواسيب لعام 1990، ولو مارس عملياته من المملكة المتحدة بدلا من روسيا لكان الاختصاص القضائي للمحاكم الانجليزية، ولهذه الأسباب تم تسليم المتهم إلى الولايات المتحدة، حيث تمت إدانته وحكم عليه بعقوبة سالبة للحرية[1].

الفرع الثاني: إجراءات طلب التسليم.

يقصد بإجراءات طلب التسليم تلك القواعد ذات الطبيعة الإجرائية التي تتخذها الدول الأطراف في عملية التسليم وفقا لقوانينها الوطنية وتعهداتها لإتمام عملية التسليم، بهدف التوفيق بين المحافظة على حقوق الإنسان وحريته، وبين تأمين الصالح العام الناشئ عن ضرورات التعاون الدولي في مكافحة الجريمة، بحيث لا يفلت أي مجرم من العقاب[2].

ولا ريب في أن هذه الإجراءات تتقاسمها الدولتان الطالبة والمطلوب منها التسليم، سيما وأن طلب التسليم هو الأداة التي تحركها الدولة الطالبة لاسترداد الشخص المتهم أو

[1]- طارق فوزي الفقي، المرجع السابق، ص. 272.
[2]- حسين بن سعيد بن سيف الغافري، الجهود الدولية في مواجهة جرائم الإنترنت، المرجع السابق، ص.31.

المحكوم عليه، بحيث تعبر صراحة عن رغبتها في استلام الشخص المطلوب، إذ بدون ذلك الطلب لا يمكن أن ينشأ الحق في التسليم[1].

بسبب خطورة النتائج المنجرة عن هذا الإجراء استلزمت الاتفاقيات الدولية والتشريعات الوطنية تقديم طلب التسليم كتابياً، بحيث يشمل الطلب جملة من البيانات، تختلف باختلاف الغرض من التسليم، بحيث إذا كان التسليم من أجل المحاكمة فإن الطلب لا بد أن يتضمن عرضا مفصلا عن هوية المطلوب تسليمه، الوقائع المنسوبة إليه، أوصافه، جنسه، صورته إن أمكن، الإجراءات المتخذة ضده، كما يتم تقديم بيان دقيق للفعل المكون للجريمة، تاريخ ارتكاب ذلك الفعل، نسخة من النصوص المطبقة، أوراق الإجراءات الجزائية التي صدر بها الأمر رسميا لإحالة المتهم إلى جهة القضاء الجزائي، أو التي تؤدي إلى ذلك بقوة القانون، أو أمر القبض أو أي ورقة صادرة من السلطة القضائية ولها ذات القوة.

إن تقديم الوثائق السالف ذكرها يتقرر إذا كان الغرض من التسليم المحاكمة، أما إذا كان الغرض منه تنفيذ العقوبة، فإنه يتوجب إلى جانب الوثائق السالف الإشارة لها، تقديم الحكم الصادر بالعقوبة، وإن كان غيابيا فتقدم معلومات بخصوص ظروف غياب الشخص عن المحاكمة في حالة إدانته غيابيا، حق الطعن، وكل التفاصيل حول شكل ذلك الطعن أو المحاكمة، ناهيك عن المعلومات المتعلقة بالعقوبة الصادرة ضد الشخص المطلوب تسليمه، وكذا المدة التي قضاها في الحبس تنفيذاً لتلك العقوبة، والمعلومات التي تثبت أن الشخص المطلوب تسليمه هو نفسه الذي تمت إدانته.

للإشارة فإن المشرع الجزائري اشترط في مجال الوثائق المسلمة ضرورة تقديم أصول الأوراق المبينة أعلاه، أو نسخ رسمية منها، كما استلزم تحرير طلبات التسليم والوثائق المدعمة لها بلغة الدولة الطالبة، مع إرفاقها بترجمة إلى لغة الدول المطلوب منها التسليم أو إلى اللغة الفرنسية.

[1]- لحمر فافة، المرجع السابق، ص. 99.

تقدم الوثائق السالفة الذكر مع طلب التسليم، وذلك حتى تتمكن الدولة من الفصل في طلب التسليم طبقا لاتفاقيات التسليم وقانون الإجراءات الجزائية، وإغفال أي وثيقة من الوثائق المذكورة يؤدي إلى رفض طلب التسليم، باستثناء الوثائق التي تتعلق بظروف غياب الشخص عن المحاكمة في حالة إدانته غيابيا أو تلك المتعلقة بحق الطعن، إذ لا تؤثر تلك المعلومات على عملية التسليم، ذلك أن الدولة المطلوب إليها التسليم يمكنها إعادة مطالبة الدولة الطالبة بتكملتها إذا رأتها غير كافية، وتكون المطالبة بالمعلومات التكميلية في آجال معقولة تحددها الدولة المطلوب منها التسليم، وفي هذا يتوجب الذكر أن بعضا من الاتفاقيات حددت أجل 30 يوما لتكملة المعلومات، على أنه يكون في الإمكان تمديد الأجل بـ 15 يوماً بناء على طلب رسمي يقدمه الطرف الطالب، وفي حال عدم تقديم هذا الأخير لتلك المعلومات خلال المدة المقررة، فإن ذلك يعد تنازلاً طوعيا عن طلبه غير أنه يكون للطرف الطالب إمكانية تقديم طلب جديد للتسليم من أجل نفس الجريمة.

تطبق الإجراءات السابق تحديدها إذا كانت الجزائر هي الدولة المطلوب منها التسليم، أما إذا كانت هي طالبة التسليم، فإنه يتوجب عليها احترام الشروط والإجراءات التي حددتها الاتفاقية التي تربطها بالدولة المطلوب منها التسليم، وكذا مراعاة ما ينص عليه قانون الدولة المطلوب منها التسليم من شروط وإجراءات يجب اتخاذها لطلب التسليم.

لعلّ ما ينبغي التنويه إليه في هذا المقام هو الجهة التي يقدم إليها طلب التسليم، وفي هذا الإطار يمكن القول أن طلب التسليم يقدم عبر القنوات الدبلوماسية، بحيث يقدمه وزير خارجية الدولة الطالبة إلى وزير خارجية الدولة المطلوب منها التسليم، ثم يحال الطلب إلى الجهة التي تتولى فحص الطلب وهو الأمر الذي أشارت له غالبية الاتفاقيات، وكذا القانون الداخلي.

بهذا يمكن القول أن طلبات التسليم تتم كأصل عام عبر القنوات الدبلوماسية، بحيث يرسل طلب التسليم عبرها، ومرد ذلك أن التسليم عمل من أعمال السيادة تباشره حكومتي الدولة الطالبة، والدولة المطلوب منها التسليم.

ولئن كان المبدأ العام هو أن طلبات التسليم تتم عبر القنوات الدبلوماسية، فإنه ينبغي الإشارة إلى أن هذا المبدأ يرد عليه استثناء، ومفاد هذا الأخير تقديم الطلب ما بين وزارتي العدل للدولتين الطالبة والمطلوب منها التسليم، كما يمكن أن توجه تلك الطلبات من وزير العدل والنائب العام.

للإشارة فإنه بعد أن يقدم طلب التسليم إلى وزير الخارجية في الجزائر من خلال الطريق الدبلوماسي، تتم عملية تسليم الطلب بعد فحص المستندات إلى وزير العدل ليتحقق هذا الأخير من سلامة الطلب، ويمنح له الضوء الأخضر لبدء العمليات اللاحقة له، وخلال هذه المرحلة تقوم النيابة العامة بدورها في متابعة إجراءات التنفيذ.

بعد إتباع الإجراءات السالف ذكرها، وبعد نقل الملف بما فيه من مستندات ووثائق، ومحاضر، ينبغي على الجهة المختصة وهي الغرفة الجنائية بالمحكمة العليا الفصل فيه، بحيث تحدد جلسة في أجل ثمانية أيام كحد أقصى، يبدأ حسابها من تاريخ تبليغ المستندات إليها، ويجوز أن تمدد تلك المدة إلى ثمانية أيام إضافية إذا طلب ذلك الشخص المطلوب تسليمه أو النيابة العامة.

بعد أن تحدد الجلسة وتنعقد بالتاريخ المحدد، يتم استجواب الأجنبي ويحرر محضر بذلك بحضور محامي مقبول لدى المحكمة العليا ومترجم إذا تمسك المعني بذلك، وذلك كله في جلسة علنية كأصل عام، على أنه يمكن أن تنعقد جلسة سرية بناء على طلب النيابة العامة أو طلب الشخص المطلوب تسليمه.

بعد التأكد من هوية الشخص المطلوب تسليمه تتم كافة إجراءات جلسة المحاكمة وفقا لما تقرره القواعد العامة، كما يتحقق القاضي المختص من توفر كافة الشروط القانونية المنصوص عليها في المادة 702 من قانون الإجراءات الجزائية الجزائري[1] ويكون له بعد ذلك إما إصدار قرار قبول التسليم أو رفضه.

[1]- تنص المادة 702 من ق.إ.ج.ج،سابق الإشارة إليه:"يوجه طلب التسليم إلى الجكومة الجزائرية بالطريق الدبلوماسي ويرفق به إما الحكم الصادر بالعقوبة حتى ولو كان غيابيا وإما أوراق الإجراءات الجزائية التي صدر بها الأمر رسميا=

ويصدر القاضي قرار رفض التسليم إذا ما تبين له أن الشروط القانونية للتسليم غير مستوفاة، أو إذا اتضح له وجود خطأ في هوية الشخص المطلوب تسليمه، وعليه عند رفض التسليم ينبغي تسبيب الطلب كون أن الرفض يكون نهائيا غير قابل لأي طعن، ثم بعد ذلك يجب إعادة الملف إلى وزير العدل خلال مدة 8 أيام من انقضاء المواعيد المقررة في المادة 707 من قانون الإجراءات الجزائية الجزائري ويكون على وزير العدل خلال هذه الحالة إخطار الدولة الطالبة بقرار رفض التسليم.

هذا بشأن رفض الطلب، أما في حالة قبول طلب التسليم، فإنه يتوجب على الغرفة الجنائية بالمحكمة العليا الموافقة على طلب التسليم، مع تكليف النائب العام لدى المحكمة العليا بإطلاع وزير العدل بمضمون القرار، ليقوم هذا الأخير بالتوقيع على مرسوم الإذن التسليم.

وبعدها تقوم السلطات الجزائرية بتبليغ الدولة الطالبة بقرارها مع تحديدها لمكان وتاريخ تسليم الشخص المطلوب، فإن انقضت مدة شهر من تاريخ تبليغ المرسوم لحكومة الدولة الطالبة دون أن يقوم ممثلو هذه الأخيرة باستلام الشخص المقرر تسليمه، فإنه يفرج عنه، ولا يكون لهم فيما بعد المطالبة بتسليمه للسبب الذي طلب من خلاله تسليمه لهم لأول مرة.

=بإحالة المتهم إلى جهة القضاء الجزائي أو التي تؤدي إلى ذلك بقوة القانون وإما أمر القبض أو أية ورقة صادرة من السلطة القضائية ولها ذات القوة على أن تتضمن هذه الأوراق الأخيرة بيانا دقيقا للفعل الذي صدرت من أجله وتاريخ هذا الفعل.
ويجب أن تقدم أصول الأوراق المبينة عاليه أو نسخ رسمية فيها.
ويجب على الحكومة الطالبة أن تقدم في الوقت ذاته نسخة من النصوص المطبقة على الفعل المكون للجريمة وأن ترفق بيانا بوقائع الدعوى."

خاتمة

خاتمة

يعد شرف البحث عن الحقيقة من أنبل الرغبات الإنسانية، فهي المحرك لكل نشاط علمي، ولكل ما تفرزه الحضارة من جديد، وفي المجال الجنائي تعتبر معرفة الحقيقة الشرط الأول للعدالة، فبدون حقيقة لا توجد عدالة، وبدون عدالة لا يوجد أمن ولا نظام ومن ثم لا يوجد تقدم اجتماعي.

وعليه فقد حاول الباحث عبر ثنايا هذه الدراسات الماثلة إماطة اللثام عن الحماية الجنائية للمستندات الإلكترونية باعتبارها إشكالية نحسبها من أهم موضوعات السياسة الجنائية المعاصرة، والتي تعد من نتاج الثورة المعلوماتية التي جاء بها الحاسب الآلي التي كان من بين إيجابياتها تغيير أوجه الحياة إلى الأحسن والأفضل.

حيث تم من خلال هذا البحث محاولة التطرق إلى مختلف النقاط المهمة التي أثارتها إشكالية هذا الموضوع، وهذا كله لتوضيح مدى فاعلية هذه الحماية الجزائية في تحقيق الثقة والأمان في البيئة الإلكترونية، لا سيما وأن هذه التعاملات غالبا ما تتم في وسط مفتوح وعبر عالم افتراضي، وبين أشخاص قد لا يجمعهم مكان واحد.

وقد تم ذلك عن طريق محاولة وضع اليد على مواطن القوة والخلل في بعض التشريعات خاصة التشريع الجزائري، وكذا عن طريق الاسترشاد بما جاءت به تشريعات مقارنة من نصوص وقوانين، كما تم الإستعانة بما اجتهد بشأنه القضاء خلال بعض الأحكام ذات الصلة، وما أعطاه الفقه من حلول لبعض المشكلات، وفي سبيل تحقيق ما سبق ذكره تم تقسيم هذه الدراسة إلى بابين حيث تم التطرق في الباب الأول إلى دراسة النظام القانوني للمستند الإلكتروني، ذلك أن إلقاء الضوء على مدى الحماية الجزائية المقررة للمستند لا تتأتى إلا بالبحث في نظامه القانوني بالدرجة الأولى، خاصة وأن أهم ما يميز هذا المستند هو صفته الإلكترونية التي تجعله يتم بطرق معلوماتية آلية، فضلا عن ذلك فإن ظهوره والتعامل به قد أدى إلى اختفاء الكتابة التقليدية ذات الوجود المادي الملموس، وكذا اختفاء التوقيع الخطي التقليدي ليحل محلهما الكتابة الإلكترونية والتوقيع الإلكتروني.

وقد أثار البحث في هذا الباب الكثير من الإشكالات على المستوى التنظيمي والقانوني وكذا التقني حول كيفية حماية هذه المستندات التي قد تحوي على بيانات ومعلومات قد تكون على قدر كبير من الأهمية، سواء كانت هذه الحماية قانونية أو فنية، كما أثير التساؤل حول مدى القوة الثبوتية لهذه المستندات سواء من الناحية المدنية أو من الناحية الجزائية.

وقد تم تقسيم هذا الباب إلى فصلين، حيث تم التطرق في الفصل الأول إلى الضوابط القانونية للمستند الإلكتروني، أما الفصل الثاني فتم التطرق فيه إلى الضوابط الفنية لهذا المستند، ومن خلال هذا الباب تم التوصل إلى النتائج الآتية:

- إن المفاهيم المتعلقة بالمستند الإلكتروني الواردة في التشريعات المقارنة الأجنبية والعربية لم تتوصل إلى إبراز كل المميزات والخصوصيات المتعلقة بالمستند الإلكتروني، وإن المشرع الجزائري لم يضع تعريفاً محدداً لهذا المستند وبناء على ذلك فإن التعريف الأمثل للمستند الإلكتروني يتمثل في أنه كل وثيقة أو ورقة أو محرر أو مجموعة محررات إلكترونية تتضمن معلومات وبيانات مكتوبة ومسجلة بطريقة إلكترونية آلية وموضوعة على دعامة إلكترونية، على أن تكون هذه الوثيقة أو هذه المحررات تتضمن معلومات وبيانات متعلقة بواقعة لها أهمية قانونية ويستوي أن تكون هذه المحررات متضمنة لتوقيع إلكتروني تثبت هوية صاحبها، أو تكون غير موقعة.

- بالرغم من تدخل المشرع الجزائري في أكثر من موضع بنصوص قانونية لتنظيم الكتابة الإلكترونية إلا أنه أغفل بيان الإجراءات الواجب إتباعها لإضفاء الصفة الرسمية على المستند الإلكتروني، ذلك أن إبرام العقد الرسمي التقليدي يتطلب حضور المعنيين بالأمر أمام الموظف المختص حتى يتمكن من التحقق من رضائهما بالعقد ومن تمام أهليتهما، وهو الأمر الذي لا يتحقق في العقد الإلكتروني الرسمي كون أن المتعاقدين لا يجمعهما مجلس عقد واحد، لا سيما وأن من خصائص هذا العقد أنه مبرم عن بعد دون الحضور الفعلي لطرفيه، وعليه فإن سد الفراغ القانوني في هذه الحالة يتطلب وضع نصوص قانونية تكرس التعاون ما بين الموظف المختص في البلد الذي يوجد فيه أحد المتعاقدين

مع الموظف في البلد الذي يتواجد فيه المتعاقد الآخر بحيث يتمكن كل منهما من التحقق من رضاء المتعاقد الموجود أمامه وسلامة إرادته وكذا خلوها من العيوب.

- أظهرت الدراسة الماثلة أن التطور التكنولوجي قد أدى إلى ميلاد صور جديدة للمستندات الإلكترونية لتواكب المعاملات الحديثة سواءً بين الأفراد فيما بينهم أو بين الأفراد والإدارات، وكذا الجهة الحكومية سواء كان ذلك من الناحية المدنية أو التجارية، وهو ما تبناه المشرع الجزائري مؤخراً من خلال تعديل نصوصه القانونية أو من خلال استحداث نصوص قانونية جديدة.

- إن أهم ما يميز المستند الإلكتروني هو غياب العلاقة المباشرة بين أطرافه ومن ثم فإن الأطراف الفاعلة في تحرير المستند الإلكتروني تكمن في طرفيه وهما المرسل (أو منشأ المستند) والمرسل إليه، وأنه إلى جانب هذين الطرفين لا بد من إدخال طرف ثالث موثوق يسمى بالوسيط الإلكتروني وهو ما تبناه المشرع الجزائري في نصوص القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين.

- أثبتت الدراسة أن المشرع الجزائري أسوة بغيره من التشريعات المقارنة بما فيها الفرنسي والمصري قد اعترف في نصوصه القانونية بالكتابة الإلكترونية والتوقيع الإلكتروني كعنصرين من عناصر المستند الإلكتروني بصفة خاصة والدليل الإلكتروني بصفة عامة، وهو الأمر الذي ظهر جليا إبتداءا من سنة 2005، وذلك بموجب القانون رقم 05-10 المعدل والمتمم للقانون المدني الجزائري، كما أولى للإثبات الإلكتروني اهتماماً بالغا حيث أقر مبدأ التكافؤ الوظيفي بين الكتابة الخطية والكتابة الإلكترونية وبين التوقيع الخطي والتوقيع الإلكتروني، كما منح لهما نفس الحجية في الإثبات المدني.

ومن ثم فإنه لم يعد إحداث التوقيع بواسطة وسيلة إلكترونية عقبة أمام الاعتراف به وقبوله كعنصر في دليل الإثبات، وهو ما أخذ به التشريع الجزائري في نص المادة 09 من القانون 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين، فضلاً عن ذلك فقد أصبح التوقيع الإلكتروني - بعد مساواته بالتوقيع التقليدي- أداة تصلح لتوثيق التصرفات التي تتم

بواسطة الوسائط الإلكترونية، وقد أنهت هذه المساواة من حيث المنظور الوظيفي سلطة القاضي التقديرية في الأخذ بالتوقيع الإلكتروني أو رفضه.

- لقد أثبتت الدراسات الماثلة أن خلق بيئة إلكترونية آمنة للتعامل عبر الإنترنت لا يتم إلا عن طريق اعتماد وسائل حماية فنية لبيانات وعناصر المستند الإلكتروني، وذلك لتوفير حماية وقائية من مخاطر الاعتداء على هذه المستندات، إذ تلك الحماية وإن بدت في ظاهرها بعيدة عن الإطار الجنائي، إلا أن التعمق في الأمر يؤدي بنا إلى القول بغير ذلك، لا سيما وأن خرق هذه الوسائل قد يشكل أفعالاً إجرامية معاقب عليها. كما أن تقييم جدوى هذه الوسائل الفنية يرتبط بمدى استيعابها لعناصر أمن المستند الإلكتروني من سرية وتكامل في البيانات وعدم إنكارها.

ومن ثم كان لا بد من توفير آليات ووسائل تكفل تحديد هوية المتعاقدين، وتضمن التعبير عن إرادتهم على نحو صحيح، وأن التوقيع الإلكتروني ينسب للشخص مصدره ولا يتأتى ذلك إلا باستحداث تقنية التصديق أو التوثيق الإلكتروني، وذلك عن طريق اللجوء إلى طرف ثالث محايد موثوق به يسمى بمقدم خدمة التصديق وهو ما تبناه المشرع الجزائري بداية في المادة 03 من المرسوم التنفيذي 162/07 ثم في نصوص القانون 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين. هذا وقد حرصت مختلف التشريعات المقارنة على تنظيم المركز القانوني للقائم بعملية التصديق على التوقيع الإلكتروني (مقدم خدمات التصديق)، وفرضت شروط معينة في من يقدم هذه الخدمة إيماناً منها أن ذلك يعد أحد أهم عناصر الحماية الوقائية للتوقيع الإلكتروني، فبقدر التزامه بقدر ما تتضاءل المخاطر الناجمة ضده.

- ما يلاحظ على المشرع الجزائري من خلال نصوص القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين، أنه استحدث مخططا هيكلياً يضم ثلاث سلطات للتصديق، إحداها وطنية للتصديق الإلكتروني وهيئتين تؤطران وتشمل هاتين الهيئتين التصديق الإلكتروني الفرع الحكومي والاقتصادي، كما اتبع الازدواجية في جهة التصديق حسب نوع المتدخل وحدد مهام كل سلطة على نحو تكمل فيه كل منهما عمل

الأخرى، فضلا عن اعتماده لنظام التصديق الإلكتروني حتى في قطاع الدولة، رغبة منه في عصرنة هذا القطاع وتحسين مستوى الخدمات وهو الأمر الذي تجسد بصدور القانون 15-03 المتعلق بعصرنة العدالة، والذي بموجبه استحدث منظومة معلوماتية مركزية للمعالجة الآلية للمعطيات وجعلها تابعة لوزارة العدل، كما أجاز لها في نفس القانون أن تمهر الوثائق والمحررات القضائية التي تسلمها وزارة العدل بتوقيع إلكتروني.

- يتم التأكد من صحة التوقيع الإلكتروني عن طريق شهادة التصديق الإلكتروني التي يصدرها مقدم خدمات التصديق والتي هي عبارة عن مستند في شكل إلكتروني يبين أن التوقيع الإلكتروني صحيح وصادر ممن نسب إليه، وأنه يستوفي الشروط والضوابط المطلوبة فيه، وهو الأمر الذي يرسخ الثقة والأمان لدى المتعاملين، كما يساهم في تدعيم وسيلة الإثبات الإلكتروني، وذلك من خلال تحديد هوية مرسل المستند والموافقة على مضمونه والتأكد من سلامته، ومن ثم ضمان عدم قابليته للإنكار.

- يعتبر التشفير أحد أهم سبل الحماية الفنية لعناصر المستند الإلكتروني والذي قد يتم باستخدام مفاتيح سرية خاصة وعامة بين المرسل والمرسل إليه حيث يتم بها تشفير الرسائل والبيانات وفك شفرتها، وهو ما تبناه المشرع الجزائري في نصوص القانون 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين.

- في مجال التأمين الفني للمستند الإلكتروني ظهرت الحاجة إلى وجود وسائل تأمينية حديثة تكون لها القدرة على حماية هذه المستندات وما تتضمنه من بيانات ومعلومات، كما يكون لها القدرة كذلك على مجابهة كافة ما يستجد من أشكال وأساليب الاعتداء وكذا المساس بأمن وخصوصية المعلومات المعالجة آلياً، ومن ثم فإن المستند الإلكتروني يمكن تأمينه باستخدام تقنية "الجدران النارية" أو باستخدام أدوات القياس الحيوي مثل بصمة الإبهام وحدقة العين وبصمة الصوت، هذا ويمكن تحقيق ذات الغرض باستخدام الشبكة الافتراضية.

- أظهرت الدراسة ضرورة الحاجة إلى البحث عن وسيلة لحفظ وتخزين المستندات الإلكترونية وهذا حتى يتمكن من له مصلحة من الرجوع إليها عند الحاجة ومن استعمالها كوسيلة لإثبات التصرفات القانونية الإلكترونية التي تتم عبر الوسائط الافتراضية، وذلك في حالة ما إذا وقع نزاع بشأن هذه التصرفات، وقد تبين لنا عدم وجود نظام قانوني واضح في الجزائر ينظم عملية حفظ المستندات الإلكترونية ويحدد شروطها وضوابطها الفنية والتقنية ويبين الجهات المنوط بها حفظ هذه المستندات، باعتبار الحفظ عاملاً رئيسياً لضمان سلامة المستندات الإلكترونية إلى جانب كونه شرطاً ضرورياً لحجيتها في الإثبات.

أما الباب الثاني من هذه الدراسة فقد تم التطرق فيه إلى الأحكام التنظيمية والإجرائية للمستند الإلكتروني من الناحية الجزائية، وذلك بدءاً بالتعرض لجرائم الاعتداء على المستند الإلكتروني بعنصريه سواء كانت ماسة بالمحرر أو ماسة بالتوقيع الإلكتروني، خاصة وأن الأفعال الإجرامية التي قد تطال هذه المستندات قد تتصف بسمات وخصائص تميزها عن غيرها من الجرائم التقليدية، كما تم التطرق في هذا الباب أيضا إلى الأحكام الإجرائية المتعلقة بمتابعة مرتكب الجريمة الماسة بالمستندات من الناحية الجزائية سواء على المستوى الوطني أو على المستوى الدولي، وذلك لما يثيره من إشكالات في مجال جمع الأدلة المعلوماتية وتحديد مرتكب الفعل، لا سيما وأنها أدلة قابلة للمحو والإتلاف في وقت قصير. فضلاً عن ذلك فإن هذه الأفعال الإجرامية قد تمس كيانات منطقية ومستندات إلكترونية ليس لها وجود مادي إلا إذا تم طباعتها على الورق، وقد تم التوصل فيه إلى النتائج الآتية:

- لقد أثبتت الدراسة الماثلة من خلال التعرض لجريمة التزوير المعلوماتي أن المشرع الجزائري قد جعل جريمة التزوير تنصب على المحررات التقليدية فقط، ولم يتخذ أي موقف لتوسيع مفهوم المحرر من أجل إدماج المحررات والمستندات المعلوماتية ضمن المحررات محل جريمة التزوير، كما أنه لم يورد نص في قانون العقوبات الجزائري يعرّف فيه جريمة التزوير مما يستفاد منه أن المشرع لم ينص على جريمة التزوير المعلوماتي لا كجريمة مستقلة في جرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات،

ولا كجريمة ضمن القواعد العامة العقابية التي تجرّم فعل التزوير كما فعل نظيره المشرع الفرنسي، رغم مصادقته على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات والتي تعرضت لجريمة التزوير واعتبرته الفعل الذي يتم باستخدام وسائل تقنية المعلومات لتغيير الحقيقة في البيانات تغييرا من شأنه إحداث ضرر، وأمام هذا النقص التشريعي الوارد في قانون العقوبات لعدم مسايرة المشرع الجزائري لأحكام الاتفاقية سالفة الذكر، فإن المشرع الجزائري مطالب بأن يوسع المحل الذي يقع عليه فعل التزوير على نحو يشمل المحرر التقليدي أو أي محرر آخر للفكر مهما كانت طبيعته، كما يتوجب عليه أن يوسع من طرق التزوير وأن لا يحصرها في طرق محددة كما فعل في المادة 214 من قانون العقوبات الجزائري وذلك حتى يستطيع مواكبة أحكام الإتفاقية.

- بما أن المشرع الجزائري لم ينص على جريمة التزوير المعلوماتي، فإنه لم يتطرق كذلك في نصوصه العقابية لجريمة استعمال مستند إلكتروني مزور، رغم تطرقه لها في أحكام الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، ومن ثم فإنه مطالب باستدراك النقص واستحداث نصوص عقابية ينص فيها على هذه الجريمة لا سيما في ظل التوجه الحالي الرامي إلى تجسيد فكرة التجارة الإلكترونية والحكومة الإلكترونية.

- ثبت من خلال التعرض لجريمة الإتلاف المعلوماتي أن المشرع الجزائري أسوة بالتشريع الفرنسي عمل على تجريم فعل إتلاف المستندات الإلكترونية بطريقة غير مباشرة، وذلك تبعاً لمعالجة تجريم إتلاف المعلومات وأنظمة معالجة البيانات والمعطيات الآلية (دون أن يتعرض لفعل إتلاف المستند الإلكتروني)، حيث ظهر ذلك من خلال القانون رقم 04-15 المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات والذي عبّر فيه بطريقة غير مباشرة عن هذه الجريمة تحت مصطلح "التخريب الذي يطال منظومة المعالجة الآلية للمعطيات" ودون أن يورد في هذا القانون مادة صريحة يعاقب فيها على أفعال الإتلاف التي قد تطال المستندات الإلكترونية، كما أن المشرع لم يتطرق إلى استخدام الفيروسات والبرامج الخبيثة لإتلاف المكونات المنطقية للحاسب الآلي من مستندات وبرامج كأحد وسائل الركن المادي للجريمة، فضلا عن ذلك فإنه حتى قانون

15-04 المتعلق بالتوقيع والتصديق الإلكتروني جاء خاليا من أي نص يعاقب على إتلاف التوقيع الإلكتروني والمستند الإلكتروني.

وأمام هذا النقص فإن المشرع الجزائري مطالب باستحداث نصوص قانونية تكون فيها حماية المستند الإلكتروني من الإتلاف والتخريب والتدمير حماية أصلية مباشرة وليست حماية تبعية لحماية الأنظمة المعلوماتية والبرامج، وأن تتضمن النصوص عبارات ومصطلحات دقيقة ومباشرة تنص على فعل إتلاف هذه المستندات، مع تشديد العقاب على مثل هذه الأفعال، لا سيما وأن الأضرار والخسائر التي يلحقها هذا الإتلاف بالمكونات المعنوية للحاسب تفوق بكثير الأضرار التي يلحقها إتلاف الوسائل والمكونات المادية الأخرى.

- من خلال دراسة جريمة السرقة المعلوماتية تبين أنه وإن كان الاتجاه الراجح فقها يرى أن المستندات الإلكترونية يمكن أن تكون محلاً للسرقة، وأنها أموال معنوية يمكن أن تكون ذات قيمة اقتصادية قابلة للتداول إلا أن بعض التشريعات كالتشريع الفرنسي والجزائري لم تنص على هذه الجريمة بصورة صريحة في نصوصها العقابية، وهو الأمر الذي يحدث نوعا من الفراغ التشريعي ويضعنا أمام تأويلات عدة لعبارات المادة 350 من قانون العقوبات خاصة وأنها لم تشترط صراحة أن يكون المال موضوع السرقة مادياً. وأمام هذا الوضع فإن المشرع الجزائري مطالب بتدارك النقص وحسم الجدل واستحداث نص صريح يجرم فيه السرقة المعلوماتية على نحو يجعل فيه فعل الاختلاس منصباً على الأشياء المادية وغير المادية بلفظ واضح ومباشر دون حاجة إلى تفسير أو تأويل، وذلك على نحو تصبح فيه المادة 350 من قانون العقوبات تشمل إلى جانب السرقة التقليدية السرقة المعلوماتية.

- على الرغم من تنظيم القانون 15-04 لبعض جرائم الاعتداء على التوقيع والتصديق الإلكترونيين، إلا أن المشرع الجزائري من خلال هذا القانون لم يتمكن من وضع وسائل الحماية الجنائية لجميع صور الاعتداء على التوقيع الإلكتروني على غرار جرائم

الاحتيال، التزوير، الدخول والبقاء غير المصرح بهما مما يستدعي العودة مرة أخرى إلى القواعد العامة ضمن قانون العقوبات.

- عدم كفاية وفعالية وسائل الحماية الجنائية التي أقرها المشرع للتوقيع والتصديق الإلكترونيين خاصة في ظل حصره لجرائم الاعتداء على المنظومة الإلكترونية في مؤدي وطالب خدمة التصديق الإلكتروني، مهملاً بذلك أطرافا أخرى يمكن أن تتدخل بارتكاب هذه الجرائم كالقراصنة وغيرهم.

- إن الطبيعة الخاصة للجرائم الواقعة على المستند الإلكتروني جعلت من إجراءات التحقيق تتميز بخصوصية فرضتها البيئة الرقمية، والتي حولت الدليل الجنائي التقليدي إلى دليل من نوع آخر يسمى بالدليل الإلكتروني والذي هو عبارة عن معلومات مخزنة في الحاسب الآلي أو وسائل إلكترونية أخرى يتم الحصول عليها من خلال إجراءات فنية وقانونية لتقديمها للقضاء.

- أجاز المشرع الجزائري تفتيش المنظومة المعلوماتية بموجب القانون 09-04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وبذلك يكون قد قطع الخلاف الفقهي حول مدى إمكانية تفتيش المكونات المعنوية للحاسب الآلي من عدمه، كما سمح بأن تستعين السلطات المكلفة بالتفتيش بكل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها.

- سمح المشرع الجزائري بموجب القانون 09-04 بجواز امتداد التفتيش إلى أنظمة معلوماتية أخرى مرتبطة أو جزء منها في حالة تجاوز النظام المشتبه فيه إلى أنظمة أخرى مرتبطة به على أن لا يتم ذلك إلا بعد إعلام السلطة المختصة بذلك، كما أجاز تفتيش هذه الأنظمة المتصلة حتى ولو كانت خارج إقليم الدولة على أن يكون ذلك بمساعدة السلطات الأجنبية وفقاً للاتفاقيات الدولية، وكذا مبدأ المعاملة بالمثل.

- يجب أن يراعى أثناء التفتيش مجموعة من الضمانات التي تحدد نطاقه المكاني والزمني وهذا نظراً لخطورته ومساسه بالحريات الشخصية للأشخاص وكذا حرمة مساكنهم، فهو من أشد إجراءات التحقيق أثراً على الحرية الشخصية المكفولة بموجب الدساتير والقوانين، وإن كان قد تم التطرق لهذه الضمانات في مواضع متفرقة من هذه الدراسة.

- يترتب على التفتيش الذي يتم وفقاً للإجراءات المنصوص عليها قانوناً أثر يتمثل في ضبط الأشياء التي تفيد في كشف الحقيقة عن الجريمة المرتكبة، وهذه الأشياء قد تكون مادية تنصب على جميع الأجهزة والأدوات التي تم تخزين المعلومات فيها، وقد تكون معنوية تتمثل في المعطيات المعالجة إلكترونياً بما فيها المستندات الإلكترونية ما دام أنها عبارة عن نبضات أو ذبذبات إلكترونية قابلة لأن تسجل وتخزن على وسائط مادية، وهو ما سارت عليه التشريعات المقارنة بما فيها المشرع الجزائري بموجب القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها.

- إن اللجوء إلى الخبرة الفنية في مجال الجرائم الواقعة على المستندات الإلكترونية مسألة ضرورية أثناء التحقيق في هذه الجرائم ذات الطبيعة الفنية والتقنية، خاصة عندما تواجه جهات التحقيق مسألة فنية لا تملك تلك السلطات الخبرة الفنية اللازمة لإجرائها.

- إلى جانب إجراءات التحقيق التقليدية تم استحداث إجراءات تحقيق جديدة تتماشى مع البيئة الافتراضية وتساعد على كشف الجرائم الواقعة على النظم المعلوماتية، وهذه الإجراءات قد تساعد على جمع البيانات الإلكترونية المخزنة عن طريق التجميع في الوقت الفعلي لبيانات المرور، أو عن طريق مراقبة الاتصالات الإلكترونية أو اعتراض الاتصالات السلكية واللاسلكية.

- بالرغم من أن المشرع الجزائري أجاز المراقبة الإلكترونية بموجب القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، إلا أنه لم ينظم فيه كل المسائل المتعلقة بهذا الإجراء على خلاف المشرع

الفرنسي الذي نظمها تنظيماً دقيقا من حيث كيفية إجرائها وحفظها وحتى كيفية إتلاف هذه التسجيلات بعد الانتهاء من التحقيق والمحاكمة، وعليه فإن المشرع الجزائري مطالب باستحداث نصوص قانونية تتعلق بمآل التسجيلات الإلكترونية بعد انتهاء مرحلتي التحقيق والمحاكمة.

- عمد المشرع الجزائري إلى الموازنة بين الصالح العام في حماية المجتمع من الجريمة والصالح الخاص في حماية حق الفرد في الخصوصية بوضع تدابير استثنائية، بحيث استوجب القانون 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون الإجراءات الجزائية أن تتم عملية اعتراض المراسلات السلكية واللاسلكية وتسجيل الأصوات دون المساس بالسر المهني المنصوص عليه في أحكام نفس القانون.

والجدير بالذكر أن المشرع الجزائري بالرغم من أنه نظم إجراء الأمر باعتراض المراسلات السلكية واللاسلكية بإحكام، إلا أنه لم يتطرق لمصير التسجيلات بعد انتهاء الغرض المقصود منها ومن ثم فإنه يتوجب عليه التدخل لإتمام أحكام هذا الإجراء.

- إن التصدي للجرائم الواقعة على المستندات الإلكترونية على المستوى الدولي يتطلب تعاوناً بين الدول من الناحية الإجرائية لا سيما وأنها جرائم عابرة للحدود، ومن ثم لابد من التنسيق والتعاون بين الدول من أجل إيجاد إستراتيجيات وآليات محكمة سواء في مجال تبادل المعلومات المتعلقة بالجريمة والمجرمين، أو في مجال التعاون في تنفيذ الأحكام القضائية المتعلقة بتسليم المجرمين.

بناء على كل ما سبق طرحه من نتائج، يتضح أن المنظومة القانونية الوطنية لم توفق في معالجة كل الجوانب القانونية المتعلقة بمسألة الحماية الجزائية للمستندات الإلكترونية سواء من الناحية الموضوعية أو الإجرائية، وينبغي لتجاوز ذلك سعي المشرع الجزائري إلى التدخل لسد النقص والقصور من جهة، ومواكبة المستجدات العلمية والتطورات التقنية التي أفرزها الواقع العملي من جهة أخرى، ولا يتأتى ذلك إلا بإتباع التوصيات الآتية سواء على المستوى التشريعي أو الميداني الفعلي أو على المستوى الدولي:

- ضرورة إصدار قانون يتعلق بمكافحة جرائم الاعتداء على النظم المعلوماتية يرسي فيه المشرع دعائم نظرية متكاملة للمستند الإلكتروني على نحو يتناول فيه مفهوم واضح ودقيق لهذا المستند، وكذا تكوينه وأوضاعه وشروط صحته وقوته في الإثبات وكذا أهم تطبيقاته، وأن يتم فيه وضع الإطار العام للقواعد الفنية والتقنية التي يلجأ إليها المتعاملون بالمستند الإلكتروني وأن ينص على جميع صور المساس بهذا المستند.

- نقترح أن يضيف المشرع الجزائري نصا قانونيا في باب التزوير في المحررات ضمن نصوص قانون العقوبات يعرف فيه التزوير على النحو الآتي: «كل تغيير في الحقيقة بطريق الغش في محرر مكتوب أو في أي دعامة أخرى تحتوي تعبيراً عن الفكر» على نحو يكون فيه هذا النص أشمل وأعم، حيث يمكن أن تدرج فيه كل المستندات المعلوماتية حتى وإن كانت غير معالجة آلياً، وهو ما يضمن حماية جزائية فعالة ورادعة لأفعال التزوير التي قد تطال بيانات المستند الإلكتروني.

- نقترح على المشرع الجزائري تعديل نص المادة 350 من قانون العقوبات على نحو يجعل فعل الاختلاس فيها منصباً على الأشياء المادية وغير المادية بلفظ صريح وواضح دون الحاجة إلى تأويل أو تفسير، وأن يجعل عقاب السرقة فيها ينصب على البيانات والمستندات الإلكترونية على نحو تصبح فيه المادة 350 من قانون العقوبات تشمل إلى جانب السرقة التقليدية السرقة المعلوماتية.

- نناشد المشرع الجزائري بضرورة التدخل لتعديل نصوص القانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين لا سيما في أحكامه الجزائية على نحو يستحدث فيه نصوص تعاقب كل الأفعال التي قد تطال التوقيع الإلكتروني على المستند كأفعال الاحتيال والتزوير والدخول والبقاء غير المصرح بهما.

- على الرغم من قناعتنا بإمكانية التسرب الكلاسيكي كحيلة إجرائية في مجال الرقمية إلا أننا نناشد المشرع الجزائري بأن يكرسه كواقع قانوني درءاً للخلاف وذلك بتأطيره للتسرب الرقمي على نحو ما فعل المشرع الفرنسي.

- حبذا لو يتدخل المشرع الجزائري ويوسع من المعطيات محل التحفظ من قبل مقدم الخدمة لتشمل جميع المعطيات المخزنة، وأن لا 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.

- ضرورة تكافل الدول العربية لاستحداث اتفاقيات دولية أخرى تجرم المساس بالمستندات الإلكترونية .

- العمل على تجسيد فكرة التخصص عن طريق إيجاد قضاء متخصص للنظر في الجرائم المعلوماتية ومن بنيها الجرائم الواقعة على المستندات الإلكترونية، وذلك لصعوبة كشف هذه الجرائم وإثباتها والتحقيق فيها وحاجتها إلى معطيات خاصة قد لا تتوافر في القضاء العادي، كما ينبغي تكوين إطارات فنية متخصصة في مجال النظم المعلوماتية وهو ما يستلزم العمل على إجراء دورات تدريبية ومحاضرات عملية ونظرية لرجال القانون، وبصفة خاصة القضاة منهم والمحامين، خاصة وأن التخصص أصبح سمة عصرية تتجه نحوه مختلف العلوم في الوقت الراهن.

- ضرورة تنظيم مؤتمرات وأيام دراسية لمناقشة كل ما يستجد بشأن حماية النظم المعلوماتية من الناحية الجزائية، على ألا تكون هذه الأخيرة حكراً على رجال القانون، بل تسعى لإشراك مختصي المعلوماتية في هذا الشأن، وذلك للوصول إلى حلول عملية وأكثر واقعية.

- ضرورة تعزيز التعاون والتنسيق الدولي بين الدول مع بعضها البعض وبين الدول والمؤسسات الدولية المعنية بهذه المشكلة وخاصة الإنتربول سواء في مجال المساعدات القضائية المتبادلة أو في مجال تسليم المجرمين أو في مجال التدريب، والعمل على دراسة ومتابعة المستجدات في هذا المجال على الساحة العالمية.

- العمل على وضع مواقع إلكترونية متخصصة للتبليغ عن جرائم تقنية المعلومات بصفة عامة وإرسالها إلى الجهات المختصة وهو ما يصطلح عليه بالبلاغ الرقمي، وهو ما انتهجته العديد من الدول وعلى رأسها فرنسا.

- حث الدول ودعوتها إلى الاهتمام بالمؤسسات العلمية المتخصصة في مجال تقنية المعلومات وتقديم الدعم المادي والمعنوي لها لتكون مصدر دعم متكامل لمؤسسات الدولة القائمة على مكافحة الجرائم المتعلقة بالمستندات الإلكترونية، وإعداد أجهزة متخصصة للخبرة في مواجهة هذا الإجرام المستحدث.

- الدعوة إلى إنشاء قسم خاص لدراسة قانون تقنية المعلومات بصورة عامة وشبكة الإنترنت بصورة خاصة بكليات الحقوق بالجامعات العربية، وحث الدارسين والباحثين على التعمق والإكثار من البحث في هذا النوع من الجرائم مقارنة بين الفقه والنظام، حيث أن هذه الموضوعات تعتبر من المستجدات التي تستحق الاهتمام بالإضافة إلى تكثيف دراسة التعامل بالحاسب الآلي ونظم المعلومات.

- ضرورة وضع سياسة أمنية محكمة لأجل المحافظة على أمن وسلامة وسرية المعلومات.

في الأخير نأمل أن يأخذ المشرع الجزائري هذه التوصيات بعين الاعتبار وذلك من أجل ترسيخ الثقة والأمان في المعاملات الإلكترونية، خاصة في ظل التوجه نحو عالم رقمي معلوماتي يعد التعامل فيه بالمستند الإلكتروني سمة من سماته وعلامة دالة عليه.

وختاماً نقول أننا حاولنا من خلال هذه الدراسة الإجابة على التساؤلات التي طرحناها حول الحماية الجزائية للمستند الإلكتروني، فإن كان في هذا البحث كمال فهو لله سبحانه وتعالى، وإن اعتراه نقص فهو منّي، ولم لا وأنا بشر أجتهد فأخطئ وأصيب، فإن أصبت فأجري على الله، وإن أخطأت فأدعوه ألا يحرمني أجر المجتهدين، إنه نعم المولى ونعم النصير.

تمت بحمد الله وعونه.

قائمة المصادر والمراجع

قائمة المصادر والمراجع

أولا: المصادر.

- القرآن الكريم.
- علي بن هادية، بلحسن البليش، الجيلاني بن الحاج يحي، القاموس الجديد للطلاب، المؤسسة الوطنية الجزائرية للكتاب، الجزائر، 1987.

ثانيا : المراجع باللغة العربية.

أ- المراجع العامة:

1- أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، ج1، الجرائم ضد الأشخاص والجرائم ضد الأموال، طبعة منقحة ومتممة في ضوء النصوص الجديدة، ط6، دار هومه، الجزائر، 2007.

2- أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، ج2، جرائم الفساد- جرائم المال والأعمال- جرائم التزوير، منقحة ومتممة في ضوء قانون 20 فبراير 2006 المتعلق بالفساد، ط 9، دار هومة، الجزائر، 2008.

3- أحمد بركات مصطفى، مسؤولية البنك عن تقديم المعلومات والاستشارات المصرفية، دار النهضة العربية، مصر، 2009.

4- أحمد سفر، أنظمة الدفع الإلكترونية، ط1، منشورات الحلبي الحقوقية، لبنان، 2008.

5- إيمان مأمون أحمد سليمان، إبرام العقد الإلكتروني وإثباته، الجوانب القانونية لعقد التجارة الإلكتروني، د.ط، دار الجامعة الجديدة، الأزاريطة، الإسكندرية، 2008.

6- بخراز يعدل فريدة، تقنيات وسياسات التسيير المصرفي، ط4، ديوان المطبوعات الجامعية، الجزائر، 2008.

7- بلعليات إبراهيم، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري، ط1، دار الخلدونية، الجزائر، 2009.

8- حمدي أحمد سعد أحمد، القيمة العقدية للمستندات الإعلانية، دراسة مقارنة بين القانون المدني (المصري والفرنسي) والفقه الإسلامي، دار الكتب القانونية، مصر، 2007.

9- خالد ممدوح إبراهيم، إبرام العقد الإلكتروني، دراسة مقارنة، ط1، الدار الجامعية، الإسكندرية، مصر، 2007.

10- خالد ممدوح إبراهيم، حجية البريد الإلكتروني في الإثبات، دراسة مقارنة، ط1، دار الفكر الجامعي، الإسكندرية، مصر، 2008.

11- رحيمة الصغير ساعد نمديلي، العقد الإداري الإلكتروني، دراسة تحليلية مقارنة، ط1، دار الجامعة الجديدة، الإسكندرية، مصر، 2007.

12- سمير حامد عبد العزيز الجمال، التعاقد عبر تقنيات الاتصال الحديثة (دراسة مقارنة)، دار النهضة العربية، القاهرة، مصر، 2006.

13- صلاح علي حسين، القانون الواجب التطبيق على عقود التجارة الإلكترونية ذات الطابع الدولي، د.ط، دار النهضة العربية، القاهرة، مصر، 2012.

14- الطاهر لطرش، تقنيات البنوك، ط2، ديوان المطبوعات الجامعية، الجزائر، 2003.

15- الطيب زروتي، الوسيط في الجنسية الجزائرية، دراسة تحليلية مقارنة بالقوانين العربية والقانون الفرنسي، مطبعة الكاهنة، الجزائر، 2002.

16- عاشور عبد الجواد عبد الحميد، دور البنك في خدمة تقديم المعلومات، دراسة مقارنة في القانونين المصري والفرنسي، دار النهضة العربية، القاهرة 2008.

17- عبد الرحمن خلفي، القانون الجنائي العام (دراسة مقارنة)، دار بلقيس، دار البيضاء، الجزائر، 2017.

18- عبد الرحمن خلفي، محاضرات في قانون الإجراءات الجزائية، دار الهدى، الجزائر، 2010.

19- عبد الرؤوف مهدي، شرح القواعد العامة للإجراءات الجنائية، دار النهضة العربية، القاهرة، 2013.

20- عبد الصبور عبد القوي علي مصري، التنظيم القانوني للتجارة الإلكترونية، ط1، مكتبة القانون والإقتصاد، الرياض، 1433هـ- 2012م.

21- عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، ط2، دار هومة، الجزائر، 2011.

22- عجة الجيلالي، مدخل للعلوم القانونية، نظرية القانون بين التقليد والحداثة، دار الخلدونية، الجزائر، د.س.ن.

23- عصام عبد الفتاح مطر، التجارة الإلكترونية في التشريعات العربية والأجنبية، دار الجامعة الجديدة، الأزاريطة- الإسكندرية، 2009.

24- علاء التميمي، التنظيم القانوني للبنك الالكتروني على شبكة الانترنت، دار الجامعة الجديدة، الإسكندرية، 2012.

25- علي صادق أبو هيف، القانون الدولي العام، الأصول والمبادئ العامة، أشخاص القانون الدولي العام، النطاق الدولي، العلاقات الدولية، التنظيم الدولي، المنازعات الدولية، الحرب والحياد، ط الحادية عشر، منشأة المعارف، الإسكندرية، د.س.ن.

26- علي عبد القادر القهوجي، قانون العقوبات، القسم العام، المكتبة القانونية، الدار الجامعية، 1994.

27- علي محمد أحمد أبو العز، التجارة الإلكترونية وأحكامها في الفقه الإسلامي، ط1، دار النفائس، الأردن، 2008.

28- عوض محمد عوض، المبادئ العامة في قانون الإجراءات الجنائية، د.ط، دار المطبوعات الجامعية، القاهرة، 1999.

29- فادي محمد عماد الدين توكل، عقد التجارة الإلكترونية، ط1، دار الثقافة، الأردن، 2008.

30- فوزية عبد الستار، شرح قانون الإجراءات الجنائية، ط2، دار النهضة العربية، القاهرة، 2011.
31- القاضي غسان، قانون العقوبات الاقتصادي(دراسة مقارنة حول جرائم رجال الأعمال والمؤسسات التجارية، المخالفات المصرفية والضريبة الجمركية وجميع جرائم التجار) طبعة مزيدة ومنقحة منشورات الحلبي الحقوقية، بيروت- لبنان، 2004.
32- مجدي محبوب محب حافظ، موسوعة جرائم الخيانة والتجسس، دراسة في التشريع المصري والتشريعات العربية والأجنبية والشريعة الإسلامية، ط1، المركز القومي للإصدارات القانونية، القاهرة، 2007.
33- محمد سعيد جعفور، مدخل إلى العلوم القـــانونية، ج1، الوجيـــز في نظريـــة القانون، ط 19، دار هومة، الجزائر، 2012.
34- محمد عبد الودود عبد الحفيظ أبو عمر، المسؤولية الجزائية عن إفشاء السر المصرفي، ط1، دار وائل للنشر، الأردن 1999.
35- محمد فريد الشافعي، التجارة الإلكترونية وإشكالية تسليم المنتجات عير شبكة الاتصالات الدولية الإنترنت (دراسة مقارنة بين الفقه الإسلامي والقانون الوضعي)، دار الكتاب الحديث، القاهرة، مصر، 2009.
36- محمد فواز المطالقة، النظام القانوني لعقود إعداد برامج الحاسب الآلي، دار الثقافة، عمان- الأردن، 2004.
37- محمود محمد أبو فروة، الخدمات البنكية الإلكترونية عبر الانترنت، ط1، دار الثقافة، عمان- الأردن، 2009.
38- محمود نجيب حسني، النظرية العامة للقصد الجنائي- دراسة تأصيلية مقارنة للركن المعنوي في الجرائم العمدية -، ط3، دار النهضة العربية، القاهرة، 1988.
39- مصطفى كمال طه، وائل بندق أنور، الأوراق التجارية ووسائل الدفع الإلكترونية الحديثة، دار الفكر الجامعي، الإسكندرية، 2006.

40- منتصر سعيد حمودة، الإرهاب الدولي جوانبه القانونية ووسائل مكافحته في القانون الدولي العام والفقه الإسلامي، د.ط، دار الجامعة الجديدة، الإسكندرية، 2006.
41- منصور رحماني، الوجيز في القانون الجنائي العام، فقه- قضايا، دار العلوم للنشر، عنابة، 2006.
42- نادية فوضيل، الأوراق التجارية في القانون الجزائري، دار هومة، الجزائر، 2006.
43- ناهد فتحي الحموري، الأوراق التجارية الإلكترونية، دراسة تحليلية مقارنة، ط1، دار الثقافة، عمان- الأردن،2009.
44- ياسر الأمير فاروق، مراقبة الأحاديث الخاصة في الإجراءات الجنائية، ط1، دار المطبوعات الجامعية، الإسكندرية، مصر، 2009.

ب- المراجع المتخصصة:

1- إبراهيم الدسوقي أبو الليل، الجوانب القانونية للتعامل عبر وسائل الاتصال الحديثة، دار النهضة العربية، القاهرة، مصر، 1999.

2- أحمد أبو الروس، جرائم التزييف والتزوير والرشوة واختلاس المال العام من الوجهة القانونية والفنية، المكتب الجامعي الحديث، الإسكندرية، مصر، 2004.

3- أحمد خليفة الملط، الجرائم المعلوماتية، ط2، دار الفكر الجامعي، الإسكندرية، 2006.

4- أحمد عاصم عجلية، الحماية الجنائية للمحررات الالكترونية، دراسة مقارنة، دار النهضة العربية، القاهرة، 2014.

5- أحمد عزمي الحروب، السندات الرسمية الإلكترونية، دراسة مقارنة، ط1، دار الثقافة، عمان- الأردن، 2010.

6- أحمد عوض بلال، قاعدة استبعاد الأدلة المتحصلة بطريقة غير مشروعة، د.ط، دار النهضة العربية، القاهرة، مصر، سنة 1994.

7- أحمد محمود مصطفى، جرائم الحاسبات الآلية في التشريع المصري، دراسة مقارنة، ط1، دار النهضة العربية، القاهرة، 2010.

8- أسامة أبو الحسن مجاهد، الوسيط في المعاملات الالكترونية وفقا لأحدث التشريعات في فرنسا، مصر، الأردن، دبي، البحرين، الكتاب الأول، المدخل لقانون المعاملات الإلكترونية -العقد الإلكتروني- الإثبات الإلكتروني، دار النهضة العربية، القاهرة، 2007.

9- أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دراسة مقارنة في القانون الفرنسي والأمريكي والمصري وفقا لآخر التعديلات التشريعية، دار النهضة العربية، القاهرة، 1428هـ-2008م.

10- أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني -دراسة مقارنة-، ط1، دار النهضة العربية، 2006.

11- آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، ط2، دار هومه، الجزائر، 2007.

12- الأنصاري حسن النيداني، القاضي والوسائل الإلكترونية الحديثة، دار الجامعة الجديدة، الإسكندرية، 2009.

13- أيمن أحمد الدلوع، التنظيم القانوني للتوثيق الالكتروني، دار الجامعة الجديدة، الإسكندرية، 2016.

14- أيمن عبد الحفيظ، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، دار النهضة العربية، القاهرة –مصر، 2005.

15- إيهاب فوزي السقا، جريمة التزوير في المحررات الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2008.

16- بلال أمين زين الدين، جرائم نظم المعالجة الآلية للبيانات في التشريع المقارن والشريعة الإسلامية، دار الفكر، الإسكندرية، 2008.

17- بولين أنطونيوس أيوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، دراسة مقارنة، ط 1، منشورات الحلبي الحقوقية ، بيروت- لبنان، 2009.

18- تامر محمد سليمان الدمياطي، إثبات التعاقد الإلكتروني عبر الإنترنت -دراسة مقارنة-، ط1، منشأة المعارف، الإسكندرية ، مصر، 2009.

19- ثروت عبد الحميد، التوقيع الإلكتروني، ماهيته، مخاطره وكيفية مواجهته ومدى حجيته في الإثبات، دار النيل للطباعة والنشر، القاهرة، 2001.

20- جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات، دار البداية للنشر، الأردن، 2007 .

21- جعفر مشيمش، جريمة التزوير –دراسة مقارنة–، ط1، منشورات زين الحقوقية، بيروت- لبنان، 2009.

22- جلال محمد الزعبي، أسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية، دراسة مقارنة، ط1، دار الثقافة، عمان- الأردن، 2010.

23- جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، ط1، دار النهضة العربية، القاهرة، 1992.

24- جميل عبد الباقي الصغير، الحماية الجنائية والمدنية للبطاقات الإلكترونية الممغنطة، دار النهضة العربية، القاهرة، سنة 1999.

25- جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، 2001.

26- جميل عبد الباقي الصغير، جرائم الإنترنت، الأحكام الموضوعية والجوانب الإجرائية، دار النهضة، القاهرة، 2010.

27- جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي، الأحكام الموضوعية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، 2012.

28- حسين بن سعيد بن سيف الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت، دراسة مقارنة، دار النهضة العربية، القاهرة- مصر، 2009.

29- خالد حربي السعدي، جريمة إتلاف برامج ومعلومات الحاسب الآلي في التشريعين الكويتي والمقارن، ط1، دار النهضة العربية، القاهرة- مصر، 2012.

30- خالد محمد كدفوري المهيري، جرائم الكمبيوتر والإنترنت والتجارة الإلكترونية، ط2، معهد القانون الدولي، دار الغرير للطباعة والنشر، دبي، د.س.ن.

31- خالد مصطفى فهمي، النظام القانوني للتوقيع الإلكتروني في ضوء التشريعات العربية والاتفاقيات الدولية، دار الجامعة الجديدة، الإسكندرية، 2007.

32- خالد ممدوح إبراهيم، أمن المعلومات الالكترونية، الدار الجامعية، الإسكندرية- مصر، 2008.

33- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، ط1، دار الفكر الجامعي، الإسكندرية- مصر، 2009.

34- خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر، أساليب وثغرات، دار الهدى للنشر، عين مليلة- الجزائر، 2010.

35- رامي متولي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق، ط1، دار النهضة العربية، القاهرة، مصر، 2011.

36- زيبحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى للطباعة والنشر، الجزائر، 2011.

37- سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت (الجرائم الواقعة في مجال تكنولوجيا المعلومات)، ط1، دار النهضة العربية، القاهرة، 1999.

38- سليم سعداوي، عقود التجارة الالكترونية -دراسة مقارنة-، ط1، دار الخلدونية، الجزائر، 2008.

39- السيد عتيق، جرائم الإنترنت، دار النهضة، القاهرة، مصر، 2000.

40- شمسان ناجي صالح الخليلي، الجرائم المستخدمة بطرق غير مشروعة لشبكة الأنترنت، دراسة مقارنة، دار النهضة العربية، القاهرة، 2009.

41- شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الالكترونية، دار الجامعة الجديدة، الإسكندرية، مصر، 2007.

42- ضياء يحي السادات، مبادئ استخدام الحاسب الآلي والإنترنت وجهود مكافحة الجرائم الناشئة عنها، منشأة المعارف، الإسكندرية ، مصر،2012.

43- طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة، مصر، 2009.

44- عامر محمود الكسواني، التجارة عبر الحاسوب، ماهيتها، إثباتها، وسائل حمايتها والقانون الواجب التطبيق عليها في كل من الأردن ومصر وإمارة دبي، دراسة مقارنة، ط1، دار الثقافة، الأردن، 2009.

45- عايد رجا الخلايلة، المسؤولية التقصيرية الإلكترونية -المسؤولية الناشئة عن إساءة استخدام أجهزة الحاسوب والأنترنت- دراسة مقارنة، ط1، دار الثقافة، الأردن، 2009.

46- عباس العبودي، الحجية القانونية لوسائل التقدم العلمي في الإثبات المدني، المكتبة القانونية، عمان، الأردن، 2002.

47- عبد الصبور عبد القوي مصري، الجريمة الالكترونية، ط1، دار العلوم، القاهرة، مصر، 2008.

48- عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية، الكتاب الثاني، الحماية الجنائية لنظام التجارة الالكترونية، دار الفكر الجامعي، الإسكندرية، 2002.

49- عبد الفتاح بيومي حجازي، مقدمة في التجارة الالكترونية العربية، الكتاب الأول، (شرح المبادلات والتجارة الالكترونية التونسي)، دار الفكر الجامعي، الإسكندرية، 2002.

50- عبد الفتاح بيومي حجازي، التجارة الالكترونية في القانون العربي النموذجي لمكافحة جرائم الكمبيوتر والانترنت، ط1، دار الفكر الجامعي، الإسكندرية، 2006.

51- عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، ط1، دار الفكر الجامعي، الإسكندرية، 2006.

52- عبد الفتاح بيومي حجازي، التزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، 2008.

53- عبد الفتاح بيومي حجازي، التوقيع الالكتروني في النظم القانونية المقارنة، دار الفكر الجامعي، الإسكندرية- مصر، د.س.ن.

54- عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، ط2، دار النهضة العربية، القاهرة، 2002.

55- عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنت (الجرائم الإلكترونية) دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والإنترنت مع الإشارة إلى جهود مكافحتها محليا وعربيا ودوليا، ط1، منشورات الحلبي الحقوقية، لبنان، 2007.

56- عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، تقديم فتوح الشاذلي، دار الثقافة للطباعة والنشر، عمان- الأردن، 1999.

57- علاء حسين مطلق التميمي، حجية المستند الالكتروني في الإثبات المدني، ط1، دار النهضة العربية، القاهرة، 2009.

58- علاء حسين مطلق التميمي، الأرشيف الإلكتروني وكيفية المحافظة على المستند الإلكتروني عبر الزمن، دراسة مقارنة، ط1، دار النهضة العربية، مصر، 2010.

59- علاء حسين مطلق التميمي، المستند الالكتروني، عناصره وتطوره ومدى حجيته في الإثبات المدني، دراسة مقارنة، ط2، دار النهضة العربية، مصر، 2011.

60- على عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، دراسة مقارنة، المكتب الجامعي الحديث، د.ب.ن، سنة 2012.

61- علي حسن محمد الطوالبة، التفتيش الجنائي في نظم الحاسوب والإنترنت، ط01، عالم الكتاب الحديث، د.ب.ن، سنة 2010.

62- علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعية الجديدة للطباعة والنشر والتوزيع، الإسكندرية، مصر، 1997.

63- عمر أبو الفتوح عبد الحفيظ الحمامي، الحماية الجنائية للمعلومات المسجلة إلكترونياً، دراسة مقارنة، دار النهضة العربية، القاهرة، 2010.

64- عمر محمد بن يونس، نطاق الجريمة الإفتراضية، (تفسير الدخول والتصريح به في إطار تشريعات الإساءة إلى الحاسوب)، ط1، د.د.ن، د.ب.ن، 2005.

65- فائزة يونس الباشا، السياسة الجنائية لجرائم الكمبيوتر التشريع الليبي (نموذجا و مقارنا)، دار النهضة العربية، القاهرة، 2013.

66- فتحي محمد أنور عزت، الحماية الجنائية الموضوعية والإجرائية للاعتداء على المصنفات والحق في الخصوصية والكمبيوتر والإنترنت في نطاق التشريعات الوطنية والتعاون الدولي، ط1، دار النهضة العربية، القاهرة، 2007.

67- فؤاد حسين العزيزي، الجرائم المعلوماتية -دراسة مقارنة-، دار الفكر الجامعي، الإسكندرية- مصر، 2014.

68- لزهر بن سعيد، النظام القانوني لعقود التجارة الإلكترونية، د.ط، دار هومه، الجزائر، 2012.

69- لورانس محمد عبيدات، إثبات المحرر الإلكتروني، دار الثقافة للنشر، الأردن، 2005.

70- ماجد عمار، المسؤولية القانونية الناشئة عن استخدام فيروس برامج الكمبيوتر ووسائل حمايتها، دار النهضة العربية، القاهرة، 1989.

71- محمد أمين الرومي، المستند الالكتروني، ط1، دار الفكر الجامعي، الإسكندرية، 2007.

72- محمد أمين الرومي، النظام القانوني للتوقيع الإلكتروني، دار الكتب القانونية، مصر، 2008.

73- محمد أمين الشوابكة، جرائم الحاسوب والانترنت (الجريمة المعلوماتية)، ط1، دار الثقافة، الأردن، 2006.

74- محمد حسين منصور، الإثبات الإلكتروني، دار الفكر الجامعي، الإسكندرية، 2006.

75- محمد حسين منصور، الإثبات التقليدي والإلكتروني، دار الفكر الجامعي، الإسكندرية، 2006.

76- محمد حسين منصور، المسؤولية الإلكترونية، ج1، ط1، منشأة المعارف، الإسكندرية، مصر، 2006.

77- محمد خالد جمال رستم، التنظيم القانوني للتجارة والإثبات الالكتروني في العالم، منشورات الحلبي الحقوقية، لبنان، 2006.

78- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الإسكندرية، مصر، 2007.

79- محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، الهيئة المصرية العامة للكتاب، مصر، 2003.

80- محمد سعيد أحمد إسماعيل، أساليب الحماية القانونية لمعاملات التجارة الإلكترونية، دراسة مقارنة، ط1، منشورات الحلبي الحقوقية، بيروت، لبنان، 2009.

81- محمد فتحي، تفتيش شبكة الأنترنت لضبط جرائم الاعتداء على الآداب العامة، ط2، المركز القومي للإصدارات القانونية، مصر، 2012.

82- محمد محمود المكاوي، الجوانب الأخلاقية والاجتماعية والمهنية للحماية من الجرائم المعلوماتية (جرائم الكمبيوتر والانترنت) المكتبة العصرية للنشر، مصر، 2010.

83- محمد مروان، نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري، ج1، ديوان المطبوعات الجامعية، الجزائر، 1999.
84- محمد نصر محمد، الوسيط في الجرائم المعلوماتية، ط1، مركز الدراسات العربية للنشر والتوزيع، د.ب.ن، سنة 2015.
85- محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، ط1، دار الثقافة، عمان- الأردن، 1430هـ-2009م.
86- مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، ط1، دار النهضة العربية، القاهرة، 2012.
87- مدحت محمد عبد العزيز إبراهيم، الجرائم المعلوماتية الواقعة على النظام المعلوماتي، دراسة مقارنة، ط1، دار النهضة العربية، القاهرة، 2015.
88- مصطفى أبو مندور موسى، الجوانب القانونية لخدمات التوثيق الإلكتروني، دراسة مقارنة، دار النهضة العربية، مصر، 2004.
89- مصطفى محمد موسى، أساليب إجرامية بالتقنية الرقمية ماهيتها ومكافحتها، دار الكتب القانونية، مصر، 2005.
90- مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، ط1، مطابع الشرطة، القاهرة، 2009.
91- مصطفى محمود موسى، المراقبة الإلكترونية عبر شبكة الإنترنت (دراسة مقارنة)، سلسلة اللواء الأمنية في مكافحة الجريمة الإلكترونية، الكتاب الخامس، دار الكتب القانونية، القاهرة، 2005.
92- معوان مصطفى، التجارة الإلكترونية ومكافحة الجريمة المعلوماتية (قواعد الإثبات المدني والتجاري)، ط1، دار الكتاب الحديث، القاهرة- مصر، 2008.
93- منير محمد الجنبيهي، ممدوح محمد الجنبيهي، تزوير التوقيع الإلكتروني، دار الفكر الجامعي، الإسكندرية، 2006.

94- ناير نبيل عمر،الحماية الجنائية للمحل الالكتروني في جرائم المعلوماتية، دراسة في المحل الالكتروني المسبوغ بالحماية القانونية وبحث المفردات المشمولة بالرعاية وآلية التطبيق في القانون المصري والمقارن، دار الجامعة الجديدة، الإسكندرية، 2012.

95- نائلة عادل محمد فريد قورة، جرائم الحاسب الآلية الاقتصادية، ط1، منشورات الحلبي الحقوقية، لبنان، 2005.

96- نبيل مهدي زوين، المحررات الإلكترونية، دراسة قانونية.

http://www.lawjo.net/vb/attachent.p...1&d=1282599206.

97- نجوى أبو هيبة، التوقيع الإلكتروني، تعريفه ومدى حجيته في الإثبات، دار النهضة العربية، مصر، 2004.

98- نعيم مغبغب، حماية برامج الكمبيوتر الأساليب والثغرات، دراسة في القانون المقارن، ط1، منشورات الحلبي الحقوقية، بيروت- لبنان، 2006.

99- نهلا عبد القادر المومني، الجرائم المعلوماتية، ط1، دار الثقافة، الأردن، 2008.

100- هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت، دار النهضة العربية، القاهرة، 2000.

101- هشام رستم، الجوانب الإجرائية للجرائم المعلوماتية، ط1، مكتبة الآلات الحديثة، مصر، سنة 1994 .

102- هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دار النهضة العربية، القاهرة، 1997.

103- هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة، 2006.

104- هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها، ط1، دار النهضة العربية، القاهرة، 2007.

105- هلالي عبد اللاه أحمد، جرائم الحاسب والإنترنت بين التجريم الجنائي وآليات المواجهة، دار النهضة العربية، مصر، 2015.

106- وائل أنور بندق، قانون التوقيع الإلكتروني (قواعد الأونيسترال ودليلها الإرشادي)، دراسات تشريعية، ط1، مكتبة الوفاء القانونية، الإسكندرية، 2009.
107- يوسف أحمد النوافلة، حجية المحررات الإلكترونية في الإثبات، دار وائل للنشر، الأردن، 2007.

ج- الأطروحات والمذكرات العلمية.

- **أطروحات الدكتوراه:**

1- أيمن عبد الحفيظ عبد الحميد سليمان، إستراتيجية مكافحة الجرائم الناشئة عن استخدام الحاسب الآلي، دراسة مقارنة، رسالة مقدمة للحصول على درجة الدكتوراه في علوم الشرطة، أكاديمية الشرطة، كلية الدراسات العليا، مصر، 2003.
2- عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، رسالة دكتوراه في القانون الجنائي، كلية الحقوق، جامعة عين شمس، مصر، 2004.
3- سليمان محمد أحمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الانترنت)، رسالة لنيل شهادة الدكتوراه في علوم الشرطة، كلية الدراسات العليا، القاهرة، 2007 .
4- ياسين محمد المدهون، النظام القانوني لحماية التجارة الإلكترونية، رسالة لنيل درجة الدكتوراه في الحقوق، كلية الحقوق، جامعة عين شمس، مصر، 1428هـ- 2007.
5- محمد عبيد الكعبي، الحماية الجنائية للتجارة الإلكترونية، أطروحة لنيل شهادة الدكتوراه في الحقوق، كلية الحقوق، جامعة القاهرة، 2009.
6- نور خالد عبد المحسن العبد الرزاق، حجية المحررات والتوقيع الالكتروني في الإثبات على شبكة الانترنت، رسالة للحصول على درجة الدكتوراه في الحقوق، كلية الحقوق جامعة عين شمس، مصر، 2009.

7- رشدي محمد علي محمد عيد علي، الحماية الجنائية للمعلومات على شبكة الإنترنت، دراسة مقدمة لنيل درجة الدكتوراه في الحقوق، كلية الحقوق، قسم القانون الجنائي، جامعة القاهرة، سنة 2009.

8- سامح أحمد بلتاجي موسى، الجوانب الإجرائية للحماية الجنائية لجرائم الإنترنت، رسالة دكتوراه في الحقوق، كلية الحقوق، جامعة الإسكندرية، سنة 2010.

9- خليفي مريم، الرهانات القانونية للتجارة الإلكترونية، رسالة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، السنة الجامعية 2011- 2012.

10- طارق فوزي الفقي، الجوانب الإجرائية في الجرائم المعلوماتية –دراسة مقارنة–، رسالة للحصول على درجة دكتوراه في الحقوق، كلية الحقوق، جامعة المنوفية، مصر، 1432هـ- 2011 م.

11- فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية، رسالة دكتوراه، جامعة عين شمس، القاهرة، 2012.

12- محمد عبد الله محمد العوا، المسؤولية الجنائية الناشئة عن جرائم الأموال عبر الانترنت، أطروحة لنيل درجة دكتوراه في الحقوق، كلية الحقوق، قسم الدراسات العليا، القانون الجنائي، جامعة الإسكندرية، 2012.

13- بوعناد فاطمة زهرة، مشروعية الدليل الالكتروني في مجال الإثبات الجنائي، أطروحة دكتوراه في العلوم، تخصص علوم قانونية، فرع علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة جيلالي اليابس، سيدي بلعباس، 2013-2014.

14- حطاب كمال، الحماية الجنائية للتجارة الإلكترونية، أطروحة دكتوراه في العلوم تخصص علوم قانونية، فرع علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة جيلالي ليابس- سيدي بلعباس، السنة الجامعية 2014- 2015.

15- جندولي فاطمة زهرة، عقود التجارة الإلكترونية في العلاقات الخاصة الدولية، رسالة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، تلمسان، سنة 2017- 2018.

16- رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة مقدمة لنيل شهادة الدكتوراه علوم في القانون الخاص، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، جامعة أبو بكر بلقايد، تلمسان، السنة الجامعية 2017-2018.

- **<u>مذكرات الماجستير</u> :**

1- قارة آمال، الجريمة المعلوماتية، رسالة ماجستير في القانون الجنائي والعلوم الجنائية، كلية الحقوق- بن عكنون-، جامعة الجزائر، السنة الجامعية 2001- 2002.

2- نبيلة هبة مولاي علي هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، رسالة مقدمة للحصول على درجة ماجستير في العلوم الجنائية، كلية الحقوق، جامعة الإسكندرية، مصر، السنة الجامعية 2005- 2006.

3- نجاة عباوي، جرائم المعلوماتية في التشريع الجزائي الجزائري، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة بشار، 2008.

4- محمد حسين علي محمود، التزوير باستخدام الوسائل الالكترونية، رسالة ماجستير في الحقوق ، كلية الحقوق ،جامعة القاهرة، 2011.

5- سوير سفيان، جرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، السنة الجامعية 2010- 2011.

6- لحمر فافة، تسليم المجرمين في التشريع الجزائري على ضوء الاتفاقيات الدولية، مذكرة لنيل شهادة الماجستير في القانون العام، تخصص القوانين الإجرائية والتنظيم القضائي، كلية الحقوق والعلوم السياسية، جامعة وهران، السنة الجامعية 2013-2014.

د- المقالات والأبحاث:

1- إبراهيم الدسوقي أبو الليل، التوقيع الالكتروني ومدى حجيته في الإثبات" دراسة مقارنة"، مجلة الحقوق، فصلية علمية محكمة تصدر عن مجلس النشر العلمي بجامعة الكويت، ملحق ع الثالث، السنة التاسعة والعشرون، 2005.

2- إبراهيم الدسوقي أبو الليل، توثيق التعاملات الإلكترونية ومسؤولية جهة التوثيق اتجاه الغير المتضرر، بحوث مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، مج الخامس، كلية الشريعة والقانون وغرفة تجارة وصناعة دبي، جامعة الإمارات العربية المتحدة، 9-11 ربيع الأول 1424هـ- الموافق 10-12 ماي 2003.

3- أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني -دراسة مقارنة-، بحوث مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، مج الثاني، كلية الشريعة والقانون وغرفة تجارة وصناعة دبي، جامعة الإمارات العربية المتحدة، 9-11 ربيع الأول1424هـ- الموافق 10-12 ماي 2003.

4- الأنصاري حسن النيداني، حجية المحررات الإلكترونية في الإثبات في المواد المدنية وسلطة القاضي إزاءها، مجلة الفكر القانوني والاقتصادي، مجلة فصلية محكمة تصدرها كلية الحقوق جامعة بنها، جمهورية مصر العربية، عدد خاص بالمؤتمر العلمي السنوي الرابع لكلية الحقوق بجامعة بنها، مصر، 2010.

5- باسم رمزي معروف دياب، جريمة تزوير المحرر الرسمي، الأمن والحياة، إعلامية- أمنية- ثقافية، جامعة نايف العربية للعلوم الأمنية، ع (340)، س التاسعة والعشرون، رمضان 1431هـ، أغسطس/سبتمبر 2010.

6- باطلي غنية، حجية المستند الالكتروني، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية، كلية الحقوق جامعة الجزائر، ع3، سبتمبر، 2011.

7- بن فردية محمد، الدليل الجنائي الرقمي وحجيته أمام القضاء الجزائي، المجلة الأكاديمية للبحث القانوني، مجلة تصدر عن كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة، بجاية، الجزائر، ع 2014.

8-بودالي محمد، التوقيع الالكتروني، إدارة ، مجلة المدرسة الوطنية للإدارة، مجلة سداسية تصدر عن مركز التوثيق والبحوث الإدارية، مج 13، ع 02، العدد 26، 2003.

9-بوعزة هديات، نظام الدفع الإلكتروني بين المزايا والمخاطر، مجلة دراسات قانونية، مجلة علمية محكمة تصدر دوريا عن مخبر القانون الخاص الأساسي، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، ع11، س2014.

10-تركي بن محمد العطيان، جرائم الحاسب الآلي "دراسة نفسية تحليلية"، مجلة البحوث القانونية والإقتصادية، مجلة فصلية محكمة يصدرها أساتذة كلية الحقوق، جامعة المنصورة،ع السابع والثلاثون، أبريل 2005.

11-حسين بن سعيد بن سيف الغافري، الجهود الدولية في مواجهة جرائم الإنترنت، منشورة على موقع المنشاوي للدراسات والبحوث. www.minshawi.com.

12-حوالف عبد الصمد، نظام الدفع الإلكتروني، الحجة، مجلة دورية تصدر عن منظمة المحامين لناحية تلمسان، الإتحاد الوطني لمنظمات المحامين الجزائريين، ع2، أكتوبر 2011.

13-خالد حامد أحمد مصطفى، المعلوماتية والمسؤولية الجزائية، الفكر الشرطي، دورية ربع سنوية- علمية محكمة ومفهرسة تعنى بالأبحاث الشرطية، تصدر عن مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، الإمارات العربية المتحدة، مج العشرون، ع الرابع، العدد رقم (79)، أكتوبر 2011.

14- خالد علي العراقي علي إسماعيل، مكافحة جرائم التوقيع الالكتروني بدولة الإمارات العربية المتحدة، الفكر الشرطي، دورية ربع سنوية علمية محكمة ومفهرسة تعني بالأبحاث الشرطية تصدر عن مركز بحوث الشرطة للإمارات العربية المتحدة، مج الثاني والعشرون، ع 85، أبريل سنة 2003.

15- ذياب البداينة، أمن المعلومات، دراسات مستقبلية، مجلة علمية محكمة يصدرها مركز دراسات المستقبل، جامعة أسيوط، ع8، س السادسة، يوليو (تموز) 2003.

16- راشد بن حمد البلوشي، الدليل في الجريمة المعلوماتية، مجلة الحقوق للبحوث القانونية والإقتصادية، مجلة فصلية محكمة تصدرها كلية الحقوق، جامعة الإسكندرية، ع1، 2008.

17- رايس محمد، الحماية الجنائية للسند الإلكتروني في القانون الجزائري، مجلة الدراسات القانونية، ع1، 2006-2008، ط1، منشورات الحلبي الحقوقية، بيروت- لبنان، 2009.

18- رضا متولي وهدان، النظام القانوني للعقد الإلكتروني، مجلة البحوث القانونية والإقتصادية، مجلة فصلية محكمة يصدرها أساتذة كلية الحقوق جامعة المنصورة، ع الثاني والأربعون، أكتوبر 2007.

19- سرحان حسن المعيني، التحقيق في جرائم تقنية المعلومات، الفكر الشرطي، دورية ربع سنوية، علمية محكمة ومفهرسة تعنى بالأبحاث الشرطية، تصدر عن مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، الإمارات العربية المتحدة، مج العشرون، ع الرابع، العدد رقم (79)، أكتوبر 2011.

20- عادل عبد الله خميس المعمري، التفتيش في الجرائم المعلوماتية، الفكر الشرطي، دورية ربع سنوية، عملية محكمة ومفهرسة تعنى بالأبحاث الشرطية، تصدر عن مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، الإمارات العربية المتحدة، مج الثاني والعشرون، ع3، العدد رقم (86) – يوليو 2013.

21- عادل علي المانع، إشكالية الحماية الجنائية لملكية المعطيات المعالجة آليا، مجلة البحوث القانونية والإقتصادية، كلية الحقوق، جامعة المنصورة، ع التاسع والعشرين، أفريل 2001.

22- عبد الإله محمد النوايسية، جريمة الدخول غير المشروع في تشريعات الجرائم الإلكترونية العربية، المجلة القانونية والقضائية، مجلة متخصصة محكمة، نصف سنوية، تصدر عن مركز الدراسات القانونية والقضائية، وزارة العدل، دولة قطر، ع الأول، السنة العاشرة، جوان 2016.

23- عبد الرحمن محمد خلف، نظرة حول المشكلات القانونية والعملية لمواجهة الجريمة المعلوماتية، مجلة كلية الدراسات العليـــا، متخصصة في علـوم الشرطـــة، مجلة علمية -نصف سنوية- محكمة، تصدر عن كلية الدراسات العليا بأكاديمية مبارك للأمن، القاهرة، ع الحادي والعشرون، يوليه 2009- شعبان 1430.

24- عبد المحسن بدوي أحمد، حقوق الملكية الفكرية وتكنولوجيا المعلومات، الأمن والحياة، إعلامية- أمنية- ثقافية، ع (325)، س الثامنة والعشرون، جمادى الآخرة 1430هـ- يونيو 2009.

25- عثمان الصديق أحمد محمد، المستند الإلكتروني، أهمية وضرورة إصدار تشريع يكفل حجيته ويضع ضوابطه له. www.lebramy.gov

26- عدنان إبراهيم سرحان، الوفاء الإلكتروني، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، دبي، 2003.

27- عمار كريم كاظم، ناريمان جميل نعمة، القوة القانونية للمستند الإلكتروني، مجلة مركز دراسات الكوفة، مج 5، ع السابع، الكوفة، 2003.

28- كريم كريمة، تأثير استعمال التقنيات الحديثة في تحقيق الأمن القانوني، ملتقى وطني حول الأمن القانوني، يومي: 05 و06 ديسمبر 2012، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، الجزائر.

29- ليلى الزوين، عرض دول الجرائم الإلكترونية المالية، سلسلة ندوات محكمة الاستئناف بالرباط، تأثير الجريمة الإلكترونية على الائتمان المالي، ع السابع، مطبعة الأمنية، الرباط، المغرب،2014.

30- محمد سامي الشوا، الحماية الجنائية للكيانات المنطقية "برامج الحاسب الآلي"، مجلة البحوث القانونية والإقتصادية، مجلة نصف سنوية محكمة تصدرها كلية الحقوق، جامعة المنوفية، ع4، س2، أكتوبر 1993.

31- محمد حسن السراء، الأساليب الحديثة والمهارات المتقدمة في تحقيق الجرائم الإلكترونية، الفكر الشرطي، دورية ربع سنوية- علمية محكمة ومفهرسة تعنى بالأبحاث الشرطية، تصدر عن مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، الإمارات العربية المتحدة، مج الحادي والعشرون، ع الثاني، العدد رقم (81)، أبريل 2012.

32- محمد زلايجي ، حجية دليل الحاسوب الآلي في النطاق الجنائي، دراسات قانونية، مجلة سداسية تصدر عن مخبر القانون الخاص الأساسي ، كلية الحقوق، جامعة أبو بكر بلقايد، تلمسان، ع 07، سنة 2010.

33- محمد زهير محمد أبو العز، جرائم الكمبيوتر في مجال البنوك، مجلة البحوث القانونية والإقتصادية، دورية- علمية- محكمة، كلية الحقوق، جامعة المنصورة، ع الثامن والأربعون، أكتوبر 2010.

34- محمد عقاد، جريمة التزوير في محررات الحاسب الآلي، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون، دار النهضة العربية، القاهرة ، 1995.

35- محمد قدري حسن عبد الرحمن، جرائم الإحتيال الإلكتروني، الفكر الشرطي، دورية ربع سنوية، علمية محكمة ومفهرسة تعنى بالأبحاث الشرطية، تصدر عن مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، الإمارات العربية المتحدة، مج العشرون، ع الرابع، العدد رقم (79)، أكتوبر 2011.

36- مصطفى نعوس، حق الدولة في استخدام القوة في الفضاء الإلكتروني للدفاع عن النفس، مجلة الحقوق، مجلة علمية محكمة ربع سنوية تعنى بنشر الدراسات القانونية والشرعية، تصدر عن مجلس النشر العلمي، جامعة الكويت، ع1، السنة الثامنة والثلاثون، جمادى الأولى 1435هـ- مارس 2014.

37- مقالة مفصلة تحت عنوان "السجل الطبي الإلكتروني" مأخوذة من الموقع الإلكتروني ويكيبيديا الموسوعة الحرة، العنوان الإلكتروني سجل-طبي-إلكتروني.

ar-wikipedia-org/wiki/

38- ناجي الزهراء، التجربة التشريعية الجزائرية في تنظيم المعاملات الإلكترونية المدنية والتجارية، المؤتمر المغاربي الأول حول المعلوماتية والقانون المنعقد في الفترة من 28 إلى 29 أكتوبر 2009، أكاديمية الدراسات العليا، طرابلس، ليبيا،2009- 2010.

39- هروال نبيلة هبة، ماهية جرائم الإنترنت، المعيار، مجلة دورية تصدر عن المركز الجامعي تيسمسيلت، الجزائر، ع5، جوان 2012 .

40- هشام محمد فريد رستم، الجرائم المعلوماتية أصول التحقيق الجنائي الفني وآلية التدريب التخصصي للمحققين، دراسات أمنية، مجلة الأمن والقانون، تصدرها كلية شرطة دبي، القيادة العامة لشرطة دبي، ع 2، س السابعة، ربيع الأول، 1430هـ- يوليو 1999.

ثانيا: المراجع باللغة الأجنبية

a- Les ouvrages généraux :

1- André Huet et Renée Koering Joulin, Droit pénal international, 2ème éd, puf, 1994.

2- Angelo Castelletta, Responsabilité médicale, droits des malades, Ed. D. Paris, 2002.

3- Béatrice Clément , Gérard Clément, Frédérique Dubost, Jean- Philippe Vincentini, fiches de droit pénal spécial ,ellipses édition, Paris, 2012 .

4- F. jacques et autres, Droit civil, Les obligations, 8ème éd, sirey, Paris, 2013.

5- Jean Larguier, Phillippe conte, Stéphanie Fournier, droit pénal spécial, 15éd, édition dalloz, France, 2013.

6- Jean Pradel, Michel Danti-Juan, droit pénal spécial, 3ème édition, Edition CUJAS, paris, 2004.

7- Marc Dupont, Claudine Esper, Christian Paire, Droit hospitalier, 3ème éd., De Paris, 2001.

8- Michael Véron, Droit pénal spécial, 14ème éd, édition dalloz, paris, 2012.

9- Tahar Hadj Sadok, Les risques de l'entreprise et de la banque, édition Dahleb, Algérie, 2007.

10- Thierry Fossier, droit pénal spécial, T2, affaires, entreprises, et institution publiques, bibliothèque nationale de paris, 2013.

11- Thierry Garé, droit pénal spécial, T1, personnes et bien, 2ème éd, bibliothèque nationale de paris, 2013.

b- <u>Les ouvrages spéciaux</u> :

1- Alain Buquet, manuel de criminalistique moderne et de police scientifique, 5ème édition augmentée et mise à jour, puf, 2011.

2- Bensoussaan (A), Informatique Télécoms Internet, 4éme éd, éditions Francis Lefebvre, 2008.

3- Cédric Manara, droit du commerce électronique, LGDJ, l'extenso édition, France, 2013.

4- Céline Castets-Renard, droit de l'internet: droit français et européen, 2ème édition, Montchrestien, l'extenso édition, paris, France, 2012.

5- Christiane Feral-Schuhl, Cyber Droit , le droit a l'épreuve de l'internet, dalloz, paris, 2011-2012.

6- Coudol (T.P), La signature électronique, introduction technique et juridique a la signature électronique sécurisée, preuve et écrit électronique, édition litec, 2001.

7- Daniel Martin, Frederic Paul Martin, cybercrime, menace, vulnérabilité et ripostes, puf ,2001.

8- Daniel Martin, Fréderic Paul Martin, cybercrime, menace, vulnérabilité, riposte, puf, 2001.

9- Daniel Martin, la criminalité informatique, cybercrime, sabotage, piratage, etc. évolution et répression, puf,1998.

10- Eric Przyswa, cybercriminalité et contrefaçon, fyp édition, France, 2010.

11- Frédéric-Jérome Pensier et Emmanuel Jez, la criminalité sur l'internet, 1ère édition, puf, paris, 2000.

12- Hubert Bitan, droit et expertise des contrats informatiques (contrat de communication électronique vision expertale de la protection des données), édition lamy, France, 2010.

13- Isabelle De Lamberterie, les actes authentiques électroniques, la documentation française, paris, 2002.

14- Jacques Larrieu, Droit de l'internet, 2ème éd. , Ellipses édition, paris, 2010.

15- Lionel Bochurberg, internet et commerce électronique, 2ème éd, Delmas, 2001.

16- Myriam Quéméner, Joel Ferry, cyber criminalité défi mondial ,2éme éd, édition economica, paris, 2009.

17- Olivier D'Auzon, les droits des internautes à l'ère de l'économie numérique, éditions du puits fleuri, France, 2009.

18- Xavier Liant De Bellfond, le droit du commerce électronique, puf, paris, 2005.

19- Yves Bismuth, Droit de l'informatique, éléments de droit à l'usage des informations, Nouveau édition, l'Harmattan, paris, Mise à jour au 1er octobre 2014.

c- Les Thèses :

1- B. Chankire, Problèmes juridique posée par l'internet dans la vente internationale de marchandises, DEES droit des affaires, des université D'abomey- Calavi (République de Bénin), 2004.

2- S. Caidi, la preuve et la conservation de l'écrit dans la société de l'information, Faculté des études supérieures, université de Montréal, Décembre 2002.

d- Les articles :

1- Cécile Manaouil, Marie Graser, Olivier Jarde, Le dossier médical du patient majeur, droit, déontologie et soin, vol. 3, N°4, décembre 2003.
2- Emmanuel Dreyer, sur internet , tout ce qui n'est pas permis est interdit, hebdomadaire , n°44, recueil Dalloz, décembre 2012.
3- Eric Caprioli, Le juge et la preuve électronique, réflexion sur le projet de loi portant adaptation de la preuve aux technologies de l'information et relatif à la signature électronique .www.caprioli-avocats.com
4- Jaques Larrieu, Christian Le Stanc, et Pascal Tréfigny, droit du numérique, recueil dalloz, hebdomadaire, n° 40, novembre 2014.
5- Michel Jaccard, Problèmes juridiques liés à la sécurité des transactions sur le réseau .http://www.signele.com.date
6- Myriam Quéméner, les nouvelles disposition de lutte contre la cybercriminalité issues de la loi du 13 novembre 2014 renforçant la lutte contre le terrorisme, Aj pénal , mensuel, Dalloz, n°3, janvier 2015.
7- Oliver(J.M), l'authenticité en droit positif français, PA, 28 juin1993.
8- Philippe Baumard, la cybercriminalité comportementale:historique et régulation, revue française de criminologie et de droit pénal, n°03, octobre 2014.

9- Sédallian (V), preuve et signature électronique: www.internet-juridique.net.

10- Sophie Sontag- Koenig, la signature électronique en procédure pénale, une évolution amorcée, n°3, AJ pénal, mensuel, Dalloz, mars 2014.

رابعا: الاتفاقيات و النصوص التشريعية.

أ- الاتفاقيات الدولية:

- اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية بتاريخ 15-11-2000.

- La convention sur la Cybercriminalité et son Rapport explicatif ont été adopté par le Comité des Ministres du conseil de l'Europe à l'occasion de sa 109e session, le 8 novembre 2001. La Convention a été ouvert à la signature à Budapest, le 23 novembre 2001, à l'occasion de la Conférence Internationale sur la Cybercriminalité, et elle est entrée en vigueur le 1er juillet 2004.

ب- النصوص التشريعية الوطنية :

- قانون رقم 17-78 الصادر في 06 يناير سنة 1978 المتعلق بحماية البيانات الإسمية للمواطنين.
- القانون رقم 2000-03 مؤرخ في 5 جمادى الأولى عام 1421 الموافق 5 غشت س2000، يحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، ج.ر، ع. 48 الصادرة بتاريخ 06 أوت س 2000.
- قانون رقم 04-15 المؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر س 2044، يعدل ويتمم الأمر رقم 66- 156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو س 1966 والمتضمن قانون العقوبات، ج.ر، ع. 71 الصادرة بتاريخ 10 نوفمبر 2004 .
- القانون رقم 05-02 المؤرخ في27 ذي الحجة عام 1425 الموافق 06 فبراير 2005 المعدل والمتمم للأمر 75-59 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975 والمتضمن القانون التجاري، ج.ر، ع.11، س 2005.

- قانون رقم 05-10 المؤرخ في 13 جمادى الأولى عام 1426هـ الموافق 20 يونيو 2005 المعدل والمتمم للأمر رقم 75-58 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر س1975 المتضمن القانون المدني الجزائري، ج.ر، ع.44، س.2005.
- القانون رقم 06-22 المؤرخ في 29 ذي القعدة عام 1427 الموافق 20 ديسمبر سنة 2006، يعدل ويتمم الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، ج.ر، ع. 84، س.2006.
- القانون رقم 06-23 المؤرخ في29 ذي القعدة عام 1427 الموافق 20 ديسمبر 2006 المعدل والمتمم للأمر رقم 66-156المؤرخ في 18 صفر عام 1386 الموافق 8 يونية سنة 1966 والمتضمن قانون العقوبات الجزائري، ج.ر، ع. 84، س. 2006.
- قانون رقم 09-04 مؤرخ في 14 شعبان عام 1430 الموافق 5 غشت س 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، ج.ر، ع. 47 الصادرة في 16 غشت 2009.
- قانون رقم 14-03 مؤرخ في 24 ربيع الثاني عام 1435 الموافق 24 فبراير سنة 2014 المتعلق بسندات ووثائق السفر، ج.ر. ع. 16، س. 2014.
- قانون 15-03 المؤرخ في 11 ربيع الثاني عام 1436 ه الموافق ل 01 فبراير 2015 المتعلق بعصرنة قطاع العدالة، ج.ر، ع06، لسنة 2015.
- قانون رقم 15-04 مؤرخ في 11 ربيع الثاني عام 1436 الموافق أول فبراير س 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج.ر، ع. 06 الصادرة في 10 فبراير 2015.
- قانون رقم 16-01 مؤرخ في 26 جمادى الأولى عام 1437 الموافق 6 مارس سنة 2016، يتضمن التعديل الدستوري، ج.ر، ع14، س.2016
- قانون رقم 18-05 مؤرخ في 24 شعبان عام 1439 الموافق 10 مايو س2018، يتعلق بالتجارة الإلكترونية، ج.ر، ع.28، الصادرة في 16 مايو 2018.

- الأمر رقم 66-155 المؤرخ في18 صفر عام 1386 الموافق8 يونيو 1966، المتضمن قانون الإجراءات الجزائرية المعدل و المتمم، ج.ر، ع.48، س1966.
- الأمر رقم 66-156 المؤرخ في 18 صفر سنة 1386 الموافق 8 يونيو 1966المتضمن قانون العقوبات الجزائري المعدل والمتمم،ج.ر.ع. 49، س 1966.
- الأمر رقم 75-58 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر س1975 المتضمن القانون المدني الجزائري، المعدل والمتمم، ج.ر، ع.78، السنة الثانية عشرة، صادرة بتاريخ 24 رمضان عام 1395ه- الموافق 30 سبتمبر س.1975.
- المرسوم الرئاسي رقم14-252 مؤرخ 13 ذي القعدة عام 1435 الموافق 8 سبتمبر سنة 2014، يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر سنة 2010، ج.ر، ع.57 س. 2014.
- المرسوم الرئاسي رقم 15-261 مؤرخ في 24 ذي الحجة عام 1436 الموافق ل 8 أكتوبر سنة 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر، ع. 53، سنة 2015.
- المرسوم رئاسي رقم 19-172 مؤرخ في 3 شوال عام 1440 الموافق 6 يونيو سنة 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها، ج.ر، ع.37، سنة 2019.
- المرسوم التنفيذي رقم 98-257 مؤرخ في 3جمادى الأولى عام 1419 الموافق 25 غشت س 1998، يضبط شروط وكيفيات إقامة خدمات 'انترنات' واستغلالها، ج.ر، ع. 63، الصادرة بتاريخ 04 جمادى الأولى عام 1419 هجري.
- المرسوم التنفيذي رقم 07-162 مؤرخ في 13 جمادى الأولى عام 1428هـ الموافق لـ 30 مايو سنة 2007 يعدل و يتمم المرسوم التنفيذي رقم 01-123 المؤرخ في 15 صفر عام 1422 هـ الموافق لـ 09 مايو 2001 والمتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية، وعلى مختلف خدمات المواصلات

السلكية واللاسلكية، ج.ر، ع.37، س.2007، الصادرة بتاريخ 21 جمادى الأولى عام 1428هـ الموافق ل 7 يونيو س.2007.

ج- **القوانين الأجنبية.**

- **القوانين العربية:**

- قانون رقم 150 لسنة 1950 المتضمن قانون الإجراءات الجنائية المصري، معدل ومتمم.
- القانون عدد 57 لسنة 2000 المؤرخ في 13 جوان 2000 يتعلق بتنقيح وإتمام بعض فصول من مجلة الالتزامات والعقود.
- قانون رقم 83 لسنة 2000 مؤرخ في 09 أوت 2000، المتعلق بالمبادلات والتجارة الإلكترونية، ج.ر. ع.64 الصادر في 11 أوت 2000.
- التنظيم القانوني رقم 85 لسنة2001 المؤرخ في 31 ديسمبر 2001 المتعلق بالمعاملات الإلكترونية الأردني، ع.4524، والذي أصبح ساري المفعول بتاريخ31 مارس 2002.
- قانون إمارة دبي رقم 28 لسنة 2002 بشأن المعاملات الالكترونية.
- قانون رقم (2) لسنة 2002 بشأن المعاملات والتجارة الإلكترونية في الإمارات العربية الصادر بتاريخ 30 ذي القعدة 1422 الموافق 12 فبراير 2002.
- مرسوم بقانون رقم (28) لسنة 2002 بشأن المعاملات الالكترونية البحريني، الصادر بتاريخ 7 رجب 1423هـ الموافق 14 سبتمبر 2002، ج.ر، ع. 2548 الأربعاء 18 ديسمبر 2002، المعدل والمتمم.
- القانون رقم 15 لسنة 2004 المتعلق بتنظيم التوقيع الالكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات.
- قانون اتحادي رقم (1) لسنة 2006 في شأن المعاملات والتجارة الإلكترونية، ج. ر، ع442، س. السادسة والثلاثون بتاريخ 2006/1/31.
- قانون رقم 20 لسنة2014 في شأن المعاملات الإلكترونية الكويتي.

- قانون رقم 15 لسنة 2015 المتعلق بالمبادلات الالكترونية الأردني.
- قرار بقانون رقم (15) لسنة2017 بشأن المعاملات الإلكترونية الفلسطيني.
- مرسوم بقانون رقم (54) لسنة 2018 بإصدار قانون الخطابات والمعاملات الالكترونية الصادر بتاريخ 20 ربيع الأول 1440هـ الموافق 28 نوفمبر 2018 ج.ر 3395.
- قانون العقوبات المصري رقم 58 لسنة 1938 طبقا لآخر تعديلات سنة 2018.
- قرار رقم 109 لسنة 2005 بتاريخ 15-05-2005 المتعلق بإصدار اللائحة التنفيذية للتوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة وتكنولوجيا المعلومات المصري.

- **القوانين الغربية:**

- Loi Type de la commission des Nations Unies pour le droit commercial international sur le commerce électronique (1996).
- Loi Type de la Commission des Nations Unies pour le droit commercial international sur les signatures électroniques (2001).
- Règlement (UE) N°910/2014 du Parlement Européen et du Conseil du 23 juillet 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.
- Directive 1999/93/CE du Parlement Européen et du Conseil du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques, JOUE L 13 du 19-01-2000.
- 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), J.O.C.E , L.178 du 17/07/2000.

- Code pénal français créé par Loi 88-19 1988-01-05 art.1 JORF 6 janvier 1988 Abrogé par Loi n°92-1336 du 16 décembre 1992-art .372 (V) JORF 23décembre 1992 en vigueur le 1er mars1994.

- Code de Procédure Pénale modifié par la loi n° 2010- 768 du 09 juillet 2010

- Code de procédure pénale français (dernière modification du texte le 19 avril 2015).

- loi n°93-1013 du 24-08-1993 Art. 20 JORF 25 aout 1993 en vigueur le 2 septembre 1993) modifié le code de procédure pénal français.

- loi n°2000-230 du 13 mars 2000 – art .1 JORF 14 mars 2000, modifier code civil français.

- loi 2003-239 du 18 mars 2003 pour la sécurité intérieure en France, modifiée 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

- Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

- Loi n° 2015-912 du 24 juillet 2015modifier code pénal français.

- Ordonnance n°2000-916 du 19 septembre 2000 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002 modifier code pénal français.

- 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.

خامسا: المواقع الالكترونية

- www.woloo3.com
- www.emarataloyoun.com
- www.aljazeera.net
- www.DW.com
- http://or.wikipedia.org/wiki/معاهدة ماستريخت
- http://or.wikipedia.org/wiki/يوروبول
- http://ar.m.wikipedia.org/wil

الـــفهرس

الـــفهرس