وزارة التعليم العالي و البحث العلمي

جامعة الجيلالي اليابس. سيدي بلعباس

كلية الحقوق والعلوم السياسية

قسم الحقوق

قواعد الأمن المعلوماتي

- دراسة مقارنة-

رسالة مقدمة لنيل شهادة الدكتوراه في العلوم تخصص علوم قانونية، فرع قانون خاص

إشراف الأستاذ الدكتور:

من إعداد:

أ.د. معوان مصطفى

*** بوربابة صورية**

أعضاء لجنة المناقشة:

أ. د/. **بودالي محمد**	أستاذ التعليم العالي	جامعة سيدي بلعباس	رئيساً
	مشرفاً ومقرراً أ. د/ **معوان مصطفى**	أستاذ التعليم العالي	جامعة سيدي بلعباس
د/ **شول بن شهرة**	أستاذ محاضر "أ"	جامعة غرداية	عضواً
د/ **بورويس لعيرج**	أستاذ محاضر "أ"	جامعة بشار	عضواً

السنة الجامعية: 2015-2016م

شـــكـــر و عـــرفـــان

الحمد الله رب العالمين و الصلاة و السلام على أشرف الأنبياء والمرسلين سيدنا ونبينا محمد وعلى آله وأصحابه أجمعين... وبعد

يطيب لي أن أتوجه بوافر الشكر و التقدير و العرفان لكل من ساهم في إنجاز هذا الجهد العلمي المتواضع، وأخص بالذكر أستاذي الكريم: أستاذ التعليم العالي ***د.معوان مصطفى*** *الذي أشرف عليا مرشدا و موجها و معلما و الذي كان لأرائه السديدة و توجيهاته القيمة و مجهوداته الوفيرة أكبر الأثر في إنجاز هذه الرسالة.*

و جزيل الشكر و التقدير لسعادة الدكتورة رنا إبراهيم العطور بالجامعة الأردنية-عمان- على تقديمها يد المساعدة و توجيهها لي أثناء تربصي بالجامعة الأردنية عرفانا بما قدمته من جهد ملحوظ و مشكور لتطوير هذه الدراسة و دعمها.

كما أتوجه بجزيل الشكر و العرفان لأعضاء لجنة المناقشة و على ملاحظاتهم القيمة و السديدة التي سيكون لها الفضل في إثراء هذه الرسالة و خروجها بصيغتها النهائية.

و يطيب لي أن أتقدم بوافر الشكر و التقدير للجميع من من مد يد العون و لم أخصه بالذكر على حسن تجاوبهم و صادق تعاونهم و جزاهم الله عني خير جزاء.

و أخر دعواتنا أن الحمد لله رب العالمين...

الـبـاحثـــة

إهـــــداء

إلـى والدتـي و والـدي طـاعـة و إحـسانـا

إلـى إخـوانـي و أخـواتـي حـبـا و تقـديـرا و وفـاء

إلـى أسـاتـذتـي فـخـرا و اعـتزازا

إلـى أصـدقـائـي و صديـقـاتـي مودة و إخـلاصـا

أهـدي هذا العـمـل المتـواضـع

قائمة بأهم المختصرات

باللغة العربية

ق.ع.ج: قانون العقوبات الجزائري

ق.ع.ف: قانون العقوبات الفرنسي

ق.إ.ج.ج: قانون إجراءات جزائية جزائري

ق.إ.ج.ف: قانون إجراءات جزائية فرنسي

ج.ر: جريدة رسمية للجمهورية الجزائرية

ع. عدد

ص: صفحة

ط. طبعة

ج: جزء

د.ج: دينار جزائري

Principal Abréviation

Bull.crim : Bulletin criminel de la cour de cassation

C.A : Cour D'appel

C.P.F : Code pénal français

C.P.P.F : Code de procédure pénal français

Cass.crim : chambre criminelle de la cour de cassation

D : Recueil Dalloz

Dr.Pén : Revue Droit Pénal

Ed : édition

Ibid : même ouvrage

IP : Internet Protocol

JCP : La semaine juridique édition général

L.C.E.N : Loi pour la confiance dans l'économie numérique

Op.cit : opus citatum, locution latine qui signifié, ouvrage précédemment

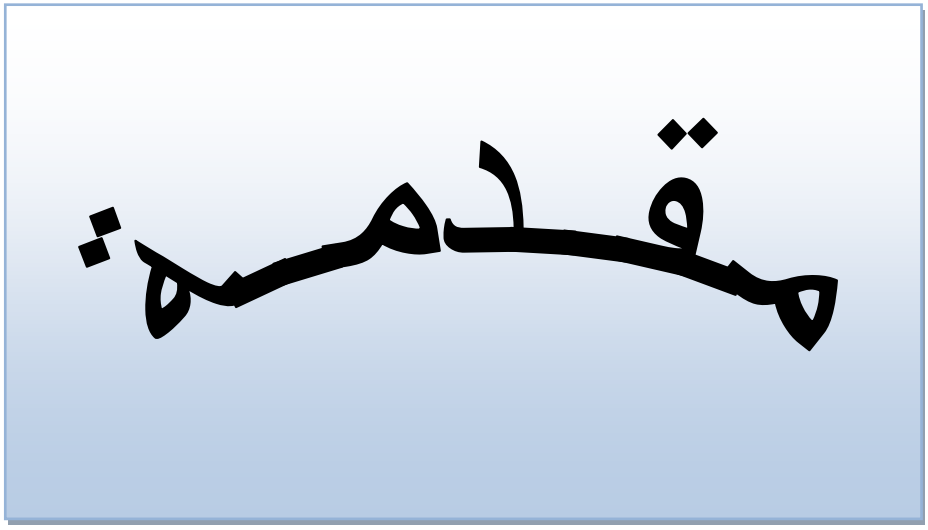
P : Page

STAD : Système de traitement Automatisée des données

T : Tribunal

TCP : Transmission Control Protocol

TGI : Tribunal de Grand Instance



شهد العالم عبر تاريخه سلسلة من التطورات التكنولوجية أثرت في أسلوب حياة الإنسان ومعيشته و متطلباته الضرورية، و ظهرت قمة هذا التطور عند المزاوجة بين تقنيات الحواسيب وشبكات الاتصال أدت إلى ظهور نظم المعلومات المتطورة و شبكات المعلومات.

حيث أحدثت تقنية المعلومات تغيرات مستمرة و مضطردة في أساليب العمل كافة، إذ أصبحت عملية نقل المعلومات عبر الشبكات المحلية و الدولية المفتوحة و أجهزة الحاسوب من الأمور الروتينية و الاعتيادية في العصر الحالي، و إحدى سماته التي لا يمكن الاستغناء عنها لدورها الواضح والفعال في تسهيل متطلبات الحياة ، من خلال تقليل حجم الأعمال وتطوير أساليب خزن و توفير المعلومات.

و في السنوات الأخيرة برز التحدي الكبير في مجال تقنية المعلومات حتى أصبح العصر يسمى بمسماها " عصر المعلومات" أو" عصر المعلوماتية" و المجتمع بـ " المجتمع المعلوماتي"، ذلك أن المعلومات [1] أصبحت في ظل هذا التطور التكنولوجي، الأداة التي تقاس بها قوة الشعوب، فمن يملك المعلومة يملك القوة، و في ظل تنامي أهمية و قيمة المعلومات و الوسائل التقنية التي تعالجها و البيئة التي تستخدم هذه المعلومات والأشخاص الذين لهم الدور في إعدادها و تفعيلها؛

و بطبيعة الحال كل ذلك ليس له أهمية ما لم تكن لتلك المعلومات قيمة، التي تتوقف في معظم الأحيان على قدر أهميتها و مغزاها و حداثتها بالنسبة للمستفيدين منها[2]، فالقضية الحساسة هنا

---

[1]- اتفق أكثر الكتاب و المحللين في المجال العلمي و الاجتماعي، على اختلاف خلفياتهم على أن المجتمع قد شهد تحولا جذريا منذ الثمانينات، و هم يحددون أصل هذا التحول في النظم الآلية لمعالجة و تخزين و بث المعلومات، و يرون كذلك منذ نفس التاريخ تقريبا أن البشرية أقبلت على حضارة جديدة تتأسس على المعرفة حيث تؤدي فيها المعلومات دور المادة الخام الأولية، و يتعاظم فيها دورها كمورد إستراتيجي، و هي أكثر أهمية حتى من مصادر المعادن و الطاقة و رأس المال: **د. علي جعفر**، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص و الحكومة– دراسة مقارنة– الطبعة الأولى، منشورات زين الحقوقية، لبنان، 2013، ص 05.

[2]– **د. زكي حسين الوردي**، و **د. مجبل لازم المالكي**، المعلومات و المجتمع، ط1، الوراق للنشر و التوزيع، 2002، ص 35.

هي قيمة و أهمية المعلومة، حيث تعد قيمة المعلومات واستخدامها من القضايا الجوهرية في علم المعلومات.

و قد أحدثت المعلومات ثورة لحالها خاصة مع التطور السريع لتكنولوجيا الاتصالات وتأثيرها على أساليب العمل و تطور الخدمات و نشر أفاقها عبر مجالات و قطاعات متعددة في المجتمع، كما أظهر ازدياد استخدام التكنولوجيا الحديثة في مجال الاتصال والتواصل والتعاملات المختلفة، و التي أساسها و قوامها الاعتماد على نظام تقني معلوماتي من أجهزة الحاسبات الآلية بمختلف أشكالها و أحجامها و شبكات لاتصال العالمية" الانترنت" و بقدر ما ساهمت هذه التقنيات في تيسير الأعمال و في تنمية وتطوير المجتمعات، إلا أن هناك العديد من العقبات تقف في سبيل ذلك التطور و ترتبط به بعض المخاطر؛

و إحتمال التعرض للفشل أو التخريب و التلاعب مما يعرض أمن المجتمعات وبالتالي الأمن القومي و الاقتصادي للتهديد و الخطر، و لهذا أضافت المعلومات و تكنولوجيا المعلومات نموذجا جديدا في مجال الأمن ألا و هو الأمن المعلوماتي.

و الشيء المتفق عليه هو أن القرن الواحد و العشرين سيكون مجتمع المعلومات، حيث سيفقد الزمان و المكان معناهما، و سيكون لتطور تقنية و قنوات الاتصال أثر على معنى الحرية و التواصل و الحياة الخاصة، و يتغيب بالتالي معنى الحدود و الجغرافيا، و لن يبقى أي مجال خارجا عن دائرة تأثير هذا التطور.

إن ذلك التطور و الإبداع المذهل في مجال تقنية المعلومات و تكنولوجيا الاتصالات أو ما أصطلح عليه بـ" الفوران التكنولوجي الهائل"[3] و الذي يشهد كل يوم تقدما يعجز الإنسان العادي بقدراته المحدودة على مجابهته و ملاحقته و الوقوف على خباياه و أسراره التي أصبحت تفوق كل تصور؛

---

[3]- **د. مصطفى أبو مندور موسى**، خدمات التوثيق الإلكتروني: تدعيم للثقة و تأمين التعامل عبر الانترنت– دراسة مقارنة، ندوة الجوانب القانونية للتعاملات الإلكترونية، مسقط، 23 نوفمبر 2008، ص 02.

و أي تطور في هذا المجال لا شك أنه يحتاج إلى جهد و صبر و وقت للوقوف على مردوده الايجابي و فوائده التي تعم على العالم كله، و تأمين الاستفادة منه في كل المجالات، في مقابل ذلك إكتشاف مخاطره و إشكالاته إما للقضاء عليها أو على الأقل الحد منها بكافة الوسائل و السبل.

فكان لذلك التطور التكنولوجي المشرق من ناحية أخرى وجه مظلم و جوانب سلبية ومخاطر عدة على الأشخاص و على حياتهم الخاصة، و كذا على أمن تعاملاتهم وسرية وسلامة بياناتهم سواء المتداولة أو المخزنة عبر أنظمة المعالجة الآلية للبيانات وحتى على سلامة و أمن النظام المعلوماتي من جانبه التقني في حد ذاته.

و لم تتوقف تلك المخاطر على الأشخاص العاديين، بل تعدى ذلك إلى المساس بأمن وسلامة أنظمة و معلومات المؤسسات و الإدارات و الحكومات و المنظمات في ظل ما شهدته الحكومات في أغلب دول العالم من تحول نحو الحكومات الإلكترونية عملا بمبدأ العصرنة و التوجه نحو التكنولوجيا، و تعدى تأثيرها المجال الإجتماعي إلى المجال السياسي و الاقتصادي، و لم تعد القضية قضية أشخاص عاديين بل امتدت إلى المسائل الوطنية والقومية و أمن الدول و المنظمات الدولية، مما يتطلب التكافل و التعاون الدولي في هذا المجال.

و تحقيقا للتوازن بين التنمية في مجال الاتصالات و المعلومات، و تناسبها مع احتياجات الشعوب في استفادتهم من مجتمع المعلومات وهو ما دعت إليه العديد من

المؤتمرات الإقليمية و الدولية بهدف تضييق ما أصطلح عليه " بالفجوة الرقمية " [4] التي قد يعرفها العالم من جراء هذا التطور الهائل و ما يترتب عليه من أثار؛

فأصبح من الممكن استغلال هذه التكنولوجيا و إختراق أي نظام معلوماتي و إستخدامه في التجسس و تهديد أو النيل من أمن الدول و سلامة البنية التحتية المعلوماتية التي تعتمد عليها

---

[4]- د.**معوان مصطفى**، الإثبات في المعاملات الإلكترونية في التشريعات الدولية– التوقيعات و البصمات الرقمية– دار الكتاب الحديث، الجزائر، 2010، ص 121.

الحكومات، خاصة و أن الحكومات باتت تعتمد على تقنيات المعلومات الحديثة [5]، وتقديم الخدمات العامة عبر نظم المعلومات الإلكترونية التي شكلت نظم الإدارة الحديثة في التعامل مع المواطنين، و كذا تهديد السلامة العامة و ترويع المواطنين باستهداف تلك النظم مما يزعزع الثقة في هذه التعاملات.

و هكذا وجد العالم نفسه أمام ظواهر متغيرة و غير محدودة و يصعب التحكم فيها، هي ظواهر جرمية نمت و إزدهرت بنماء و تطور التقنية الرقمية، و اختلفت التعبيرات والاصطلاحات المستخدمة للدلالة عليها، و طرحت بشأنها العديد من التساؤلات تتعلق بماهيتها و أشكالها بإعتبارها جريمة مستحدثة و متميزة بالبيئة التي تحدث فيها، عن غيرها من الجرائم التقليدية، و تعددت المحاولات الفقهية الرامية إلى تصنيفها و ضبطها بحسب موضوعها أو الوسيلة التي ترتكب بها أو ما تستهدفه تلك الجريمة، و كذا البحث في كيفية مواجهتها بتطبيق نصوص قائمة وضعت في وقت سابق على ظهور التقنية الرقمية، ودون الخروج على مبادئ النصوص من حيث شرعيتها و تفسيرها و عدم القياس عليها.

غير أن الدول التي تعاملت مع هذا النوع الحديث من الإجرام حاولت خلق إطار قانوني موحد لها يقوم على تصنيفها و ضبطها و تحديد العقاب المناسب لها، مع إمكانية تشديده كل

ما دعت الحاجة [6] إلى ذلك تحقيقا للأمن و سلامة الأشخاص و حرياتهم وللوقاية من تأثيراتها عليهم.

و من هنا كانت أسباب طرح هذا الموضوع و البحث فيه و عن سبل توفير الحماية لتعزيز الأمن في مجال المعاملات التي تتم في عالم إفتراضي و رقمي و محاولة الوصول إلى كل ما

---

[5]– يظهر جليا توجه الجزائر نحو الحكومة الإلكترونية، و اعتماد الإدارات على النظم المعلوماتية في التعاملات مع الأشخاص من خلال القوانين الحديثة التي تتطلب ذلك و من بينها ما صدر مؤخرا بشان قطاع العدالة، القانون رقم ***03-15*** المؤرخ في أوّل فبراير سنة 2015 يتعلق ***بعصرنة العدالة***.

و كذلك فيما يخص قطاعات أخرى مثل قطاع المواصلات و الاتصالات، و الصحة، و الضمان الاجتماعي إلى غير ذلك.

[6]- من الدول الأوروبية التي تنبهت إلى هذا النوع من الإجرام و سايرته من الجانب القانوني، نجد دولة فرنسا التي كانت دائما سباقة لوضع قوانين مناسبة مع وجود اجتهادات و حلول قضائية لإدانة مرتكبيها، بداية من أول ا**لقوانين** لسنة ***1978 و1988*** إلى غاية التعديلات التي أدخلتها على **قانون العقوبات** حتى سنة ***2014***.

يخدم الأمن بمعناه الشامل و الواسع و التأكيد على الأمن القانوني إلى جانب الأمن التقني في مجال المعاملات الإلكترونية؛

و البحث في القواعد و الأسس التي يقوم عليها الأمن المعلوماتي و مبادئه، وهي المعروفة باسم الثالوث (Confidentiality ,Integrity , Availability) وهي السرية والسلامة و التوفر (الإتاحة) و هنالك اتجاه حديث يضيف إليها مبدأ رابعا هو المساءلة[7].

لذلك و من اجل الوصول إلى نظام معلوماتي آمن يضمن أمن و سلامة البيانات المتضمنة فيه و بالتالي أمن و سلامة الأشخاص و المنظمات و الدول، لابد من تصنيف ومعالجة القضايا الأمنية المتعلقة به سواء من الناحية التقنية و ذلك من خلال : أمن البيئة المحيطة بالنظام المعلوماتي و أمن و وثوقية العاملين على إدارة النظام المعلوماتي ، و كذا أمن التجهيزات الشبكية و الحاسبات و إستخدام ما توفره التكنولوجيا من طرق وأساليب الحماية، وأهم شيء بطبيعة الحال هو أمن نقل البيانات و المعلومات و حفظها واسترجاعها.

أو من الناحية القانونية من خلال توفير حماية قانونية موضوعية و إجرائية، و ذلك بمسايرة التشريعات للتطور التقني في المجال المعلوماتي و مجابهة مخاطره، و أخد كل التدابي ر و الإجراءات القانونية لمحاولة ردع مرتكبي الجرائم الحديثة التي تهدد مبادئ الأمن المعلوماتي و معاقبتهم، مع ضرورة توحيد تلك التشريعات لمختلف تلك الجرائم وضرورة التعاون الدولي [8] في هذا المجال و على اتخاذ التدابير والاحتياطات اللازمة وتوفير سبل الحماية والسلامة المعلوماتية.

---

[7] – **أمن المعلومات**، الاجتماع الثاني لرؤساء الإدارات المختصة بتقنية المعلومات بالنيابات العامة العربية، المركز العربي للبحوث القانونية والقضائية، مجلس وزراء العدل العرب، جامعة الدول العربية، بيروت – لبنان، 5–7 مارس 2012، ص 2.

[8]- عملا على توحيد تشريعات الدول، صدرت أول **إتفاقية أوروبية** رائدة بشأن الإجرام الإلكتروني هي **إتفاقية بودابست** كنموذج تعتمد عليه كل الدول الأوروبية كطرف في الاتفاقية و كل دولة صادقت عليها و بضرورة إعتماد الحد الأدنى من الجرائم المنصوص عليها في تشريعاتها العقابية، تحقيقا لتعاون الدولي في هذا المجال و بإعتبار تلك الجرائم من الجرائم العابرة للحدود و حتى لا يتهرب مرتكبيها من العقاب.

و الأمر ذاته بالنسبة للدول العربية التي أعدت مشروعا **لاتفاقية الإجرام المعلوماتي** منذ **2004** و التي اعتمدت **كإتفاقية عربية** موحدة تحت إسم ***الاتفاقية العربية بشأن مكافحة جرائم تقنية المعلومات*** المحررة بالقاهرة في **21 ديسمبر 2010** والتي صادقت عليها الجزائر مؤخرا في سنة **2014**.

و لا شك في أن التطور الحالي الذي لحق ثورة الاتصالات عن بعد و ما أفرزته هذه الثورة من وسائل الكترونية متقدمة ومتعددة قد انعكس أثره على الجرائم التي تمخضت عن ذلك بحيث تميزت هذه الجرائم بطبيعة خاصة من حيث الوسائل التي ترتكب بها، ومن حيث المحل الذي تقع عليه ومن حيث الجناة الذين يرتكبونها، لدرجة يمكن القول أن الأساس في خطر هذه الجرائم يكمن في أنها في طبيعتها تجمع بين الذكاء الاصطناعي والذكاء البشري، مما يجعل إثباتها جنائيا قد يكون في منتهى الصعوبة .

أهداف و أهمية الدراسة

إن موضوع قواعد الأمن المعلوماتي موضوع في غاية الأهمية، يمس بشكل مباشر كل المتعاملين في البيئة الإلكترونية و مع الوسائط الالكترونية، حيث ينعكس على حماية مصالحهم و معاملاتهم و التي توفرها مبادئه، إضافة إلى حيوية الموضوع و حداثته التي قد ترجع إلى حداثة إستخدام الأدوات التقنية و برامج الحماية فنية و القانونية، و إلى قلة الدراسات التي تطرقت إلى نظم حماية المعلومات من مختلف الجوانب.

و مما جذب الانتباه نحو أهمية و ضرورة توفير الأمن المعلوماتي كذلك و ما يقوم عليه من مبادئ هو تأثير المنظومة الرقمية على مختلف المجالات و كافة المعاملات بما فيها تأثيرها على المنظومة القانونية فيما يتعلق بظاهرة الجرائم المعلوماتية تحديدا، حيث لم تعد الجريمة تقوم على مفهومها الضيق التقليدي، بل أصبح لها مفهوم حديث و بيئة غير البيئة التقليدية تختلف من حيث عناصرها و مكوناتها؛

كما تبرز أهمية الدراسة في محاولة إثراء الجانب النظري و نسق المعلومات التي توضح قواعد الأمن المعلوماتي و مهددات و مخاطر السلامة المعلوماتية على قواعده، و دور التطورات التقنية و القانونية في الحد من تلك المخاطر و سبل مواجهتها.

و أن الهدف الرئيسي من وراء هذا الموضوع هو التعرف على قواعد الأمن المعلوماتي في ظل المواكبة التقنية و القانونية و أنظمة حمايتها عبر مختلف المستويات.

و دراسة طبيعة وإشكالية حماية وسلامة البيئة المعلوماتية، وكيفية التصدي لأي فعل من شأنه المساس بسلامة المعلومات و وسائل تناقلها أو خزنها من خلال الإعلام والحاسبات والمعلومات

وإبراز الحماية التقنية و القانونية الجزائية بالتحديد في مسائل بعض الجرائم المعلوماتية التي تشكل تهديدا لقواعد و مبادئ الأمن المعلوماتي وفق ما جاء في النصوص القانونية .

إشكالية الدراسة:

تنحصر المشكلة الرئيسية للدراسة في : تحديد ما هي الحماية المطلوبة لتحقيق الأمن المعلوماتي ؟ و ما هو نطاق الجرائم التي تهدد الأمن المعلوماتي؟

إضافة إلى أهم الإشكالات الفرعية التي قد تطرحها دراسة قواعد الأمن و السلامة المعلوماتية منها ما يأتي:

ما المقصود بالأمن و السلامة المعلوماتية؟ ما هي عناصره ومبادئه و كيفية تفعيل دورها؟

ما هي البيانات أو المعلومات الأساسية والمراد حمايتها؟ أو ما هو محل الحماية من مخاطر المعلوماتية؟ ما هي الجرائم المتعلقة بالفضاء الإفتراضي؟

ما مدى استيعاب المجتمع وتطلعه لجرائم إختراق البيئة المعلوماتية في المجتمعات الإفتراضية، وإشكالياتها وسبل حماية نظم الأمن المعلوماتي؟

هل توجد حماية فنية أو تقنية كافية تضمن السلامة المعلوماتية والأمن المعلوماتي؟

والأهم من ذلك هل توجد قوانين وتشريعات لحماية المعلومات والأنظمة المعلوماتية من كل إعتداء أو إختراق أو أي فعل من شأنه المساس بسلامتها؟

وما هو موقف المشرع الجزائري من ضمان سلامة المعلومات المتداولة عبر شبكات الاتصال أو المخزنة في الحاسب أو في النظام معلوماتي؟

ما مدى مواكبة التشريعات الاجرائية لمقتضيات التحقيق و التحري في الجرائم المعلوماتية؟

و تنحصر كذلك إشكاليات الدراسة في التعرف على قواعد الأمن المعلوماتي و عناصره من مختلف جوانبه الفنية و القانونية، و كذا سبل مواجهة أخطار و مهددات الأمن المعلوماتي والسلامة المعلوماتية في ضوء تزايد نسبة الاختراقات و التعديات غير المشروعة، و الحاجة الملحة لاتخاذ كافة الوسائل و الإجراءات اللازمة لحماية المعلومات و أنظمة معالجتها التي تزداد أهميتها لما لها من قيمة؟.

و انطلاقا من صعوبة إيجاد وسائل حماية دائمة في ظل ذلك التطور التقني المتسارع، وظهور وسائل اختراق و انتهاك الحقوق ذات قدرات متطورة مما استوجب البحث عن الحماية القانونية سواء على المستوى الداخلي أو الدولي كون تلك الوسائل قد تتعدى حدود الدول.

صعوبات الدراسة:

يعتبر موضوع البحث في قواعد الأمن المعلومات من جهة من الدراسات الحديثة و من جهة أخرى لا تتوفر فيه مراجع متخصصة بالقدر الكافي و هذه من الصعوبات الجوهرية التي واجهت الباحث، إضافة إلى كونه موضوع هو متخصص في المسائل التقنية أكثر منه في المسائل القانونية مما يتطلب لاستيعابه دراية تقنية إلى جانب المعرفة القانونية

منهج الدراسة:

نعتمد في دراستنا هذه على كل من المنهج الوصفي، التحليلي، المقارن و ذلك في إطار التكامل المنهجي من خلال وصف ظاهرة الأمن المعلوماتي كتحدي جديد في مجال تقنية وتكنولوجيا المعلومات و ما جاء به و له علاقة بالجانب القانوني، و مقارنة الأنظمة القانونية المعنية بالأمن المعلوماتي والسلامة المعلوماتية والجرائم الالكترونية من بينها القانون الفرنسي والأردني و نرجع في الأساس إلى اتفاقية بودابست باعتبارها أول اتفاقية دولية ذات علاقة بالموضوع و النموذج الأمثل لتشريعات الجرائم الالكترونية في الاتحاد الأوروبي وغيره من الأنظمة و كذا بالرجوع إلى الاتفاقية العربية بشأن جرائم تقنية المعلومات الموقعة سنة 2010 بمصر و التي صادقت عليها الجزائر مؤخرا و أصبحت معنية بأحكامها إضافة إلى التشريع الجزائي الجزائري، كما نعتمد المنهج التحليلي من اجل تحليل و دراسة النصوص القانونية المعتمدة.

خطة الدراسة:

في سبيل الإجابة على الإشكالات محل الدراسة قمت باعتماد خطة ثنائية مقسمة إلى فصل تمهيدي كمدخل يشتمل على المفاهيم العامة و الضرورية لدراسة قواعد الأمن المعلوماتي، وباب أول يشتمل على الجوانب الموضوعية للجرائم الماسة بقواعد الأمن المعلوماتي و التي هي في الأساس بعض الجرائم الإلكترونية التي تشكل تهديدا للمبادئ

والقواعد التي يقوم عليها الأمن المعلوماتي من مساس بأمن و سلامة المعلومات و سريتها(فصل أول)، و من أفعال ترتكب بواسطة الحاسب الآلي و الأنظمة المعلوماتية (فصل ثاني) وكذا من جرائم ذات الصلة بالأنظمة المعلوماتية و الملكية الفكرية (فصل ثالث).

أما الباب الثاني يتم التطرق فيه إلى الجوانب و الإجراءات الوقائية و علاجية للأمن المعلوماتي متمثلة في العقوبات المقررة للجرائم التي تم التعرض لها كجانب وقائي ردعي (فصل أول) و كذا الإجراءات المتبعة في التحقيق و الاستدلال للكشف عن تلك الجرائم بعد وقوعها ومدى خصوصيتها بالنسبة لهذا الشكل الحديث من الإجرام (فصل ثاني)، وإلى التعاون الدولي في مجال مكافحة الجرائم الماسة بقواعد الأمن المعلوماتي وعلى مختلف الأصعدة(فصل ثالث).

الفصل التمهيدي:
التأطير المفاهيمي لقواعد الأمن المعلوماتي

الفصل التمهيدي:

الإطار المفاهيمي لقواعد الأمن المعلوماتي

أدى التطور التكنولوجي إلى أتساع مفهوم الأمن، خاصة مع المخاطر التي تحدثها تقنية المعلومات و تهديدها بالمساس بسلامة المعلومات و آمن أنظمة معالجتها أو فيما يعرف بمخاطر المعلوماتية.

و لمواجهة هذا الخطر ظهر مفهوم جديد للأمن و هو ما يعرف بالأمن المعلوماتي والسلامة المعلوماتية، حيث كان هـذا الأخير أكثر الموضوعات في عصر المعلومات إثارة للجدل القانوني، و نتساءل لماذا كان أحدث وأخر إفرازات عصر المعلومات – من بين موضوعاتها وتحدياتها وقطاعاتها – أكثرها إثارة للجدل وأكثرها محلا للاهتمام؟ و عن مدى الالتزام بالحماية ضد هذه المخاطر؟.

و إن استظهار واستطلاع بداية تطور ونماء التقنية المعلوماتية و تطور تأثر النظام القانوني بموضوعاتها وفقا لما سيتم توضيحه لاحقا يظهر أن الخصوصية و حماية الحياة الخاصة من مخاطر التقنية كانت أولى الموضوعات اهتماما في أواخر الستينيات، ثم تبعها الاهتمام بجرائم الكمبيوتر ومن ثم الملكية الفكرية لمصنفات المعلوماتية وتحديدا البرامج اعتبارا من النصف الثاني للسبعينيات ومطلع الثمانينيات، ومن ثم مسائل الموقع الإلكتروني والتجارة الإلكترونية مترافقة مع مسائل أمن الأعمال المصرفية والمالية مترافقة مع آمن المعلومات في بداية ومطلع التسعينيات.

هذا الموضوع الذي تسعى الدول و الحكومات و المؤسسات و الأفراد إلى تحقيقه من جراء ما شوهد من أخطار و خسائر نتيجة الاختراقات المعلوماتية بمختلف أشكالها، و يأتي هذا الفصل لاستعراض المفاهيم الأساسية للسلامة المعلوماتية و قواعد الأمن المعلوماتي قبل الخوض في صلب الموضوع و ذلك ببيان كل من مفهوم الأ من المعلوماتي(مبحث أول)، وعناصر نظام الأمن المعلوماتي التي يقوم عليها(مبحث ثاني)، و كذا التطرق للحماية الفنية لقواعد الأمن المعلوماتي قبل التطرق إلى الحماية القانونية(مبحث ثالث) على النحو الآتي:

المبحث الأول:

ماهية الأمن المعلوماتي

لقد كان للتطور التكنولوجي و التقدم العلمي و التقني في مجال أمن و تقنية المعلومات بالغ الأثر في حماية الأجهزة و الوسائل العلمية التي تحقق قدرا من الحماية تتماشى مع التقدم العلمي و التطور الخطير في أساليب الاختراق التي تستهدف أنظمة المعلومات و ما تتضمنه من المعلومات.

و حيث احتلت المعلومات في الوقت الحاضر مكانا متميزا لما لها من قيمة مادية ومعنوية، و من الخطورة أن لا تحاط بحماية قانونية و إن توفرت الحماية الفنية، و لكن قبل الخوض في عناصر تلك الحماية لابد من أن نقوم أولا بـتحديد مـاهية السلامة المعلوماتية أو الأمن المعلوماتي، يتطلب ذلك بيان كل من التعريف الفقهي والقانوني للأمن المعلوماتي (مطلب الأول)، إلى جانب بيان العناصر و المبادئ التي يقوم عليها الأمن المعلوماتي (المطلب الثاني) باعتبارها مقومات أساسية تحتاج للتوضيح.

المطلب الأول: المفهوم الفقهي و القانوني للأمن المعلوماتي

هناك عدة تعاريف جاءت لتوضيح المقصود بالسلامة المعلوماتية أو ما يعرف بالأمن المعلوماتي.

يقصد بالأمن المعلوماتي من زاوية أكاديمية هو"العلم الذي يبحث في نظريات وإستراتجيات توفير الحماية للمعلومات من المخاطر التي تهددها من أنشطة الاعتداء عليها" [9].

أما من الناحية التقنية فيقصد به: "الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية[10] والخارجية"[11].

أما من الناحية القانونية فإن أمن المعلومات هو:" محل دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات، ومكافحة أنشطة الإعتداء عليها أو إستغلال نظمها في إرتكاب الجريمة "[12]،

---

[9]- **د.هالة كمال أحمد نوفل** : بحث حول "استطلاع رأي النخبة حول جرائم اختراق البيئة المعلوماتية الافتراضية واستشراف الاتجاهات الحديثة في مجال أمن المعلومات" مقدم للمؤتمر السادس لجمعيات المكتبات والمعلومات السعودية – البيئة المعلوماتية الآمنة: المفاهيم والتشريعات والتطبيقات– المنعقد بمدينة الرياض في 6–7 أبريل 2010، ص11.

[10]– من **الأخطار الداخلية** التي تهدد سلامة المعلومات نجد الأخطاء التي يرتكبها الموظفون داخل المؤسسة من خلال الدخول إلى النظام وعبر استعمال وسائل التعريف العائدة للمستخدم المخول بذلك كاستعمال كلمات المرور لأحد المستخدمين واسمه، أو عبر استغلال نطاق وصلاحيات المستخدم الشرعي، ومصدر هذا الاستخدام قد يرجع إلى خطأ تشارك الموظفين لكلمات المرور ووسائل التعريف، أو بسبب الحصول عليها عن طريق إستراق النظر أو نحو ذلك من الأساليب، أما الأخطار الخارجية فتكون في الغالب بانتحال شخص أجنبي عن المؤسسة شخصية أوصفة موظف أو مستخدم للدخول للنظام بهذه الصفة وبهدف الإطلاع على المعلومات السرية للمؤسسة لاستخدامها في أغرض أخرى أومن أجل الفضول فقط، أو بهدف تدميرها للانتقام من صاحب المؤسسة أو لإثبات شخصيته ومهاراته كما يحصل في بعض الأحيان

[11]– د. **خالد ممدوح إبراهيم**، أمن المعلومات الإلكترونية، الدار الجامعية، الإسكندرية، 2008، ص27

[12]– د. **عبد الرحمان شعبان عطيات** ، امن الوثائق والمعلومات، ط1، جامعة نايف العربية للعلوم الامنية، الرياض، 2004، ص 122/د. **خالد ممدوح إبراهيم**، المرجع نفسه، ص 27.

وهو لا شك هدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظم معالجتها.

يتضح من هذه التعاريف أن السلامة المعلوماتية لا تنحصر عناصرها فقط على أمن وسلامة الأنظمة المعلوماتية[13]، بل هي تخص أمن وسلامة الأنظمة المعلوماتية والمعطيات بصفة شاملة أو عامة، إذ تشمل إضافة إلى الجانب الأمني سرية وضمان تواجد تلك المعطيات في صبغة صحيحة أوفي شكلها الصحيح وحماية المعلومات ذات قيمة مهما كان نوعها.

لكن عند الحديث عن السلامة المعلوماتية وحتى يتضح المقصود بذلك لابد من تحديد العناصر المشكلة لها فيما يخص المقصود بسلامة المعلومات (المرقمة) وسلامة الأنظمة المعلوماتية، وهذا ما سوف أتولى توضيحه فيما يأتي:

الفرع الأول: سلامة المعطيات والمعلومات

وبهدف الإحاطة بمفهوم المعلومات (أولاً) نحاول أن نجد تعريف محدد وشامل وكذا تمييزها عن بعض المصطلحات التي قد تتداخل معها (ثانياً).

كما أن مصطلح المعطيات قد يتداخل أو يتشابه في معناه مع مصطلحي المعلومات والبيانات، لذلك سوف يتم تبان ما المقصود بهته المصطلحات كلا على حدا:

البند الأول: المقصود بالمعلومات

هناك عدت مفاهيم وردت بشأن تعريف المعلومات سواء من الناحية الفقهية أو من الناحية القانونية ، نوجزها فيما يلي:

أولا: التعريف الفقهي للمعلومات

إنقسم الفقه في تعريف المعلومات إلى اتجاهين اثنين الأول يعرفها تعريفا واسعا والاتجاه الثاني يعرفها تعريفا ضيقا:

1) المفهوم الواسع للمعلومات

---

[13]- يقصد بالأنظمة المعلوماتية:" أنظمة المعالجة الآلية للمعطيات" و لقد عرفها المشرع الجزائري في **القانون رقم 09-04** المؤرخ في 05 أوت 2009 يتضمن ***القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها***، الجريدة الرسمية للجمهورية الجزائرية العدد 47 الصادرة بتاريخ 16 أوت 2009.

من أبرز الفقهاء الذين تزعموا هذا الاتجاه نجد الفقيه الفرنسي (CATALA) الذي عرف المعلومات على أنها:"كل رسالة يمكن نقلها إلى الغير بأي وسيلة من الوسائل"[14].

ونظرا لمرونة هذا التعريف واستيعابه لكل الوسائل لنقل الرسالة أو المعلومة ومنها الوسائل المعلوماتية وكل جديد في مجال التكنولوجيا الرقمية، فإن بعض الفقهاء الفرنسيين قد تبنوا نفس التعريف ومنهم الفقيه (M. VASSEUR) الذي عرف المعلومات بأنها: "النقل المادي المجرد لأحداث معينة تم الحصول عليها من مصادر متنوعة"[15].

ونفس الشيء بالنسبة لتعريف الفقيه (GALLOUX) الذي عرف المعلومات على أنها: "الهيئة أو الحالة الخاصة للمادة أو الطاقة التي يمكن نقلها أو إبلاغها للغير"[16].

وبالرغم من أسبقية هذا الاتجاه في وضع التعريف القانوني للمعلومات في وقت لم تكن فيه المعلوماتية قد حظيت بالاهتمام الفقهي والتشريعي، إلا أن هناك من انتقد هذه التعاريف، وأخذ عليها أنها لم تهتم بمحتوى المعلومة التي تحملها الرسالة أو قيمتها المالية، أو مدى الاستفادة منها بقدر انشغالهم بإمكانية نقلها أو تداولها بين مختلف الوسائل[17]، فليس كل رسالة تنقل إلى الغير تمثل معلومة تستوجب الحماية، و إنما الحماية تشمل بعض المعلومات التي لها ميزة أو قيمة معية و ليس كل المعلومات.

2) <u>المفهوم الضيق للمعلومات</u>

نظرا للانتقادات التي وجهت للمفهوم الواسع للمعلومات أخذ غالبية الفقه يتجهون إلى وضع تعريف للمعلومات بما يناسب الاتجاهات الحديثة التي تركز على القيمة المالية التي تحملها المعلومة أكثر من تركيزها على وسائل تناقلها.

---

[14] - **CATALA**, Ebauche d'une théorie juridique de l'information D .1984, P 87.

مشار إليه لدى : د. **أيمن عبد الله فكري** ، جرائم نظم المعلومات - دراسة مقارنة-دار الجامعة الجديدة للنشر، الإسكندرية، 2007، ص41.

[15]-**MICHEL Vasseur** ; ¨ Des responsabilités en cours par le banquier a raison des informations avais et conseil dispenses a ses client » revue banque , 1983, p 948 مشار إليه لدى د.**محمد سامي عبد الصادق**، خدمة المعلومات الصوتية والإلتزمات الناشئة عنها، 2005، ص 37

[16]- **GALLOUX** (J-C) : Ébauche d'une définition juridique de l'information, D 1994, chron, p229.

مشار إليه لدى د.**سامي عبد الصادق**، المرجع نفسه، 37 .

[17]- مشار إليه لدى **محمد سامي عبد الصادق**، المرجع نفسه، ص 38 .

من بين تلك التعريفات ما جاء به الفقيه الفرنسي Elis DRAGON على أنها: "كل رسالة ذات معنى تنقل إلى الغير وتتوقف قيمتها المالية على نوعية مضمونه الإعلامي" [18].

وهذا ما يذهب إليه جانب كبير من الفقه المصري إلى الأخذ بالمفهوم الضيق للمعلومات، حيث عرفها البعض على أنها: "كل رسالة تحمل معنى و تتحدد قيمتها المالية حسب كثافة و نوعية مضمونها الإعلامي"[19]، و في ذات المعنى يعرفها البعض الأخر: "كل رسالة تحمل معنى و دلالة، و تتوقف قيمتها المالية على ثقلها الإعلامي"[20].

كما يعرفه البعض الأخر على أنها: "كل ما يقوم بمال من أرقام وبيانات وغير ذلك، مادام يمثل معارف ذات قيمة مالية"[21].

ومن بين أهم التعريفات الجامعة والمانعة نجد من عرفها على أنها: "مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح لأن تكون محلا للتبادل والاتصال أو التفسير والتأويل أو المعالجة سواء بواسطة الأفراد أو الأنظمة الإلكترونية، وهي تتميز بالمرونة بحيث يمكن تغييرها و تجزئتها و جمعها و نقلها بوسائل و أشكال مختلفة" [22].

وما يمكن استخلاصه من التعاريف السابقة أن المعلومات هي عبارة عن رسالة ذات معنى ولها قيمة مالية، وقد تتخذ عدت صور مهما كان شكلها (عادية أو مشفرة) ويمكن نقلها واسترجاعها أو تداولها بمختلف الوسائل.

ثانيا: التعريف التشريعي للمعلومات

ورد في عدة نصوص قانونية استعمال كلمة " معلومات" أو كلمات أخرى قريبة منها مثل "بيانات" أو"معطيات" ففي القانون الجنائي الفرنسي [23] مثلا نجده يعاقب على بث معلومات خاطئة (المواد

---

[18] - **ELISE Dragon**, Etude sur le statut juridique de l'information, D . 1998, chron , p 65/
مشار إليه لدى **محمد سامي عبد الصادق**، المرجع نفسه، ص38 .

[19]- د. **محمود عبد المعطي خيال**: التأمين على المعلومات، ط 1999، القاهرة، ص 12،13.

[20]– **د. أيمن إبراهيم العشماوي**، المسئولية المدنية عن المعلومات، دار النهضة العربية، القاهرة،2004، ص34.

[21]–د. **محمد حسام لطفي**، عقود خدمات المعلومات، دراسة في القانونين المصري والفرنسي، القاهرة، 1994، ص65.

[22]– د. **خالد ممدوح إبراهيم**، أمن الجريمة الإلكترونية، المرجع السابق، ص 27.

[23] -**Art. 322-14 Du C.P.F** dispose que « Le fait de communiquer ou de divulguer une fausse information dans le but de faire croire qu'une destruction, une dégradation ou une détérioration dangereuse pour les personnes va être ou a été commise est puni de deux ans d'emprisonnement et de 30000 euros d'amende..

14/322 و 10/411) دون أن يقدم تعريفا للمعلومات، كما يعاقب أيضا على إفشاء معلومات ذات طبيعة سرية، و ذلك من خلال جريمة إفشاء سر المهنة (م13/226)[24].

وبالإضافة إلى المجال الجنائي هناك نصوص أخرى، حيث عرفتها إتفاقية بودابست لمكافحة الجريمة المعلوماتية بتعريف المعلومات أو المعطيات المعلوماتية على أنها:

"كل تمثيل للوقائع أو المعلومات أو المفاهيم تحت أي شكل، وتكون مهيأة للمعالجة الآلية بما في ذلك برنامج معد من ذات الطبيعة و يجعل الحاسب يؤدي المهمة"[25].

كما نجد عدة دول عربية والتي أخذت بالتعريف الذي نص عليه في قانون الأونيسترال النموذجي للتجارة الإلكترونية، فمثلا نجد قانون التجارة الإلكترونية البحريني لعام 2002 المادة الأولى منه تعرفها على أنها: "النصوص والصور والأصوات والرموز وبرامج الحاسب والبرمجيات وقاعدة البيانات"[26].

وكذلك بالنسبة لمشروع قانون التجارة الكويتي من خلال المادة الثانية على أنها: "مفردات يتم تبادلها على شكل رقمي أو تماثلي أو بما يشابهها في ذلك الصوت والصورة والبيانات والرموز بأنواعها وأنظمة الحاسب وقواعد البيانات والنصوص" ولقد فسرت المذكرة الإيضاحية للقانون هذا التعريف، ونوهت إلى أن هذا المصطلح يشمل أي شكل من المفردات اللغوية أو غير اللغوية مقروءة أو مسموعة أو منظورة،

Est puni des mêmes peines le fait de communiquer ou de divulguer une fausse information faisant croire à un sinistre et de nature à provoquer l'intervention inutile des secours.-

Art. 411-10 Du C.P.F dispose que « Le fait de fournir, en vue de servir les intérêts d'une puissance étrangère, d'une entreprise ou organisation étrangère ou sous contrôle étranger, aux autorités civiles ou militaires de la France des informations fausses de nature à les induire en erreur et à porter atteinte aux intérêts fondamentaux de la nation est puni de sept ans d'emprisonnement et de 100000 euros d'amende ».

[24]- د. **أيمن إبراهيم ألعشماوي**، المرجع السابق، ص 28

Art. 226-13 Du C.P.F dispose que « La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15000 euros d'amende ».

كذلك المادة 301 من **قانون العقوبات الجزائري المعدل بالقانون رقم 82-04 المؤرخ في 13فيفري1982**

[25]- تعرف بيانات الحاسب وفقاً **للاتفاقية الدولية حول الإجرام ألمعلوماتي** والمبرمة بتاريخ 23 جوان 2001 باللغة الفرنسية **Convention sur la cybercriminalité Budapest, le 23.06.2001**

Article 1- b. « données informatiques » désigne toute représentation de faits, d'information ou de concepts sous une forme qui se prête à un traitement informatique exécute une fonction..... "

[26]- كما عرفها **القانون الأردني** و كذلك مشروع **قانون التجارة الإلكترونية** الكويتي

ويتم تبادلها بشكل رقمي أو تماثلي، إضافة إلى فتح المجال أمام أي شكل تقني مشابه ومستحدث ويكون قابلا للتداول[27].

و نجد كذلك الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الموقعة بالقاهرة بتاريخ 2010 تعرف البيانات على أنها: " كل ما يمكن تخزينه و معالجته و توليده و نقله بواسطة تقنية المعلومات، كالارقام و الحروف و الرموز و ما إليها..."[28]

أما بالنسبة للمشرع الجزائري فلقد نص حديثا على تعريف للمعلومات أو بالأصح المعطيات من خلال الأمر رقم 06-09 المتعلق بمكافحة التهريب المادة 02/ط على أنها: "المعلومات: كل المعطيات المعالجة أو غير المعالجة، المحللة أو غير المحللة وكل وثيقة أو تقرير وكذا الإتصالات الأخرى بمختلف أشكالها بما فيها الإلكترونية ونسخها المحقق في صحتها المصادق على مطابقتها"[29].

وعرف معطيات معلوماتية على أنها:" أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها"[30] .

ومن الملاحظ أن هناك علاقة بين المعلومات والمعطيات إذ تعتبر هذه الأخيرة وفقا للمشرع الجزائري أنها عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة، وبذلك نرجع للفرق الموضح تالياً بأن البيانات أو المعطيات هي المادة الخام للمعلومات.

كذلك القانون الجنائي المعدل والمتمم بموجب القانون 04-15 نجد المواد 394 مكرر وما بعدها والتي تتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات على أن تضاعف العقوبة في حالة تغيير أو حذف لمعطيات المنظومة إذا ترتبت عن فعل الدخول أو البقاء عن طريق الغش في كل أو جزء من

---

[27]- **أيمن عبد الله فكري**، مرجع سابق، ص 45.

[28]- الفقرة الثالثة من المادة الثانية من ***الاتفاقية العربية لمكافحة جرائم تقنية المعلومات***، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010 و المصادق عليها من قبل الجزائر بموجب ***المرسوم الرئاسي رقم 14-252*** المؤرخ في 08 سبتمبر 2014، ج.ر عدد 57 بتاريخ 28 سبتمبر 2014.

[29]- الأمر **رقم 06-09** المؤرخ في 15 يوليو 2006 ***المتعلق بمكافحة التهريب***، الجريدة الرسمية عدد 47 بتاريخ 19 يوليو 2006.

[30]- **المادة 02/ج** من **القانون رقم 09-04** المؤرخ في 05 أوت 2009 يتضمن ***القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها***، الجريدة الرسمية للجمهورية الجزائرية العدد 47 الصادرة بتاريخ 16 أوت 2009.

منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك، وبذلك نجد المشرع الجزائري يتحدث عن المعطيات بصفة عامة وبأي شكل هي عليه.

*** المعلوماتية و المعلومة**

تعرف المعلوماتية على أنها "علم المعلومات الخاضعة للمعالجة الإلكترونية" [31]، وأن المعلومة إجمالا هي كل مادة معرفة قابلة لأن تتمثل في إشارات متعارف عليها من أجل حفظها أو معالجتها أو بثها، و رغم إختلاف التعريفات إلا أن المهم في ذلك أن تكون المعلومة خاضعة لنظام المعالجة الآلية على أن يكون هذا النظام أمن و محمي.

و يقصد بالمعالجة الآلية:" مجموعة العمليات المحققة بواسطة الوسائل الأوتوماتيكية و التي لها علاقة بجمع و تسجيل و تعديل و حفظ و تحطيم و بث المعطيات، و استغلالها بوجه عام"[32].

و المعلوماتية في نهاية الأمر لا تخرج عن استعمالات الكمبيوتر و ما تفرضه من تقنيات حتمتها مظاهر التقدم في هذا المجال، و لا تخرج هذه الاستعمالات بدورها عن مستويين، فالأول يعرف بالمعالجة الآلية للبيانات أي استعمال جهاز الحاسوب في حزن المعلومة ومعالجتها دون أن يرتبط بشبكة الاتصالات، و الثاني يعرف بتبادل المعطيات الالكترونية أي نقل المعلومة من موقع على موقع باستعمال وسائل الاتصال الحديثة [33]، أي الربط بين عدد من الحواسيب في أماكن مختلفة، و هو ما يفترض ارتباط جهاز الحاسوب بشبكات الاتصال وقواعد البيانات.

و لا شك أن المعالجة الآلية للبيانات أو المعلومات و في جميع أشكالها قد يتم فيها خرق لقواعد الأمن المعلوماتي و السلامة المعلوماتية، بل إنها تسهل الاعتداء على المعلومات وأنظمة معالجتها بفضل الإمكانات الكبيرة في عالم الاتصالات و تقنية المعلومات التي أضحت تغزو جميع الميادين.

و تعرف ظاهرة الإجرام المعلوماتي بأنها:" الأفعال غير المشروعة المرتبطة بنظم الحواسيب" [34] و أن محلها هو دائما معطيات الحاسب بدلالاتها المختلفة و الواسعة.

ثالثاً: التمييز بين المعلومات والبيانات والمعطيات

---

[31]- القاضي **علي كحلون** ، الجوانب القانونية لقنوات الإتصال الحديثة و التجارة الإلكترونية، دار إسهامات في أدبيات المؤسسة، تونس، 2002، ص 347.

[32] -**Art 5** de la **loi français** n° 78-17 du 6 janvier 1978 relative ***à l'informatique, aux fichiers et aux libertés***.

[33]- **علي كحلون**، مرجع سابق، ص 348.

[34]- **فهد عبد الله العبيد العازمي** ، الإجراءات الجنائية المعلوماتية، رسالة لنيل درجة الدكتوراه في الحقوق، جامعة عين شمس، كلية الحقوق، مصر، 2012، ص 35.

هناك علاقة بين مصطلح المعلومات ومصطلح البيانات أو المعطيات، إذ كثيرا ما يقع الخلط بين هذه المصطلحات، ولذلك من الأحسن إبراز الفرق، فتعرف البيانات على أنها: "مجموعة من الحقائق التي تعبر عن مواقف وأفعال معينة حدثت في الماضي أو الحاضر أو ستحدث في المستقبل سواء كان التعبير بالكلمات، أو الأشكال، أو الرموز" [35]، أما المعلومات فهي بيانات خضعت للتشغيل والتحليل والتفسير لتحقيق أغراض معينة وتمكينهم من الحكم السديد على الظواهر والمشاهدات"[36].

لذلك يرى البعض أن البيانات هي معلومات في حالة كمون، و المعلومات هي بيانات في حالة حركة ونشاط، ولذلك فإن البيانات تمثل حقائق رقمية أو غير رقمية، والمعلومات هي كل نتيجة مبدئية أو نهائية مترتبة على تشغيل البيانات، أو تحليلها أو استقراء دلالتها أو استنباط ما يمكن استنباطه منها وحدها أو متداخلة مع غيرها، فالمعلومة وفقا للرأي السابق تأتي في مرحلة تالية ومتأخرة على البيانات[37]، ويعتبر البعض الأخر كذلك البيانات عبارة عن بعض المعطيات المجردة التي يتم تجميعها وتصنيفها وتوصيف محتواها داخل الحاسب الآلي أو أية وسيلة أخرى من وسائل الإتصال الحديثة، حيث تساعد بعد تحليلها على إعطاء المعلومات[38].

وقد وفق جانب من الفقه حين فرق بين المعلومات والبيانات بالقول : " إن المعلومات هي نتيجة معالجة البيانات" وذلك لأننا نستخدم البيانات لاستنتاج المعلومات [39] و بذلك تشكل البيانات المادة الخام التي يتم تجهيزها للحصول على المعلومات، فالمعلومة لذا أصحاب الرأي السابق تأتي في مرحلة تالية ومتأخرة على البيانات، لذا تعد المعلومة القيمة المضافة، أما البيانات فهي المادة الخام بالنسبة لها.

---

[35]- مشار إليه لدى، **أيمن عبد الله فكري**، جرائم نظم المعلومات، المرجع السابق، ص 39.

[36]- د. **إبراهيم أحمد الصعيدي**: نظام التشغيل الإلكتروني للبيانات، مطبعة المعرفة، 1981، ص 13 / مشار إليه لدى د. **أيمن عبد الله فكري**، جرائم نظم المعلومات، مرجع سابق، ص 39

[37]- د. **أيمن عبد الله فكري**، المرجع نفسه، ص 40.

[38]- **عبد الرشيد مأمون ومحمد سامي عبد الصادق:** حقوق المؤلف و الحقوق المجاورة في ضوء قانون حماية حقوق الملكية الفكرية الجديد رقم 82 لسنة 2002، الكتاب الأول، دار النهضة العربية، القاهرة، 2004، ص120.

[39]– د **محمد سامي عبد الصادق**، المرجع السابق، ص 39،40.

أما المعطيات فقد ورد تعريف لها في الحكم الفرنسي الصادر في 1981 بأنها: "إعادة إبراز المعلومات وفقا للشكل الاصلاحي بغرض تسهيل معالجتها بوسائل إنسانية أو آلية"[40] فما يميز المعطيات هي شخصيتها الشكلية سواء كانت في شكلها الخام أو المعالجة أو المبرمجة.

ومن ذلك يمكن إعتبار مصطلح البيانات أو المعطيات كمصطلح عام يشمل كل الحقائق والعمليات التي يمكن معالجتها لاستنتاج منتج نهائي في شكل معلومات.

الفرع الثاني: تحديد طبيعة و شروط المعلومات

تتطلب السلامة المعلوماتية و قواعد الأمن المعلوماتي تحديد كل من الطبيعة القانونية للمعلومات ، و الشروط الواجب توافرها في المعلومة حتى تحض بالحماية على النحو الآتي:

البند الأولً: الطبيعة القانونية للمعلومات

يوجد خلاف فقهي حول الطبيعة القانونية للمعلومات، حيث يعتبرها جانب من الفقه أنها تعد أموالا منقولة وانه يمكن تقويمها بالمال إنطلاقا من القيمة الإقتصادية لها، وبالتالي تصح أن تكون محلا للحقوق المالية وعلى الأخص حق الملكية، وعلى أساس أنه يمكن إستغلالها في تحقيق أرباح مادية أو تحسين أداء المشروعات الإنتخابية، و بالتالي يجوز أن يرد عليها جميع أنواع التعاملات التجارية[41].

وباعتبار المعلومات مال مقوم سواء كانت مبتكرة أو غير مبتكرة، فهي تتمتع بالحماية القانونية، ذلك لأنها إذا كانت مبتكرة فهي محمية بمقتضى قانون حماية الملكية الفكرية، وإذا كانت غير ذلك فهي محمية بموجب القواعد العامة في القانون المدني باعتبارها مال منقول.

ويرى جانب من الفقه الفرنسي أن المعلومات أموالا ذات طبيعة خاصة انطلاقاً من أن غياب الكيان المادي للمعلومات[42] لا يجعلها محلا لحق مالي من نوع الحقوق المتعارف عليها في الفقه، والتي ترد على كيانات مادية، وإن جاز اعتبارها محلا لحق ملكية أدبية أو فنية أو صناعية[43].

وبالتالي فإن المعلومات التي لا تكون محلا للحقوق الأدبية أو الفنية أو الصناعية، يلزم بالضرورة استبعادها عن طائفة الأموال، ولا يعني هذا الاستبعاد أن تظل هذه المعلومات بدون حماية في حالة ما

---

[40]– د. **أيمن عبد الله فكري**، مرجع سابق، ص 40.

[41]- **خالد ممدوح إبراهيم**، أمن الجريمة الإلكترونية، مرجع سابق، ص 34.

[42]– الكيان المادي يسمى Hard Ward

[43]– د. **خالد ممدوح إبراهيم**، أمن الجريمة الإلكترونية، المرجع السابق، ص 34.

تعرضت لسوء استعمال، كالاستيلاء عليها أو استخدامها استخداما غير مشروع، فإن المسؤولية في هذه الحالة تقوم وفق قواعد المسؤولية المدنية المستندة إلى نص المادة 1382 من القانون الفرنسي[44].

وفي حالة الاعتراف بالخطأ تكون المحكمة قد إعترفت بوجود الحق وهو الحق في المعلومات[45]، ومعناه أن يكون للمعلومات طبيعة خاصة تسمح بأن يكون الحق الوارد عليها من نوع الملكية العلمية.

البند الثاني: الشروط الواجب توافرها في المعلومة

حتى تحضا المعلومة بحماية قانونية فلا بدا أن تتوفر على مجموعة من الشروط متفق عليها والمتمثلة فيما يأتي:

أولا: أن يتوفر في المعلومة التحديد و الإبتكار

الخاصية الأولى التي تتميز بها المعلومة هي أن تكون محددة ومبتكرة وإلا اعتبرت غير حقيقية، فإذا ما اعتبرنا المعلومة تعبير وصياغة محددة تجعل الرسالة ما قابلة للتبليغ عن طريق علامات أو إشارات معينة، ومن الضروري أن تكون محددة وبصفة خاصة في مجال الإعتداءات على الأموال، فهذا النوع من الإعتداءات يفترض دائما وجود شيء محدد[46].

أما بخصوص الإبتكار فهو كذلك أمر أساسي، فأي معلومة غير مبتكرة تعد معلومة شائعة وعامة، ومتاحة للكل و ليس خاصة بشخص معين.

ثانيا: أن يتوفر في المعلومة السرية و الإستئثار

السرية صفة ضرورية لحصر نطاق المعلومة وجعل حركة الرسالة أو تداول المعلومة محدد في دائرة من الأشخاص أوفي نطاق مجال معين، حيث أنه لا يمكن أن نتحدث عن الجرائم الخاصة بالسرقة

---

[44] – **art 1382** Du **C.C.F dispose que** : « Tout fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute du quel il est arrivé à le réparer ».

[45]- د. **خالد ممدوح إبراهيم**، أمن الجريمة الإلكترونية، المرجع السابق، ص 35

[46] - **Pierre Catala**, les transformations de droit par informatique, Emergences du droit de l'informatique,1983, P264 .

مشار إليه لدى د. **سليم عبد الله الجبوري** ، مرجع سابق، ص 39/ود. **خالد ممدوح إبراهيم** ، أمن الجريمة الإلكترونية، المرجع السابق، ص 31،

والنصب وخيانة الأمانة، إذا انعدم هذا الحصر، وكذلك لأن المعلومة غير السرية تقبل التداول ومن ثم تكون بمنأى عن أي حيازة، كما في حالة الرقم السري الخاص باستعمال بطاقات الإئتمان[47].

ويقلل الطابع السري في هذه الحالات المختلفة من إستخدام المعلومات ويقصرها فقط على دائرة المؤتمنين عليها والدين يجدون أنفسهم هكذا منتفعين بحق الإستئثار عليها[48].

المطلب الثاني: عناصر و مبادئ الأمن المعلوماتي

للأمن المعلوماتي عناصر أساسية و مبادئ و هي التي يقوم عليها موضوع الدراسة سواء بالنسبة للحماية الفنية و التقنية لها أو بالنسبة للحماية القانونية.

و يبدو أن قواعد الأمن المعلوماتي تتعلق ابتداءً بسرية المعلومات لذا لابد من بيان سلامة المعلومات أو سلامة المحتوى (الفرع الأول)، بالإضافة إلى ضمان الوصول إلى المعلومات واستمرارها وعدم إنكار التصرف (الفرع الثاني).

الفرع الأول: سرية المعلومات وسلامتها

عند الحديث عن السلامة المعلوماتية فإن ما قد يتبادر إلى الذهن، هو الإطلاع أو الكشف عن معلومات من المفروض بقائها سرا، والحقيقة غير ذلك أو لا تتوقف عند ذلك، إذ أن الأمن المعلوماتي أو السلامة المعلوماتية لا تتوقف على سرية المعلومات فقط بل هناك شروط أو مبادئ أخرى لها أهمية مماثلة للسرية.

البند الأولً: سرية المعلومة

ويعني ذلك أن يتم التأكد من عدم تعرض المعلومات للأخطار المتمثلة في إمكانية الكشف عنها أو الإطلاع عليها من قبل أشخاص غير مخول لهم أو غير مسموح لهم بذلك، وفي الحالة التي يكون فيها مالكي هذه المعلومات يرغبون في حفظ سريتها[49].

لذا فإن هذا الجانب الذي يتطلب الوثوقية أو الأمنية، يتطلب في ذات الوقت اتخاذ التدابير اللازمة لحماية سرية المعلومات الحساسة وضمان التوصل إلى المعطيات حصريا من قبل المستعملين

---

[47]– د. **خالد ممدوح إبراهيم**، أمن الجريمة الإلكترونية، المرجع نفسه، ص31.

[48]– **محمد سامي الشوا**، ثروة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، 1994، ص 176.

[49]- د. **خالد بن سليمان الغثبر** ، ود. **محمد بن عبد الله القحطاني** ، أمن المعلومات بلغة ميسرة، الطبعة الأولى، مكتبة الملك فهد للنشر، الرياض، 2009، ص 13. (كتاب لمركز التميز لأمن المعلومات، جامعة الملك سعود).

المرخصين[50]، أو عدا مالكيها[51] و هذا كما سبق بيانه يعد جانب من الجوانب للأمن المعلوماتي أو للسلامة المعلوماتية.

لكن السؤال الذي يمكن طرحه بهذا الخصوص، و خاصة فيما يتعلق بالمعلومات التي يحرص على سريتها بالنسبة للمؤسسات والشركات، فهل يمكن إتاحتها كلها لجميع الأفراد بالمؤسسة ما عدا جزء بسيط من المعلومات التي يجب أن تبقى سرا؟

وهنا نقصد أن الأصل الإباحة والاستثناء هو الحظر إقتداءا بالمبدأ المستعار من فقه الشريعة "الأصل في الأشياء الإباحة"، وخاصة أن البعض ينادي إلى الحاجة إلى تبسيط نظم السرية بالمؤسسة وإتاحة المعلومات بقدر الإمكان، ولكن قد يتناقض هذا المبدأ مع قاعدة "المعرفة على قدر الحاجة" والتي تقضي بمنع كل المعلومات عن الجميع باستثناء ذلك الجزء البسيط الذي لا يستغني عنه الفرد حتى يستطيع ويتمكن من القيام بعمله[52].

ومع ذلك فإن المبدأ الأخير قد يستعمل في الجهات ذات الطابع الأمني الصرف مثل الهجمات العسكرية التي تهدف إلى تحقيق الأمن بأي ثمن و بأي طريقة كانت، إلا أنه لا يكون صالحا في الشركات التي يكون هدفها الرئيسي هو الربح دائما وتحقيق زيادة الإنتاج و النمو السريع و بأقل تكلفة[53].

و يبقى دائما أن نرجع لتعريف السر أو أساس الذي يقوم عليه السر، وهو ما نقصد به المصلحة التي يحميها القانون على أن يكون نطاق العلم بالسر أو الواقعة في عدد معين من الأشخاص.

البند الثاني: سلامة المعلومات أو سلامة المحتوى

من خلال الشرط السابق والمتعلق بتأمين سرية المعلومات وحمايتها، فهل يعني ذلك عدم الاطلاع على المعلومات، أم يمكن الإطلاع عليها مع عدم تغييرها؟

---

[50]– من التدابير التي تتخذ أو تستعمل للحفاظ على سرية المعلومات المرقمنة أو المتضمنة في الرسالة الإلكترونية خاصة أثناء تداولها عبر شبكة العالمية للمعلومات، هو إستعمال تقنيات التشفير أو أرقام سرية تكون خاصة بالمستعمل فقط وحتى لا يمكن الإطلاع عليها من الغير أو العبث بمحتواها، وهذا ما سيتم توضيحه في العنصر الخاص بالحماية الفنية للسلامة المعلوماتية تبعا.

51- د. **عوض حاج علي أحمد ود . عبد الأمير خلف حسين،** أمنية المعلومات وتقنية التشفير، الطبعة الأولى، دار جامد للنشر والتوزيع، عمان (الأردن)، 2005، ص 36.

[52]- م. **حسن طاهر داود،** جرائم نظم المعلومات،الطبعة الأولى، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2000، ص 30،29.

[53]– المرجع نفسه، ص 30.

الإجابة عن ذلك صعبة [54]، ولكن خلافا لما ورد سابقا فإنه لا يعنينا في هذا المقام سوا اتخاذ التدابير اللازمة والضرورية لحماية المعلومات من التعديل[55]؛

ولا يعنينا المحافظة على سرية المعلومات، ولكن الأمر في هذه المسألة قد يختلط بين سرية المعلومات وسلاماته، وفي المثال الأتي ما يدل على أن هناك بعض المعلومات التي قد تبدو بسيطة ولا تحتاج إلى تأمين لكن الحقيقة غير ذلك:

في الوحدة الدولية لأبحاث الفيزياء النووية بسويسرا، قام أحد المتسللين[56] (Hackers)[57] منذ عدة سنوات بالدخول إلى الحاسب الرئيسي بالوحدة وقام – على سبيل المزاح – بتغيير رقم واحد في قيمة النسبة التقريبية"ط" (π) والتي تساوي 3,142857 حيث جعلها 3,143857، وقد نتج عن هذا التعديل البسيط الذي لم يتنبه له الباحثون خسارة ملايين الدولارات بسبب النتائج الخاطئة للأبحاث، لأن الحاسب الآلي استخدم المساحة الخاطئة والمحيط الخطأ للدوائر في حساباته، حيث يدخل هذا الرمز في كثير من الحسابات[58].

و من أمثلة المعلومات التي تتطلب سلامتها من الإطلاع وعدم التعديل نجد الحساب البنكي أو الرصيد المالي الذي قد يتعرض إلى السطو أو تحويل للمبالغ مثلا من 10000 دج إلى 100000 دج وغير ذلك.

---

[54]– د. **عصام أحمد البهجي** ، حماية الحق في الحياة الخاصة في ضوء حقوق الإنسان والمسؤولية المدنية، دار الجامعة الجديدة، مصر، 2005، ص 97.

[55]– د. **خالد بن سليمان الغثبر ومحمد بن عبد الله القحطاني**، المرجع السابق، ص 23.

[56]– **التسلل** أو **القرصنة** تعني إستخدام الخبرة الحاسوبية لأغراض غير مشروعة، أغراض القرصنة، من قبيل النفاذ إلى النظم الحاسوبية دون أن يكون مخول بذلك والعبث بالبرامج والمعطيات.

[57]- توجد بعض المصطلحات المترادفة في عالم القرصنة في مجال الحاسب الآلي و شبكة الانترنت منها: ا **لهاكرز** ويطلق على المقتحم التقليدي الذي يقوم بالتلصص على الغير في قطاع المعلومات و إذا ما واجهته حماية لا يستطيع تخطيها، فهو ليس له علاقة بتكنولوجيا المعلومات.

أما **الكراكر**: فيطلق على الشخص المقتحم الخبير في مجال المعلومات و استخدام الحاسب الآلي و يعتمد عمله على كسر الحماية الموجودة حول الشبكات و أجهزة الحاسب الآلي لذلك فإنه يستطيع اختراق الشبكات و إقتحام البرامج، وبالتالي الهاكرز يستعين بالكراكر إذا ما صادفه أي نوع من الحماية، ولكن جرت العادة على إطلاق لفظ الهاكر على كليهما أو إستخدام لفظ القرصنة عموما.

د. **أيمن عبد الحفيظ**، الاتجاهات الفنية و الأمنية لمواجهة الجرائم المعلوماتية، بدون ناشر،2005، ص 144.

[58]– **حسن طاهر داود**، مرجع سابق، ص30.

و بالتالي فإن سلامة المعلومات لا يعني فقط عدم تعديلها بل سلامتها من أي استخدام غير مشروع، بفعل تعرض محتواها إلى الانتهاك سواء بالتعديل أو المحو أو التدمير وغير ذلك كما سيتم توضيحه لاحقا عند الحديث عن الحماية الجنائية للسلامة المعلوماتية، وذلك طبعا في أي مرحلة من مراحل المعالجة الآلية أو التبادل الإلكتروني للمعلومات.

الفرع الثاني: ضمان الوصول إلى المعلومات واستمرارها وعدم إنكار التصرف

إضافة إلى عنصر سرية المعلومات و سلامتها فإن من ركائز الأمن المعلوماتي أن يضمن وصول المعلومات كما تم إرسالها و أن لا يتم إنكارها من مرسلها كما يلي:

البند الأول: ضمان الوصول إلى المعلومات واستمرارها

إن المحافظة على سرية المعلومات وسلامتها أمر مهم ولكن هذه المعلومات ليس لها قيمة، إذا كان مالكها لا يستطيع الوصول إليها أي أنها غير متوفرة، أوقد يحتاج وصوله إليها إلى وقت طويل.

وقد لا يتحقق هذا العنصر في حالة ما إذا استعمل المهاجمون، أو الجاني المعلوماتي وسائل يمكنه من خلالها منع المستفيدين أو أصحاب المعلومات من الوصول إليها بكل سهولة، ومن بين تلك المسائل المستخدمة نجد مهاجمة الأجهزة أو الشبكات من خلال إدخال فيروسات قد تقوم بمحو المعلومات أو إتلافها أو شل وتعطيل عمل الأجهزة التي تخزن المعلومات[59].

لذا فإنه يعتبر من أهداف وشروط السلامة المعلوماتية التأكد من استمرار التفاعل مع المعلومات واستمرار عمل النظام المعلوماتي[60]، لذا يجب التصدي لتلك الأعمال أو الهجمات التي يقوم بها هؤلاء الأشخاص لحرمان المستفيدين من الوصول إلى المعلومات.

و هذا ما سيتم توضيحه عند الحديث عن الأخطار التي تواجه أمن المعلومات وأمن الأنظمة المعلوماتية.

البند الثاني: عدم إنكار التصرف (Non Repudiation)

تتمثل في خدمة أو وظيفة من خلالها يمنع أي كيان أو مستخدم من أن ينكر أي عمل سابق تم إجرائه[61] كأن يتم إنكار إرسال معلومات أو رسالة معينة، أو إنكار كذلك تلقي أي رسالة إلكترونية.

---

[59]– د. **خالد بن سليمان الغثبر ومحمد بن عبد الله القحطاني**، مرجع سابق، ص 24.

[60]– د. **خالد ممدوح إبراهيم**، أمن المعلومات الإلكترونية، المرجع السابق.ص 85.

[61]– د. **هالة كمال أحمد نوفل**، المرجع السابق، ص16.

لذلك عند وقوع مثل هذا الخلاف بين الأطراف المتصلة رقميا في إنكار ما تم من تصرفات، فإنه يجب توفير إجراء معين أو وسيلة محددة لحل هذا النزاع، ويتم ذلك من خلال إشراك طرف ثالث محايد و موثوق به[62]، وهذا ما تحققه وظائف التوقيع الإلكتروني من خلال هيئات التصديق أو المصادقة الإلكترونية، وبالتالي لا يمكن لآي طرف إنكار أي تصرف صادر منه.

وتجدر الإشارة إلى وجود صور خاصة للمعلومات:

– الرسالة الإلكترونية، البرامج، المحرر الإلكتروني، التوقيع الإلكتروني، الفيروسات.

كل هذه الأشكال والصور هي في الأصل عبارة عن معلومات تبث أو ترسل أو تودع من خلال وعلى جهاز الحاسب الآلي وشبكة الاتصالات.

المبحث الثاني

عناصر نظام الأمن المعلوماتي

إن أي نظام معلوماتي حتى يتسم بالفعالية يجب أن يشمل مجموعة من العناصر والمكونات ذات الصلة بنظام المعلومات المرقمنة، وبالرغم من أن الأنظمة المعلوماتية في تطور مستمر إلا أنه يواجه دائما مشاكل وأخطار الإختراق والإتلاف، وهذه الأخطار هي كذلك في تطور بشكل يساير تطور الأنظمة المعلوماتية ويمكن تحديد ذلك بما يلي:

المطلب الأول: العناصر الأساسية لنظام المعالجة الآلية

تتطور أجهزة الحواسيب بشكل دائم ومستمر، وفي مقابل ذلك التطور هناك من الطرق المستخدمة لإختراقها، مما يستلزم أو ينبغي معه تطوير أو تكوين الأفراد العاملين في أقسام وقواعد المعلومات لكي يتمكنوا من مواجهة وتفادي حالات الاختراق والتلاعب المقصود أو غير المقصود في هته الأنظمة، وذلك بأخذ كل الإحتياطات والتدابير اللازمة:

الفرع الأول: منظومة الأجهزة الإلكترونية وملحقاتها

---

[62]– د. **عوض حاج علي أحمد ود. عبد الأمير خلف حسين**، مرجع سابق، ص 37.

نقصد بمنظومة الأجهزة الإلكترونية وملحقاتها، جهاز الحاسب الآلي ومكوناته الداخلية والخارجية وكذا شبكة الانترنت، بالإضافة إلى العنصر البشري.

البند الأول: المقصود بجهاز الحاسب الآلي ومكوناته

إن الحديث عن أي نظام معلوماتي، يتعين معه وجود جهاز الحاسب الآلي وكل مكوناته المادية والمعنوية، وشبكة الإتصال الخاصة بتناقل المعلومات، وكذا الأشخاص أو الأفراد الذين لهم تأثير فعال في أداء عمل الحواسيب.

أولا: تعريف الحاسب الآلي

تعددت وتنوعت التعريفات التي أعطيت لجهاز الحاسب الآلي:

لغتا: الحاسب في اللغة [63] مصدره الفعل حسب أو نحوه، وعلم الحساب علم الأعداد وهي العدد والتدبير الدقيق، والحسب العد والإحصاء والحسب ما عد[64].

وكلمة الحاسب يقابلها في اللغة الإنجليزية COMPUTER، وكلمة ORDINATEUR في اللغة الفرنسية، وكلمة COMPUTER المشتقة من الكلمة COMPUT اللاتينية والتي تعني أيضا يحسب[65]، وقد وضعت مصطلحات عربية كثيرة للدلالة عليه مثل الحاسب الآلي والحاسب الإلكتروني[66]، أو الحاسوب أو الكمبيوتر.

أما الحاسب إصطلاحا فقد عرف على أنه: "آلة حسابية إلكترونية ذات سرعة عالية ودقة كبيرة يمكنها قبول البيانات وتخزينها ومعالجتها للحصول على النتائج المطلوبة"[67].

كما عرف بأنه: "آلة قادرة عل إجراء عمليات حسابية ومنطقية (لغايات علمية وإدارية ومحاسبية..) بصورة تلقائية، وذلك بواسطة برامج تحدد تسلسل هذه العمليات"[68].

---

[63]- **المعجم الوجيز** – مجمع اللغة العربية – وزارة التربية والتعليم، طبعة 1995، ص 178: مشار إليه لدى د. **فتوح الشاذلي، وعفيفي كامل عفيفي** ، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة في القانون– دراسة مقارنة– الطبعة الثانية، منشورات حلبي الحقوقية، بيروت، لبنان، 2007، ص 21.

[64]- **خثير مسعود:** الحماية الجنائية لبرامج الكمبيوتر، أساليب وثغرات، دار الهدى، عين مليلة، الجزائر طبعة 2010، ص 21.

[65]- د. **هشام محمد فريد رستم** ، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الكاتبة، أسيوط، مصر، طبعة 1995، هامش الصفحة 7/ ود.**فتوح الشاذلي وعفيفي كامل عفيفي**، مرجع سابق، ص21

[66]- " **إلكتروني**" لغتا عبارة عن جسيمات دقيقة ذات شحنة كهربائية سالبة، مشار إليه لدى د. **فتوح شاذلي وعفيفي كامل عفيفي**، المرجع نفسه، ص 21.

[67]- د. **محمد على العريان:** الجرائم المعلوماتية، دار الجامعة الجديدة الإسكندرية ،مصر، 2004،ص 56.

وأيضا عرفه جانب من الفقه المصري بأنه: "جهاز إلكتروني يستطيع أن يقوم بأداء العمليات الحسابية والمنطقية للتعليمات المعطاة له بسرعة كبيرة قد تصل عشرات الملايين من العمليات الحسابية في الثانية الواحدة، وبدرجة علية الدقة، وله القدرة على التعامل مع كم هائل من البيانات وكذلك تخزينها واسترجاعها عند الحاجة إليها"[69].

و لقد عرفته الموسوعة الشاملة لمصطلحات الكمبيوتر بأنه: "جهاز إلكتروني يستطيع ترجمة أوامر مكتوبة بتسلسل منطقي، لتنفيذ عمليات إدخال البيانات Data in put أو إخراج المعلومات Information out put، وإجراء عمليات حسابية أو منطقية أو يقوم بالكتابة على أجهزة الإخراج أو التخزين"[70].

إذن الحاسب الآلي هو جهاز لإستقبال البيانات لمعالجتها أو تخزينها وإسترجاعها عند الحاجة مستعينا في ذلك ببرامج تم وضعها مسبقا.

والحاسب الآلي منذ ظهوره وتطوره مر بعدة أجيال، تنوعت فيها الحاسبات وإختلفت تقسيماتها، غير أنها جمعتها خاصية واحدة كونها تشتمل على عنصرين أساسيين عنصر مادي وعنصر معنوي.

وأجهزة الحاسبات الآلية تشمل ثلاثة أنواع متميزة هي حاسبات تناظرية (قياسية)[71]، وحاسبات رقمية[72]، وأخرى مختلفة أو خليطة تجمع بين الإثنين السابقين[73].

ثانيا: عناصر الحاسب الآلي

الحاسب الآلي عبارة عن وحدة متكاملة من العناصر والمكونات المادية والمعنوية، لا يمكن تشغيله بمعزل عن بعضها البعض.

---

[68]– مشار إليه لدى أ. **خيثر مسعود**، مرجع سابق، ص 22.

[69]– **محمود حسام محمود لطفي** : الحماية القانونية لبرامج الحاسب الإلكتروني، دار الثقافة للطباعة والنشر، 1987، ص 6 مشار إليه لدى :د.**محمد علي العريان**، مرجع سابق، ص 65/ وكذا: أ. **خيثر مسعود**، مرجع سابق، ص 22.

[70]– د. **محمد علي العريان**، مرجع سابق، ص 57.

[71]– **الحاسبات التناظرية**: هي حاسبات لا تقوم بمهمة التخزين مثل عداد السرعة والعداد الحراري، و إستخداماتها قليلة في مقابل الحاسب الرقمي.

[72]– **الحاسب الرقمي**: يعتبر كذلك لأن البيانات المدخلة إليه تخزن في ذاكرته على شكل أرقام وعند إسترجاعها تراها في شكلها المقروء وليس كما هي مخزنة أو مسجلة في الذاكرة، لذلك فهو يقوم بجمع البيانات ويختزن النتائج لحين طلبها وهو كثير الاستعمال والانتشار/ مشا إليه لدى: د. **محمد علي العريان**، مرجع سابق، ص58.

[73]– د. **محمد علي العريان**، المرجع نفسه، ص 58.

1: العناصر المادية للحاسب الآلي

يتشكل الحاسب الآلي من عناصر مادية ملموسة، إنطلاقا من جهاز الحاسب الآلي إلى مختلف الوسائط المادية المستعملة في العمليات التي تمر بها البيانات والمعلومات من مراحل الإدخال والتسجيل إلى غاية مرحلة التخزين.

و من المكونات المادية الرئيسية لأي نظام معلوماتي نجد وحدات الإدخال، ووحدة التشغيل المركزية وأخيرا وحدات الإخراج[74].

أ) **وحدات الإدخال:** وهي العناصر التي يمكن من خلالها للشخص إدخال البيانات أو الأوامر[75]، ومن بين أهم وسائل الإدخال نجد:

1- **لوحة المفاتيح:** عبارة عن وسيلة لإدخال المعلومات والبيانات للنظام المعلوماتي، وتشمل على عدة مفاتيح لكل منها وظيفته التي يقوم بها في عملية إدخال المعلومات أو كتابة البيانات المدخلة للنظام المعلوماتي[76].

2- **الفأرة:** هي جهاز متصل بالحاسب يتم تحريكها باليد وعن طريقها يحرك السهم الذي يظهر على شاشة الحاسب، ثم يضغط على الأمر المراد تنفيذه ويتولى الجهاز تنفيذ ذلك[77].

3- **مشغل الأقراص الممغنطة أو الأسطوانات.**

4- **الماسح الضوئي:** من خلال هذا الجهاز يتم إدخال البيانات والمعلومات للحاسب الآلي أو عن طريق نسخه للصور والمستندات، بحيث يمكن للنظام المعلوماتي التعامل معها وفقا لطبيعتها، وهو يشبه آلة تصوير المستندات والأوراق، غير أنه بمساعدة برنامج خاص يتمكن من قراءة الأوراق المدخلة للنظام المعلوماتي بإعتبارها صورة أو نص مكتوب[78] بالتعديل عليها حال كونها

---

[74]- د. **خالد ممدوح إبراهيم:** أمن الجريمة الإلكترونية، مرجع سابق، ص 21.

[75]- د. **عبد الفتاح بيومي حجازي** : مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، الطبعة الأولى، الإسكندرية، 2006، ص 61.

[76]- **المعجم الموحد لمصطلحات الحاسبات الإلكترونية،** عمان المملكة الأردنية الهاشمية، 1981، ص 750: مشار إليه لدى :د. **أيمن عبد الله فكري،** مرجع سابق، ص 53.

[77]- د. **عبد الفتاح بيومي حجازي،** مبادئ الإجراءات الجنائية في جرائم الكمبيوتر، مرجع سابق، ص61.

[78]- **د. عبد الفتاح بيومي حجازي** ، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر و الانترنت، المرجع نفسه، ص 62/ د. **أيمن عبد الله فكري،** مرجع سابق، ص 53.

خزنت في جهاز الحاسب الآلي، ثم إعادة طبعها مرة أخرى بالمواصفات التي يحددها المجرم المعلوماتي[79]، وغالبا ما يستخدم هذا الجهاز في عمليات التزييف والتزوير.

5- **مشغل الأسطوانات :** تقوم هذه الوحدة بتشغيل الأسطوانات المدمجة، أو قرص الليزر وقراءة البيانات والمعلومات التي يريدها المجرم المعلوماتي لغرض إجرامي[80].

ب) **وحدات المعالجة المركزية :** تعتبر وحدة التشغيل المركزية وحدة تلقي الأوامر عن طريق عناصر الإدخال ثم معالجتها وإخراجها بالصورة التي يرغبها مشغل الجهاز[81]، ومن أهم مكوناتها[82]:

- **وحدة الذاكرة:** وهي الوحدة التي تقوم بحفظ البيانات والنتائج بشكل مؤقت وتقاس بالوحدات التالية:
  - بيت Bit وهي أصغر وحدة قياس
  - بايت Byte وهو يساوي 8 Bit
  - كيلوبايت وهو يساوي 1024 Byte
  - وحدة الحساب والمنطق
  - وحدة التحكم[83]

ج) **وحدات الإخراج:** وهي وحدة إخراج النتائج وإظهارها في أشكال مختلفة ومن أمثلة هذه الوحدات:

1- **شاشة العرض :** تتمثل في شاشة تلفزيونية تقوم بعرض النتائج في شكل نصوص مكتوبة أو صور أو رسومات المعالجة آليا أو المخزنة في النظام المعلوماتي، أو المدخلة إلى جهاز الحاسب الآلي[84].

2- **الطابعة:** عبارة عن وحدة لإخراج النتائج في صورة أوراق ونسخ مطبوعة من البيانات والمعلومات الصادرة عن النظام المعلوماتي[85].

---

[79]- د. **أيمن عبد الله فكري**، المرجع نفسه، ص 53.

[80]- د. **عبد الفتاح بيومي حجازي** ، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر و الأنترنت، دار الكتب القانونية، مصر، 2005 ، ص62.

[81]- المرجع نفسه، ص 62-63.

[82]- د. **خالد ممدوح إبراهيم:** أمن الجريمة الإلكترونية، مرجع سابق، ص 21.

[83]- تفاصيل أكثر لدى: د. **أيمن عبد الله فكري**، مرجع سابق، ص 60-63.

[84]- د. **أيمن عبد الله فكري**، المرجع نفسه، ص 63.

[85]-د. **ممدوح خالد إبراهيم** : أمن الجريمة الإلكترونية، المرجع السابق، ص 25/ د. **عبد الفتاح بيومي حجازي** : الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، ص 20/د. **أيمن عبد الله فكري**، مرجع سابق، 63.

3- **الميكروفيلم:** جهاز خاص يتم توصيله بالحاسب للحصول على مخرجات في صورة فيلم ميكروفيلم، ويمكن قراءته عن طريق أجهزة خاصة تسمى جهاز قارئ الميكروفيلم[86].

4- **القرص الصلب:** وهي وحدة إدخال وإخراج للمعلومات المطلوبة للنظام المعلوماتي[87].

5- **وحدة القرص المرن :** يقوم القرص المرن بنفس وظيفة القرص الصلب تقريبا، وهو كذلك وحدة إدخال وإخراج وحفظ أو تخزين المعلومات، فهو من أشهر وسائط التخزين التي تستخدم مع الحاسبات الصغيرة والمتوسطة نظرا لسهولة استخدامه وكثرة تداوله وقلة كلفته المادية[88].

2:الكيانات المعنوية

يتمثل الكيان المعنوي للحاسب الآلي فيما يخص برامج المعالجة الآلية وهناك من يطلق عليه مصطلح الكيان المنطقي[89] وكذا المعلومات أو البيانات وذلك على التفصيل الآتي:

أ. تعريف برامج الكمبيوتر وتحديد طبيعتها:

البرنامج هو وسيلة للمعالجة الآلية، وبدونه فإنه لا فائدة من النظام المعلوماتي أو الحاسب الآلي فهو بمثابة الروح المحركة لهذا الجهاز أو الآلة.

ويرى البعض أنه يعتبر بالنسبة للحاسب الآلي بمثابة العقل للإنسان الذي يفكر به ولذلك يقال بأن البرنامج هو فكر الحاسب الذي يوجهه الوجهة التي يريدها مما يقتضي القول بأن الحاسب مجرد عالم أو منفذ غبي للأوامر التي يتضمنها برنامجه[90].

- المفهوم القانوني لبرامج الكمبيوتر:

بالرجوع للتشريع الجزائري نجده خاليا من تعريف للبرامج، كما لم تعرف في القانون المتعلق بحق المؤلف والحقوق المجاورة المعدل سنة 2003 [91].

---

[86]- د. **أيمن عبد الله فكري**، المرجع نفسه، ص 64.

[87]- د. **عبد الفتاح بيومي حجازي** : الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، مرجع سابق، ص 21/د. **أيمن عبد الله فكري** ، مرجع سابق، 64.

[88]- د.**أيمن عبد الله فكري** ، المرجع نفسه، ص 64/ د.**عبد الفتاح بيومي حجازي** : الدليل الجنائي والتزوير في جرائم الكمبيوتر ولأنترنت، مرجع سابق، ص 21.

[89]- د. **فتوح شادلي وعفيفي كامل عفيفي**، مرجع سابق، ص 26/ أ. **خثير مسعود**، مرجع سابق، ص 24.

[90]- **نفس المرجع**، ص 25

[91]- عدل **قانون حق المؤلف والحقوق المجاورة** بموجب الأمر رقم **03-05** المؤرخ في 19 يوليو 2003 ، جريدة الرسمية للجمهورية الجزائرية عدد 44 ، بتاريخ 23 يوليو 2003.

أما المشرع الفرنسي فقد عرفها بموجب القرار الوزاري المتعلق بإثراء اللغة الفرنسية [92] الصادر بتاريخ 22 ديسمبر 1981 بأنها: "مجموعة البرامج والمراحل والقواعد وأحيانا الوثائق المتعلقة بسير مجموعة من الإستعلامات"

وقد عرفه المشرع الأمريكي في قانون حق المؤلف الصادر في 1976 المعدل بقانون 1980 بأنه: مجموعة عمليات متتابعة يتم القيام بها بغرض الإستخدام المباشر وغير المباشر من جهاز الكمبيوتر من أجل الحصول على نتائج معينة"[93].

وقد إتصف هذا المفهوم بالضيق لأنه لم يشمل وصف البرامج أو المستندات الملحقة بالبرامج.

2- **البيانات والمعلومات:** تعتبر كذلك من الكيانات المعنوية للمنظومة المعلوماتية و لقد سبق تعريفها و الإشارة إليها.

الفرع الثاني: شبكة تناقل المعلومات

تعتبر شبكة الإنترنت ثمرة من ثمرات التطورات في مجالات الإتصالات، حيث تقوم بدور بالغ الأهمية وجد فعال بالنسبة لنظم الإتصالات ذلك أنها سهلت عملية التراسل بين الحواسيب في مختلف أنحاء العالم، إذ تقوم بنشر المعلومات وتوفر فرص نقلها وإتاحتها على نطاق واسع وتبادل وإستخدام الملفات، ولكن في مقابل هته الميزة فإنها أتاحت فرصة سرقة المعلومات أو إتلافها بعد الإطلاع عليها من خلال إستخدام الفيروسات أومن خلال الدخول عبر منظومات الإتصال المختلفة، لذلك من اللازم اتخاذ إجراءات الحماية وضمان أمن الشبكات.

البند الأول : نبذة تاريخية عن الانترنت

كان أول من أنشأ هذه الشبكة هم الأمريكيون على يد مجموعة من الخبراء، و ذلك في الفترة ما بين 1959 و 1969 ، و كانت تعرف بـ Arpanet و تعرف حاليا باسم Internet، و التي كانت حكرا على و كالة المخابرات الأمريكية(CIA) و هي وكالة حكومية استعملتها لأغراض أمنية للمحافظة على استمرار الاتصالات عند حدوث هجوم نووي بحيث لا يؤثر ما عسى أن يدمر من بنية تقنية الاتصالات على عمل الشبكة ككل[94].

---

92 – J .O.R.F, du 17 janvier 1982 مشار إليه لدى: أ. **خثير مسعود**، المرجع السابق، ص 25.

93– مشار إليه لدى:د. **أيمن عبد الله فكري**، مرجع سابق، ص 56/ أ. **خثير مسعود**، المرجع السابق، ص 25.

94– **محمد علاء نصيرات**، حجية التوقيع الإلكتروني في الإثبات، دار الثقافة للنشر و التوزيع، عمان، الأردن، 2005، ص 53.

و بعد أن وجدت الوكالة بديلا أفضل قامت بإتاحتها للجمهور، و هي تعتبر أوسع و أضخم شبكة عالمية للتبادل الإلكتروني، و تقوم على الربط بين أجهزة الحاسب الآلي على مستوى العالم عبر خطوط اتصال مستقلة أو من خلال أسلاك الهاتف[95].

و أصبحت اليوم الانترنت الفضاء الواسع للتبادل في مختلف المجالات و على الأخص في النشاطات التجارية.

البند الثاني: أهم خدمات الإنترنت

لقد وضع المشرع الجزائري في المرسوم التنفيذي رقم 98-257 شروط و كيفيات إقامة خدمات "أنترنات" و استغلالها[96] و المتمثلة في:

أولا: خدمة الويب الواسعة النطاق

و يطلق عليها الشبكة العنكبوتية العالمية للمعلومات ، و هي تعد من أهم خدمات الانترنت [97]، و هي خدمة تفاعلية لإطلاع أو احتواء صفحات متعددة الوسائط Multimédia، مدعمة بالنصوص و الرسوم البيانية ، و الصوت و الصورة، موصولة بينها عن طريق صلات تسمى نصوص متعددة Hypertexte [98].

هذه الخدمة تمتاز بقدرة هائلة في الإبحار عبر فضاء الانترنت مما يجعلها أكثر شعبية للمتعامل عبر الانترنت.

ثانيا: البريد الإلكتروني E.mail

كذلك يعد البريد الإلكتروني من أهم خدمات الانترنت و التي تسمح بتبادل رسائل إلكترونية بين المتعاملين في اتجاهين مختلفين أو أكثر.

---

[95]- **محمد علاء نصيرات**، المرجع نفسه، ص 54.

[96]- **المرسوم التنفيذي** رقم 98-257 المؤرخ في 25 أوت 1998، ***يضبط شروط و كيفيات إقامة خدمات انترنت واستغلالها*** ، جريدة رسمية عدد 63 بتاريخ 26 أوت 1998، ص 5، المعدل بموجب المرسوم 200-307 المؤرخ في 14 أكتوبر 2000 ، ج ر عدد 60 بتاريخ 15 أكتوبر 2000.

[97]- **إبراهيم بختي**، مرجع سابق، **ص 28**.

[98] - **حسب المادة 1/02 من المرسوم التنفيذي رقم 98-257** ***يضبط شروط و كيفيات إقامة خدمات انترنت واستغلالها .***

و الرسائل الإلكترونية هي بمثابة تبادل و قراءة و تخزين المعلومات في شكل رسائل معطيات بين الموزعات الموجودة في مواقع متباعدة، و يمكن المرسل إليه (أو المرسل إليهم) قراءة الرسالة المبعوثة عبر البريد الإلكتروني في وقت حقيقي أو في وقت مؤجل[99].

ثالثاً: تلنات Tel net

خدمة النفاذ إلى حواسب متباعدة بصيغة المحاكاة الطرفية[100]، و هي خدمة للربط عن بعد تمكن المستخدم للشبكة من التنقل عبر مختلف (الحواسيب) الشبكات الجزئية المتصلة بالانترنت للحصول على معلومات معينة في مجال محدد[101].

رابعاً: بروتوكول نقل الملفات TTP

هي خدمة تعبئة الملفات عن بعد، فإنه بفضل هذه الشبكة يمكن جلب الملفات و تحويلها عبر الشبكة العالمية، و قد تكون هذه الملفات عبارة عن تقارير أو بحوث أو برامج، و بالتالي فهذه الخدمة تعتبر وسيلة التبادل السريع، و يستعان بها في خدمة تحديث مواقع الانترنت(La mise a jour des sites web)[102].

خامساً: خدمة منبر التحاور " NEWS GROUPS"

و هي خدمة تسمح بتبادل المعلومات بين مجموعة المستعملين ذوي الإهتمام مشترك حول موضوع معين، و هي وسيلة اتصال مباشر بين الأفراد و المؤسسات.

كما سبق و أن بينا أن هذه الخدمات ورد النص عليها في مراسيم تنظيمية، و هذا يعني أن المشرع الجزائري وضع تنظيمات فيما يخص شبكة الانترنت .

المطلب الثاني:مهددات الأمن المعلوماتي

---

[99] – جاء هذا التعريف ضمن التعريفات التي جاءت في ملحق قائمة الخدمات ذات القيمة المضافة للمرسوم التنفيذي **رقم 01-123 المؤرخ في 09 ماي 2001، *يتعلق بنظام الإستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية، و على مختلف خدمات المواصلات السلكية و اللاسلكية*** ، جريدة رسمية عدد 27 سنة 38 بتاريخ 13 ماي 2001. ص.13.

[100] – المادة **3/02** من المرسوم السابق رقم 98-257.

[101] - د. إبراهيم بختي، مرجع سابق، ص 29.

[102] – د. إبراهيم بختي، المرجع نفسه، ص 28.

تواجه الأنظمة المعلوماتية بعض الأخطار والمشاكل المعاصرة التي تغزو أنظمة المعلومات وتساهم في تدميرها أو سرقة الخزين المعلوماتي المحفوظ في أجهزة الحاسوب أو قاعدة البيانات ومن أهم هذه المشاكل ما يأتي:

الفرع الأول: الفيروسات وأشباهها

تعتبر الفيروسات من أهم أسباب ارتكاب جرائم الحاسوب وأكثره ا إنتشارا في الوقت الحاضر وهي أنواع وفي تطور دائم ومستمر مع تطور وسائل الحماية الفنية.

وهي في الغالب تحدث إتلافا للبيانات والمعلومات الموجودة داخل النظام المعلوماتي أو بما يسمى "تدمير المعلومات" ومعظم الجرائم الأخرى التي سيتم توضيحها في الباب الأول من هذه الدراسة، ترتكب بعدة أساليب قريبة الشبه تتمثل في أربعة أنواع من الفيروسات هي، برامج الدودة، القنبلة المعلوماتية (المنطقية والزمنية)، الباب الخفي و برمجيات ويب التفاعلية وسنتعرض لكل نوع منها بالتوضيح الموجز على النحو التالي:

البند الأول: الفيروسات

وهي عبارة عن برامج خبيثة a malicious program تتسلل إلى البرمجيات بحيث تدخل إليها وتنسخ نفسها على برامج أخرى في الحاسب الآلي [103] أوهي عبارة عن برمجيات مشفرة للحاسب الآلي مثل أي برمجيات أخرى يتم تصميمها بهدف محدد وهو إحداث أكبر ضرر ممكن بأنظمة الحاسب الآلي، وتتميز بقدرتها على ربط نفسها بالبرامج الأخرى وإعادة إنشاء نفسها حتى تبدوا وكأنها تتكاثر وتتوالد ذاتيا[104]، بالإضافة إلى قدرتها على الانتشار من نظام إلى أخر، إما بواسطة قرص ممغنط أو عبر شبكة الاتصالات بحيث يمكنها أن تنتقل عبر الحدود من أي مكان إلى أخر في العالم[105].

وتسمى عادة باسم أول مكان تكتشف فيه أو باسم مصممها، أي إن الفيروس عبارة عن برنامج يتميز بثلاث خواص هي التضاعف، التخفي، إلحاق الأذى بالآخرين ويتمثل النشاط التدمير ي لها في أنها

---

[103]- **محمد أمين الشوابكة** ، جرائم الحاسوب و الأنترنت– الجريمة المعلوماتية، ط 4، دار الثقافة للنشر و التوزيع، عمان، الاردن، 2011، ص238

[104]– **أسامة بن غانم العبيدي**، الإتلاف المعلوماتي، مجلة دراسات المعلومات، عدد الرابع، يناير 2009، ص104.

[105]– **حسن طاهر داود** ، أمن شبكات المعلومات، مركز البحوث بمعهد الإدارة العامة بالمملكة العربية السعودية، الرياض، 2004، ص 166.

تقوم بمسح البيانات والمعلومات المخزنة على وسائط التخزين وإتلافها، لذا يطلق على هذه العملية اسم مسح البيانات وتحويلها إلى صفر[106].

وهناك اختلاف جوهري بين فيروسات الحاسب الآلي و فيروسات الإنترنت على الرغم من إتفاقهما من حيث التقنية، وذلك من حيث إمكانية الانتشار الواسع فهي كبيرة جدا في مجال الإنترنت ومقيدة بالصدفة بالنسبة لفيروسات الحاسب الآلي[107]، هذا من جهة ومن جهة أخرى نجد أن إمكانيات فيروس شبكة الإنترنت تفوق تلك المقررة لفيروس الحاسب الآلي.

فالأول طالما أن الشبكة تعمل فإرساله مستمر على النحو الموضوع له حتى ولو تم إغلاق أجهزة الحاسب الآلي أو الشبكات أو الخوادم، في حين أن النوع الثاني يكمن في الجهاز المصاب به ولا ينتقل إلى الجهاز الأخر إلا بالعدوى به عن طريق انتقال ملف أو برنامج ما من الجهاز المصاب إلى جهاز أخر أو عن طريق القرص المرن أو القرص الصلب أو القرص الممغنط، ومن أبرز الهجمات الفيروسية التي شهدها عالم الحاسبات والمعلومات هجوم الفيروس الباكستاني المعروف باسم المخ Brain واقتحامه لحوالي 350 ألف من حاسبات IBM والحاسبات المتوافقة معها[108].

و للفيروسات أنواع متعددة فهي تنقسم من حيث التكوين والأهداف إلى:

أ- فيروسات عامة العدوى: وهو ينتقل إلى أي برنامج أو ملف ويهدف إلى تعطيل نظام التشغيل بكامله.

ب- فيروسات محدودة العدوى: حيث تصيب نوع معين من النظم وتتميز عن سابقتها بأنها بطيئة الانتشار[109].

ج- فيروسات عامة الهدف: تمتاز بسهولة الإعداد واتساع القوة التدميرية لها وغالبية الفيروسات تندرج تحت هذا النوع ومن الأمثلة عليها فيروس مايكل انجلوا الذي ظهر في 1992/3/26[110].

---

[106]- د. **عمر محمد ابو بكر بن يونس** ، الجرائم الناشئة عن استخدام الانترنت، رسالة دكتوراه في القانون الجنائي، جامعة عين شمس، كلية الحقوق،2004، ص364_376.

[2]- **منير محمد الجنبيهي وممدوح محمد الجنبيهي**، مرجع سابق، ص69.

[3]- **منير محمد الجنبيهي وممدوح محمد الجنبيهي**، مرجع سابق، ص69.

[109]- **نادية أمين محمد على**، الفيروسات و طرق الوقاية منها كوسيلة لأمن المعلومات، المؤتمر الدولي لأمن المعلومات المنعقد بمحافظة مسقط بسلطنة عمان في الفترة من 18-2005/12/20، ص 5،6.

مشار اليه لدى:د. **على جعفر**، جرام تكنولوجيا المعلومات الحديثة، الواقعة على الأشخاص و الحكومة، ط1، منشورات زين الحقوقية، لبنان، 2013، ص 553.

د- فيروسات محدودة الهدف: تقوم بتغيير الهدف الأصلي من عمل البرنامج أو الملف التي تصيبه دون أن تصيبه بالعطل وهو يحتاج إلى مهارة عالية ومعرفة بالتطبيق المستهدف ومن الأمثلة عليه فيروس ماك ماج Mac Mag الذي ظهر عام 1988[111].

وتنقسم من حيث الأضرار التي تحدثها بأنظمة الحاسب الآلي إلى:

1. **الفيروسات التي تصيب الملفات التنفيذية** : يقصد بالملفات التنفيذية تلك الملفات التي تكون من نوع EXE، BAT COM، حيث أن تلك الملفات هي المسئولة عن تشغيل البرامج الموجودة على الحاسب وبالتالي فإن إصابة هذه الملفات يؤدي إلى تعطيل البرنامج بالكامل – خاصة النوع الأول والثاني[112].

أما النوع الثالث فيكاد يكون غير مستخدم في نظم التشغيل الحالية – وبرنامج الفيروس عندما يصيب هذه الملفات فإنه إما أن يقوم بحذف الجزء الأول من الملف التنفيذي وكتابة نفسه في هذا المكان، الأمر الذي يؤدي إلي توقف عمل الملف التنفيذي بشكل جزئي ويعرف هذا النوع من الفيروسات باسم فيروسات الكتابة الفوقية Over Writing viruses وإما أن يقوم برنامج الفيروس بنسخ نفسه في الجزء الأخير من الملف التنفيذي وبالتالي فإن الملف التنفيذي يظل يعمل بشكل طبيعي حتى ينشط الفيروس ويقوم بمهامه التخريبية، ويعرف هذا النوع من الفيروسات باسم فيروسات الكتابة غير الفوقية Non Over Writing Viruses[113] .

2. **فيروسات الكتابة المباشرة:** وهذا النوع من الفيروسات لا يقوم بنسخ نفسه في ملف عادي مثل النوع الأول، و إنما يقوم بكتابة نفسه مباشرة على ا لقرص صلب[114] في مكان محدد يسمي Boot Record Area وهذا المكان يحتوي على مجموعة من البيانات التي يقوم نظام التشغيل بكتابتها علي القرص الصلب والتي تسمي FAT أو بمعنى آخر فإن هذا النوع من الفيروسات عندما يصيب الحاسب فإنه يؤدي إلي عدم قدرة نظام التشغيل على التعامل مع الملفات بالرغم من أن هذه

---

[110]- **محمد أمين الشوابكة**، مرجع سابق، ص239.

[111]- **منير محمد الجنبيهي وممدوح محمد الجنبيهي**، مرجع سابق، ص70.

[112]- **عفيفي كامل عفيفي**، مرجع سابق، ص203.

[113] - **محمد سامي الشوا**، مرجع سابق، ص192.

[114]- د. **علي جعفر**، مرجع سابق، ص 554.

الملفات مازالت موجودة علي القرص الصلب ولم يتم حذفها ومن أشهر هذه الفيروسات فيروس تشرنوبل[115].

3. الفيروسات الصغيرة تعتبر ضمن أغلب الفيروسات الشائعة وتأثيرها ينصب على برامج معالجة النصوص حيث تقوم بإدخال كلمات وعبارات وجمل غير مرغوب فيها وغير متوقعة ، وهو غالبا ما يقوم بتعديل الأمر "حفظ" ليشغل نفسه بعد ذلك تلقائيا ، وقد تصيب أيضا الملفات الخاص بمستندات النصوص النشطة HTML المحتوية على نصوص جافا وأنواع أخرى من الرموز التنفيذية، مما يؤدي إلى انتشارها، ومن أمثلها فيروس ميليسا الذي ظهر 1999 والذي انتشر عبر البريد الإلكتروني out lock[116].

ومنذ عام 2004 حدث تطور كبير في طريقة تصميم الفيروسات خاصة فيروسات الإنترنت التي غالبا ما تعتمد على شبكة الإنترنت حيث أصبحت لا تحتاج إلى الرسائل الإلكترونية لكي تصل إلى ضحاياها من الحاسبات الشخصية والخادمة كفيروس خطوط الإنترنت بلا ستر وبلسيا اللذان ظهرا في أواخر عام 2003 وانتشرا على خطوط الإنترنت حول العالم ، فهما وبمجرد أن تشعر بأن أحد الحاسبات قد اتصل بالإنترنت تقوم على الفور بالانتقال له وإصابته [117]، وهناك أيضا فيروسات مواقع الإنترنت التي تصيب الحاسب الآلي بمجرد أن يقوم الزائر بالدخول إلى الموقع الذي خبأ الفيروس داخل صفحاته، وهذه النوعية غالبا ما تكون موجودة وبكثرة على المواقع الإباحية لكونها تجتذب الكثير من مستخدمي الشبكة المعلوماتية.

4- **حصان طروادة** Trojan Horse: هي عبارة عن برامج فيروسية لديها القدرة على الاختفاء داخل برامج أخرى أصلية للمستخدم بحيث عندما تعمل البرامج الأصلية ينشط الفيروس وينتشر ليبدأ أعماله التخريبية، و هو يختلف عن الفيروس في أنه لا يتكاثر ولا يلتصق بالملفات و إنما هو برنامج مستقل بذاته يحمل في طياته توقيت و أسلوب استيقاظه[118]، وهو يؤدي إلى تعديل هذه البرامج وتزوير المعلومات ومحو بعضها، وقد يصل الأمر إلى تدمير النظام بأكمله و هذه البرامج

---

[115]- **أحمد خليفة الملط**، الجرائم المعلوماتية، دار الفكر الجامعي، مصر، 2004 ، ص 649.

[116]- **منير محمد الجنبيهي وممدوح محمد الجنبيهي**، مرجع سابق، ص74.

[117]- **محمد العريان**، مرجع سابق، ص88-89.

[118]- **علي جعفر**، مرجع سابق، ص 555.

هي في الأساس من الناحية التقنية برمجيات اختراق وتجسس [119] تهدف إلى جمع المعلومات والبيانات كاسم المستخدم وكلمات السر الخاصة به وغيرها ومن ثم إرسالها إلى صاحب البرنامج أو مصممه[120].

وغالبا ما يتم ذلك والمستخدم الضحية متصل بشبكة الإنترنت، حيث توجد بعض المواقع التي تحمل حصان طروادة في ملفات خاصة تسم ى الكوكيز COOKIES FILE التي تلحق مستخدم الشبكة أثناء تصفح الشبكة، فيلحق الأذى بالجهاز وبخصوصية المستخدم.

ولا توجد نوعية واحدة لحصان طروادة إذ يندرج تحته العديد من الأنواع من بينها برامج قامت بكتابتها بعض شركات البرمجيات الكبرى، وعندما يقوم أحد المستفيدين باستخدام أحد منتجات هذه الشركات تقوم هذه البرامج بعمل حصر شامل لكل مكونات النظام المادية والمنطقية الخاص بالمستفيد وعند اتصال المستفيد بشبكة الإنترنت يتم إرسال هذه المعلومات إلى تلك الشركات التي تستخدمها في عملياتها التسويقية ومن أبرز هذه الشركات شركة مايكروسوفت[121].

وهناك قصة نشرتها إحدى الصحف العربية عن أجهزة اتصال متطورة للغاية حصلت عليها إحدى الدول العربية من دولة عظمى على سبيل الهدية تبين بعد فحصها أنها تحتوى على حصان طروادة أعد خصيصا لجمع معلومات عن استخدام الجهاز وعن التردد التي استخدمت عليه[122].

البند الثاني: برامج الدودة Worm Software

هي عبارة عن برامج تقوم باستغلال أية فجوة في أنظمة التشغيل لكي تنتقل من حاسب لآخر، أومن شبكة لأخرى عبر الوصلات التي تربط بينها وذلك دون حاجة إلى تدخل إنساني لتنشيطها وهذا هو الاختلاف بينها وبين حصان طروادة الذي دائما ما يعتمد على التدخل الإنساني لمباشرة نشاطه كما سنرى لاحقا، كذلك هي لا تلتصق بأنظمة التشغيل في أجهزة الحاسب الآلي التي تصيبها مثلما تفعل الفيروسات كما رأينا وتتكاثر هذه البرامج أثناء عملية انتقالها بإنتاج نسخ منها ودونما الحاجة إلى برامج

---

[119]– **جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات،ط1**، دار البادية للنشر،عمان– الأردن، 2007، ص 198، 199.

[120]– **أحمد خليفة الملط**، مرجع سابق، ص651.

[121]- شركة دولية تعمل في مجال تقنية الحاسوب مقرها في ضاحية ريدمونت، سياتل، واشنطن، و.م.الأمريكية.

[122]– **محمد علي العريان**، مرجع سابق، ص97.

وسيطة تساعدها على التكاثر، وتعمل على تقليل كفاءة الشبكة أو التخريب الفعلي للملفات والبرامج ونظم التشغيل[123].

ولقد ظهرت هذه النوعية من البرامج الضارة لأول مرة في عام 1988 على يد الطالب الأمريكي Roper Tappan Morris وهي ما عرفت بدودة موريس Morris التي تسببت في تدمير الآلاف من شبكات الحاسب الآلي المنتشرة في الولايات المتحدة بالإضافة إلى إعاقة طريق ومسلك الشبكات، ناهيك عن الخسائر المادية الكبيرة في مواجهة هذه الدودة وقد أدين موريس بإنتهاك قانون الإحتيال وإساءة إستخدام الكمبيوتر، وحكم عليه بالحبس لمدة ثلاثة سنوات، وبالعمل 400 ساعة في الخدمة الإجتماعية وغرامة مالية قدرها 10.500 دولار بالإضافة إلى تكاليف المراقبة[124].

كما تم إكتشاف حالة من برامج الدودة أطلق عليها مصطلح "البرامج الدودية ضد القتلة مستخدمي الدرة ورمز إليها برمز "wank" حيث غزت تلك البرامج مرتين خلال عام 1989 شبكة علوم الأرض والفضاء بالولايات المتحدة الأمريكية، كنوع من أنواع الإحتجاج على إطلاق مكوك فضاء يحمل مجسما فضائيا مغطى ببودرة نووية[125].

البند الثالث: القنبلة المعلوماتية Bomb

هي نوع من البرامج الخبيثة صغيرة الحجم يتم إدخالها بطرق غير مشروعة وخفية مع برامج أخرى، فهي ليست ملفا متكاملا وإنما شفرة تنضم إلى مجموعة ملفات البرامج عن طريق تقسيمها إلى أجزاء مبعثرة هنا وهناك حتى لا يمكن التعرف عليها بحيث تتجمع فيما بينها بحسب الأمر المعطى لها في زمن معين أو حدوث واقعة معينة، فهي مصممة لتبقى ساكنة وغير فعالة إلا في الزمن المحدد أو الواقعة المحددة لذا يتعذر اكتشافها لمدة قد تصل لأشهر وأعوام، ويؤدي اجتماعها هذا إلى انعدام القدرة على تشغيل البرنامج عبر جهاز الحاسب الآلي وتستخدم هذه البرامج لإتلاف المعلومات والبيانات وتغيير برامج ومعلومات النظام[126] .

كما قد تستخدم كبرامج لحماية الملكية الفكرية من القرصنة وخاصة تلك التي تحدث عبر شبكة الإنترنت، فالذي يملك حقوق النسخ قد يجيز للغير نسخ مصنفه عبر شبكة الإنترنت إلا أن هذه الإجازة

---

[123]– **أحمد خليفة الملط**، مرجع سابق، ص651.

[124]– **أحمد خليفة الملط**، نفس المرجع، ص652.

[125]– **أسامة بن غانم العبيدي**، مرجع سابق، ص108.

[126]– **محمد أمين الشوابكة**، مرجع سايق، ص240.

قد تكون لفترة محددة بفترة زمنية قصيرة تختفي بعدها البرمجية أو الملف المنسوخ بسبب القنبلة الموقوتة[127].

وتعرف القنبلة المعلوماتية بمصطلح الشفرة الموقوتة و أكثر ما تبرز في البرامج المؤقتة التي تشتمل عليها الحملات الإعلانية كما هو الشأن في المجلات التي يوزع معها بعض الأسطوانات هدية و التي تحتوى على بعض البرامج ، وهناك أيضا بعض المواقع على شبكة الإنترنت التي تشتمل على بعضا من هذه البرامج كذلك من الممكن أن تظهر في البرامج المدخرة التي لا يفقد مالكها عليها حقوق الملكية فهو يقوم بتأجيرها فقط ، فإذا توقف المستأجر عن دفع القيمة الايجارية المتفق عليها عدا ذلك إخلالا بالعقد المبرم بين المالك والمستأجر مما يدفع بالمالك إلى أن يرسل له قنبلة موقوتة أو أن تكون القنبلة أصلا موجودة في البرنامج المستأجر فلا يرسل المالك ما يوقف انفجارها وهذا النوع من البرامج الضارة ينقسم إلى قسمين هما :

1- **القنبلة المنطقية** Logic Bomb: وهذا النوع ينشط بمجرد حدوث واقعة معينة مثل بدأ التشغيل أو عند إنجاز أمر معين في الحاسب الآلي [128] أو عند بدأ تشغيل برنامج معين ومن الأمثلة على ذلك زرع القنبلة المنطقية لتعمل لدى إضافة سجل موظف بحيث تنفجر لتمحو سجلات الموظفين الموجودة أصلا في المنشأة مثلما حصل في ولاية لوس أنجلس الأمريكية [129] عندما تمكن أحد الأشخاص العاملين في إدارة المياه والطاقة من وضع قنبلة منطقية في نظام الحاسب الآلي الخاص بها ، مما أدى إلى تخريب النظام عدة مرات.

2. **القنبلة الزمنية** Time Bomb: وهذا البرنامج ينشط في تاريخ معين محدد بالذات فهو يثير حدثا في لحظة زمنية محددة بالساعة واليوم والسنة والوقت اللازم ومن الأمثلة الواقعية قيام شخص يعمل بوظيفة محاسب خبير في نظم المعلومات بوضع قنبلة زمنية في شبكة المعلومات الخاصة بالمنشأة بدافع الانتقام ، حيث انفجرت بعد مضي ستة أشهر من رحيله عن المنشأة[130].

وترتب على ذلك إتلاف كل البيانات المتعلقة بها، ومن الأمثلة الواقعية التي استخدمت القنابل الزمنية ما قام به أحد المتخصصين في برمجيات الحاسبات الآلية في بريطانيا من وضع قنبلة

127- **أحمد خليفة الملط**، مرجع نفسه، ص653.

128- **محمد أمين الشوابكة**، مرجع سابق، ص240.

129- **أسامة بن غانم العبيدي**، مرجع سابق، ص108.

130- **أسامة بن غانم العبيدي**، نفس المرجع، ص109.

زمنية في نظام إحدى الحاسبات الآلية أدت إلى محو أكثر من مائتي برنامج، إضافة إلى محو النسخ الأصلية عند تشغيلها لإنتقال آثار القنبلة الزمنية إليها، وقد تم القبض على المجرم وحكم القضاء البريطاني بالسجن لمدة ثلاثة سنوات.

وفي ألمانيا قام أحد مبرمجي الحاسب الآلي بزرع برنامج قنبلة زمنية في نظام المعلومات الخاص بالشركة التي يعمل بها وقام ببرمجة القنبلة الزمنية بعد عامين من تاريخ فصله من الشركة وقد ترتب على ذلك إتلاف نظام معلومات الشركة في الوقت الذي قام بتحديده، مما أدى إلى إتلاف البيانات والمعلومات المخزنة في شبكة معلومات الشركة

البند الرابع:الباب الخفي Back Door

نشأت هذه البرامج في الأصل كآلية يستخدمها المبرمجون لتضمن لهم مدخلا خاصا للأنظمة التي يقومون ببرمجتها، خاصة عندما يتسبب خطأ برمجي في التوقف التام للنظام، وفي بعض الأحيان يقومون بذلك لأسباب خبيثة أو على الأقل مشبوهة.

ومع الوقت أصبحت تستخدم من قبل الهاكر في الولوج الأنظمة المعلوماتية وإختراقها، وأنوع شفرة الباب الخفي كثيرة ومتعددة، ولكنها تجتمع في كونها تعطي ولوجا خاصا يتجاوز الإجراءات الروتينية، ورغم أن البعض يخلط بينها وبين حصان طروادة إلا أنه يمكن التفريق بينهما من حيث أن الأخير يوحي للمستخدم بأنه برنامج ذو منفعة، في حين أن برامج الباب الخفي تقوم بعملها في الخفاء[131].

البند الخامس: برمجيات ويب التفاعلية

قد يسيء بعض المبرمجين توظيف بعض البرمجيات المخصصة لمواقع الإنترنت التفاعلية والتي تكون عبارة عن ملفات تنفيذية يتم تحميلها وتشغيلها على جهاز المستخدم فور اتصاله بالموقع الموجودة عليه، ومن هذه البرمجيات برمجيات جافا وأكتف أكس، ورغم أن هاتين الوسيلتين صممتا بهدف تسهيل تفاعل زوار مواقع الإنترنت إلا أنه متى ما تم برمجتها عن قصد بأعمال أخرى يمكنها أن تلحق بأجهزتهم الكثير من الأضرار[132].

الفرع الثاني: أشكال الجرائم التقنية كمهددات الأمن المعلوماتي

---

[131]- د. **أيمن عبد الله فكري**، مرجع سابق، ص154-157.

[132]- د. **نائلة عادل محمد فريد قورة**، جرائم الحاسب الآلي الاقتصادية،الطبعة الأولى، منشورات حلبي الحقوقية، بيروت، لبنان، 2005، ص 106 وما بعدها.

تتنوع أشكال تهديد الأمن المعلوماتي و قواعده و التي تترتب عليها إثر سلبية نتيجة الاعتداء على حقوق الغير و على المعلومات السرية و الأمنية للأفراد و الشركات و الدول واستغلالها في أعمال الإساءة.

و أن ازدياد عمليات الاعتداء، و ابتكار التقنيات التي تسهم في زياد قدرات المخترقين والمتسللين إلى الشبكات و النظم المعلوماتية، مما يحتم اتخاذ سبل فعالة لمواجهة مهددات ومخاطر الأمن المعلوماتي من الناحية القانونية و الإستراتيجية و الفنية ، و قبل استعراض هذه السبل سيتم تخصيص هذا العنصر لتوضيح بعض أشكال التهديدات المحتملة ضد قواعد الأمن المعلوماتي من خلال الجرائم المعلوماتية.

و الجريمة المعلوماتية قد تقع على الحاسب الآلي ذاته و ما يتصل به من ملحقات، و قد تقع على معلومات و أموال الغير بإستخدام الحاسب كوسيلة لذلك.

غير أنه يجب الاشارة بخصوص ما سبق ذكره أنه لا يمكن الفصل بين أجهزة الحاسب الآلي وملحقاته و شبكات الانترنت، لانه لا يمكن ارتكاب جريمة على الانترنت إلا باستخدام الحاسب الآلي، و تعرف الجرائم التي تستخدم هذه التقنيات الالكترونية بأنها ذلك النوع من الجرائم التي تتطلب الماما خاصا بتقنيات و برمجيات الحاسب الآلي و نظمه المعلوماتية، و يرتكب المقترف لهذا النوع من الإجرام سلوكا يخالف قواعد و أصول استخدام تلك النظم و البرامج المعلوماتية بإختراق أو تدمير أو سرقة معلومات مختزنة على تلك الأجهزة أو المواقع الالكترونية أو تزييفها أو تزويرها أو استغلالها استغلالا منافي لقواعد القانون[133] مما يعرض مرتكبيها للمساءلة القانونية و مقاضاتهم،

فضلا على أنه ليس هناك تعريف أو مفهوم تشريعي جامع للجريمة المعلوماتية أو جرائم الإلكترونية[134]،و من أشكال الجرائم ما يأتي:

البند الأول: قرصنة المعلومات والتجسس المعلوماتي

قد يسمع الكثير عن ما يسمى بالهاكرز أو مخترقي الأجهزة، ونتساءل كيف يتم ذلك و هل الأمر بسيط أو يحتاج إلى ذكاء فائق للمجرم ولدراسة فنية؟، في حقيقة الأمر إنه مع إنتشار برامج القرصنة ووجودها في الكثير من المواقع أصبح من الممكن إختراق أي جهاز أو نظام معلوماتي وبدون عناء فور إنزال إحدى البرامج، وخاصة مع وجود ثغرات في هته الأجهزة أو الأنظمة.

---

[133]- **راشد محمد المري**، الجرائم الإلكترونية في ظل الفكر الجنائي المعاصر– دراسة تحليلية تأصيلية مقارنة– رسالة دكتوراه في القانون الجنائي، كلية الحقوق، جامعة القاهرة، 2013، ص 14

[134] - **Olivier ITEANU**, Tous Cybercriminels, La fin d'Internet ; Jacques-Marie Laffont Editeur, Paris, 2004, P25.

و من أثار تلك التهديدات التعرض للتهديدات التالية

أولا: التعرض للسرقة و الاحتيال عن طريق تغيير المعلومات التي يتم إدخالها في النظام أو تغيير المخرجات التي تخرج منه

ثانيا: التجسس الصناعي عن طريق تنزيل الأسرار الصناعية من كمبيوتر إلى إحدى الشركات و إرسالها بالبريد الإلكتروني مباشرة إلى منافستها[135].

البند الثاني: أخطار تهدد خصوصية المعلومات وإنتهاك السرية المعلوماتية

توفر تقنية المعلومات الجديدة إمكانية خزن أو حفظ وإسترجاع وتحليل كميات هائلة من البيانات الشخصية التي يتم تجميعها من قبل المؤسسات والدوائر والوكالات الحكومية، ومن قبل الشركات الخاصة، وأكثر من هذا فإنه يمكن خزن وحفظ المعلومات والبيانات الشخصية في قاعدة مؤتمنة هي قاعدة البيانات، ويمكن نقلها عبر مختلف مناطق البلد في ثوان معدودة وبتكاليف منخفضة نسبيا[136] إن هذا يبين بوضوح كيفية أو إمكانية تهديد الخصوصية.

وتتزايد مخاطر التقنيات الحديثة على حماية الخصوصية ، كتقنيات رقابة (كاميرات) الفيديو، وبطاقات الهوية والتعريف الالكترونية ، وقواعد البيانات الشخصية، ووسائل اعتراض ورقابة البريد والاتصالات ، ورقابة بيئة العمل وغيرها.

المبحث الثالث:

الحماية الفنية لقواعد الأمن المعلوماتي

إن التطورات الحاصلة في مجال إعداد برامج وتقنيات الحماية من الأخطار والمشاكل التي تهدد الأنظمة المعلوماتية، تعتبر من العمليات المعقدة والصعبة التي تتطلب الكثير من الجهد والوقت والموارد المالية، ومن تقنيات الحماية المعلوماتية.

قبل التحدث عن الجرائم المعلوماتية والأساليب الجرمية الواقعة على المعلومات والأنظمة المعلوماتية، لابد من وقاية فنية وإجراءات تقنية للمحافظة على سلامتها من أي اعتداء أو اختراق أو تلاعب وتعديل أو اعتراض غير مشروع.

---

[135]- **راشد محمد المري**، نفس المرجع، ص 49.

[136]– م. **يونس عرب**، الخصوصية و حماية البيانات، بحث منشور على الانترنت، ص 15

وكذلك حتى تتحقق أهداف السلامة المعلوماتية فيما يتعلق بالسرية والموثوقية وكذا التكاملية وسلامة المحتوى كما تم توضيحه، لكن ما يمكن ذكره انه لا يمكن حصر أو توقيف المخاطر الأمنية والسيطرة على الجرائم المعلوماتية بصفة دقيقة ولعدة أسباب منها أن الانترنت حديثة الانتشار، والكل يعلم انه إذا حضر الانترنت قلت نسبة الأمن مهما كان الجهاز المتصل به.

ونظرا للتطور التكنولوجي المتجدد والمستمر فان المخاطر كذلك في استمرار، ولا تقف عند زمن معين، أو على نمط محدد فالخير والشر في صراع دائم لم يتوقف منذ القدم[137].

وذلك لأنه كلما تم اكتشاف وسيلة أمنية لحماية المعلومات والأنظمة المعلوماتية، إلا وجدت ثغرة[138] يمكن النفاذ منها واختراق تلك الأنظمة والحصول على المعلومات، فمهما اخترع الإنسان من وسائل حماية فهو ليس بكامل، وبالتالي مهما تطورت التقنيات إلا وجدا ما يخترق تلك التقنيات.

إلا أنه لا يمنع من أخذ بعض الاحتياطات والتدابير الأمنية على الأقل للمحافظة على المعلومات والأنظمة المعلوماتية، ومن بين تلك الأساليب ما سيتم توضيحه من خلال العناصر الآتية:

المطلب الأول: وسائل الأمن المعلوماتي

وسائل امن المعلومات والأنظمة المعلوماتية عبارة عن آليات وإجراءات وأدوات ومنتجات تستخدم للوقاية والتقليل من مخاطر المعلوماتية والتهديدات التي تتعرض لها الأنظمة المعلوماتية.

و يتم الحفاظ على أمن المعلومات بإتخاد التدابير و الإحتياطات و كافة الإجراءات الضرورية الممكنة، عن طريق الإدارات و بمشاركة كافة القطاعات لمنع وقوع الجريمة المعلوماتية، و لا شك مختلف وسائل الحماية التقنية و حتى القانونية تهدف لحماية و تأمين الحماية لعناصر النظام الأمني للمعلومات[139].

ولوسائل الأمن أصناف متعددة سواء من حيث الطبيعة أو الغرض من اجل فرض الحماية وهي كالآتي:

الفرع الأول: وسائل الأمن المتعلقة بالدخول إلى الشبكة

137– د. **محمد محمود المكاوي** ، الجوانب الأخلاقية والاجتماعية و المهنية للحماية من الجرائم المعلوماتية، (جرائم الكمبيوتر و الانترنت)ط 1، المكتبة العصرية للنشر و التوزيع، مصر، 2010، ص 250.

138– يقصد **بالثغرة** : المنفذ أو الخلل الفني الذي من خلاله ينفد إلى النظام المعلوماتي

139– **فهد عبد الله العبيد العازمي** ، مرجع سابق، ص 33./**عمر ابوبكر بن يونس** ، امن المعلومات، مقال منشور على الموقع www.arablaw.org

هي الوسائل التي تساعد في التأكد من أن الشبكة ومصادرها استخدمت بطريقة مشروعة من خلال تعين الوسائل التي تعتمد على تحديد حقوق المستخدمين، أو الإجراءات والأدوات والوسائل التي تتيح التحكم بمشروعية استخدام الشبكة[140].

الفرع الثاني: الوسائل التي تهدف إلى منع إفشاء المعلومات لغير المخول لهم

وهذه الوسائل الهدف من ورائها الحفاظ على سرية المعلومات وهي تشمل:

- تشفير المعطيات والملفات
- إجراءات حماية نسخ الحفظ الاحتياطية
- الحماية المادية للأجهزة ومكونات الشبكة

الفرع الثالث: الوسائل الهادفة لحماية التكاملية و سلامة المحتوى

هي وسائل الهدف من ورائها ضمان عدم تغير و تعديل محتوى المعطيات من قبل أشخاص أو جهات غير مخول لهم بذلك و هي تشمل التقنيات التالية:

- تقنيات الترميز
- التوقيعات الالكترونية وأحسنها التوقيع الرقمي أو البصمة الرقمية التي تعتمد على تقنيات التشفير
- وضع برمجيات تحري الفيروسات وغيرها[141].

الفرع الرابع: وسائل الأمن المتعلقة بالتعريف بالشخص المستخدم وتوثيق الاستخدام والمشروعية

هي الوسائل التي تهدف إلى ضمان استخدام النظام أو الشبكة من قبل الشخص المخول بذلك وهي تشمل الوسائل التالية:

- كلمات السر بأنواعها
- البطاقات الذكية المستخدمة للتعريف
- وسائل التعريف البيولوجية التي تعتمد على سمات ذاتية معينة في شخص المستخدم متصلة ببنائه البيولوجي
- المفاتيح المشفرة وتضم ما يعرف بالأقفال الالكترونية التي تحدد مناطق النفاذ[142].

---

[140]– د.**محمد محمود المكاوي**، مرجع سابق، 258.

[141]–د.**أيمن عبد الله فكري**، مرجع سابق، ص 161.

[142]– د.**أيمن عبد الله فكري**، المرجع نفسه، ص 161.

الفرع الخامس: الوسائل والأدوات الفنية لتوفير أمن المعلومات والاتصالات

من بينها وعلى سبيل المثال ما يلي:

- استخدام تكنولوجيا الفخ الايجابي وهو فلتر يقوم بتصعيد التداخل في القنوات ويرفض دخول غير المشتركين إلى تلك القناة
- تطبيق نظم إدارة وامن المعلومات والاتصالات
- استخدام خطوط تليفونات واتصالات مأمونة
- استخدام تكنولوجيا التشفير والترميز
- استخدام تكنولوجيا SSI وهي تكنولوجيا تتضمن بروتوكولا امنيا للانترنت فيكون الدخول إلى النظام لمن هم مرخص لهم بذلك.
- استخدام تكنولوجيا التوقيع الرقمي في مهر الرسالة الالكترونية، لتحقق من نسب المستند الالكتروني أو الرسالة الالكترونية لصاحبها أو مرسلها[143].
- استخدام وسائل التأكد من صحة وسلامة المراسلات الالكترونية.
- استخدام البرامج المضادة للفيروسات وتحديثها بانتظام.
- استخدام تكنولوجيا الجدران النارية، لحماية نظم الحاسبات و المعلومات.
- استخدام تكنولوجيا الكشف عن وسائل التنصت في النظم والشبكات
- استخدام الـ COOKIES FILE لإزاحة الوسائل التي تستخدم في الدخول غير المشروع للنظام للتلصص عليه[144].

وإلى غير ذلك من الوسائل الفنية و التقنية الكثيرة التي يمكن استخدامها للوقاية أو على الأقل للتقليل من اختراق الأنظمة المعلوماتية و مكافحة الأفعال إجرامية.

المطلب الثاني: التشفير كوسيلة تقنية لحماية قواعد الأمن المعلوماتي

يعد التشفير من أهم تقنيات الحماية وسلامة الأنظمة المعلوماتية وكذا المعلومات المخزنة والمتداولة.

الفرع الأول: تعريف التشفير

---

[143]– **محمد محمود المكاوي**، مرجع سابق، ص 259.

[144]– د.**أيمن عبد الله فكري**، مرجع سابق، ص 162.

إن فكرة نظام التشفير هي إخفاء المعلومات الموثوقة بطريقة معينة بحيث يكون معناها غير مفهوم للشخص غير المخول[145].

وتتم الحماية الفنية بواسطة التشفير من خلال تعمية المعلومات الالكترونية، وبحيث لا يمكن إعادة ترتيبها وتنظيمها إلا باستخدام مفتاح معين لفك الشيفرة [146]، وتكون المعلومات المخلوطة غير مفهومة لمن لا يملك هذا المفتاح.

أو هو عبارة عن عملية تعمية وحجب المعلومات، أو تغير صيغة الكتابة من شكلها المفهوم إلى شكل غير مفهوم من قبل الناس عمامة، وتكون مفهومة من شخص محدد فقط وهو المرسل إليه[147].

فهو برنامج أو منهج لخلط البيانات من خلال استخدام لوغاريتمات أو خوارزميات بحيث لا يمكن قراءتها.

وهذه البرمجية تتولى فرض شفرة تحمي في الظاهر المعلومات، بحيث تمنع الغير ممن ليس لهم الحق في التعامل مع الموقع من الدخول إليه والحصول على خدماته، ما لم يصرح له المالك بذلك، فهو علم تحويل الكتابة إلى أسرار[148].

ويكون تصريح المالك للغير بالاطلاع على المعلومات المشفرة باستخدام مفتاح فك التشفير وهو عبارة عن منتج أو آلة أو مركب تم تصميمه لكي يقوم بفك شفرة الدخول .

كما ورد تعريفه في المادة 29 من القانون الفرنسي رقم 2004-575 المتعلق الثقة في الاقتصاد الرقمي[149].

ويحظى التشفير وتقنياته في الوقت الحالي باهتمام استثنائي خاصة في ميدان أمن المعلومات والسلامة المعلوماتية، ويرجع ذلك إلى كون الحماية التي يوفرها التشفير تمثل الوسيلة الأكثر أهمية

---

[145]– د. **عوض حاج علي أحمد ود. عبد الأمير خلف الحسين/** أمنية المعلومات وتقنيات التشفير، مرجع سابق، ص34.

[146]- د. **عبد الرحمن شعبان عطيات**، مرجع سابق، ص 130.

[147]– د. **محمد محمود المكاوي**، مرجع سابق، ص 271 وما بعدها.

[148]– د. **أبو بكر عمر بن يونس**، مرجع سابق، ص 379، وكذا د. محمد محمود المكاوي، مرجع سابق، ص271.

[149]- **Art 29** de **la loi n°2004-575** du 21 juin 2004 **pour la confiance dans l'économie numérique** définit les moyens de cryptologie comme « tout matériel ou logiciel conçu ou modifie pour transformer des données ,qu'il s'agisse d'information ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète » trouver sur le site ; www.legifrance.gouv.fr

لتحقيق وظائف وأهداف السلامة المعلوماتية المتمثلة في السرية والموثوقية والتكاملية وضمان عدم التعديل.

وبذلك فهو يحافظ على ما يمكن أن تتعرض له المعلومة في مختلف مراحلها بدايتا من بثها من مرسلها وتناقلها إلى غاية وصولها كما هي إلى المرسل إليه دون تعديل أو تغيير في محتواها، بل قد يمنع التشفير حتى الوصول أو الدخول إلى النظام معلوماتي أو موقع معين ما لم يكن صاحب النظام أو مخول له بالدخول إليه.

أصبح التشفير يدخل في مختلف الوسائل التقنية [150] المنصبة على تحقيق حماية عناصر السلامة والأمن المعلوماتي.

وبذلك يعد التشفير وبوجه عام الإستراتيجية الشمولية لتحقيق أهداف الأمن والسلامة المعلوماتية.

الفرع الثاني: طرق التشفير

هناك منظومتين للتشفير:

البند الأول: منظومة التشفير المتناسق أو التماثلي

وتسمى بالتشفير السيميتري Symétrique وهذه الطريقة تعتمد على مفتاح سري واحد متبادل[151]، ويعني ذلك أن مرسل الرسالة الإلكترونية ومستقبلها يستخدمان نفس المفتاح للتشفير ولفك رموز الرسالة[152]، ولكن نظرا لضرورة إطلاع الطرف المتعاقد مع صاحب التوقيع على الرقم السري وإلى كل من يتعاقد معه، وما قد يؤدي إليه ذلك من فقد الأمن والسرية مما أدى إلى ظهور منظومة أدق وأوثق.

البند الثاني: منظومة التشفير اللامتناسق أو اللاتماثلي (Asymétrique)

---

[150]- و هذا ما تبناه المشرع الجزائري من خلال التنظيمات التقنية لبعض تطبيقات البطاقات الالكترونية من خلال **المرسوم تنفيذي** رقم 116- 10 المؤرخ 18 أبريل 2010يحدد ***مضمون البطاقة الإلكترونية للمؤمن له اجتماعيا و المفاتيح الإلكترونية لهياكل العلاج لمهني الصحة وشروط تسليمها واستعمالها وتجديده*** ، ج.ر عدد 26 بتاريخ 21 أبريل 2010.

و كذا **قرار** مؤرّخ في 26 ديسمبر سنة 2011 ***يحدد المواصفات التقنية لجواز السفر الوطني البيومتري الإلكتروني،*** ج.ر العدد الأول بتاريخ 14 يناير 2012.

[151]- م.**عمر حسن المومني**، التوقيع الإلكتروني وقانون التجارة الإلكترونية، ط1، دار وائل للنشر، عمان- الأردن، 2005، ص 55.

[152]- **د.عبد الفتاح بيومي حجازي** ، النظام القانوني لحماية التجارة الإلكترونية، الكتاب الأول ، ط1، دار الفكر الجامعي، الاسكندرية- مصر ، 2002، ص197.

هذا النوع من التشفير تم اكتشافه في الولايات الأمريكية المتحدة عام 1978 من طرف ثلاث علماء رياضيات[153]، ولقد جاء هذا النظام حلا لمشكلة التوزيع غير الأمن للمفاتيح في مجال التشفير المتناظر، خصوصا عند استخدام مفتاح واحد.

يستخدم التشفير اللامتناظر مفتاحين مرتبطين بعلاقة رياضية معقدة عند بنائهما [154]، ويدعى هذين المفتاحين بالمفتاح العام (Public Key) والمفتاح الخاص (Private Key).

فالمفتاح الخاص يكون معروفا لدى شخص واحد أوجهة واحدة فقط، وتحت السيطرة والسلطة المطلقة لصاحب التوقيع وهو المرسل [155]، الذي يتعين عليه توفير شروط السلامة لحماية مفتاحه الخاص من مخاطر استعماله من طرف الغير، وهذا المفتاح يستعمل لتشفير المحررات وتوقيعها[156].

في حين المفتاح العمومي كما يدل عليه اسمه، هو مفتاح معروف عادة على نطاق أوسع [157]، ويستخدم من قبل شخص موثوق به للتثبت من صحة التوقيع الإلكتروني، ويمكن معرفته لأكثر من جهة في حال استدعت الظروف ذلك ولا يقصد من ورائه بقائه سرا[158].

وبالرغم من أن كلا المفتاحين مرتبطين ببعضهما رياضيا، فإنه في حال تم تصميم نظام التشفير اللاتماثلي وتم تطبيقه بشكل أمن، فإنه حسابيا لا يمكن التوصل إلى معرفة المفتاح الخاص من خلال معرفة المفتاح العام.

الفرع الثالث: جدران الحماية

جدران الحماية تعد أجهزة و برامج تعزل الشبكة المحلية عن الشبكات الأخرى بصفة جزئية أو كلية، فهي عبارة عن أجهزة حاسب آلي تقع بين الشبكة المحلية و الشبكة العالمية كبوابة لحماية معلومات الشبكة المحلية و التحكم في الدخول إليها[159].

---

[153]– **عمر حسن المومني**، مرجع سابق، ص56.

[154]– د. **عبد الفتاح بيومي حجازي**، النظام القانوني لحماية التجارة الإلكترونية، الكتاب الأول، مرجع سابق، ص 211.

[155]– د. **نجوى أبو هبة**، التوقيع الالكتروني تعريفه و مدى حجيته في الإثبات، دار النهضة العربية، سوريا، بدون تاريخ، ص 53.

[156]– **المادة 12/01** من ***اللائحة التنفيذية لقانون التوقيع المصري*** الصادرة بقرار من وزارة الإتصالات و تكنولوجيا المعلومات، رقم 109 لسنة 2005، الوقائع المصرية، العدد 115 بتاريخ 25 ماي 2005 .

[157] – **المادة 11/01** من **اللائحة التنفيذية لقانون التوقيع المصري** السابقة، تعرف المفتاح الشفري العام بأنه:" أداة إلكترونية متاحة للكافة، تنشأ بواسطة عملية حسابية خاصة، وتستخدم في التحقق من شخصية الموقع على المحرر الإلكتروني، والتأكد من صحة وسلامة محتوى المحرر الإلكتروني الأصلي".

[158] – د. **عبد الفتاح بيومي حجازي**، النظام القانوني لحماية التجارة الإلكترونية، الكتاب الأول، مرجع سابق، ص 197.

و هي تعد بمثابة الدرع الأول للتحكم في دخول المستخدم من داخل أو خارج المنشأة بدون أن يكون مصرحا له بذلك[160]، مع منع و إعاقة أي اتصالات مشبوهة أو استقبال مواقع الكترونية محددة.

حيث يعمل كأداة لتصفية مرور البيانات بين الشبكة الداخلية المحمية و الشبكة الخارجية بهدف حماية البيانات الموجودة في الحاسبات الخاصة بالمنظمة أو المؤسسة من أي محاولة للعبث أو التعديل أو التغيير أو إتلاف، حيث تعتمد في عملها على التحقق من صلاحية المستخدم و نظام الدخول و الخروج و التشفير و برامج الحماية من الفيروسات.

الفرع الرابع: وسائل آمن أخرى

بحسب العديد من الخبراء فإن الشخص الذي يملك جهاز كمبيوتر شخصي أو محمول عليه إتباع عدد من الوسائل الآمنة:

- عدم فتح أي ملف برسائل الكترونية غير معروفة
- عدم تنزيل برامج مجهولة من مواقع منتديات غير معروفة
- عدم إيقاف أو إطفاء برامج مكافحة الفيروسات والجدار الناري
- عدم الإفصاح عن كلمة السر لأي شخص وعدم كتابتها على مقصوصات ورقية
- اختيار كلمات سر غير متداولة وقوية ولا تدل على شخصية الشخص
- عدم حفظ صورة شخصية في الأجهزة ونقلها لبطاقة الذاكرة
- تحديث وتغيير كلمات السر بين فترة و أخرى

---

[159]- **منصور بن سعيد القحطاني**، مهددات الأمن المعلوماتي و سبل مواجهتها، رسالة ماجستير في العلوم الادارية، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم العلوم الإدارية، 2008، ص 57.

[160]-**محمود الرشيدي**، العنف في جرائم الانترنت– أهم القضايا: الحماية و التأمين، ط1، الدار المصرية اللبنانية، القاهرة، 2011، ص 143.

الباب الأول:
الجوانب الموضوعية لقواعد الأمن المعلوماتي

الباب الأول:

الجوانب الموضوعية لقواعد الأمن المعلوماتي

تطرقنا في الفصل التمهيدي من هذه الدراسة إلى أهم المفاهيم والمبادئ المتعلقة بالسلامة المعلوماتية و الأمن المعلوماتي و أهدافه، والى ضرورة الحماية الفنية والتقنية للنظام المعلوماتي والمعلومات المخزنة به أو المرسلة عبر وسائل الاتصال حفاظا على أمنها وسلامتها من كل اعتداء، و سوف نتعرض في هذا المقام إلى الحماية القانونية للمعلومات والأنظمة المعلوماتية من خلال دراسة قانونية نستمد أحكامها من ما جاء في التشريعات الدولية والوطنية، وكذا الاتفاقيات التي جاءت بشان الجرائم المعلوماتية أو الالكترونية وفي مقدمتها اتفاقية بودابست [161] لسنة 2001، و الإتفاقية العربية بشأن مكافحة جرائم تقنية المعلومات المحررة بالقاهرة سنة 2010.

و لقد اعتمدت في تحديد وتقسيم أنواع الجرائم المعلوماتية بحسب التقسيم والترتيب الوارد في اتفاقية بودابست باعتبارها النموذج الأمثل لدول الاتحاد الأوروبي وعدة دول أخرى [162]، في تقديم نموذج عن قائمة جرائم المجال السيبيرني و كحد أدنى أو نسبي، على أن تقوم دول الاتحاد و الدول المصادقة عليها بسن تشريعات داخلية تتوافق مع ما جاء في الاتفاقية، يمكن من خلالها مكافحة هذه الجرائم، وبهدف وجود تجانس بين القوانين على المستوى القومي[163] والدولي[164].

---

[161]- تعد الاتفاقية الوحيدة المتعددة الأطراف المعنية **بمكافحة الجرائم الكمبيوتر والانترنت** ، وهي تمثل ركيزة أساسية منذ دخولها حيز النفاذ في الأول من يوليو لعام 2004 على مستوى دول أعضاء مجلس الاتحاد الأوروبي ، ولقد وقعت عليها العديد من الدول من غير أعضاء مجلس اروبا مثل كندا واليابان وجنوب إفريقيا، كما صادقت عليها الولايات المتحدة الأمريكية.

[162]- هناك دول أخرى غير دول الاتحاد الأوروبي أبدت عن موافقتها على هذه الاتفاقية من بينها دول جنوب إفريقيا وأمريكا، وذلك بحث الاتفاقية على ضرورة التعاون الدولي للوقوف في وجه الجرائم الالكترونية كونها جرائم عابرة للحدود.

[163]– تجدر الإشارة إلى الأمر نفسه بالنسبة للدول العربية أنه تم الاستعانة بالقانون العربي النموذجي او الاسترشادي بشأن مكافحة جرائم الكمبيوتر والإنترنت وما في حكمها، حيث وضع هذا القانون القواعد الأساسية التي يتعين على المشـ رع العربي اللجو اليها عند سن قانون وطني لمكافحة هذه الجـرائم سواء أكان القانون الوطني مستقلا لمكافحة هذه الجرائم المستحدثة ام كان تعديلاً لقانون العقوبات المطبق بالفعل في أي دولة عـ ربية. وقد أشار هذا القانـ ون الاسترشادي لأنواع الجـ رائم التي تقع بطريق الكمبيوتر والإنترنت بصفة عامة ومحدداً عقوبتها وأحال إلى التشريع الوطني كل ما يتعلق بأركان هذه الجرائم وكذلك العقوبات التي تطبق عليها و صدر أخيرا في شكل اتفاقية عربية تم إعتمادها في إجتماع مجلس الوزراء العرب بالقاهرة سنة 2010، و صادقت عليها الجزائر سنة 2014

ومن هذا المنطلق كذلك صدرت الاتفاقية العربية بشان جرائم تقنية المعلومات و التي صادقت عليها الجزائر مؤخرا سنة 2014، و هي بذلك تعد نموذج و قانون يوضح الجرائم المتعلقة بتقنية المعلومات و التي لا شك أنها تمثل شكل من أشكال الجرائم الماسة بقواعد الأمن المعلوماتي، و مع ما جاء في بعض القوانين لمقارنة الخاصة مثل القانون الفرنسي وقوانين عربية أخرى منها القانون الأردني، على أن لا ننسى موقف المشرع الجزائري من الحماية الجزائية للجرائم المعلوماتية[165].

مع تدعيم توفير الحماية ببعض التطبيقات والأحكام القضائية وبعض النماذج عن الجرائم الواقعية بهذا الشأن.

لذلك و من خلا هذه الدراسة سوف أقوم بالتطرق إلى بعض أشكال تلك الجرائم التي تشكل مساسا بأهم قاعدة من قواعد الأمن المعلوماتي و هي سرية و سلامة المعلومات والأنظمة المعلوماتية(فصل أول) و إلى الجرائم ذات الصلة أو المرتكبة بواسطة الحاسب الألي(فصل ثاني) و لا شك أن للجرائم المعلوماتية علاقة بالملكية الفكرية بعتبار أحد عناضر المنظومة المعلوماتية يتشكل من برامج معلوماتية نظمها هذا القانون و نحاول التفصيل في تلك العلاقة (فصل ثالث)وفق ما يأتي:

الفصل الأول:

الجرائم ضد سلامة المعلومات والنظم المعلوماتية

عرف القرن العشرين تطورا مذهلا في مجال الاتصال و تقنية المعلومات، و أ مام اختلاف الدهنيات و المستويات العلمية لمستعملي هذه الوسائل ظهرت ممارسات غير مشروعة، أدت إلى

---

[164]– بهدف مواجهة جرائم المساس بأنظمة المعالجة الآلية، قامت الجزائر بتأسيس اشتراك بينها وبين الاتحاد الأوروبي عقد بتاريخ 22 أبريل 2002 وصادقت عليه الجزائر بموجب القانون رقم 1144/2003

[165]– الجزائر كباقي الدول لم تسلم من خطورة الجرائم المعلوماتية بصفة عامة وجرائم الاعتداء على نظم المعالجة الآلية بصفة خاصة كونها تحتل جزء من الفضاء الالكتروني، ومن ذلك قام المشرع الجزائري بسد ما كان من فراغ قانوني في هذا المجال ولو بجزء بسيط فجرم ما سماه بـ: " **المساس بأنظمة المعالجة الآلية للمعطيات** " من خلال تعديله ***لقانون العقوبات*** بموجب ***القانون رقم 15/04 بتاريخ 10 نوفمبر 2004.***

ظهور طائفة جديدة من الجرائم العابرة للحدود، مختلفة عن باقي الجرائم التقليدية ، وقد سميت بالجرائم المعلوماتية أو الالكترونية أو جرائم الانترنت.

و تدخل هذه الجرائم في نطاق دراسات القانون الجنائي الوطني ، و التي تقع في صميم القسم الخاص لقانون العقوبات، و باعتبارها أفعال تتخطى حدود الدولة فتعد أيضا من اهتمامات القانون الجنائي الدولي ، كما تدخل في عداد الجريمة المنظمة التي تقوم على أساس تنظيم هيكلي و تدرجي له الاستمرارية لتحقيق مكاسب طائلة ، و أمام انتشار ظاهرة الجريمة المعلوماتية أو جرائم الانترنت ، مقابل النقص التشريعي خاصة في التشريع الوطني يدفعنا الأمر للبحث عن الأسلوب الأمثل للتعامل مع هذه الظاهرة بسبب ما خلفته من حيرة لدى رجال القانون ، من جهة بسبب حداثتها و غموضها و من جهة أخرى ل عدم إمكانية تطبيق النصوص القانونية ال تقليدية التي لا تتناسب مع طبيعة هذه الظاهرة، التي تغزو مجتمعنا بمختلف فئاته.

كما أن ملفات المتابعة القضائية لها تعد شبه معدومة ، مما يتطلب سن نصوص تشريعية و تفعيلها لمكافحة هذه الجريمة التي خرقت كل المبادئ و الأسس القانونية.

و من اجل ذلك يجب الوقوف عند هذه الظاهرة الجديدة من خلال الدخول إلى صلب الموضوع و مقتصرين على بعض الجرائم التي تشكل مساسا بقواعد الأمن المعلوماتي، و ذلك وفقا لما جاء في الاتفاقات الدولية و التشريعات المقارنة.

وإن الهدف من دراسة هذه الجرائم هو لحماية قواعد الامن المعلوماتي و السلامة المعلوماتية من خلال حماية السرية، و سلامة و توفر البيانات المعلوماتية والأنظمة المعلوماتية [166]، ذلك أن هذه النشاطات وفقا لما جاء في اتفاقية بودابست وما جاء في مذكرتها التفسيرية [167] تمثل الأخطار الأساسية والتهديدات الرئيسية لأمن الحاسبات وسلامة البيانات المخزنة أو المرسلة وكذا على نظم المعالجة الآلية، و تتمثل الجرائم محل الدراسة في جريمة الدخول أو البقاء غير المصرح به(المبحث الأول) ، جريمة الإتلاف المعلوماتي(المبحث الثاني)، و جريمة الاعتراض غير القانوني(المبحث الثالث) و كذا إساءة استخدام الحاسب الآلي(المبحث الرابع) كما يأتي:

---

[166]– نص المشرع الجزائري على هذه من خلال تعديله **لقانون العقوبات** سنة 2004، وكذا اغلب التشريعات المقارنة محل الدراسة

[167]– **المذكرة التفسيرية لاتفاقية بودابست** بتاريخ 08 نوفمبر 2001 على الموقع التالي:

http://convention.coe.

المبحث الأول:

الدخول أو البقاء غير المشروع إلى نظام معلوماتي

إن انتهاك النظام المعلوماتي يعد فعلا غير مشروع و يهدد سلامة النظام المعلوماتي وأمنه، و مساسا بسلامة و سرية المعلومات المتضمنة فيه، لذلك فهو يشكل جريمة من جرائم السلوك المجرد و التي لا يتطلب فيها المشرع أن تحقق نتيجة معينة، بل بمجرد اختراق النظام تقوم الجريمة كما تعد

الأساس الذي تقوم عليه باقي جرائم نظم المعلومات، بحيث إذا لم يتم اختراق النظام لا يمكن ارتكاب الأفعال الجرمية الأخرى[168]، وهذا ما سأقوم بتوضيحه فيما يأتي:

المطلب الأول: مفهوم الدخول والبقاء غير المشروع للنظام المعلوماتي

تعد جريمة الاختراق المعلوماتي [169] ظاهرة إجرامية حديثة ذات خطورة [170] كبيرة كونها تؤثر على تكنولوجيا المعلومات في عالم الجريمة المستحدثة، وتحويلها إلى مفاهيم جديدة فيما يعرف بالجرائم الالكترونية.

كما تكمن قوة تأثير هته الجريمة في ارتباطها بكل الجرائم التي يتم ارتكابها ضد نظم المعالجة الآلية للمعلومات، وعند تحليل عناصر ومكونات هته الجريمة، يتبين أنها ذات طبيعة مزدوجة أو ثنائية[171] قد تترتب عليها جرائم أخرى، و إضافة إلى كونها جريمة شكلية و مجردة [172]، فانه من

---

[168]– فمثلا في جريمة الإتلاف الفيروسي للأنظمة المعلوماتية لا يمكن للفيروس القيام بعملية الإتلاف ما لم يتم اختراق النظام المعلوماتي ، وبالتالي تقع هذه الجريمة بطريق غير مباشر، والدليل على هذا الارتباط ما جاء في حكم القضاء الأمريكي في شأن واقعة Morris والذي تم بموجبه معاقبته على جريمة الدخول الغير مشروع لنظام معلوماتي تابع للحكومة الفدرالية : د. **نسرين عبد الحميد نبيه**، مرجع سابق، ص 85.

[169]- تعددت المسميات لهذا الفعل ولكن المضمون واحد، هو خطورة هذه الجريمة حيث أصبحت تشكل تهديدا لأمن المعلومات و الأنظمة المعلوماتية و كذا لحياة الأشخاص و خصوصياتهم و هذا ما أكدته التقارير الإعلامية حيث ورد في مقال لصحفية جريدة الخبر لـ **رزيقة أدرغال** تحت عنوان " **الانترنت في الجزائر وسيلة للتشهير و انتهاك لخصوصية الغير** ، و حيث جاء فيه أن تحولت الشبكة العنكبوتية في الجزائر، من وسيلة للدردشة والتواصل الاجتماعي، إلى وسيلة للتشهير" ، والمساس بالحياة الخاصة للآخرين والاحتيال، إذ تشير آخر أرقام المديرية العامة للأمن الوطني إلى ارتفاع معدل الجريمة الالكترونية لعام 2014 بتسجيل 75 قضية، تورّط فيها 205 شخص مقارنة بمعدل الجريمة إلكترونية التي سجلت سنة 2013، **أغلبها تتعلق باختراق أنظمة المعالجة الآلية للمعطيات** ، والقذف والمساس بحرمة الحياة الخاصة، إضافة إلى قضايا انتحال هوية الغير والنصب والاحتيال، جريدة الخبر، الجزائر في 17 يناير 2015.

لمزيد من التفاصيل عن واقع الجرائم الالكترونية حسب التقارير الإخبارية و ما جاء في هذا المقال، مشار إليه في الملحق رقم 01.

[170]– ولقد أشارت المذكرة التفسيرية لاتفاقية بودابست بان الدخول غير المشروع أو غير المصرح يعد من الجرائم المعلوماتية الأساسية ضد السرية وسلامة وتوافر البيانات والأنظمة، وأنها تمثل تهديدا رئيسيا على امن الأنظمة المعلوماتية وما تتعرض له أنظمة المعالجة والإرسال الآلي للبيانات

[171]- د. **أيمن عبد الله فكري** ، مرجع سابق، ص 219/ وكذلك أ. **رشيدة بوكر**، جرائم الإعتداء على نظم المعالجة الألية في التشريع الجزائري المقارن، منشورات حلبي الحقوقية، لبنان، 2012 ، ص 159.

[172]- يقصد **بالجريمة الشكلية** وفقا للمفهوم القانوني بأنها تتوافر في كل جريمة عندما يكتفي المشرع بتوافر السلوك الإجرامي المنصوص عليه بالقانون دون تطلب توافر نتيجة مادية، واكتفاء المشرع بالنتيجة القانونية التي حددها مراعاة منه لضرر

الممكن أن تتحول إلى جرائم مادية ذات نتيجة بمعنى أنه قد لا يمكن تحديد الجرائم التي ترتبط بها أو تترتب عنها.

و هذا ما اثأر جدلا فقهيا حول مدى انطباق وصف جريمة تقنية المعلومات عليها، وبالتالي هل تستوجب الحماية الجزائية أم لا؟

كان الخلاف يدور في اتجاهين [173] وكل اتجاه كان له مبرراته، إلا أن اغلب الفقه يرى ضرورة تجريم هذا الفعل بحد ذاته لما ينطوي عليه من خطورة وما يترتب عليه من نتائج باعتبار هذا السلوك خطوة أساسية لارتكاب بقية جرائم تقنية المعلومات الأخرى[174].

كما أن المعلومات التي قد يتم الوصول إليها من خلال هذا الفعل قد تكون على قدر من الأهمية، كما هو الحال في المعلومات المتعلقة بالأسرار العسكرية للدولة، أو المهنيةوغيرها كثير.

إذ أن مجرد الولوج أو البقاء في النظام والاطلاع على ما يحتويه يعد مساسا بسلامة النظام و سرية المعلومات، حتى ولو لم يتم ارتكاب جرائم لاحقة على هذا التصرف، أو حتى لو كان الهدف [175]

محتمل على المصلحة المحمية، أي بمعنى أن المشرع يتجه إلى وضع حماية وقائية للمصلحة التي ينبغي حمايتها بتجريم السلوك الذي يمكن أن يؤدي إلى الاعتداء عليها استقلالا: د.**أيمن عبد الله فكري**، مرجع سابق، ص 219.

[173]– **يرى اتجاه فقهي:** انه لا ضرورة تستدعي تجريم مجرد الدخول أو إلقاء غير المصرح بهما إلى نظام المعالجة الآلية، وخاصة إذا لم يكن لذا الفاعل نية لارتكاب جريمة لاحقة على الدخول، ويبرر ذلك على ان هذا السلوك لا يخرج عن كونه طريقة لعرض القدرات والمهارات التقنية والذهنية التي يتمتع بها الشخص الذي قام بهذا التصرف وهذا الأمر لا يشكل ب حد ذاته جريمة تستدعي معاقبة الفاعل الى جانب ذلك فانه لم يحصل إتلاف من وراء هذا الاختراق فانه من الصعب الكشف عنه لأنه لا يترك أثرا يدل على ذلك ومن الصعب كذلك على جهات التحقيق الكشف عنها لما تنطوي عليه من تعقيدات وصعوبات فنية. مشار إليه لدى: د. **نائلة عادل محمد فريد قورة** ، المرجع السابق، ص 318.وكذا **نهلا عبد القادر مومني** ، الجرائم المعلوماتية، دار الثقافة للنشر و التوزيع، عمان– الأردن، 2008 ، ص 157/ أ.**رشيدة بوكر** ، مرجع سابق، ص 160.

أما **الاتجاه الثاني** يرى ضرورة تجريم هذا الفعل، حتى ولو لم يكن بقصد ارتكاب جريمة لاحقة فيما بعد، ويدعم هذا الاتجاه رأيه بالإشارة إلى أن هناك خسائر مادية قد تترتب على حالات الدخول غير المصرح به إلى نظام المعالجة الآلية، بل قد تكون هذه الخسائر نتيجة مجرد محاولة وقف هذا الدخول: مشار إليه لدى د.**نائلة عادل محمد فريد قورة** ، المرجع نفسه، ص 317. و كذلك أ. **رشيدة بوكر**، نفس المرجع السابق، ص 160

[174]– لقد اعتبر **المشرع الأمريكي** جريمة الدخول غير المصرح به نقطة البداية لأية جريمة معلوماتية أخرى من خلال قوانين إساءة استخدام الحاسبات الآلية لسنتي 1984 و1986 مشار اليه لدى د. **نائلة عادل محمد فريد قورة**، مرجع سابق، ص 320.

[175]– قد تختلف أهداف الاختراق باختلاف المخترق، فمنهم من يخترق أجهزة و أنظم ة الغير لمجرد إثبات الذات أو إشباع فضوله بمدى قدرته للوصول إلى هذا النظام، كما قد يكون الهدف من الاختراق هو الوصول إلى النظام المعلوماتي بما يحتويه من معلومات اما من اجل سرقتها أو إتلافها أو تعطيل النظام عن أداء وظيفته

من هذا السلوك المجرد هو إثبات الذات والقدرات التقنية والذهنية على اختراق الأنظمة والحواجز الالكترونية.

وأن ترك هؤلاء الأشخاص ومن يأتون بهذا السلوك بدون عقاب قد يؤدي إلى التمادي في الاعتداء على أنظمة المعالجة الآلية.

غير أن التشريعات قد أدركت الطبيعة الخاصة لفعل الدخول إلى النظام وحسمت ذلك الخلاف بالنص على هذه الجريمة إما في قانون العقوبات بإدراج بعض النصوص تعاقب على هذا النوع من الجرائم[176] أو في قانون مستقل[177]، بل ذهبت إلى ابعد من ذلك من خلال تجريم فعل الدخول بدون تصريح و على النتيجة في تشديد العقاب إذا ترتب على هذا الدخول أضرارا لاحقة عليه مست النظم المعلوماتية والمعلومات على حد سواء.

وما يمكن الإشارة إليه في هذا الصدد أنه في شريعتنا الغراء وديننا الحنيف، أن الإتيان بمثل هذا الفعل غير جائز فهو بمثابة الدخول إلى بيوت دون إذن من أصحابها، وهذا يمثل جريمة مستقلة بذاتها فيما يعرف بانتهاك حق الخصوصية وهو أمر مؤثم شرعا وقانونا فجاءت تعاليم الإسلام بضرورة الاستئذان حفاظا على أسرار البيوت وحماية للخصوصيات[178].

وعليه يلزم وضع كافة الضمانات التي تكفل الوقاية من هذا النوع من الجرائم الحديثة و هو الدخول غير المصرح به أو النفاذ إلى نظم المعالجة الآلية دون علم أو إذن من أصحابها.

---

[176]– كما فعل المشرع الفرنسي المادة 1/321 من **قانون العقوبات المعدل**، والمشرع الجزائري في المادة 394مكرر فقرة 1 عقوبات.

[177]– قام المشرع الأردني بنص على هذا السلوك من خلال تجريم فعل الدخول غير المصرح به الى نظام معلوماتي من خلال **قانون مؤقت رقم 30 لسنة 2010 متعلق بجرائم أنظمة المعلومات**، المادة الثالثة منه.

كذلك نجد **القانون الإماراتي لمكافحة جرائم تقنية المعلومات رقم 2 لسنة 2006** ،الجريدة الرسمية العدد 442، النص الكامل على الموقعwww.atsdp.com/forums/2061-a htm

كذلك بالنسبة لمشرع سلطنة عمان حيث أصدر **مرسوم سلطاني رقم 12/2011 بشأن قانون مكافحة جرائم تقنية المعلومات** ، الجريدة الرسمية العدد 929.

[178]- قال تعالى: " يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَدْخُلُوا بُيُوتًا غَيْرَ بُيُوتِكُمْ حَتَّى تَسْتَأْنِسُوا وَتُسَلِّمُوا عَلَى أَهْلِهَا ذَلِكُمْ خَيْرٌ لَكُمْ لَعَلَّكُمْ تَذَكَّرُونَ" سورة النور، أية رقم 27.

و أن الدخول غير المصرح به لنظم المعالجة الآلية يقصد به الهجوم على مواقع الانترنت و تعمد الوصول إلى جهاز كمبيوتر دون الحصول على إذن، أو تجاوز الحدود المسموحة [179] أو مجرد الولوج غير المسموح به في نظام الحاسب الآلي و التواجد به دون إحداث أدنى ضرر لصاحبه سوى اختراق النظام والاطلاع على ما بداخله من معلومات مختزنة، و سواء كان في شكل بقاء بالنظام أو أي جريمة أخرى، فقد اعتد به المشرع الجزائري و كذا في القانون المقارن عند تجريم هـ فعل الدخول استقلالا وما يترتب عليه من جرائم أخرى مثل التغيير أو الإتلاف أو التعييب والتخريب، أو تعطيل النظام أو أي إضرار بنظام المعالجة الآلية.

كما أن الاختراق لا يطال الأجهزة أو الأنظمة المعلوماتية إلا إذا كانت موصولة بشبكة الانترنت التي توصل الجهاز بالمحترفين[180] مما يشكل تهديدا كذلك لأمن الانترنت[181] و شبكات الاتصال .

المطلب الثاني: أركان جريمة الدخول أو البقاء غشا

ويستفاد من ما تم توضيحه ومن النصوص التي جاءت بشأن هذه الجريمة أنها تقوم على أركان مثلها مثل سائر الجرائم و المتمثلة فيما يأتي:

الفرع الأول: الركن المادي

انطلاقا من النصوص القانون السابق الإشارة إليها[182]، فان الركن المادي لهذه الجريمة هو نشاط جرمي يتمثل في الدخول المنطقي أو الاتصال بطريق الغش مع نظام معلوماتي بغرض اختراقه كله أوفي جزء منه، أو قد يتمثل في البقاء في النظام المعلوماتي دون وجه حق.

والدخول في هذه الحالة لا يقصد به الدخول بالمعنى المادي أو التواجد المادي للشخص، وإنما مجرد الاتصال بالنظام المعلوماتي بالطرق الفنية اللازمة سواء عن طريق بث فيروسات لاختراق النظام أو

---

[179]– د.**خالد بن سليمان الغثبر** ، اختراق المواقع الالكترونية حال الأزمات تشخيص وحلول مركز التميز لأمن المعلومات، على الموقع :/coeia.ksu.edu.sa اطلع عليه بتاريخ 2013/12/16

[180]– **نبيل صقر**، الوسيط في شرح جرائم الأموال، دار الهدى، عين مليلة، الجزائر، 2012، ص 218.

[181]– أن المحترفين و الموهوبين في عالم الكمبيوتر و الانترنت يستطيعون إختراق تلك الأنظمة من خلال استغلال الثغرات والخلل الموجود في بنية شبكة الانترنت و الأنظمة المعلوماتية ز الدخول لأجهزة و حسابات الغير دون شعورهم بذلك، وهذا الأمر تصدر عناوين الصحف في العالم بتاريخ 28 يوليو 2008 من جراء التصريحات التي أدلى بها المخترقين وكذا ما إكتشفه خبراء الأمن الرقمي بعد ذلك و تحذيرهم بشأن أمن الانترنت.

Nicolas ARPAGIAN, La Cyber sécurité, éd. ITICIS, Alger, 2014, p 31.

[182]- المادة **394 مكرر عقوبات جزائري** ، المادة 323_1 **عقوبات فرنسي**، المادة **3** من قانون المتعلق بجرائم نظم المعلومات الاردني، المادة **2**من **اتفاقية بودابست لسنة 2001** بشأن الجرائم الالكترونية

عن طريق استخدام أرقام سرية تسمح بهذا الدخول المنطقي [183] أو اتصال تلفوني أو استخدام كرت ممغنط[184].

غير أن شيوع استخدام نظم المعالجة الآلية من قبل معظم الأشخاص وفي شتى المجالات، فإنه قد يتم اللجوء إلى تأمينها وحمايتها فنيا من خلال وضع برامج وحواجز أمنية، ومن هنا يثور تساؤل حول عناصر الركن المادي وهل تعد الحماية الفنية عنصرا من عناصره أم شرط لكي تفرض الحماية الجنائية؟

نوضح ذلك من خلال التطرق إلى الأمور الآتية:

البند الأول: مدى ضرورة خضوع النظام المعلوماتي للحماية الفنية

إن مسألة مدى خضوع النظام المعلوماتي للحماية الفنية حتى تكفل له الحماية الجزائية، كانت محل خلاف و جدل فقهي وقانوني.

فبالنسبة لبعض الدول تستلزم تشريعاتها أن يكون هناك إنتهاك لتدابير الأمن حتى تقوم المسؤولية الجزائية مثل التشريع الأمريكي الفدرالي لجرائم الحاسب الآلي لسنة [185]1984 والذي تم تعديله في كل من سنة 1986 و1994 و1996، و كذلك التشريع الألماني[186].

والبعض الآخر لا يرى ضرورة لذلك منها التشريع السويدي [187] وكذلك فعل المشرع الفرنسي من أول قانون صدر بشأن المعلوماتية إبتداءا من سنة 1988[188] إلى أخر تعديل لقانون العقوبات سنة

---

[183] **-Myriam QUEMENER**, **Yves CHARPENEL** ; Cybercriminalité droit pénal appliqué, éd Economica , Paris,2012,P 72,73.

[184]- د. **نائلة عادل محمد فريد قورة**، مرجع سابق، ص 315.

[185]- مشار إليه لدى د. **سليم عبد الله الجبوري** ، مرجع سابق، ص 322/ د.نائلة عادل محمد فريد قورة، نفس المرجع السابق، ص 320 وما بعدها.

[186]– تطلب المشرع الألماني لتجريم الدخول غير المصرح به أن يحصل المخترق على معلومات نتيجة لهذا الدخول وان تكون المعلومات مشمولة بنظم أمنية: مشار إليه لدى د.نائلة فريد قورة، مرجع نفسه، ص 358.

[187]– يعتبر التشريع السويدي رقم 289 من أولى التشريعات الأجنبية التي صدرت لتجريم الدخول غير المشروع سنة 1973 المادة 21 منه، وتلتها الوليات الأمريكية المتحدة.عبد الله الجبوري، ص 322ونائلة ص 358

[188]**-Loi n°88-19** du 5 janvier 1988 SUR **LA FRAUDE INFORMATIQUE** (LOI GODFRAIN), JORF du 6 janvier 1988 page 231 , legifrançe.gov.fr

2004 وان كانت المذكرة التفسيرية لقانون 1988 أشارت إلى الحماية الفنية لنظم المعالجة الآلية حتى تقوم المسؤولية الجزائية، لكن المشرع في إصداره لقانون الغش المعلوماتي لم يشر إلى ذلك.

أما بخصوص المشرع الجزائري فهو كذلك لم يشر إلى هذا الشرط من خلال تعديله لقانون العقوبات سنة 2004 وإنما جرم مجرد الدخول بغش إلى أنظمة المعالجة الآلية للمعطيات في المادة 394 مكرر.

ونفس الشيء نلاحظه على التشريع الأردني حيث جاء خاليا من هذا الشرط عند الرجوع إلى القانون المؤقت الخاص بجرائم الأنظمة المعلوماتية لسنة 2010[189].

و كذلك الاتفاقية العربية بشأن جرائم تقنية المعلومات المحررة بالقاهرة سنة 2010 عندما نصت على هذا الفعل بموجب المادة 1/06 و لم تشر إلى شرط الحماية الفنية للنظام المخترق.

أما من جانب الفقه فان الآراء تضاربت وكان لكل رأي حججه،

الرأي الأول : يرى جانب من الفقه الفرنسي ضرورة الحماية الفنية و وجود نظام امني حتى تقوم المسؤولية الجزائية، على اعتبار أن القانون يجرم الاعتداء على نظم الأمن و اختراقها، و أن هذه الجريمة لا تقع إلا إذا كان النظام غير مفتوح للجمهور [190]، و يستند أنصار هذا الاتجاه في تعزيز وجهة نظرهم إلى اعتبارات قانونية، وهي أن الاعتداء على نظام أمن يعد عنصرا مفترضا في جميع جرائم نظم المعالجة الآلية للمعطيات كما هو مبين في الأعمال التحضيرية لمناقشة القانون رقم 19 لسنة 1988 حول الغش المعلوماتي[191]، وكذلك ما جاء به القانون المتعلق بالمعلوماتية والحريات لسنة 1978[192] باعتباره سابقة تشريعية مهمة في هذا الشأن، إذ يفترض من خلال المادة 29 منه على أن

189- **القانون الأردني المؤقت بشأن جرائم أنظمة المعلومات** رقم 30لسنة 2010، الجريدة الرسمية صفحة 5334 عدد 5056 بتاريخ 2010/09/16.

190 - **Myriam QUEMENER** , **Yves CHARPENEL**, op.cit, P72_75.

191- بالرجوع إلى الأعمال التحضيرية للقانون رقم (19) لسنة 1988 حول الغش المعلوماتي، طلب بعض أعضاء البرلمان وأصروا على ضرورة الحماية الفنية وان الحماية الجزائية تقتصر فقط على الأنظمة المحمية فنيا، مشار إليه لدى: د.**علي عبد القادر قهوجي**، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للنشر والتوزيع، الإسكندرية، 1999، ص 123./ كذلك: أ. **رشيدة بوكر**، مرجع سابق، ص 165./ و كذا **نبيل صقر**، مرجع سابق، ص 216.

192- **Art** 29 du Loi n° **78-17** du 6 janvier 1978 relative à ***l'informatique, aux fichiers et aux libertés*** ; « Toute personne ordonnant ou effectuant un traitement d'informations nominatives s'engage de ce fait, vis-à-vis des personnes concernées, à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés». JORF du 7 janvier 1978 page 227

المسئول عن النظام المعلوماتي يلتزم بتامين هذا النظام وبالضرورة، و وفقا لأصحاب هذا الرأي فانه لا ينبغي حصر هذه الحماية على المعلومات الاسمية، وإنما يجب أن يشمل كل المعلومات[193].

إضافة إلى ذلك فان أنصار هذا الاتجاه يعتبرون أن هذا الشرط تقتضيه متطلبات العدالة والمنطق، بحيث أن القانون الجنائي لا ينبغي أن يقوم بحماية الأشخاص الذين لا يأخذون الحيطة اللازمة المتطلبة من الرجل العادي[194]، وبالتالي وجود نظام الحماية، أو حماية نظام معلوماتي بإجراءات أمنية يمكن اعتباره التزاما قانونيا على كل من يقوم بإدارة نظام للمعالجة الآلية.

أما **الاتجاه الثاني**: وهو الغالب[195] يرى انه ليس من الضروري لقيام مسؤولية جزائية أو لحصول جريمة الدخول غير المصرح به لنظام معلوماتي أن يكون هذا النظام متوفر على حماية فنية أو جهاز أمان.

و يستند هذا الاتجاه على نصوص القانون العريقة والتي جاءت خالية من هذا الشرط [196]، و من المستقر عليه في مبادئ القانون الجزائي انه لا يجوز إضافة عنصر لم ينص عليه القانون و كذا فإن قواعد القانون الجزائي تفسر تفسيرا ضيقا، كما أنه لا يجوز تقييد النص المطلق أو تخصيص النص

ولقد أبقى المشرع الفرنسي على صيغة المادة 29 في مضمونها عند تعديله لقانون العقوبات في المادة 17/226 ، وأعاد صياغتها بموجب القانون رقم 2004_801 المعدل والمتمم لقانون العقوبات والقانون رقم 78-17

Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF n°182 du 7 août 2004 page 14063, texte n° 2.

والصياغة الجديدة للمادة 226 عقوبات فرنسي جاءت خالية من أي عبارة تشير إلى شرط الحماية الفنية إلى أنها أحالت بخصوص ذلك إلى المادة 34 من القانون 78-17 السالف الذكر وجاءت كما يأتي:

Art 226-17 du C.P.F ; « Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende » **.**

193- د. أحمد خليفة الملط، **مرجع سابق، ص 134.**

194- **نهلا عبد القادر المومني**، مرجع سابق، ص161، كذاك أ. **رشيدة بوكر**، المرجع السابق، ص166/ ود. **أيمن عبد الله فكري**، مرجع سابق، ص 231.

195- مشار إليه لدى أ.**رشيدة بوكر**، مرجع سابق، ص 167.

Xavier LEMARTELEUR, Le scan de ports : une intrusion dans un STAD ,P 3 ; publier le 13 juin 2008,disponible à l'adresse suivante ; www.juriscom.net

Murielle CAHEN , INTRUSION DANS UN SYSTEME INFORMATIQUE, disponible à l'adresse suivante ; http// www.murielle-cahen.com .

196- **أمال قارة**، مرجع سابق، 105.

العام إلا إذا وجد نص يجيز ذلك، و بالتالي عدم ذكر المشرع لعنصر الحماية يعني أن المشرع أراد استبعاده.

و كذلك يذهب أنصار هذا الرأي في الفقه الفرنسي دائما وفي تعزيز وجهة نظرهم إلى قياس جريمة الدخول غير المشروع على جريمة السرقة، بحيث أن المال يتمتع بالحماية الجنائية من السرقة سواء كان في حماية صاحبه أو لم يكن، فالجريمة تمت بغض النظر عن الصعوبة التي يتلقاها الجاني، وأنه لا يمكن للجاني أن يدفع بعدم تحوط صاحب المال فتمت سرقته [197]، و هذا القول يبين مدى ضعف حجج الرأي الأول.

و وفقا لذلك فإنه ليس من الضروري لوجود جريمة الدخول غير المشروع أن يكون النظام مشمولا بحماية فنية، إضافة إلى ذلك فإن الواقع العملي يكشف على أن أغلبية نظم المعالجة الآلية للمعطيات لا تتوفر على حماية فنية[198]، و الأخذ بالرأي الأول يعتبر غير ملائم من الناحية المنطقية و العملية، و انه سيؤدي إلى إيجاد صعوبات ومشاكل لارتباط تلك الوسائل الفنية بالنواحي التكنولوجية.

و أن هذا الأمر يتطلب مواكبة التطور التقني والتكنولوجي الذي هو في استمرار دائم، فما هو اليوم وسيلة أمنية قد يصبح غدا غير ذلك إلى غيره من الأمور.

وهذا ما أكده القضاء الفرنسي في عدة أحكام له [199] من خلال حكم محكمة استئناف باريس في حكمها الصادر سنة 1994 على أنه من غير الضروري لقيام جريمة الدخول غير المشروع أن يكون

---

[197]- د.**أيمن عبد الله فكري**، مرجع سابق، ص 333/ كذلك أنظر: أ.**رشيدة بوكر**، مرجع سابق، ص 168.

198- يرى الخبير الدولي و الرئيس المدير العام لمؤسسة **حماية الشبكات المعلوماتية** ، **عبد العزيز دردوري** ، أن ''الفايسبوك'' يحتل الصدارة في التهديد وإمكانية استغلال المعلومات الخاصة فيما يعرف بالجريمة الالكترونية، بنسبة تصل إلى 60 بالمائة، باعتباره موقع التواصل الاجتماعي الأول عبر العالم من حيث عدد المنتسبين، إذ أن نحو 10 بالمائة من سكان العالم تتدفق معلوماتهم الشخصية عبر الأنترنت بحرية ويمكن الوصول إليها وتحميلها دون تعقيدات، و شدد دردوري على ضرورة الحذر من قبول دعوات من مجهولين على مواقع التواصل بحيث أنها تمكّن الطرف الآخر من اختراق جهاز الكمبيوتر الخاص للشخص المستقبل، وبالتالي يمكنه استغلال المعلومات الشخصية في أشياء مشبوهة، حذف أو تغيير المعلومات، من خلال فيروسات يحملها الطرف المستقبل على أساس أنها رسائل إلكترونية .

وأشار الخبير الدولي إلى ضرورة أخذ هذه التهديدات محمل الجد، و الالتزام بالاحتياطات التي يجب اتخاذها في مثل هذه الحالات، مع وضع أنظمة تأمين معلوماتية، مشيرا إلى أن الولايات المتحدة فرضت على المؤسسات والمدارس والجامعات القيام بحملات تحسيسية في هذا الإطار. وأفاد الخبير دردوري، أن إدارة مواقع التواصل الاجتماعي لا **تتخذ إجراءات التأمين الكافية** لحماية خصوصيات ومعلومات مستخدميها، من الأشخاص والهيئات والمؤسسات ''على اعتبار أن أنظمة التأمين تكلّف الكثير .'' مقال نشر بجريدة الخبر الجزائرية للصحفية سلمى حراز بعنوان : " **الفيس بوك يشجع على ارتكاب الجريمة**" ، بتاريخ 17 يناير 2015.

[199]- Dans ce sens : voir la décision **CA Paris, 11ème Chambre**, 8 décembre 1997 et la décision émanant de la même cour du 30 octobre 2002 « Kitetoa ». Dans la dernière espèce la cour a décidé qu' « il ne peut être reproché à un internaute d'accéder aux, ou de se maintenir dans les parties des sites qui peuvent être

فعل الدخول تم بمخالفة تدابير الأمن الفنية، وأنه يكفي أن يكون الدخول قد تم ضد إرادة المسؤول عن النظام[200].

هذا الحكم يطرح مبدأ انه لا يمكن للخصم حتى مع غياب الحماية، أن يدخل على نظام غير مصرح له بالدخول إليه.

و مع ذلك فإن المادة 17/226 من قانون العقوبات الفرنسي المعدل أوجبت تثبيت جهاز السلامة لأنظمة معالجة البيانات التي تحتوي على معلومات شخصية.

ومن ناحية أخرى يرى الفقه الفرنسي أن من شأن اشتراط توافر الحماية الفنية تضيق مجال الحماية للمعلومات ونظم معالجتها وهو الأمر الذي يعني إلغاء الفقرة الثانية من المادة 1/323 والخاصة بتجريم البقاء غير المشروع في النظام المعلوماتي[201].

وان استبعاد هذا الشرط من النص القانوني رغم مناقشته في الأعمال التحضيرية ولجان مناقشة القانون، وبالتالي مادام المشرع لم ينص عليه صراحة فان في تطلبه خروج عن النص وعن مبدأ الشرعية الجنائية واشتراط ما لم يشترطه النص القانوني.

وبهذا الخصوص دائما فإن أكبر قضية عرضت أمام القضاء الفرنسي بشأن مدى اعتبار الحماية الفنية عنصر من عناصر الركن المادي لجريمة الدخول هو ما تم مناقشته أمام محكمة

---

atteintes par la simple utilisation d'un logiciel grand public de navigation, ces parties de site, qui ne font par définition l'objet d'aucune protection de la part de l'exploitant du site ou de son prestataire de services, devant être réputées non confidentielles à défaut de toute indication contraire et de tout obstacle à l'accès ».

[200]- Dans une **décision du 5 Avril 1994, la cour d'appel de Paris** a précisé que : « pour être punissable, cet accés ou ce maintien doit etre fait sans droit et en pleine connaissance de cause, étant précisé à cet égard qu'il n'est pas nécessaire pour que l'infraction existe que l'accès soit limité par un dispositif de protection….. ».

De plus, dans un arrêt du 3 octobre 2007, la Cour de Cassation estime que « Doit être censuré l'arrêt qui relaxe un prévenu du chef de maintien frauduleux dans un système de traitement automatisé de données alors qu'il relève que celui-ci, quand bien même il y aurait accédé régulièrement, a utilisé pendant plus de deux ans, et avec un code qui ne lui avait été remis que pour une période d'essai, une base de données qui n'était accessible qu'aux personnes autorisées. » **Murielle CAHEN** , INTRUSION DANS UN SYSTEME INFORMATIQUE , Avocat on ligne , Sur le site suivant ; www.murielle-cahen.com

Dans ce sens voir aussi ; **Thomas ADHUMEAU,** Le piratage d'un serveur de données par un Hacker: le délit de maintien frauduleux, sur le site http://gau mata.blogspot.com/2011/06/le-piratage-dun-serveur-de-donnees-par.html, le 9 juin 2011.

مشار إليه لدى: د. **أيمن عبد الله فكري**، مرجع سابق، ص 234/ أ.**رشيدة بوكر**، مرجع سابق، ص 169.

Voir aussi ;**Myriam Quéméner** et **Yves charpenel**, op.cit, P76.

[201]- د.**أيمن عبد الله فكري**، نفس المرجع السابق، ص 233.

استئناف باريس في قضية مشهورة لشركة TATI ضد الصحفي ANTOINE CHAMPAGNE بتهمة الدخول غير المصرح به في نظام المعالجة الآلية، واصدر الحكم في 30 أكتوبر 2002 بعد الاستئناف ببراءة المتهم أنطوان وأسست حكمها على انه" لا يمكن أن يلام على الدخول أو البقاء في أجزاء المواقع التي يمكن الوصول إليها باستخدام برنامج متصفح بسيط [202]، والتي هي (....) ليست موضوع حماية من طرف مستغل الموقع أومن مزود الخدمة، على أن تعتبر غير سرية في غياب أي مؤشر عكسي أو أي عقبة للدخول إلى النظام (....) تحديد خاصية السرية والمعايير الأساسية لمؤشرات وحماية هذه السرية تقوم بمبادرة مستغل أو مستثمر الموقع أو مندوبيه....."[(203)]

وبالتالي فإن المسألة القانونية التي أثارها القاضي استنادا إلى حقيقة قانونية مفادها أن مقدم الشكوى لم يمتثل لتوفير الحماية القانونية للمعلومات.

وأنه في هذه الحالة يظهر مدى التعارض مع الاجتهادات القضائية التي تعتبر أن وجود نظام حماية غير مهم لوصف السلوك على انه دخول غير مشروع.

و البعض يرى أن هذا القرار حالة استثنائية لا يمكن تعميمه مستقبلا بل وحيدا ومعللا بالعدالة والإنصاف[(204)]، وان الاجتهاد القضائي الفرنسي يعتبر آن جريمة الدخول تتحقق حتى في غياب الحماية الفنية[(205)].

و منهم من ينظر لهذه القضية على أنها أنشأة على وجود افتراض أو قرينة بسيطة، مفادها أن الدخول أو البقاء في نظام المعالجة الآلية للبيانات (وفي هذه الحالة موقع على شبكة الانترنت) غير محمي مما يتيح الوصول إليه باستخدام أداة متاحة للجمهور دون اعتراض لا يشكل جريمة احتيالية بموجب المادة 323-1 [(206)].

---

[202]- وهو برنامج نتسكاب Netscape navigateur وهو عبارة عن برنامج تصفح بسيط يمكن من الوصول إلى صفحات مواقع الشبكة العنكبوتية مثل برنامج انترنت اكسبلوري Internet explorer.

ووظيفة برنامج التصفح تمكين المشترك في الشبكة من جلب صفحات موقع وعرضها في جهازه.

[203]– أ. **رشيدة بوكر**، مرجع سابق،ص 170.

[204] - **Murielle CAHEN,** INTRUSION DANS UN SYSTEME INFORMATIQUE, disponible à l'adresse précédente.

[205] - **Valérie SEDALLIAN** ; Légiférer sur la sécurité informatique : la quadrature du cercle? 5décembre 2003, P11 sur le site www.juriscom.net

[206]- **Myriam Quéméner**, **Yves Charpenel** ; op.cit , P 74.

في حكم أخر ذهبت إليه محكمة استئناف باريس أدانت المتهم في قضية " bluetouf" حيث قام القرصان بإختراق نظام معلوماتي لوكالة الوطنية لأمن الصحة و التغذية و البيئة والعمل و سرقة الملفات بالرغم من أن دخول النظام لم يكن محميا[207].

ونفس الأمر في القانون الجزائري [208] إذ لم يشترط المشرع ضرورة وجود جهاز امن أو سلامة لحماية نظام المعالجة الآلية، و بالتالي جاء النص عام ولم يرد نص آخر يقيد من عموميته ، غير انه في بعض الحالات نجد بعض التنظيمات القانونية قد لزمت بعض الهيئات العمومية التي تتعامل بتطبيق الانظمة المعلوماتية في مؤسساتها ضرورة أن يكون الدخول إلى مركز معالجة المعطيات مؤمنا و مقتصرا على من له تصريح بالدخول [209].

يستفاد من ذلك أن الدخول أو البقاء في نظم المعالجة الآلية للمعطيات سلوك غير مشروع متى تم بدون تصريح من المسؤول عن النظام، و أن الجريمة تقوم سواء كان النظام متوفر على الحماية الفنية أم لا، و إن كان وجود تلك الحماية يساعد في إثبات أركان الجريمة خاصة الركن المعنوي و أن دخوله أو بقاءه كان بغش وعدم وجودها يجعل الإثبات أكثر صعوبة.

البند الثاني: النشاط الجرمي

---

[207] –Dans l'affaire **Bluetouff,** un pirate s'était introduit dans les systemes informatiques de l'ANSES(l'Agence Nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail). Après une première décision de relax(TGI Créteil, 23 avril 2013) des fait d'accès frauduleux à un STAD (systèmes de traitement automatisé de donnée) le prévenu est au contraire condamné en appel(Cour d'Appel de Paris, 5février 2014) pour maintien frauduleux dans un système automatisé de donnée et vol de fichiers, même si leur accès n'était pas protégé.

Laure ZICRY, Enjeux et maitrise des cyber risque, éd LARGUS de l'assurance, France, 2014,P 63

[208]- الأمر ذاته بالنسبة للتشريع الأردني المتعلق **بجرائم أنظمة المعلومات** السابق الاشارة إليه، وكذا تشريعات الدول العربية التي جاءت بشان هذه الجرائم من بينها قانون **جرائم تقنية المعلومات لسلطنة عمان**.

[209]- هذا ما جاء في المادة 2/11 **من القرار الوزاري** المشترك المؤرخ في 30 أكتوبر 2014 الذي ***يحدد كيفيات تطبيق النظام المعلوماتي لمحاسبة التسيير في المؤسسات العمومية للصحة و كذا المؤسسات المعنية بتنفيذ هذا النظام*** بقولها: يجب أن يكون الدخول إلى مركز معالجة المعطيات مؤمنا ومقتصرا على الأشخاص المرخص لهم بالدخول ، جريدة رسمية للجمهورية الجزائرية عدد 01 الصادرة بتاريخ 07 يناير 2015، ص 32.

و قد جاء قبل هذا القرار **مرسوم تنفيذي** رقم 14–106 مؤرخ في 12 مارس *2014* ***يتضمن وضع النظام المعلوماتي لمحاسبة التسير في المؤسسات العمومية*** للصحة حيث أوضحت المادة 04 منه على ما يتضمن النتظام المعلوماتي لمحاسبة التسيير بقولها: يحتوي النظام العلوماتي لمحاسبة التسيير على مدوّنة حسابات وقواعد سيرها وكذا كشوف مالية . ج.ر عدد 15 الصادرة بتاريخ 19 مارس 2014، ص 9.

إن النشاط الجرمي أو السلوك المادي في الجريمة المعلوماتية يحتاج مجموعة من المتطلبات مثل وجود بيئة رقمية واتصال بالانترنت، وهذا أمر مفروغ منه وإلا لا تعد جريمة معلوماتية

وبما أن لا جريمة بغير سلوك، فإن جريمة الدخول أو البقاء غير المشروع سواء في صورتها المجردة أو البسيطة أو المشددة لا تقوم إلا بفعلي الدخول أو البقاء، نوضح ذلك فيما يلي:

أولا: فعل الدخول

يعد فعل الدخول بحسب ما جاء في أغلب تشريعات المتعلقة بالجرائم المعلوماتية ابتداء من اتفاقية بودابست والتشريع الفرنسي وكذا الجزائري والأردني، انه السلوك أو الفعل الأساسي لقيام هذه الجريمة وبقية الجرائم الأخرى التي قد تنجر عن هذا الفعل.

وان كان التشريع قد حسم الأمر بنصه على هذه الجريمة [210]، إلا أنه لم يحدد وسيلة الدخول إلى النظام المعلوماتي مما يجعلنا نثير بعض الأسئلة حول هذا الفعل أو السلوك؟

فما مقصود المشرع بعبارة الدخول إلى نظام المعالجة الآلية؟ و كيف يكون الدخول إلى هذا النظام غير مصرح به أو بغش؟

و هل يشترط وجود نشاط أو عمل يسبق الدخول إلى النظام من أجل تجريم هذا الفعل؟

و في الأساس هل تقوم الجريمة بمجرد الدخول بغض النظر عن وسيلة الدخول أو العمل السابق لهذا الفعل؟

ذا ما سوف نحاول توضيحه فيما يأتي:

1- المقصود بالدخول غير المصرح به؟

نصت المادة 394 مكرر عقوبات جزائري" يعاقب.....كل من يدخل..... عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.." [211]

فمن خلال النص ما المقصود بالدخول؟

---

[210]- المادة 394مكرر عقوبات جزائري، المادة1/323 عقوبات فرنسي، المادة 03 من قانون جرائم أنظمة المعلومات الأردني ، و كذا المادة 1/06 من الاتفاقية العربية بشأن جرائم تقنية المعلومات.

[211]- تنص المادة 3 من **قانون جرائم أنظمة المعلومات الأردني** على أنه" كل من دخل قصدا إلى موقع إلكتروني أو نظام معلومات بأي وسيلة دون تصريح أو بما يخالف أو يجاوز التصريح....."

Et l'**Art 323-**1 de **C.P.F** Modifié par LOI n°2012-410 du 27 mars 2012 - art. 9 ; «

Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende…… »

من الواضح أن الدخول إلى نظام معلوماتي لا يكون بالتواجد المادي للمخترق، ذلك لان هذا لا يمكن تصوره بشأن الدخول إلى نظام المعالجة الآلية بالطريقة ذاتها باعتبار هذا النظام ظاهرة غير مادية.

وإنما يقصد بالدخول هو التواجد المعنوي أو المنطقي في نظام المعالجة الآلية[212] .

و لعل هذا ما جعل المشرع الفرنسي يستخدم مصطلح Accéder بدلا من مصطلح Entrée، ونفس الأمر بالنسبة لاتفاقية بودابست، ولعل هذا المصطلح هو الأكثر ملائمة في هذا المجال وعليه نتحه إلى رأي الفقه والقضاء المقارن في سبيل معرفة المعنى المقصود من هذا الفعل.

تعددت التعريفات بشأن هذا الفعل، حيث عرفه البعض على أنه "عملية ولوج غير شرعي إلى نظام التشغيل في الحاسب الآلي من قبل أشخاص لا يملكون صلاحيات الدخول، وذلك بهدف القيام بأعمال غير قانونية مثل التجسس أو السرقة أو التخريب مع الأخذ بعين الاعتبار قدرة هؤلاء الأشخاص على نقل ومسح أو إضافة ملفات وبرامج، والقدرة على التحكم بنظام التشغيل وإصدار الأوامر"[213].

أو انه إساءة استخدام الحاسب الآلي ونظامه عن طريق شخص غير مرخص له باستخدامه والدخول إليه للوصول إلى المعلومات والمعطيات المخزنة بداخله للاطلاع عليها أو لمجرد التسلية أو إشباع الشعور بالنجاح في اختراق الحاسب الآلي[214].

أو انه عملية دخول غير مصرح به إلى أجهزة الغير وشبكاتهم الالكترونية بواسطة برامج متطورة يستخدمها كل من يملك خبرة في استعمالها[215].

واغلب التعريفات التي قيلت بشأن فعل الدخول جاءت متقاربة ومتشابهة في تحديد معنى هذا السلوك المستحدث محاولتا استيعاب هذا التطور وما جاء به من جرائم.

ويلاحظ أيضا على هذه التعريفات أنها حاولت ربط عملية الدخول بعدم صلاحية أو عدم التصريح فحسب، في حين هناك من يحصر الدخول في النظام بسبب وجود ثغرات [216] فنية وهذا قول صحيح

---

[212]- د. **محمد حماد مرهج الهيتي**، جرائم الحاسوب، الطبعة الأولى، دار المناهج للنشر والتوزيع، عمان، 2006، ص 182.

[213]- **نسرين علم الدين** ،دراسة الحل الأمثل لبناء نظام مركز توليد الشهادات الرقمية المستخدمة في أمن المعلومات، رسالة ماجستير، كلية المعلوماتية، جامعة دمشق، سوريا 2009، ص 19/ مشار إليه لذا **رشيدة بوكر**، مرجع سابق، ص 178.

[214]– د.**نائلة محمد فريد قورة**، مرجع سابق، ص 326.

[215]– **خالد ممدوح ابراهيم**، أمن الجريمة الالكترونية، مرجع سابق، ص 84.

[216]– **الثغرة** تعني نقطة في نظام الحماية، أو منفذ يمكن من خلاله للمعتدي أن يخترق النظام أو يتحقق بسببه الاختراق.

Nicolas ARPAGIAN, op.cit , p31,32.

نسبيا إذ عادة ما يكون الدخول إلى نظام المعالجة الآلية نتيجة لخلل في خدمة الأمن ، و المنفذ الذي يستغله المخترقون و الهاكرز للولوج إلى الأنظمة المعلوماتية ة تحقيق اهدافهم.

ولقد سبق وأن أوضحنا هذا الأمر في القضية الشهيرة لشركة TATI والتي كان الحكم النهائي فيها ببراءة المتهم أنطوان لأنه دخل إلى النظام بسبب خلل في خدمة امن موقع الشركة.

وأن الفعل يتحقق سواء كان النظام يحتوي على جهاز أمن أم لا، كما أن التكنولوجيا أثبتت أن هناك وسائل تقنية يمكن من خلالها تحقق الوصول إلى النظام حتى وأن توفر على الحماية فنية[217].

وبالرجوع إلى نص المادة 394 مكرر عقوبات جزائري نجد أن المشرع لم يحصر فعل الدخول في وسيلة معينة[218]، ولعل ذلك يرجع إلى إدراك المشرعين أن التكنولوجيا في تطور مستمر ولا يمكن حصر فعل الاختراق في طريقة معينة، فما هو اليوم حتى من وسائل الحماية قد يصبح غدا غير ذلك، خاصةً إذا تم اكتشاف ثغرات فنية أو خلل به.

وحسنا فعل المشرع الجزائري وكغيره من المشرعين، وبالتالي فإن فعل الدخول يتحقق بأي وسيلة تقنية تصلح لذلك وهذا ما أكدته عدة أحكام قضائية منها ما صدر عن محكمة استئناف باريس في قرارها الصادر في 05 أبريل 1994 السابق الإشارة إليه.

و ان هذا الفعل يقع من أي شخص مهما كانت صفته وسواء كان مختص في المجال المعلوماتي أم لا فهي ليست من جرائم ذوي الصفة، ولقد عبر المشرع عن ذلك في المادة 394مكرر بقوله".... كل من يدخل أو يبقى....".

---

[217]- لا تتم عملية الدخول أو الاختراق المعلوماتي إلا بتوافر أدوات ووسائل تشكل عنصر أساسي في هذه العملية ومن الطرق الشائعة لتنفيذ الاختراق ما يأتي:

- **معرف عنوان الآي بي** (IP Address) وهو بمثابة البطاقة الشخصية للمستخدم على شبكة الانترنت، يمنحه مزود الخدمة للمشترك أليا بمجرد طلب الخدمة ليمكنه من الولوج الى الشبكة العالمية، وينتج عن IP معرفة بعض المعلومات الشخصية عن المستخدم في عالم الانترنت، كنوع البريد المرسل، والمواقع التي قام بزيارتها.
- حينما يتمكن المخترق من معرفة رقم IP الخاص بالضحية فانه من خلاله يتمكن من الولوج الى الجهاز والسيطرة عليه خلال الفترة التي يكون فيها الضحية متصلا بالانترنت فقط، **محمد مصطفى الشقيري** ، السرية المعلوماتية، ضوابطها وأحكامها الشرعية،ط1، دار البشائر الإسلامية، بيروت،2008،ص 345،/ أ. **رشيدة بوكر**، مرجع سابق، ص 180.
- استعمال **حصان طراودة** : ليتحقق فعل الاختراق لابد من وجود برنامج تجسسي يتم إرساله وزرعه من قبل المخترق في جهاز الضحية، ويعرف بالملف اللاصق(Patch) أو(Trojan) وأحيانا الصامت، وهو ملف يتميز بصغر حجمه ومهمته الأساسية هي التخفي والمبيت في جهاز الضحية، حيث يشكل حلقة وصل بين جهاز المخترق وجهاز الضحية.
- وهناك طرق أخرى مثل ملف تعريف الارتباط كوكيز(cookies) ورصد لوحة المفاتيح، والتفتيش في مخلفات التقنية.

[218]– الأمر ذاته بالنسبة للتشريع الفرنسي والأردني وما جاءت به إتفاقية بودابست و الاتفاقية العربية.

وإنما يكفي أن يتم الدخول مخالفا للشروط التي نص عليها القانون، أو مخالفا لإرادة من له الحق في السيطرة على النظام[219].

2- المقصود بعدم التصريح بالدخول:

الدخول إلى نظام معلوماتي لا يشكل سلوك غير مشروع إلا إذا كان هذا السلوك بدون وجه حق أو بدون تصريح من من يملك الحق أو كان مسئول عن النظام، وبالتالي عدم مشروعية الدخول إلى النظام مرتبطة بالمسئول عنه ومعرفة من له الحق أو السلطة بإعطاء التصريح، لذلك نسأل من يملك التصريح بالدخول؟ و ما هي حالات التصريح أو كيف يكون التصريح؟

لا شك أن تحديد من هو المسئول عن النظام يحدد من له الحق بالدخول إلى هذا النظام، أو بعبارة أخرى من يسيطر عليه، ويسمي الفقه الفرنسي هذا الشخص بصاحب السلطة على النظام " le maitre du systeme "[220] ، كما عرفته المادة الثانية (02) من الاتفاقية الخاصة بحماية الأفراد في مواجهة نظم المعالجة الآلية للمعلومات ذات الطابع الشخصي والتي تبناها المجلس الأوروبي في 28 يناير 1981 بقولها[221]: "كل شخص طبيعي أو معنوي، أوكل سلطة عامة أوكل مؤسسة أو جهاز يكون لهم سلطة التصرف في نظام الحاسب الآلي التابع لهم وتقرير مضمونه أو محتواه، وكيفية تنظيمه والهدف منه"

وتكمن أهمية تحديد من هو المسئول عن النظام في تحديد نطاقه وحصر الأشخاص المصرح لهم بالدخول إلى النظام، وأن غياب الحق يعني غياب تصريح بالدخول، وغير ذلك فهم غير مصرح لهم.

أما عن حالات عدم التصريح بالدخول فهي تتحقق في الحالة التي لا يملك الشخص أي تصريح أو رخصة من المسئول عن النظام وليس له علاقة بالنظام بتاتا [222] كأن لا يكون عملا بالنظام أو

---

[219]- **امال قارة**، المرجع السابق، ص 109.

[220] **-Myriam Quéméner**, **Yves Charpenel**,op.cit,P73.

[221] - **Art 2-d** de La **convention internationale pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel** N°108 du 28 janvier 1981 définie le « maitre du fichier » signifie ; « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui est compétent selon la loi nationale, pour décider quelle sera la finalité du fichier automatisé, quelles catégories de données à caractère personnel doivent être enregistrées et quelles opérations leur seront appliquées » Strasbourg, 28.I.1981 , sur le site suivant ; http://conventions.coe.int/treaty/fr/treaties/html/108.htm

[222]- من القضايا التي تخص هذه الحالة والتي طرحت على القضاء الفرنسي، نجد قضية شركة النشر والإصدار Neressis ضد الشركة ذات المسؤولية المحدودة Arkadia ، حيت ارتكت Stéphane V.C لصالح هذه الأخيرة والتي يعمل بها وفي اطار المنافسة غير المشروعة

عامل وليس له علاقة بالدخول إلى النظام، أو كان الدخول يتوقف على عضوية في جهة معينة أو يتطلب كلمة سر أو دفع مبلغ معين [223]، أو حالة أن يكون هناك تصريح جزئي والمصرح له يتجاوز

بدخوله غير المشروع لنظام المعالجة الآلية لشركة النشر والإصدار Neressis (اسم المجال www.pap.fr) وقام كذلك بالتعدي على المصنفات الفكرية من خلال الاستنساخ والنشر على الموقع الالكتروني Arkadia.com نماذج لعقود ونماذج لرسائل وخطابات منشأة وتسويقية من قبل شركة Neressis، كما قام في نفس الظروف باستخراج محتويات قاعدة بيانات هته شركة فضلا عن جمع المعلومات الشخصية بما في ذلك رقم الهاتف والبريد الالكتروني لبعض الأشخاص المحددين: كانت هذه العملية قد تضمنت مختلف اشكال الجرائم المعلوماتية وهي الدخول والبقاء غير المشروع في هدمة التجهيز الالي للمعلومات والممنوع اطلاقا الوصول اليه والجمع بطريف غير مشروع لقاعدة البيانات التي تم الدخول اليها بدون تصريح، وكذا الجمع غير المصرح للمعلومات الشخصية ...

T.G.I Pris, 13 éme ch, 18 septembre 2008.

مشار اليه لذى: أ.رشيدة بوكر، مرجع سابق، ص 193 نقلا عن الموقع الالكتروني لي المحامية ألن بنسوسان www.alain-bensoussan.com

[223]- لعل اكبر تحديد لمفهوم الدخول غير المصرح كان أمام محكمة كنساس العليا سنة 1996 في قضية الولاية ضد " Allen" وتدور وقائع القضية حول قيام هذا الأخير باستخدام حاسبه بشكل مستمر بنظام dail up الاتصال الهاتفي بالشبكة وذلك للاتصال بحاسب شركة الهاتف الجنوبية– الغربية التي تتحكم في تحويلات الاتصالات البعيدة المدى والتلاعب بها بحيث تسمح للمستخدم بالقيام بمكالمات بعيدة المدى مجانا، وعندما اتصل Allen بحاسبات الشركة المذكورة واجهته شاشة تطلب منه اسم المستخدم و كلمة العبور، ولقد اتضح للمحققين أن Allen خمن كلمة العبور بدقة وقام لاحقا بإزالة الدليل على نشاطه بإلغائه للسجلات، ولقد أعد المعمل الجنائي فقط ما يقرر أن Allen قام باستخدام الاتصال الهاتفي بالشركة المذكورة ورأى مؤشر كلمة العبور، ودافع المتهم أمام المحكمة بأنه لا يوجد دليل على دخوله الحاسب الآلي للشركة، إلا أن الادعاء اعتمد على تعريف التشريع الواسع لعبارة Access وذلك لعموميته بين التشريعات الولائية لجرائم الحاسب الآلي، والذي يقرر أن الدخول يعني الاقتراب أو إصدار أمر أو الاتصال بـ ....أو تخزين بيانات ... أو استرداد بيانات ....أو أية اشياء أخرى تؤدي إلى استخدام مصادر الحاسب الآلي، لكن المحكمة أجابت بأن هذا التعريف كان من الاتساع بحيث لو اخذ بجدية فإنه يؤدي إلى القول بعدم دستورية التشريع لغموضه، ولقد لاحظت انه إذا كان الدخول بعني الاقتراب من أية جهاز حاسب ألي مادي بدون تصريح يمكن أن يشكل جريمة، فهذا تعريف واسع لا يمكن تطبيقه، وانتهت المحكمة إلى ان المعنى الكامل والعادي يجب أن يطبق عوضا عن الترجمة المشوهة للتعريف المتوافر.

ولقد فسرت المحكمة ذلك بقولها: يعرف قاموس « Webster» الدخول كحرية أو قابلية للحصول أو الاستخدام، وهذا مشابه للبناء الذي أعدته محكمة الموضوع للوصول إلى عدم وجود دليل ظاهر يقرر أن المتهم تحصل على دخول إلى حاسبات الشركة، فحتى مرحلة ما قبل قيام المتهم بوضع اسمه وكلمة العبور على المكان المقرر في موقع الشركة لا يمكن القول بأن لديه القابلية لاستخدام حاسبات الشركة والحصول على أي شيء، وعليه لا يمكن القول بأن دخوله إلى نظم حاسبات الشركة هو أمر معروف بشكل عام، بحيث اذا كان الاسم صحيح وكلمة العبور تسمح بالدخول إلى الملفات المتواجدة في الداخل وأن الاسم الخاطئ وكلمة العبور غير الصحيحة امنع المستخدم من الدخول، وبغياب الدليل بأن Allen قد دخل عبر بحثه على كلمة العبور للوصول إلى المعلومات بالداخل فان ذلك يؤدي إلى القول بعدم دخوله إلى حاسبات الشركة/ مشار إلى هذه القضية لدى: أ.رشيدة بوبكر، مرجع سابق، ص 184، نقلا عن **أورين كير** ،ترجمة د. **عمر بن يونس** ، نطاق الجريمة

حدود هذا التصريح كالعامل أو الموظف الذي يتجاوز حدود صلاحيات التصريح أو اختصاصه ويدخل في المجال الغير مرخص له الدخول فيه، لذلك من الأفضل تحديد صلاحيات واختصاص كل عامل بالنظام بموجب نظام داخلي.

وقد اعتبر الفقه والقضاء من قبيل حالات تجاوز التصريح متى استعمل التصريح الممنوح للفاعل في غير الغرض المخصص له أو الوقت المحدد له.

وفي حالة تجاوز التصريح الزمن المحدد له فهي مسألة نتحدث عنها فيما يتعلق بجريمة البقاء غير المصرح به داخل النظام،أما تجاوز مجال التصريح والغرض المخصص له فسوف نحاول توضيحه.

فبالنسبة لتجاوز مجال التصريح فهو ما عبر عنه المشرع بقوله في جزء من النظام [224]، بمعنى أن التصريح مخصص لجزء من النظام وليس شامل لكل النظام، ومن يتعدى ذلك الجزء يكون قد اخترق النظام وتعدى مجاله إلى الأجزاء الأخرى، وفي هذه الحالة يعد غير مصرح له أو بدون حق و إن كان يملك حق الدخول إلى الجزء[225].

وفي الغالب وكما سبق الإشارة إليه أن هذا النوع من الدخول يصدر من العاملين في المؤسسات والذين لديهم تصريحات جزئية لاماكن معينة ومحددة بحسب الوظيفة التي يؤديها كل عامل، وهو الفعل الذي يترتب عليه تشديد العقوبة كون العامل كان في مركز سهل عليه ارتكاب الجريمة، وكون انه بذلك قد خان الأمانة وثقة التي وضعها فيه رب العمل بدخوله إلى مجال ليس مصرح له بالدخول فيه، وهذا ما لم ينص عليه المشرع الجزائري [226] صراحة في المواد السابقة، وإن كان المنطق القانوني والعقلي يقتضي تشديد العقاب لأن الجدير بالعامل الحفاظ على الثقة وحماية النظام وتقدير الوظيفة المنوطة به، ولا يشكل تهديدا لقواعد الامن المعلوماتي.

و على غرار المشرع الأردني وضح هذه المسألة و نص صراحة على تشديد العقاب من خلال المادة 7 من القانون السالف الذكر بقولها:" تضاعف العقوبة على الجرائم المنصوص عليها في المواد من 3

الافتراضية، تفسير الدخول والتصريح به في إطار تشريعات الإساءة إلى الحاسب الآلي، بحث منشور في مجلة القانون، جامعة نيويورك، العدد 78 نوفمبر 2003 ، ص 37،38.

1- تنص المادة 394 مكرر على انه" كل من يدخل.....في كل أو جزء من منظومة للمعالجة الآلية للمعطيات" وكذلك المادة 3 من القانون الأردني لجرائم أنظمة المعلومات لسنة 2010 بقولها:" كل من دخل قصدا إلى موقع الكتروني أو نظام معلومات بأي وسيلة دون تصريح أو بما يخالف التصريح....."

[225]- د. **أيمن عبد الله فكري** ، مرجع سابق، ص 201. ود. **محمد حماد مرهج الهيتي** ، مرجع سابق، ص 184. **ونهلا عبد القادر المومني**، مرجع سابق، ص156.

[226]- نفس الأمر بالنسبة للمشرع الفرنسي الذي جانب النص عليه في تعديله لقانون العقوبات.

إلى 6 من هذا القانون بحق كل من قام بارتكاب أي منها أثناء تأدية وظيفته أو عمله أو باستغلال أي منها"

هذا وقد يشكل تجاوز الصلاحيات أو التصريح الجزئي أو مخالفته مشاكل عديدة خاصة في حالة إثبات القصد الجنائي لذا من يملك تصريح جزئي وهل تعديه كان عن خطأ أو متعمد بحكم له صلاحية الدخول؟.

و كما ضحنا فان المشرع الجزائري فصل في ذلك وعاقب كل من دخل بغش أو بدون تصرح في كل أو جزء من نظام المعالجة الآلية للمعطيات.

أما في حالة تجاوز الغرض المخصص للتصريح بالدخول إلى النظام واستعماله في غير اختصاصه فإن الآراء الفقهية والقضائية تضاربت بخصوص هذا الشأن [227]، وما يهمنا موقف المشرع الجزائري الذي كان صريح بان مجرد الدخول بغش أو بدون تصريح يشكل جريمة في حد ذاتها، وان عدم الصلاحية تتحدد في الدخول سواء في الكل أو الجزء من النظام، وهذا كذلك موقف المشرع الأردني.

3- ضرورة وجود نشاط يسبق فعل الدخول

إن جريمة الاختراق وكما سبق أن رأينا تتحقق بعدة وسائل وأساليب، وبالتالي هل يشترط المشرع طريقة معينة يتحقق بها الدخول؟ وهل في الحالة التي يصادف فيها الشخص أن يجد معلومات سرية على شاشة الجهاز ويقراها دون أن يسبق ذلك أي فعل، فهل يشكل ذلك جريمة الدخول بدون إذن؟

بالرجوع إلى النص القانوني الجزائري لا نجد أي إشارة إلى ذلك، وعملا بالنص القانوني الفرنسي (المادة 1/323 عقوبات) لم يشر المشرع إلا على فعل الدخول المجرد إلى كل أو جزء من النظام، وعبر عنه المشرع الأردني في المادة 03 بقوله مهما كانت الوسيلة التي دخل بها.

ثانيا: فعل البقاء

إن النشاط الجرمي الذي يتكون منه الركن المادي لهذه الجريمة- الدخول والبقاء غير المشروع – قد يتخذ صورة البقاء داخل النظام، فما المقصود بالبقاء؟ وما يميز هذا السلوك عن ما يشبهه من السلوكات غير مشروعة؟

---

[227]- في هذا المعنى بخصوص القضايا والآراء التي جاءت بحكم تجاوز الغرض المخصص للتصريح بالدخول لدى: د. **نائلة محمد فريد قورة**، المرجع السابق، ص 340 وما بعدها.

لم يحدد المشرع الجزائري شأنه شان معظم التشريعات التي نصت على جرائم تقنية المعلومات، مفهوما للبقاء غير المشروع، وتولى الفقه ذلك حيث تعددت التعريفات التي قيلت بشأنه ومن بينها ما يلي:

عرف بأنه" التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام"[228]

وقيل انه "مشاركة ذات سيطرة من المخترق على عمليات الحاسوب – النظام المعلوماتي – خلال حركة الدخول والخروج"[229].

أو انه كذلك " فعل الاتصال بعد أن توافر للشخص العلم بكونه نظاما ممنوعا الدخول له واتجاه إرادته إلى البقاء على هذا الاتصال الذي حدث بطريق الخطأ"[230].

و بالتالي فهو فعل يتم من خلاله البقاء داخل النظام المعلوماتي بعد الدخول إليه خطأ أو بالصدفة، ولكن الجاني بالرغم من علمه بعدم مشروعية البقاء ضل مستمرا في الاتصال بالنظام والتجول فيه ضد إرادة من له الحق في السيطرة على هذا النظام.

وما تجدر الإشارة إليه هو أن معاهدة بودابست بشأن الجرائم الالكترونية على خلاف الاتفاقية العربية لجرائم تقنية المعلومات، لم تشر إلى هذا الفعل في المادة السادسة وإنما نصت على فعل الدخول غير المصرح فقط ، وتركت تجريم ذلك إلى التشريعات الوطنية فيما تراه مناسبا من الأفعال.

وهو شأن المشرع الأردني الذي لم ينص صراحة على تجريم هذا السلوك [231]، مما قد يترتب على القضاء في كل حالة ينظرها أن يبحث فيما إذا كان البقاء غير المشروع بعد أن تم الدخول خطأ أو سهوا إلى النظام المعلوماتي؟ وهل يأخذ حكم الدخول غير المشروع أم لا؟ أو كيف بكون الحكم في هذه الحالة؟

مما يستوجب على المشرع الأردني التدخل من جديد وتجريم هذا الفعل، لان القانون المؤقت رقم 30 لسنة 2010 بهذا يكون غير كافي، خاصة إذا كان الدخول إلى النظام مشروع ولكن البقاء فيه غير

---

[228]- **علي عبد القادر قهوجي** ، الحماية الجنائية لبرامج الحاسب الآلي ، مرجع سابق ، ص 133.

[229]- د. **عمر محمد أبو بكر بن يونس**، مرجع سابق، ص 332.

[230]- د.**أيمن عبد الله فكري**، المرجع السابق، ص 338.

[231]- لا يعاقب **القانون الأردني** بشأن جرائم تقنية المعلومات من دخل عن طريق الخطأ أو بالصدفة واستمر بالاتصال بهذا النظام ما لم يوجد نص صريح يعاقب على ذلك.

مشروع أو محدد، أوان الدخول إلى النظام كان خطأ والاستمرار في الاتصال به غير مشروع بالرغم من علم الجاني بذلك[232].

على غرار بعض التشريعات التي اتجهت إلى النص صراحة على تجريم البقاء غير المشروع، ومن بينها التشريع الفرنسي الذي جرم الدخول أو البقاء غشا في كل أو جزء من نظام المعالجة الآلية للمعطيات من خلال المادة[233] 323-1 عقوبات فرنسي المعدل والمتمم[234].

وما يمكن الإشارة إليه كذلك بالنسبة للتشريع الفرنسي انه تم استدراك هذا الفعل، وإدراج الجزء الخاص بالبقاء غير المصرح به إلى النص الفرنسي أثناء القراءة الأولى للقانون داخل مجلس الشيوخ الفرنسي، على إثر التقرير الذي تقدم به احد الأعضاء [235]، كون النص في صياغته الأولى يحكم فقط فعل الدخول غشا، وغير كافي للتطبيق على الحالة التي يتم فيها الاستمرار في البقاء بالنظام بعد أن تم الدخول خطأ أو بالصدفة[236].

هذا وقد طبق القضاء الفرنسي نص البقاء غير المشروع (المادة 323-1 عقوبات) في حكم شهير لمحكمة استئناف باريس في 5 ابريل 1994 حيث ذهبت المحكمة فيه إلى القول بأن: "القانون يجرم البقاء غشا داخل نظام المعالجة الآلية للمعطيات سواء كان الدخول قد تم عن طريق الإهمال أو الخطأ

---

[232]- يرى **جانب من الفقه** ان الدخول يكون مشروعا اذا كان بطريق المصادفة أو الخطأ أو سهوا، وكان من الواجب عند ذلك أن يقطع تواجده وينسحب فورا، فإذا بقي رغم ذلك يعاقب: أنظر في ذلك / **علي عبد القادر قهوجي** ، الحماية الجنائية للبيانات المعالجة الكترونيا، بحث مقدم لمؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، دولة الإمارات العربية المتحدة في الفترة ما بين 1-3 ماي 2000.

[233]- تقابلها المادة **394مكرر عقوبات جزائري** ، ومن بين التشريعات العربية التي نصت على جريمة البقاء المرسوم العماني رقم 2011/21 المتعلق بقانون مكافحة جرائم تقنية المعلومات المادة 3 منه .

[234] - **Art 323-1 de C.P.F** : « …….ou de se maintenir….. »

[235]- يتمثل في نص الاقتراح الذي تقدم به العضو " **Jaque Thyraud**" إلى مجلس الشيوخ واخذ به عند الصياغة النهائية للنص.

[236]- هناك جانب من الفقه يرى أنه لا داعي لتجريم هذا الفعل لأنه في الغالب يكون متضمنا في أفعال أخرى، انظر في الآراء المتعلقة بهذا الشأن كل من : د.**نائلة عادل فريد قورة** ، مرجع سابق، ص 395-397/ كذلك د. **أيمن عبد الله فكري**، مرجع سابق، ص 241.

أو تم بطريقة مشروعة إلا أنه اكتسب بعد ذلك صفة اللاّمشروعية كما لو فقد الفاعل حقه في البقاء ...نتيجة لخطأ من جانبه" [237] .

وفي حكم أخر لها بتاريخ 15 ديسمبر 1999 عندما أدانت بتهمة البقاء داخل نظام المعالجة الآلية الموظفين في ANPE الذين استخدموا Minitel الذي وضع تحت تصرفهم من قبل رب عملهم في أغراض مهنية فقط، وأفرطوا أو تجاوزوا مدة البقاء في هذه الأجهزة....."[238].

أما بالنسبة للمشرع الجزائري فقد نص صراحة على جريمة البقاء غير المشروع ضمن نفس المادة التي جرمت فعل الدخول، ومن أول ما أضافها واعتبره سلوك منفصل أو مستقل عن فعل الدخول بقوله في المادة 394 مكرر عقوبات:" يعاقب....كل من يدخل أو يبقى...."[239].

---

[237] -« …..La loi incrimine également le maintien frauduleux dans un système de la part de celui qui y serait entre par inadvertance, ou de la part de celui qui, y ayant régulièrement pénètre, se serait maintenu sur un système frauduleusement ;

Lorsque l'accés a été régulier, le maintien sur un système automatisé de données peut devenir frauduleux, lorsque par une sorte d'interversion de titre, l'auteur du maintien se trouve privé de tout habilitation » C.A de paris,5 avril 1994, NCP, 104° édition, D, paris ;2009, P 916.

مشار إليه لدى أ.**رشيدة بوكر**، مرجع سابق، ص 217 وما يليها.

وكذلك قد قضت محكمة استئناف باريس في حكم سابق لها بتاريخ 4 ديسمبر 1992 أنه" لما كان من الثابت أن حيازة كود العبور كان نتيجة خطأ في التعامل مع الملفات، فإن هذا الواقع يستبعد الطابع المتعمد الذي يقتضيه القانون، وبالتالي فإن الدخول تم بطريق الخطأ أو المصادفة لا يعاقب عليه، إلا انه يجب ألا يحتفظ بالبقاء الذي تم التوصل اليه بطريق الخطأ أو المصادفة

Dans un arrêt du 4 décembre 1992, la cour d'appel de paris a écarté les délits d'accès et de maintien dans un système de traitement automatisé de données informatiques en constatant que l'appropriation d'un code d'accès avait pu être le résultat d'une erreur de manipulation sur les fichiers , cette circonstance excluant le caractère intentionnel exigé par la loi . Ainsi, une intrusion accidentelle ne peut étre incriminée, encore faut il ne pas se maintenir dans le STAD accidentellement atteint.

C.A de paris,4 décembre 1992 disponible a l'adresse suivante ; http://www.murille-cahen.com/p-references.asp

[238] -« on été reconnus coupables de maintien frauduleux dan un systéme informatisé de données des employés de l'AMPE qui ont utilisé des minitel, mis à leur disposition par leur employeur dans un but exclusivement professionnel, et ont abusivement prolongé leur maintien dans ces appareils à l'insu de leur entourage afin de se connecter à des services de jeux ». C.A de paris, 15 décembre 1999,D ,2000,I.R cité par Philippe Andrieu, stad, Accés et maintien frauduleux.

مشار إليه لدى أ.**رشيدة بوكر**، مرجع سابق، ص 218.

[239]- حسن فعل المشرع العماني بتجريمه فعل البقاء بقوله في المادة الثالثة من المرسوم السلطاني رقم 2011/21 المتعلق بقانون مكافحة جرائم تقنية المعلومات "..... يعاقب بالسجن مدة لا تقل عن شهر ولا تزيد على ستة أشهر وبغرامة لا تقل عن مائة ريال عماني ولا تزيد على خمسمائة ريال عماني أو بإحدى هاتين العقوبتين، كل من دخل عمدا ودون وجه حق موقعا

أسوة بالمشرع الفرنسي، ورغبة منه في منع أي تهرب من العقاب أو للإدانة في الحالات التي يتم فيها الاتصال بكل أو جزء من النظام المعلوماتي والاستمرار فيه بعد الاتصال خطأ أو صدفة.

و يتمثل الركن المادي لهذه الجريمة في البقاء داخل النظام وعدم قطع الاتصال بالرغم من علم المخترق انه غير مصرح له البقاء فيه.

ذلك إن البقاء غير المشروع في النظام المعلوماتي يفترض فيه الاستمرار لوقت معين، فهو يتخذ صورة الجريمة المستمرة[240]، وقد يأخذ فعل البقاء صور متعددة منها تجاوز الوقت المسموح للبقاء فيه داخل النظام، ويمكن أن يكون البقاء لاحقا على دخول غير مشروع ويمكن أن يكون لاحقا على دخول مشروع إذا تجاوز الوقت المسموح به[241] أو الغرض الأساسي لهذا الدخول.

و في الحالة التي يكون فيها الدخول غير مشروع والبقاء غير مشروع مثل من لا يكون له الحق في الدخول إلى النظام ويدخل إليه فعلا ضد إرادة من له الحق في السيطرة عليه، ثم يبقى داخل النظام بعد ذلك، فهنا تجتمع الجريمتين أو ما يسمى بالاجتماع المادي للجرائم [242]، غير أن المشرع لم يفرق بينها من ناحية العقاب حيث جعل العقاب واحد سواء اجتمعت الجريمتين أو تحققت إحداهما دون الأخرى.

و قد ثار خلاف فقهي حول تجريم هذا الفعل، حيث يرى البعض أن جريمة البقاء غي ر المشروع يمكن الاستغناء عنها وعدم تجريمها في قانون العقوبات وذلك الأسباب التالية:

- أن هذا الفعل في الغالب يكون متضمنا في أفعال أخرى قد تغني عنه، ولا يكون في تجريمه فائدة[243].
- أن جريمة الولوج غي المشروع تكفي لتجريم هذا الفعل، لان العبرة بتحقق القصد الجنائي سواء تحقق عند الولوج أو بعد ذلك، فمن يدخل عن طريق الخطأ لن تتم مساءلته ولكن من يدخل

إلكترونيا أو نظاما معلوماتيا أو وسائل تقنية المعلومات أو جزءا منها أو تجاوز الدخول المصرح به إليها أو استمر فيها بعد علمه بذلك".

[240]- د.**نائلة عادل محمد فريد قورة**، مرجع سابق، ص 361.

[241]- د. **أيمن عبد الله فكري**، مرجع السابق، ص 238.

[242]– **أمال قارة**، مرجع سابق، ص 110.

[243]– د.**نائلة عادل محمد فريد قورة**، مرجع سابق، ص395

بطريق الخطأ ثم تتحقق لديه نية البقاء في النظام المعلوماتي بعد ذلك فانه يكون مسئولا عن جريمة الولوج غير المشروع وليس البقاء غير المشروع[244].

إضافة إلى ذلك فان هذه الجريمة ليس من السهل إيجاد دليل لإثباتها [245]، و انه من الممكن أن تكفي عنها أفعال أخرى مثل تجريم الاطلاع غير المشروع على المعلومات.

كما يمكن للمتهم أن يدعي أنه في كل مرة كان يحاول أو كان على وشك الانفصال عن النظام المعتدي عليه عند علمه بعدم مشروعية الاتصال به، وهذا ما قد يفتح باب لإمكانية الإفلات من العقاب أو المساءلة الجنائية.

و إضافة إلى ذلك و حتى نستطيع فهم هذا السلوك أو الفعل الذي قد يتداخل مع أفعال أخرى مثل الدخول غير المصرح به أو الاستعمال غير المصرح للنظام المعلوماتي، نقوم بتمييزه عن تلك الأفعال:

*** تمييز البقاء غير المشروع عن الدخول غير المشروع**

بالرجوع إلى المادة 1/232 عقوبات فرنسي وتنطبق أحكامها على المادة 394مكرر عقوبات جزائري باعتبار أنها مستوحاة منها، نلاحظ أنهما تتضمنان فعلي الدخول والبقاء غير المصرح بهما معا في نص واحد، على خلاف بعض التشريعات التي لم تتضمن فعل البقاء ونصت على فعل الدخول المجرد والمرتب للنتيجة الجرمية، منها التشريع الأردني لسنة 2010، وتشريعات أخرى فرقت بين الفعلين في نصوص متفرقة مثل التشريع الفدرالي الأمريكي الذي نص على فعل البقاء في المادة 1030 (هـ)(6)[246].

و قد أثار هذا الأسلوب في المعالجة القانونية لهذا السلوك جدلا فقهيا حول مدى انطباق البقاء مع الدخول؟

اختلفت الآراء حول إمكانية الجمع بين الدخول والبقاء بين الاتجاهين التاليين:

الاتجاه الأول : يرى إمكانية الجمع بين الدخول والبقاء بحجة أن البقاء لا يكون فقط عندما يكون الدخول مشروعا، ذلك انه بعد كل دخول غير مشروع هناك بقاء غير مشروع أي أن هناك دائما جمع بينهما، كما يرى أصحاب هذا الاتجاه انه ليس من العدالة أن يتساوى من دخل النظام ثم خرج منه

---

[244]– د. **أيمن عبد الله فكري**، مرجع سابق، ص 241.

[245]– د.**محمد سامي الشوا**، ثروة المعلومات، مرجع سابق، ص 181/ **نهلا عبد القادر مومني**، مرجع سابق، ص 161.

[246]- أ. **رشيدة بوكر**، مرجع سابق، ص 218.

مع من دخل ثم بقي فيه، أي بين من ارتكب جريمة واحدة مع من ارتكب جريمتين، وأن الأخذ بهذا الرأي يشجع على العدول عن جريمة البقاء لمن ارتكب جريمة الدخول.

وعلى خلاف الاتجاه الأول يرى أنصار **الاتجاه الثاني**[247] – وهو الاتجاه الغالب – بان كل جريمة تقع مستقلة عن الجريمة الأخرى، وأن لكل جريمة سلوكها الإجرامي الخاص بها دون الأخرى، ويستند هذا الرأي على حجتين، أولها استمدها من المبادئ التي تحكم تفسير القانون، وهي تقضي بان المشرع عندما يستخدم كلمتين أو مصطلحين مختلفين فلابد أن يكون لكل مصطلح معناه ومدلوله، فمصطلح "الدخول" لا يحتوي مصطلح "البقاء" والعكس صحيح.

و ثانيهما فسندها المنطق، وهي أن صفة الغش لا تنطبق على الدخول فقط وانما تنطبق على البقاء أيضا.

و هناك من يرد على الاتجاه الأول إلى أن الفرق بين الجريمتين، هوان الدخول جريمة مؤقتة أما البقاء فهي جريمة مستمرة [248]، وحيث أن الدخول يجرم فعل تخطي الحد أو تعدي النظام بدون وجه حق، فيما البقاء فإنه يجرم فعل الاستمرار أو التواجد داخل النظام.

كذلك يرى البعض أن الاختلاف بين جريمة الدخول غير المصرح به إلى نظام الحاسب الآلي، وجريمة البقاء في هذا النظام بعد دخوله عن طريق الخطأ، يتمثل في أن الأولى جريمة ايجابية من ناحية ووقتية[249] من ناحية أخرى، أما الثانية فهي جريمة سلبية من ناحية ومستمرة [250] من ناحية أخرى، لذلك لا يمكن الجمع بينهما في نص قانوني واحد نظرا لاختلاف الطبيعة القانونية لكل منهما.

إلا أنه إذا كان هذا الرأي صائب من ناحية الدخول غير المصرح به يشكل جريمة ايجابية ومؤقتة، فإن البعض[251] لا يتفق معه في كون البقاء غير المصرح به يشكل سلوكا سلبيا، كون الامتناع عن الخروج من النظام الذي تم الدخول إليه ليس هو مناط التجريم بل البقاء والاستمرار في النظام دون وجه حق هو مناط التجريم.

247- **رشيدة بوكر**، مرجع سابق، ص 219.

248- **نائلة عادل محمد فريد قورة**، مرجع سابق،ص 348.

249– **الجريمة الوقتية :** هي "التي يتكون ركنها المادي من تصرف يقع في وقت محدد أوفي فترة زمنية قصيرة وتنتهي بوقوع الجريمة" **نهلا عبد القادر مومني** مرجع سابق، ص 162.

250– **الجريمة المستمرة:** هي "التي يتكون ركنها المادي من تصرف أو حالة تحتمل بطبيعتها الاستمرار لفترة زمنية غير محددة من الوقت" مشار إليه لدى نفس المرجع، ص 161.

251– نائلة **عادل محمد فريد قورة**، نفس المرجع، ص 349.

***البقاء غير المصرح به وسرقة وقت نظام المعالجة الآلية:**

قد يشتبه البقاء غير المصرح به في نظام المعالجة الآلية مع مفهوم سرقة وقت نظام المعالجة الآلية، الذي يعرفه الفقه على أنه "كل استعمال للوظيفة التي يؤديها الحاسب الآلي خلال فترة زمنية دون أن يكون مصرحا بذلك للفاعل"[252]، أو هو "الاستخدام الذي يصدر ممن ليس له الحق"[253].

وبذلك فإن الاستعمال غير المصرح به لنظام المعالجة الآلية يتمثل في إشغال وقت أو خدمات النظام المعلوماتي دون ترخيص أو تصريح من صاحب العمل أو تجاوزه.

ولقد اختلفت التشريعات المقارنة في طريقة تجريمها لهذا الفعل، فمنها من جرمها صراحة وفي نص خاص مثل تشريعات بعض الولايات المتحدة[254]، ومنها من أدرجها بشكل عام ضمن المواجهة الشاملة للاستخدام غير المشروع لمال لغير.

و بخصوص المشرع الجزائري لم يستعمل هذا المصطلح لا من قريب ولا من بعيد، ولم يشر إليه في المواد التي تجرم المساس بأنظمة المعالجة الآلية، مما يسمح لمرتكبي هذا الفعل الإفلات من العقاب، وبهذا يجب على المشرع التدخل واستدراك الأمر من جديد.

و نفس الأمر بالنسبة للمشرع الفرنسي رغم إفراده فصلا لجرائم المعالجة الآلية للمعطيات من المواد 323-1 إلى 323-7 إلا انه لم يتضمن نصا صريحا يجرم سرقة منفعة الحاسب كما جرم الدخول والبقاء غشا، وعلى ذلك ثار خلاف فقهي حول تجريم هذا الفعل وتكييفه.

حيث اتجه البعض[255] إلى القول بأنها جريمة يعاقب عليها بموجب المادة 323-1 وحجتهم في ذلك أن كل استعمال غير مصرح به لنظام المعالجة الآلية لابد أن يسبقه دخول غير مصرح به، سواء كان هذا الدخول مباشرة أو تم عن طريق البقاء داخل النظام.

و انتقد جانب آخر هذا التحليل و قالوا بعدم ملائمة تطبيق النص 323-1 على هذا الفعل، وحجتهم في ذلك أن جريمة الدخول غير المصرح به هي من الجرائم الوقتية تتم بمجرد الدخول إلى النظام، أما

---

[252]- د. **خالد ممدوح إبراهيم** ، امن الجريمة الالكترونية، مرجع سابق، ص 89/ كذلك د. **أيمن عبد الله فكري** ، مرجع سابق، ص 240.

[253]- د. **هدى حامد قشقوش**، المرجع السابق، ص 81.

[254]- **رشيدة بوكر** ، مرجع سابق، ص 221/ وكذا : **محمود أحمد عبابنة** ، جرائم الحاسوب وإبعادها الدولية، الأردن، 2005، ص91.

[255]-**Vivant(M) et Le Stanc (Ch)**,Lamy droit de l'informatique,1989,N° 2479, p 1504.

مشار اليه لدى:د. **أيمن عبد الله فكري**،مرجع سابق، ص 240.

جريمة الاستعمال غير المصرح به تدخل ضمن الجرائم المستمرة كونها تقوم على فعل يستمر فترة من الزمن داخل نظام الحاسب الآلي.

كما أن البقاء غير المصرح به، و ان كان يمثل بدوره سلوك يستمر لفترة من الزمن، إلا انه يختلف عن الاستعمال غير المصرح به، كونه يمثل مجرد التواجد السلبي داخل النظام، في حين الاستعمال غير المصرح به هو استخدام للوظائف التي يقدمها النظام، أو استغلال لمنفعة الحاسب.

وكذلك يرجع السبب من وراء عدم ملائمة المادة 323-1 على هذا الفعل يرجع إلى العلة من تجريم الدخول أو البقاء غشا، وهي الحماية من الوصول إلى المعلومات غير مسموحة أو سرية، في حين ترجع علة تحريم الاستعمال غير المصر ح به الى حماية النظام نفسه من استخدام الوظائف التي يقدمها بطريقة غير مشروعة[256].

وأمام غياب نصوص صريحة للعقاب على الاستعمال غير المصرح به برزت اتجاهات [257] أخرى ترى تطبيق نصوص قانونية محددة على هذا الفعل، حيت ذهب يعضهم إلى تطبيق بعض نصوص قانون العقوبات الخاصة بالسرقة والنصب وخيانة الأمانة، في حين ذهب البعض الأخر إلى تطبيق نصوص جريمة أخرى هي إخفاء الأشياء الأخرى المتحصلة من الجريمة ولكن بالمفهوم الجديد لفكرة الإخفاء، ولكن كل هذه الآراء تعرضت للنقد.

أما بخصوص موقف القضاء المقارن، فنجد القضاء الأمريكي والذي كان يجد صعوبة في تطبيق النصوص المتعلقة بالاستعمال غير المصرح به، حيث يعد حكم محكمة أنديانا في قضية " Mc Graw" الذي انتهى بإدانة المتهم عن الاستعمال غير المصرح به تعد من أشهر القضايا وأقلها التي استطاعت فيها المحاكم أن تطبق النصوص القائمة على الاستعمال غير المسموح به لنظام الحاسب الآلي[258]، وكان هذا الحكم دافعا لإصدار بعض النصوص التي تجرم هذا الفعل صراحة خاصة مع الانتشار الواسع لاستعمال الحاسبات والأنظمة المعلوماتية.

وبعد استعراض الاتجاهات الفقهية المختلفة وأمام انعدام نصوص قانونية صريحة لتجريم فعل الاستعمال غير المصرح للنظام المعلوماتي وعدم ملائمة النصوص القائمة وعجزها عن التطبيق، مما

---

[256]- د: **نائلة عادل محمد فريد قورة**، مرجع سابق، ص 396 وما بعدها.

[257]– لمزيد من التفاصيل حول هذه الآراء لدى: **محمود أحمد عبابنة** ، مرجع سابق، ص 89/**نائلة عادل محمد فريد قورة** ، المرجع نفسه، ص 397-405.

[258]– ملخص وقائع القضية لدى: د. **نائلة عادل فريد قورة**، مرجع سابق، ص 390.

يؤثر سلبا على أحكام القضاء الذي قد يجد صعوبة في الفصل في الدعاوى المتعلقة بهذا الاستعمال غير المشروع خاصة مع الاستعمال المتزايد للحاسب الآلي والشبكات المفتوحة واقتحامها مختلف المجالات والقطاعات ونواحي الحياة، يستدعي ضرورة التدخل التشريعي والتنبه لخطورة هذا السلوك.

البند الثالث: محل النشاط الجرمي

نلاحظ من خلال المادة 394 مكرر عقوبات جزائري أن المشرع جرم الدخول أو البقاء عن طريق الغش في كل أو جزء من نظام المعالجة الآلية للمعطيات وهو المحل الذي ينصب عليه فعل الدخول أو البقاء.

وبالرجوع إلى القانون رقم 04/09[259] نجد المادة 2/ب منه قد عرفت المنظومة المعلوماتية على أنها: "نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين" .

والملاحظ على هذا التعريف أنه جاء موسعا [260]، فيكون بذلك المحل الذي ينصب عليه سلوك الجاني في جريمة الدخول أو البقاء غشا يتسع ليشمل المعلومات والنظام الذي يشملها كالحاسب الآلي فضلا عن الشبكات ذاتها.

ونفس الوضع بالنسبة للقانون الفرنسي باعتباره الأسبق في وضع نصوص للمعاقبة على جرائم نظم المعلومات، حيث نص على المحل الذي ينصب عليه فعل الدخول أو البقاء والمتمثل في نظام المعالجة الآلية للمعطيات من خلال المادة 323-1 عقوبات، حيث تعتبر هذه المادة أن الدخول إلى النظام بأكمله أو إلى جزء منه شرط جوهري لقيام الجريمة [261]، أي أن الجريمة لا تقوم إذا كان الدخول إلى المعلومات بمعزل عن نظام المعالجة الآلية.

كما أن الفقه الفرنسي أجمع [262] على أن نظام المعالجة الآلية طبقا للمادة 323-1 ينصرف إلى المعلومات والنظام الذي يحتوي عليها، وكذلك إلى الشبكات

---

[259]- القانون **رقم 04/09** المؤرخ في 05 أوت 2009 ***يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها***، جريدة رسمية عدد 47، ص 05 ، بتاريخ 16 أوت 2009.

[260]– نفس الملاحظة بالنسبة للمشرع الأردني نجده قد وسع من مفهوم النظام المعلوماتي

[261] -**Michel Veron**, droit pénal spécial,6 édition, Armand colin, paris,1998,p258. مشار إليه لدى أ. **رشيدة بوكر**، ص 244

[262]- **رشيدة بوكر**، المرجع نفسه، ص 224.

إضافة إلى ذلك نجد أن المناقشات السابقة على تبني قانون رقم 88-19 أحالت في تعريف نظام المعالجة الآلية للمعطيات إلى التعريف الوارد لها في القانون الصادر عام 1978 بشأن المعلوماتية وحماية الحريات[263].

ولقد أدى التوسع في مفهوم نظام المعالجة الآلية وفقا للقانون الفرنسي إلى أن التقاط الإشارات الناجمة عن تبادل المعلومات عبر شبكات المعلومات يعتبر دخولا لنظام المعالجة الآلية الذي يحتوي على هذه المعلومات[264].

كما أن القضاء الفرنسي وسع من مفهوم نظام المعالجة الآلية في عدة أحكام له واعتبر من قبيل أنظمة المعالجة الآلية" **un disque dur**"[265] و" **un radiotéléphone**"[266] و" **le réseau Carte bancaire**"[267].

كذلك بالرجوع إلى التقريري التفسيري لاتفاقية بودابست بشأن الإجرام السيبرني، نجدها قد أشارت إلى أن الدخول يتضمن التسلل على السلامة أو أي جزء لنظام المعلومات (الجهاز – المكونات، البيانات المخزنة على النظم الموجودة، الجداول، البيانات الخاصة بخط السير أو المضمون) ويتضمن كذلك اختراق نظام معلومات أخر متصل بشبكات الاتصال عامة أو نظام معلومات متصل بنفس الشبكة مثل الشبكة المحلية أو الانترنت (شبكة خاصة لمؤسسة).

البند الرابع: النتيجة الجرمية

---

263 - Art 5 « Est dénommé traitement automatisé d'informations nominatives au sens de la présente loi tout ensemble d'opérations réalisées par les moyens automatiques, relatif à la collecte, l'enregistrement, l'élaboration, la modification, la conservation et la destruction d'informations nominatives ainsi que tout ensemble d'opérations de même nature se rapportant à l'exploitation de fichiers ou bases de données et notamment les interconnexions ou rapprochements, consultations ou communications d'informations nominatives ». du la **Loi n° 78-17** du 6 Janvier 1978 ***relative à l'informatique, aux fichiers et aux libertés*** (*Journal officiel* du 7 janvier 1978 et rectificatif au *J.O.* du 25 janvier 1978, Modifié par ***Loi n°2004-801 du 6 août 2004 - art. 1 JORF 7 août 2004***

264 - Rapport de M. Jacques Thyraud , J.O.R.F, doc sénat,1987-88 1re section n°3 P51.

265 -Cour d'appel de Douai, 7 oct. 1992

266 -Cour d'appel de Paris, 18 nov. 1992

267 -Trib. cor. Paris, 25 fev. 2000

MAITRE ANTHONY BEM, L'INTRUSION ET LES ATTEINTES AUX SYSTEMES INFORMATIQUES SANCTIONNEES PAR LE DROIT PENAL,Article juridique publié le 10/09/2010 sur le site : http://www.legavox.fr/blog/maitre-anthony-bem/

الأساس أن يترتب على السلوك الإجرامي نتيجة معينة أو أثر ضار، وفي الغالب ما يكون هذا الأثر في شكل مادي ملموس، غي أنه في بعض الأحيان لا يكون كذلك وإنما يتمثل في الاعتداء على حق أو مصلحة يحميها القانون فحسب.

وبذلك فإن جريمة الدخول أو البقاء غشا وفقا للمادة 394مكرر فقرة 1 عقوبات جزائري لا تتطلب أي نتيجة جرمية معينة، وإنما المفهوم من هذا النص أن الجريمة تقوم بمجرد حصول اتصال بدون وجه حق أو البقاء فيه بدون تصريح.

وهو نفس الأمر بالنسبة للتشريع الفرنسي من خلال المادة 1/323 عقوبات، والمادة الثالثة فقرة أولى من قانون جرائم تقنية المعلومات الأردني رقم 30 الذي جرمت الدخول فقط دون البقاء.

ويطلق على هذا النوع من الجرائم التي لا تتطلب نتيجة مادية بـ"جرائم الخطر" [268] كونها تعبر عن حقيقة قانونية تم الاعتداء عليها دون حدوث ضرر ملموس، أو الجرائم الشكلية[269].

ولتأكيد انتماء جريمة الدخول أو البقاء غشا إلى الجرائم في شكلها البسيط أو ما يسمى بالدخول أو البقاء البسيط أو المجرد نجد أن العقاب يختلق عن الدخول أو البقاء المرتب للنتيجة الجرمية، حيث شدد المشرع العقاب في الحالة الثانية إذا ترتب على الدخول أو البقاء غشا إلى نظام معلوماتي ضرر بالمعلومات أو النظام المعلوماتي[270].

والحكمة من وراء تجريم المشرع الجزائري وكغيره من المشرعين للدخول والبقاء المجرد ترجع إلى رغبة منه في الحفاظ على سرية المعلومات الموجودة بالنظام المعلوماتي، وعلى أمن وسلامة النظام في حد ذاته ومن أي خطر.

الفرع الثاني: الركن المعنوي

إن استخدام المشرع الجزائري لمصطلح "...عن طريق الغش.." يعني أن جريمة الدخول أو البقاء من الجرائم العمدية والتي تتطلب القصد الجنائي، ولكن هل اكتفى المشرع بتوافر القصد الجنائي العام؟ أم يتطلب كذلك القصد الجنائي الخاص؟

---

[268]– **رشيدة بوكر**، المرجع السابق، ص 228.

[269]– د. **أحمد خليفة الملط**، مرجع سابق، ص 159/ د.**أيمن عبد الله فكري**، مرجع سابق، ص 219/ د. **نائلة عادل محمد فريد قورة**، المرجع السابق، ص ..

[270]– تنص المادة 394 مكرر فقرة **2عقوبات جزائري** :" ....وإذا ترتب على الدخول أو البقاء..."، تقابلها المادة 323-2/1 **عقوبات فرنسي**، والمادة 2/3 من **قانون جرائم أنظمة المعلومات الأردني**.

البند الأول : القصد العام

يتمثل القصد الجنائي العام في عنصريه العلم والإرادة

أولا: العلم

لقيام القصد الجرمي لابد أن ينصرف علم الجاني إلى قيامه بواقعة ذات أهمية قانونية في تحقيق الجريمة، أي كل واقعة متطلبة في استكمال أركان الجريمة وعناصرها الداخلة في تشكيلها.

والفاعل حتى يقع تحت طائلة العقاب لابد عليه أن يعلم انه يقوم بفعل الدخول إلى نظ ام ليس له الحق فيه، أو التجول والبقاء فيه بدون تصريح والامتناع عن قطع الاتصال، فضلا عن علم الجاني بخطورة الفعل الذي أتاه على المصلحة التي يحميها القانون [271]، كعلمه أن الدخول إلى هذا النظام محظور أو أن المعلومات الموجودة فيه الاطلاع عليها يشكل انتهاكا للسرية.

ونشير في هذا المقام إلى أن المشرع الأردني قد شدد العقاب في حالة ما إذا كان دخول الجاني إلى نظام معلوماتي دون تصريح وبهدف الاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية أو السلامة العامة أو الاقتصاد الوطني"[272]

وعليه فإذا انتفى العلم بتلك العناصر انتفى معه القصد الجرمي، كعدم علم المخترق أنه يدخل في نظام للمعالجة الآلية غير مفتوح للجمهور[273]، أو أن يكون دخوله سهوا أو صدفة.

غير أن المشرع وكنظيره الفرنسي قد تنبه إلى ما قد يترتب على الدخول أو الاتصال الخطأ بالنظام المعلوماتي، ومما ينبغي على المخترق الخروج فورا وقطع الاتصال بعد أن تنبه بأنه نظام غير مسموح له، فقام بتجريم الدخول الخطأ والاستمرار بالبقاء فيه مع العلم بذلك، وتنبه كذلك إلى النتيجة التي تترتب في هذه الحالة بما يعني أن القصد الجرمي إذا انتفى في الدخول الخطأ ثم تم البقاء في النظام أو التجول فيه مع علم الجاني بعدم مشروعيته، يجعله تحت طائلة العقاب لتوفر القصد الجرمي المتطلب في صورة البقاء[274].

---

[271]- أ. **رشيدة بوكر**، مرجع سابق، ص 336.

[272]– المادة 11 /أ من ***القانون الأردني المؤقت المتعلق بجرائم أنظمة المعلومات*** سابق الإشارة إليه.

[273]– د.**نائلة فريد قورة**، مرجع سابق، ص 356.

[274]- د.**محمد حماد مرهج الهيتي**، جرائم الحاسوب، مرجع سابق، ص 189.

في هذه الحالة فإن القصد الجنائي إن لم يتعاصر مع النشاط الجرمي في جريمة الدخول إلى النظام المعلوماتي، فإنه يتوافر مع جريمة البقاء إن توافرت أركانها[275].

على خلاف المشرع الأردني الذي جرم الدخول بدون تصريح فقط ولم يشر إلى الدخول خطأ واستمرار البقاء في النظام مع العلم بعدم مشروعية البقاء، مما يشكل جريمة أخرى، ومما يستوجب على المشرع الأردني تدارك هذا الأمر و التدخل من جديد حتى لا يفلت احد من العقاب.

ثانيا: الإرادة

إن توافر العلم بالعناصر المشكلة لجريمة الدخول أو البقاء غير المشروع لا يكفي إلا بتوافر الإرادة، من خلال اتجاه إرادة الجاني إلى ارتكاب فعل الدخول أو فعل البقاء في النظام المعلوماتي دون أن تتجه إلى إحداث النتيجة الجرمية، كونها جريمة شكلية سواء في القانون الجزائري أو القانون المقارن.

فإذا توافر القصد الجرمي بعنصريه العلم بأركان الجريمة واتجاه الإرادة إلى القيام بهذا الفعل، فإنه لا عبرة بالبواعث التي تتوافر لدى الجاني من وراء ارتكابه هذه الجريمة، لأنها لا تدخل ضمن عناصر القصد الجنائي في كل من القانون الجزائري والفرنسي كأصل عام، وبسبب أن الباعث لا أثر له في قيام الجريمة[276].

أما إذا ما ادعى الشخص مثلا أن هدفه من وراء الدخول إلى النظام هو فقط محاولة كشف قصور النظام والتغلب على الوسائل التقنية ليثبت كفاءته و قدرته على اختراق النظام و كشف الخلل الموجود به، فإنه لا يعتد بذلك.

والأهم من ذلك نجد بعض التشريعات قد شددت العقاب في حالة ما كان الهدف من وراء الدخول إلى النظام غير المصرح به، هو الاطلاع على معلومات تخص أمن وسلامة الدولة كما رأينا في القانون الأردني.

وعلى العموم فان تقدير توافر القصد الجنائي تبقى مسألة موضوعية يستقل قاضي الموضوع بتقديرها وفقا لما هو ثابت حسب وقائع كل قضية[277].

البند الثاني:القصد الجرمي الخاص

---

[275]– **عمر الفاروق الحسيني** ، المشكلات العامة في الجرائم المتصلة بالحاسب الآلي وإبعادها الدولية، ط 2، 1995، ص 128،129.

[276]– د.**أيمن عبد الله فكري**، المرجع السابق، ص 245.

[277]– د.**عمر الفاروق الحسيني**، مرجع سابق، ص 237

نتساءل هنا عن : هل اكتفى المشرع الفرنسي بالقصد الجرمي العام الذي يستفاد من مصطلح "Frauduleusement" وتبعه في ذلك المشرع الجزائري من خلال مصطلح عن طريق الغش؟ أم يستلزم إضافة إلى ذلك القصد الجرمي الخاص ؟

بهذا الخصوص ثار خلاف فقهي حول مدى ضرورة توافر القصد الخاص في جريمتي الدخول والبقاء غير المصرح بهما.

بعض الفقه [278] الفرنسي ذهب إلى اشتراط توافر القصد الخاص في هذه الجريمة والمتمثل في "الغش" على أساس أن المشرع الفرنسي استعمل هذا المصطلح الذي يختلف عن لفضي عمدا وإراديا.

و يتفق الفقه أن الغش هنا ليس المقصود منه نية الإضرار وإلا ترتب على ذلك تناقض بين الركن المادي الذي لا يتطلب النتيجة الجرمية والركن المعنوي، ويرون أن الدخول أو البقاء غير المصرح بهما يتحققان عندما يكونان بدون رضا صاحب النظام، ويستندون إلى ما قضت به محكمة باريس في قرارها المشهور الصادر في 5 أبريل 1994 بخصوص الدخول والبقاء غير المشروع إلى نظام المعالجة الآلية، حينما قضت بأن: "الدخول والبقاء يكون بدون حق مع معرفة السبب" [279].

ويخلص هذا الاتجاه إلى أن الغش يكون عند معرفة الشخص بغياب حق الدخول أو البقاء في نظم المعالجة الآلية[280].

في حين يرى إتجاه أخر [281] أن استعمال المشرع الفرنسي لمصطلح " Frauduleusement" يقتضي القصد العام وليس القصد الخاص أو نية خاصة.

وأن عبارة "بدون حق مع معرفة السبب" التي جاءت في الحكم السابق المقصود منها أن الفعل يجب أن لا يكون نتيجة خطأ بسيط، وإنما لابد أن يكون وقوعه مع العلم بعدم صفته المشروعة[282].

---

[278]– مشار إليه لدى **رشيدة بوكر**، مرجع سابق، ص 238.

[279]- « ….qui ont accédé et se maintenus dans des systémes sans droit et en pleine connaissance de cause …… » C.A de paris, 5 Avril 1994, NCP,104e édition,D , paris,2009,p 916. مشار إليه لدى **رشيدة بوبكر**، نفس المرجع، ص 238.

[280] -Voir **Raymons GASSIN**, Op.cit ,p22

[281]- مشار اليه لدى **أيمن عبد الله فكري**، مرجع سابق، ص 243.

[282]– أحمد **خليفة الملط**، مرجع سابق، ص 169.

و بالتالي نستخلص من المادة 394 مكرر عقوبات جزائري ومن المادة 323-1 عقوبات فرنسي أن المشرع يتطلب من جريمة الدخول أو البقاء غشا القصد الجرمي العام الذي يتحقق بعلم الجاني أن دخوله أو بقاءه غير مصرح به مع اتجاه إرادته إلى ذلك.

زيادة على ذلك فإن بعض التشريعات التي جرمت الدخول غير المصرح به إلى نظام الحاسب الآلي تتطلب قصدا خاصا إلى جانب القصد العام، وقد يترتب على هذا القصد تشديد العقوبة.

من ذلك التشريع الدنماركي الذي يشدد العقوبة متى أرتكب فعل الدخول بنية الإحاطة بمعلومات تتعلق بالإسرار المتعلقة بإحدى الشركات [283]، وفي البرتغال كذلك يتطلب القانون قصدا خاصا للعقاب على الدخول غير المصرح به من خلال المادة السابعة من قانون الجرائم المعلوماتية لعام 1991 [284]، حيث تعاقب 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، وتشدد العقوبة متى كان الربح أو الفائدة مرتفعين بنسبة كبيرة"

وعلى ذلك انتقد الفقه النص البرتغالي لتضييقه لجريمة الدخول غير المصرح به على نحو كبير، ورأى البعض أنه لتفادي هذا التضييق يجب أن تفسر الفائدة التي يحصل عليها الجاني لتشمل كل فائدة ذهنية أو معنوية قد يحصل عليها الفاعل من وراء دخوله إلى النظام وأن لا تقتصر على الفائدة والربح المادي[285].

المبحث الثاني:

الإتـلاف المعلوم-ـاتي

يشمل الإتلاف الاعتداء على الأجهزة والمعدات والمكونات المادية للنظام المعلوماتي وكذا على الجانب المنطقي للنظام و المعلومات المدرجة به، وبخصوص النوع الأول من الاعتداءات فانه نكون

283- رتب **المشرع الأردني** عقوبة أشد متى ارتكب فعل الدخول بهدف الاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني....." **المادة 11 من قانون جرائم أنظمة المعلومات.**

284- مشار إليه لدى د.**نائلة عادل محمد فريد قورة**، مرجع سابق، ص 369.

285- مشار إليه لدى د.**نائلة فريد قورة**، المرجع نفسه، ص396.

بصدد جريمة عادية تقليدية كون المحل المعتدى عليه مال مادي تحكمه القواعد العامة والمتعلقة بإتلاف الأموال المنقولة المادية، ولا تحكمه قواعد إتلاف المال المعلوماتي.

ومن الاعتداءات التي تقع على المكونات المادية للنظام المعلوماتي ما يتم من كسر لاسطوانات أو أشرطة ممغنطة[286]، أو حرق أو كسر جهاز الحاسب الآلي[287].

أما إتلاف المال المعلوماتي اللامادي، وهو ما يهمنا في هذا المقام، المتمثل في الاعتداء على سير نظام المعالجة الآلية للبيانات وإلحاق الضرر به، أي على نظام المعالجة الآلية للبيانات و ما يتضمنه من معلومات، من خلال مختلف التصرفات التدليسية و ما يترتب عليها من إتلاف للبيانات والمعلومات و البرامج، أو بما يؤدي إليه من تعطيل وظائف أو إفساد لنظام التشغيل[288].

والملاحظ على أغلب التشريعات المقارنة الحالية أخذت بعين الاعتبار الطبيعة اللامادية للأموال واعتبارها محلا للإتلاف وشملتها بحماية قانونية.

ومن هنا نحاول أن نبحث عن مفهوم الإتلاف المعلوماتي وما ينطبق عليه من أحكام في التشريع الجزائري والتشريعات المقارنة.

المطلب الأول: المقصود بالإتلاف

الإتلاف عموما هو تخريب الشيء محل الجريمة أو التقليل من قيمته وجعله غير صالح للاستعمال أو تعطيله[289].

والإتلاف لا يخرج عن كونه فناء الشيء أو جعله بحالة غير الحالة التي كان عليها، بحيث لا يمكن الاستفادة منه وفقا للغرض الذي وجد من أجله مما يعني أن جوهر الإتلاف هو إفقاد المال المتلف منفعته أو صلاحيته للاستعمال في الغرض الذي أعد من اجله، أو التأثير على مادة الشيء على نحو يقلل من القيمة الاقتصادية للشيء، مما يفيد ان محل الحماية الحقيقي في هذه الجريمة هو

---

[286]– **دويب حسن صابر** ، مداخلة بعنوان: القوانين العربية وتشريعات تحريم الجرائم الالكترونية وحماية المجتمع، المؤتمر السادس لجمعية المكتبات والمعلومات، السعودية،1431 هجري، ص3.

[287]– مثل ما حدث عندما قامت إحدى المنظمات الإرهابية في فرنسا سنة 1980 بإتلاف برامج وملفات أحد مراكز الحاسب الالي المتخصصة في بيع الحاسبات / **محمود أحمد عبابنة**، مرجع سابق، ص 100،99.

[288]– **محمد أمين الشوابكة**، مرجع سابق، ص 222.

[289]– د. **أسامة، بن غانم العبيدي**، جريمة الإتلاف المعلوماتي، مرجع سابق، ص 95.

قيمة الشيء وما حمايته من الناحية المادية إلا وسيلة لحماية قيمته الاقتصادية، كون الشيء يفقد قيمته أيضا بفناء مادته إما بشكل كلي أو جزئي[290].

أما الإتلاف المعلوماتي المعنوي كما سبق وأن اشرنا فإنه يتمثل في الاعتداء على سير نظام المعالجة الآلية للبيانات بالإفساد أو التعطيل، أو من خلال الاعتداء على المعلومات والبرامج بإتلافها أو محوها أو تعديلها.

و بخصوص الاعتداء على سير نظام المعالجة الآلية للمعطيات أو تخريبه، فإن المشرع الجزائري لم يتعرض إلى هذه الجريمة كونها جريمة مستقلة بذاتها، وإنما جرمها في الإتلاف غير المباشر للنظام المعلوماتي عندما تحدث عن الظرف المشدد الناتج عن جريمة الدخول والبقاء غشا وما يترتب عليه من أضرار تمس هذا النظام أو تخريبه من خلال المادة 394 مكرر الفقرة الثالثة عقوبات بقوله" إذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام إشتغال المنظومة تكون العقوبة.."

على خلاف المشرع الأردني والفرنسي الذين أدرجاها في نصوص مستقلة تشكل جريمة لحالها وصورة من صور الإتلاف المعلوماتي المباشر (المادة 232-2 عقوبات فرنسي/ المادة 4 من القانون الأردني لجرائم أنظمة المعلومات رقم 30)، وكذا كظرف مشدد يشكل جريمة إتلاف غير مباشر ناتج عن دخول أو بقاء غير مصرح إلى نظام المعالجة الآلية للمعطيات والإضرار به (المادة 323-1 فقرة 2 عقوبات فرنسي/ المادة 3 فقرة أ من القانون الأردني رقم 30).

أما الصورة الثانية للإتلاف المعلوماتي حينما يتم الاعتداء على معلومات وبيانات المعالجة ألليا أو الواردة في النظام المعلوماتي فقد تم النص عليها سواء من قبل المشرع الجزائري أو باقي المشرعين، وكجريمة مستقلة تشكل إتلافا معلوماتيا مباشرا أو كظرف مشدد ناتج عن الدخول أو البقاء غشا لنظام المعالجة الآلية للمعطيات وترتب عنه حذف أو تعديل لتلك المعلومات أو المعطيات الواردة في النظام.

ونحاول من خلال ما يأتي توضيح ذلك.

المطلب الثاني: أركان جريمة الإتلاف المعلوماتي

يأخذ الإتلاف المعلوماتي إحدى الصورتين إما بالاعتداء على سير نظام المعالجة الآلية وإعاقته، وإما بالاعتداء على المعلومات و سلامة البيانات والتلاعب بها أو ببرامج الحاسب الآلي.

ولتحقيق هذه الجريمة يستلزم توافر ركنين مادي و معنوي.

---

[290]- **محمد حماد مرهج الهيتي**، جرائم الحاسوب، مرجع سابق، ص198،197.

الفرع الأول: الركن المادي

يختلف الركن المادي في جريمة الإتلاف المعلوماتي على حسب ما إذا كان الاعتداء يمس نظام المعالجة الآلية أم المعلومات الواردة فيه، و سأتعرض لذلك بالشرح و التوضيح فيما يأتي:

البند الأول: الاعتداء على نظام المعالجة الآلية للمعطيات

يتمثل الاعتداء على نظام المعالجة الآلية و تدميره من خلال إعاقة سير عمل النظام، أو ما يسبب تباطؤ عمل نظام المعالجة الآلية للبيانات و إرباكه [291]، أو إلى ما يؤدي إلى تغيير في حالة عمل النظام على نحو يصيبه بالشلل المؤقت[292]، ولقد نصت على هذا الشكل من الاعتداءات المادتين 05 و08[293] من الاتفاقية الدولية للإجرام المعلوماتي بودابست لسنة 2001، على خلاف الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الموقعة بالقاهرة 2010.

ويتمثل الركن المادي لهذه الجريمة في إحداث ضرر بالنظام الناتج عن فعل تعطيله أو إفساده وإعاقته عن أداء وظائفه.

أولا: تعطيل النظام

و يتمثل في إعاقته أو عرقلته عن العمل كليا أو جزئيا [294]، أو بتوقف الشيء عن القيام بوظيفته فترة مؤقتة[295] و تتمثل وظيفة النظام في المعالجة الآلية للمعطيات و خزنها و استرجاعها أو إرسالها.

ثانيا:الإفساد أو التعييب

فعل التعييب وإن كان لا يعطل نظام المعالجة الآلية للبيانات، إلا أنه يجعل هذا النظام غير قادر على الاستعمال السليم، وذلك بأن جعله يعطي نتائج غير تلك التي كان من الواجب الحصول عليها[296].

---

[291]- د. **أيمن عبد الله فكري**، مرجع سابق، ص 249.

[292]– **محمد أمين الشوابكة**، مرجع سابق، ص 232.

[293]– المادة 5 و8 من اتفاقية بودابست، لدى هلالي عبد الاله أحمد، مرجع سابق، ص 91،111.

[294]– د. **عفيفي كامل عفيفي** ،جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، مرجع سابق، ص 183/ **محمد أمين الشوابكة** ، مرجع سابق، ص 218،219.

[295]– **نبيل صقر**، مرجع سابق، ص 220.

[296]– **أمال قارة**، المرجع السابق، ص 119/ كذلك أ. **خثير مسعود**، الحماية الجنائية لبرامج الكمبيوتر ، ، ص121.

و بالرجوع إلى نص المادة 323-2 عقوبات فرنسي [297] يتضح أن المشرع يستخدم مصطلحات محددة تتمثل في كل من إعاقة أو تشويه لأداء نظام المعالجة الآلية، وبالتالي تشمل كل فعل من شأنه إرباك عمل النظام[298].

و يستوي أن يكون من شان فعل ونشاط الجاني إعاقة أو إفساد نظام التشغيل أو إرسال رسائل تشغل النظام، ويستوي أن يكون فعل الجاني يؤدي إلى توقيف عمل النظام بصورة دائمة أو مؤقتة.

كما أن المشرع الفرنسي لم يشترط وسيلة معينة لارتكاب هذه الجريمة، فأي وسيلة يستخدمها الجاني[299] وتتسبب في إعاقة وإفساد النظام تجعل الجريمة قائمة ومعاقب عليها.

كما لا يشترط أن تكون إعاقة وإفساد النظام جسيمة أو كلية، وإنما يعاقب على هذا السلوك الإجرامي ولو أدى إلى إعاقة أو إفساد جزئي للنظام[300].

غير أن اتفاقية بودابست بشأن الجرائم الالكترونية أشارت في مذكرتها التفسيرية رقم 85 بتاريخ 08 نوفمبر 2001 في الفقرة 67 إلى أنه لقيام المسئولية الجزائية يجب أن تكون الإعاقة أو العرقلة جسيمة أو خطيرة، ويجب على كل طرف أن يحدد الشروط التي يجب توافرها كي تعتبر الإعاقة جسيمة.

و تعتبر الإعاقة جسيمة بالنسبة لواضعي الاتفاقية عندما تكون البيانات المرسلة من الحجم أو التواتر La fréquence ما يحمل ضررا جسيما لقدرة المالك أو المشغل بالنسبة لاستخدام الجهاز أو

---

[297] - Art 323-2 **de C.P.F** Modifié par LOI n°2012-410 du 27 mars 2012 - art. 9

Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.

Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 100 000 € d'amende

[298]- بالرجوع إلى القانون الأردني، نجد المشرع قد استعمل مصطلحات عدة فيما يتعلق بإفساد وتعطيل النظام بقوله" ....توقيف أو تعطيل عمل نظام المعلومات أو تغيير موقع الكتروني أو تعديل محتوياته أو اشغالة....." المادة 3/أ و كذا بقوله"إعاقة أو تشويش أو ايقاف أو تعطيل عمل نظام معلومات أو الوصول إليه أو تغيير موقع إلكتروني أو إلغائه أو إتلافه أو تعديل محتوياته أو اشغاله" المادة 4 من القانون السالف الذكر.

أما بالنسبة للمشرع الجزائري فأنه استخدم مصطلح التخريب عند نصه على الظرف المشدد لجريمة الدخول أو البقاء غشا، ويتمثل فعل التخريب في أن أصبح النظام أو المال غير قابل للإصلاح لما اعد له.

[299]– من الوسائل التي قد تستخدم في إفساد وتعطيل النظام نشر فيروسات بالنظام المعلوماتي مثل فيروس القنبلة المعلوماتية، أو فيروس حصان طروادة إلى غير ذلك من الوسائل المختلفة.

[300]– د.**عبد الفتاح بيومي حجازي**،النظام القانوني لحماية التجارة الالكترونية، المرجع السابق، ص36.

الاتصالات بالأجهزة الأخرى، مثال ذلك البرامج التي تحمل اعتداء على النظم والتي تأخذ شكل الامتناع عن الخدمة، أو الشفرات العدوانية كالفيروسات التي تمنع أو تبطئ بشكل ملموس عمل الجهاز، أو البرامج التي ترسل مقدارا هائلا من البريد الالكتروني إلى مرسل إليه من أجل شل وظائف اتصال النظام[301].

أما المشرع الجزائري بالنسبة لهذا الشكل من الإعتداء و كما سبق بيانه، أنه جعله صورة مشددة ناتجة عن فعل الدخول أو البقاء في نظام للمعالجة الآلية و ترتب عن ذلك تخريب نظام إشتغال المنظومة فتضاعف العقوبة عن الفعل البسيط للدخول أو البقاء، و ذلك بموجب الفقرة الثالثة من المادة 394 مكرر عقوبات.

و بخصوص الأحكام القضائية الفرنسية الصادرة بهذا الشأن نجد الحكم الذي قضى بأن يقع تحت طائلة العقاب الجناة الذين قاموا بتوصيل العديد من أجهزة الميناتل بالمراكز الخدمية المعنية، وأخذوا يرسلون بشكل ألي رسائل كثيرة مما ترتب عليه من إرباك لأنظمة المعالجة الآلية للمعلومات[302].

كما قضي[303] تطبيقا للنص 323-2 عقوبات فرنسي بإدانة شخص قام بإدخال فيروس في أحد أنظمة المعالجة الآلية للمعلومات عن طريق وضع فيروس على اسطوانات إعلانية تحتوي على ملخص لبرامج دعائية، وقد قام الجاني بزراعة هذا الفيروس على هذه الاسطوانات مع إعداد جريدة متخصصة في مجال المعلوماتية وباستخدام هذه الاسطوانات تم نقل الفيروس إلى نظام التشغيل فأتلف المعلومات.

البند الثاني: الاعتداء على المعلومات

نص عليها المشرع الجزائري على هذه الصورة من صور الاتلاف المعلوماتي كجريمة مستقلة في المادة 394 مكرر 1 بقوله" .....كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها".

و كذا كجريمة أو ظرف مشدد إذا ترتب على الدخول أو البقاء غشا حذف أو تغيير لمعطيات المنظومة من خلال المادة 394 مكرر فقرة 2 عقوبات جزائري.

---

[301]-د. **هلالي عبد الإله احمد**، مرجع سابق، ص 93،94.

[302]- مشار إليه لدى: د.**أيمن عبد الله فكري**، مرجع سابق، ص 250.

[303] – Crim, 15 Décembre 1996, BC, N° 18 مشار إليه لدى نفس المرجع، ص 250

و نفس الأمر بالنسبة للمشرع الفرنسي [304] والأردني[305] حيث اعترفا بالحماية القانونية للمعلومات باعتبارها أموال غير مادية تستوجب الحماية و بسلامتها و أمنها.

ونصت عليها المواد 04،08[306] من اتفاقية بودابست لسنة 2001 بشأن الإجرام المعلوماتي ، و كذا المادة الثامنة من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بقولها الاعتداء على سلامة البيانات غير أنها اشترطت في الفقرة الثانية لهذه المادة على الدولة الطرف أن تلتزم لتجريم الأفعال المنصوص عليها في الفقرة الأولى من هذه المادة أن تتسبب بضرر جسيم.

هذه النصوص كلها نصت على تجريم كل فعل من شانه إتلاف المعلومات المدرجة بالنظام المعلوماتي.

كما أن هذه الجريمة محلها محدد وهو المعلومات المعالجة أليا وبذلك يخرج من نطاق هذه الجريمة المعلومات التي لم تعالج أليا أ و انفصلت عن النظام بعد أن تمت معالجتها كأن يتم طباعتها على ورق[307]، غير أن المشرع لم يحدد نوعية المعلومات، بما يعني أن المشرع سعى إلى تعميم الحماية على كافة المعلومات [308]، كما انه جاء شامل لكل وسائل الإتلاف المعلوماتي ولم يقتصر أو يحدد وسيلة معينة.

---

[304] - **Art** 323-3 de C.P.F Modifié par LOI n°2012-410 du 27 mars 2012 - art. 9

« Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 euros d'amende ».

[305]- المادة 04 من **قانون جرائم أنظمة المعلومات رقم 30** :" كل من أدخل أو نشر أو استخدم قصدا برنامجا عن طريق الشبكة المعلوماتية أو باستخدام نظام معلومات، بهدف إلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ أو التقاط أو تمكين الاخريين من الاطلاع على البيانات أو معلومات....."

[306]– تنص المادة 04 من **اتفاقية بودابست** على" يجب على كل طرف أن يتبنى الإجراءات التشريعية وأية إجراءات أخرى يرى أنها ضرورية لتجريم، تبعا لقانونه المحلي، أذا حدث ذلك عمدا ودون حق، أي أضرار أو محو أو تعطيل أو اتلاف أو طمس لبيانات الحاسب،...."

[307]– د. **عبد الفتاح بيومي حجازي**، النظام القانوني لحماية التجارة الالكترونية، المرجع السابق، ص37،38.

[308]– نجد المشرع الفرنسي ميز في ذلك وشدد العقاب في حالة الاعتداء على المعلومات الشخصية المعالجة آليا من قبل الدولة من خلال تعديله لقانون العقوبات في 2012 للمادة 323–3 وأضاف فقرة ثانية .

Article 323-3 alinéa 2 de code pénal français Modifié par LOI n°2012-410 du 27 mars 2012 - art. 9

و يتمثل السلوك الإجرامي في جريمة التلاعب ببيانات ومعطيات نظام المعالجة الآلية والمساس بسلامتها في تحقق إحدى الأفعال التي وردت بالنصوص القانونية والتي تتخذ صورة الإدخال أو المحو والإزالة أو التعديل ولقد وردت على سبيل المثال وليس الحصر ، بمعنى أن أي فعل أو سلوك ينطوي أو يندرج تحت مفهوم هذه السلوكات و يشكل إتلافا معلوماتيا، يعاقب عليه بهذه النصوص، وأي فعل غيرها[309] حتى ولو تضمن الاعتداء على بيانات ومعطيات نظام المعالجة للبيانات مثل فعل النسخ أو التصوير فإنه يندرج تحت نصوص أخرى[310] ونوضح ذلك فيما يلي:

أولا: فعل الإدخال

فعل نصت عليه معظم التشريعات وعرفه الفقه على أنه "تغذية النظام بالمعلومات المراد معالجتها، أو بتعليمات لازمة لعملية المعالجة"[311]، أي يقصد بذلك إدخال بيانات أو معلومات إلى نظم المعالجة الآلية لم تكن موجودة من قبل بهدف إتلاف المعلومات المخزنة بالنظام أو الإضرار ببرامج النظام كونها معلومات تدخل إلى إليه.

وإدخال المعلومات المحرفة والمغلوطة إلى النظام المعلوماتي أمر من السهل إتيانه في أولى مراحل تشغيل نظام المعالجة الآلية أو أثناء المعالجة الآلية للبيانات و المعلومات و تحويلها إلى لغة مقروءة من قبل الآلة المستخدمة في المعالجة، ومن أسهل وأسرع الوسائل المعروفة في الوقت الراهن والتي يتم إدخالها إلى النظام المعلوماتي ويترتب عنها إتلاف معلومات وبيانات وبرامج النظام، نجد الفيروسات والقنابل المنطقية والزمنية[312].

ولقد طبق القضاء الفرنسي المادة 323-3 في العديد من أحكامه والخاصة بجريمة التلاعب بالبيانات، منها ما أيدته محكمة النقض الفرنسية عام 1994 بإدانة أحد الأشخاص بتهمة

« Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 100 000 € d'amende ».

[309]- من الأفعال التي وردت بنصوص أخرى وتندرج تحت جريمة الإتلاف نجد استعمال المشرعين مصطلح التخريب أو التدمير إلى غير ذلك..

[310]- **أمال قارة**، مرجع سابق، ص 123/ كذلك **رشيدة بوكر**، مرجع سابق، ص 258.

[311]-د. **نائلة عادل محمد فريد قورة**، مرجع سابق، ص 437.

[312]- د.**أمجد حسان**، الفيروسات إرهابا تهدد أنظمة المعلومات، مقال مقدم إلى ملتقى " الإرهاب في العصر الرقمي" المنعقد بجامعة الحسين بن طلال، البتراء، الأردن، ب 10-2008/07/12.

إتلاف المعلومات لقيامه بإدخال معلومات غير صحيحة تتعلق بالنسب الخاصة بضريبة المبيعات في نظام المعالجة الآلية، وذلك في الاستثمارات الخاصة بذلك، ثم قام بإدخال بعض هذه المعلومات إلى نظام المعالجة الآلية، كما قضت المحكمة النقض الفرنسية أن إدخال فيروس « Frodo »إلى نظام المعالجة الآلية هو سلوك معاقب عليه وفق المادة 323-3 [313] .

ثانيا: فعل المحو

نجد أن المشرع الفرنسي والمشرع الجزائري قد استعملا مصطلح الإزالة أما المشرع الأردني فقد استعمل مصطلح إلغاء أو حذف أو حجب بيانات أو معلومات[314].

ويقصد به محو وإزالة جزء من المعطيات المسجلة على دعامة، أو الموجودة داخل النظام أو نقل وتخزين جزء من المعلومات إلى المنطقة الخاصة بالذاكرة[315].

ومن القضايا [316] التي تم فيها محو وإزالة المعلومات والبيانات نجد قضية الشركة TRW Company Credit Data التي كانت تعمل على تزويد عملائها من بنوك وشركات، ومتاجر ومن خلال أنظمتها المعلوماتية بمعلومات تتعلق بالمركز الائتماني لأفراد الجمهور نظير اشتراك يدفعه هؤلاء العملاء، وكانت الشركة تحوز معلومات تتعلق بحوالي خمسين مليون شخص، وقد استغل أحد الموظفين بقسم علاقات المستهلكين هذا النشاط وقام ببيع مراكز إئتمانية جديدة قام بإختلاقها لذوي المراكز الائتمانية الضعيفة أو الرديئة مقابل مبلغ مالي يدفعه هؤلاء، حيث عمل الموظف على محو المعلومات المتعلقة بالمراكز الرديئة واستبدالها بمعلومات تحسن مركز المتعاملين معه.

---

[313]- **رشيدة بوكر**، مرجع سابق، ص 254.

[314]- استخدمت تشريعات أخرى مصطلحات لها نفس المعنى أو تؤدي إلى نفس النتيجة منها القانون النموذجي العربي بشأن الجرائم المعلوماتية في مادته الثالثة أستخدم مصطلح التدمير، كذلك اتفاقية بودابست استعملت مصطلحات الإضرار أو الإتلاف أو الطمس إضافة إلى فعل المحو.

[315]- **علي عبد القادر القهوجي**، المرجع السابق، ص 59.

[316]- مشار إليه لدى: د.**عبد الفتاح بيومي حجازي**، الحماية الجنائية للتجارة الالكترونية، مرجع سابق، ص 49.

وهذه العملية قد اشتملت على صور التلاعب بالمعلومات من محو وإزالة وتعديل، ولم يتم اكتشاف هذه الجريمة إلا بعد تبليغ تقدم به أحد الأشخاص إلى مكتب التحقيقات الفيدرالي «FBI » بعد أن تلقى عرضا بتحسين سجله الائتماني مقابل مبلغ معين يقدمه للموظف.

ثالثا: فعل التعديل

ورد كذلك هذا المصطلح في كل من القانون الجزائري والفرنسي عندما نصت المادة 394 مكرر1 عقوبات جزائري والمادة 323-3 عقوبات فرنسي على يعاقب على تعديل معلومات نظم المعالجة الآلية بطريق الغش، أما المشرع الأردني من خلال المادة 3 و 4 نجده استعمل مصطلحات عدة منها التعديل والتغيير والإضافة للبيانات أو المعلومات.

والتعديل بهذا المعنى يقصد به تغيير المعطيات أو المعلومات الموجودة داخل النظام واستبدالها بمعطيات أخرى، أو عن طريق التلاعب بمعلومات وبرامج بإمدادها بمعطيات مغايرة عن تلك التي صمم البرنامج لأجلها.[317]

ومن القضايا التي طبق عليها القضاء الفرنسي [318] فعل التعديل والإلغاء الوارد بالمادة 323-3 عقوبات ما صدر عن محكمة النقض بشأن قيام أحد الأشخاص بتعديل وإلغاء لمعلومات تتعلق باللوائح المطبقة بإحدى الشركات بطريق العمد، وقد أقرت المحكمة بأنه ليس من اللازم أن تكون هذه التعديلات أو الإلغاءات تم ارتكابها بواسطة شخص ليس الحق الدخول إلى النظام، وبناءا على ذلك أيدت حكم محكمة الاستئناف الذي أدان المتهم عن هذه الجريمة بعد أن استخلصت أركانها من قيام الشخص بتعديل البيانات والتي سبق وأن قام بتسجيلها بطريقة نهائية على نظام ألي للمحاسبة كان يقوم بالإشراف عليه.

و عليه نشير إلى أن هذه الأفعال لا يشترط اجتماعها معا حتى تقوم جريمة الإتلاف المعلوماتي كما هو وارد في النص القانوني بقول المشرع" ...الإدخال أو الإزالة أو التعديل..." وقد يجتمع في الجريمة أكثر من فعل كالتعديل والإزالة كما لاحظنا في القضايا السابق الإشارة إليها، كما قد تجتمع مع هذه الجريمة جرائم أخرى مثل الإتلاف المعلوماتي والتزوير، أو الدخول والبقاء غير المصرح مع

---

[317]- د. **نائلة محمد عادل فريد قورة**، مرجع سابق، ص447.

[318]- Cass,crim, 8 Décembre 1999, Gaz.Pal.27-28 octobre 2000, somm.P45. voir Myriam Quémener et Yves Charpenel, op.cit,p 77.

ومشار إليه كذلك لدى: د **أيمن عبد الله فكري**، المرجع السابق، ص 251.

الإتلاف المعلوماتي ولكن لكل جريمة نص خاص بها، ووفقا للتشريع الجزائري في الحالة تعدد الجنح يطبق على الجاني العقوبة الأشد وفقا للمادة 34 عقوبات[319].

وتوضيح صور والأفعال التي يتم بها الإتلاف المعلوماتي أو التلاعب بالمعلومات، يمكن ملاحظة أن هذه الأساليب قد ترتكب بها جريمة أخرى قد تتداخل معها وهي جريمة الاحتيال المعلوماتي بمختلف أشكاله بما في ذلك أنظمة التحويل الالكتروني للأموال [320]، ولعلى أكثر الأساليب انتشارا هي الإدخال غير المصرح به للمعلومات.

غير انه لحل هذا التداخل لابد من التمييز بين التلاعب بالمعلومات بذاتها وإتلافها دون أن يكون الهدف من وراء ذلك الحصول على منفعة مادية، وبين التلاعب بالبيانات المدخلة من أجل الحصول على فائدة مادية، حيث تمثل هته الحالة الأخيرة جريمة الاحتيال المعلوماتي.

كما تجدر الإشارة إلى أن التشريع الأردني قد نص على مختلف أساليب التلاعب بالبيانات المدخلة للنظام المعلوماتي وسواء كان الهدف منها الإضرار فقط أ و الإضرار من أجل الحصول على فائدة مادية فقد جعل العقاب واحد (المادة 4 من قانون جرائم أنظمة المعلومات لسنة 2010).

ولقد قضت محكمة جنح باريس في حكم صادر لها بتاريخ 13 فبراير 1990[321] على أن المتهمين الذين قاموا بتعديل ومحو المعلومات التي يحتوي عليها نظام المعالجة الآلية من أجل إجراء تحويلات غير مشروعة للأموال بتهمة النصب وبتهمة إدخال أو محو أو تعديل المعلومات المبرمجة آليا على نحو غير مشروع والتي تنص عليها المادة 323-3 من قانون العقوبات.

الفرع الثاني: الركن المعنوي

تعد جريمة الإتلاف المعلوماتي من الجرائم العمدية التي لا يكفي فيها توافر الركن المادي، بل إلى جانب ذلك يجب توافر القصد الجنائي، ولا تتطلب قصدا جنائيا خاصا، وإنما يكتفى بشأنها توافر القصد العام بعنصريه العلم و الإرادة .

---

[319]- تنص المادة 34 من ***قانون العقوبات الجزائري المعدل والمتمم*** على ما يلي:" في حالة تعدد جنايات أو جنح محالة معا إلى محكمة واحدة فإنه يقضي بعقوبة واحدة سالبة للحرية ولا يجوز أن تجاوز مدتها الحد الأقصى للعقوبة المقررة قانونا للجريمة الأشد".

[320]- أنظر في هذا الأمر كل من: **محمد خليفة الملط** ، مرجع سابق، ص 180. **ونائلة عادل محمد فريد قورة** ، مرجع سابق، ص439. **ونهلا عبد القادر مومني**، مرجع سابق، ص190. **و رشيدة بوكر**، مرجع سابق، ص 260،259.

[321]- مشار اليه لدى: أ. **رشيدة بوكر**، مرجع سابق، ص 261.

البند الأول: الاعتداء على سلامة أنظمة المعالجة الالية

إن الاعتداء على النظام بعرقلته أو تعطيله أو جعله غير صالح للخدمة أو تشويه أدائه فإنه يفترض في هذه الأفعال أن لا تكون إلا عمدية، وهذا ما يميزه عن الاعتداء غير العمدي لسير النظام كظرف مشدد لجريمة الدخول أو البقاء غشا والمترتب عن هذا الفعل [322]، ويتطلب القصد في هذه الجريمة أن يعلم الجاني أنه يقوم بأفعال من شأنها إعاقة النظام المعلوماتي عن أداء وظائفه، وأن تتجه إرادته إلى ارتكاب هذا الفعل وتحقق النتيجة منذ بداية ارتكاب الجريمة وبدون تصريح.

البند الثاني: الاعتداء على سلامة معلومات نظم المعالجة الآلية للمعطيات

بالرجوع إلى نص المادة 323-3 عقوبات فرنسي وتقابلها المادة 394 مكرر 1 عقوبات جزائري، والمادة 04 من قانون جرائم أنظمة المعلومات الأردني نجد أنها جريمة مقصودة، ويتطلب القصد العام فيها أن يعلم الجاني أنه يقوم بأحد الأفعال التي يترتب عنها إتلاف المعلومات المعالجة ألليا، أي يعلم أنه يقوم بفعل الإدخال، أو الإزالة والمحو، أو التعديل والتغيير، و أن من شأن إتيانه بهذه الأفعال قد يؤدي إلى نتيجة تغيير حالة المعلومات عما كانت عليه أو إتلافها [323]، وأن تتجه إرادته إلى ارتكاب إحدى تلك الأفعال وتحقق تلك النتيجة.

و بخصوص المشرع الجزائري والمشرع الأردني كذلك لم يحدد القصد بمعلومات معينة ودون تحديد معلومات أو أخرى حيث جاء النص عام ليشمل كل المعلومات المعالجة آليا.

و كذلك الأمر بالنسبة للمشرع الفرنسي، غير أن هذا الخير قد شدد العقاب في حالة قصد الجاني المعلومات الشخصية المعالجة أليا من قبل الدولة من خلال المادة 323-3 الفقرة 2 من قانون العقوبات المعدل سنة 2012.

المطلب الثالث: أشهر قضايا الإتلاف المعلوماتي

من أهم الأحداث و القضايا التي وقعت فعلا ما يأتي سرده:

- ✓ من أشهر الأحداث الواقعة بشأن الإتلاف المعلوماتي ما قام به طالب أمريكي يدعى روبرت موريس و هو طالب في قسم علوم الكمبيوتر بجامعة كورنيل بولاية نيويورك، الذي تعمد ببث برنامج دودة الانترنت بهدف إثبات عدم ملائمة الإجراءات التقنية القائمة لحماية الكمبيوتر و لإظهار العيوب التي إكتشفها من عدم كفاية ملائمة وسائل الأمان في شبكات الكمبيوتر، و

---

[322]- د. **علي عبد القادر قهوجي**، مرجع سابق، ص 142.

[323]- أ. **رشيدة بوكر**، مرجع سابق، ص 269.

لكنه تسبب في تدمير الآلاف من شبكات الحاسب الآلي المنتشرة في الولايات المتحدة، بالإضافة إلى خسائر مالية كبيرة في مواجهة دودة الانترنت.

و قد أدين مورس بإنتهاك قانون الاحتيال و إساءة استخدام الكمبيوتر [324]، و قد تم إدانته بالوضع تحت المراقبة لمدة 03 سنوات، و القيام بالعمل لمدة 400 ساعة في خدمة المجتمع و غرامة عشرة آلاف و خمسون دولار ، فضلا عن تكاليف وضعه تحت المراقبة، و قد دافع موريس عن نفسه بأنه لم تكن لديه النية إلى تحقيق الضرر الذي وقع و نفى عن نفسه توفر القصد الجنائي لإحداث الإتلاف، و لكن المحكمة رفضت الدفع بالقول أنه لا يشترط أن تتجه النية لتحقيق الضرر بل يكفي أن تتجه النية للدخول غير المشروع على نظام حاسب فدرالي[325].

- ✓ قضية الجحيم العالمي: تعامل مكتب التحقيقات الفدرالية مع قضية عرفت باسم مجموعة الجحيم العالمي GLOBAL HELL حيث تمكنت هذه المجموعة من اختراق مواقع البيت الأبيض و الشركة الفدرالية الأمريكية و الجيش الأمريكي و وزارة الداخلية الأمريكية، و قد أدين إثنين من هذه المجموعة جراء تحقيقات الجهات الداخلية في الولايات المتحدة، و قد ظهر من التحقيقات أن هذه المجموعة تهدف فقط إلى مجرد الاختراق أكثر من التدمير أو التقاط المعلومات الحساسة، و قد مضت مئات الساعات في التحقيق و ملاحقة و متابعة هذه المجموعة عير الشبكة و تتبع أثار أنشطتها، حيث كلف التحقيق مبالغ كبيرة لما تطلبه من وسائل معقدة في متابعة هذه المجموعة[326].
- ✓ قام مبرمج في ألمانيا الديمقراطية (قبل توحيدها) بزرع برنامج يحتوي قنبلة زمنية في النظام المعلوماتي الخاص بالشركة التي عمل بها، و تم برمجة القنبلة بحيث تنفجر بعد سنتين لتركه العمل بها و في حوالي الساعة الثالثة و وفقا للتاريخ المحدد و كما سجل هذا الأخير في البرنامج، فإن الاستفهام الخاص بيوم و ساعة سند التنفيذ ظل مستمرا و كان متأكدا من لحظة التدمير ستراعى بكل دقة، و فعلا سبب ذلك حادث أدى إلى انهيار النظام المعلوماتي

---

[324]- **محمد أمين الشوابكة** ، مرجع سابق الإشارة إليه، ص 240.

[325]– د.**أيمن عبد الله فكري**، مرجع سابق الإشارة إليه، ص 196.

[326]– نفس المرجع، ص 171.

الخاص بالشركة فإن أكثر من 300 طرفية ظلت لا تعمل لبضعة أيام و كان من الصعب اكتشاف الفاعل نظرا للتفاوت في الزمن بين لحظة ارتكاب الفعل و لحظة تحقيق النتيجة[327].

إضافة إلى هذه الحوادث هناك قضايا أخرى معروفه منها: قضية فيروس ميلسا، و حادثة شركة أوميغا، و غيرها كثير، و بخصوص الجزائر فإن أغلب القضايا التي تم ضبطها من قبل رجال الدرك متعلقة بالتهديد و الشتم و السب، و لكن مملا لا شك فيه أن الجزائر لن تسلم من خطر هذه الجريمة كونها تشغل حيزا من الفضاء الافتراضي و كونها اندمجت في تكنولوجيا المعلومات و الاتصالات خاصة بعد إدخال تقنية الجيل الثالث، بحيث تعتبر مهددة بمخاطر هذه التكنولوجيا.

المبحث الثالث:

الاعتراض غير القانوني

ان تبادل المعلومات و المعطيات الكترونيا عن طريق الحواسيب و الشبكات، و مختلف وسائل الاتصال أصبح أمرا مشاعا نظرا لارتباط الغالبية العظمى من الدول بشبكة الانترنت و ازدياد اعتمادها على نظم المعلومات و الاتصالات ازديادا مضطردا، حتى أصبحت تلك النظم عاملا أساسيا و ضروريا في إدارة جميع القطاعات المختلفة كالقطاع التجاري و المصرفي والأمني و غيرها من المجالات.

كما أن تشريعات الدول لم تقتصر على تجريم إختراق النظم المعلوماتية أو البقاء فيها كما سبق بيانه، بل امتدت الحماية و شملت حتى تلك المعلومات و البيانات المتداولة أو المرسلة عبر تلك الوسائل، و سواء تعلق الأمر باعتراض هذه المعلومات و إعاقة سيرها و التجسس [328] عليها أو بقرصنتها و الاستحواذ عليها و استغلالها لأغراض معينة.

---

[327]- د.**عبد الله حسين علي محمود** ، سرقة المعلومات المخزنة في الحاسب الآلي ،"شرطة دبي"، الطبعة الرابعة، دار النهضة العربية، القاهرة، بدون سنة نشر، ص 121.

[328]- **التجسس المعلوماتي** أو الالكتروني يقتصر على التنصت على نوع معين من المعلومات المتعلقة بالأمن القومي والسياسة الخارجية للدول الأخرى، و يعرف على انه إستخدام وسائل تقنية المعلومات الحديثة للدخول بشكل غير مسموح وغير قانوني إلى أنظمة المعلومات الالكترونية الخاصة بالدول و الحكومات و التنصت عليها، بقصد الإستحصال على ما لديها من معلومات مهمة تتعلق بنظامها و اسرارها، تشمل جميع انواع المعلومات العسكرية و الأمنية و السياسية والاقتصادية و العلمية و الاجتماعية، مشار إليه لدى:د. **علي جعفر**، مرجع سابق، ص 569.

إن مختلف التشريعات الحديثة تصدت لمثل هذه الأفعال و جرمتها بالتنصيص عليها صراحة بموجب نصوص خاصة [329]، أو من خلال استقراء نصوص عامة كونها جريمة لها علاقة بحق الخصوصية و احترام سرية الاتصالات و المراسلات.

و لما قد تتسم به المعلومات و البيانات المرسلة أو المتداولة عبر مختلف وسائل الاتصال من سرية و خصوصية المراسلات أو للأهمية التي تكتسيها، فقد نصت عليها الاتفاقية الأوروبية بودابست للإجرام المعلوماتي السابق الإشارة إليها من خلال مادتها الثالثة، كما جاء في مذكرتها التفسيرية بخصوص هذه الجريمة أن الحق في احترام المراسلات مكفول عن طريق المادة الثامنة [330] من الاتفاقية الأوروبية لحقوق الإنسان.

إضافة إلى ذلك فإن الحق في احترام المراسلات مكفول دستوريا في مختلف دساتير دول العالم[331]. و كذلك نجد الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الموقعة بالقاهرة في 2010 قد نصت على جريمة الاعتراض القانوني من خلال مادتها السابعة على أن تأخذ بها الدول العربية في قوانينها العقابية أو القوانين الخاصة بمكافحة جرائم تقنية المعلومات [332]، و التي دعت الدول العربية على التعاون في هذا المجال و مكافحة هذا النوع من الإجرام.

المطلب الأول: المقصود بالاعتراض غير القانوني

329– من التشريعات العربية الحديثة و التي نصت على جريمة الاعتراض غير القانوني نجد القانون الاردني المؤقت المتعلق بتقنية المعلومات المادة 05 منه السابق الإشارة إليه، و كذلك المرسوم السلطاني رقم 12 لسنة 2011 ***المتعلق بجرائم تقنية المعلومات لسلطنة عمان.***

330– حيث نصت المادة الثامنة من ***الاتفاقية الأوروبية لحقوق الإنسان لسنة 1950*** ما يلي" 1– لكل إنسان الحق في احترام حرمة حياته الخاصة ، وحرمة منزله ومراسلاته . 2– يمنع تدخل السلطة العامة في ممارسة الإنسان لحقه المذكور الا في الأحوال التي يبينها القانون ، وفي حالة حماية الأمن القومي للمجتمع الديمقراطي ، او لحماية سلامة الناس او للمصلحة الاقتصادية او لمنع حالات الفوضى او ارتكب الجرائم ، او لحفظ الصحة والأخلاق العامة ، او لحماية ورعاية حقوق وحريات الآخرين" .

331– جاء في المادة 39 من ***الدستور الجزائري لسنة1996 المعدل و المتمم*** أن " لا يجوز انتهاك حُرمة حياة المواطن الخاصة، وحرمة شرفه، ويحميهما القانون.
سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة".

332– لقد صادقت مجموعة من الدول العربية على هذه الاتفاقية من بينها الأردن في 08 يناير سنة 2013 و مؤخرا العراق ب 03 سبتمبر 2013 ، و الجزائر في 8 سبتمبر 2014

ورد تحديد معنى الاعتراض في إطار المادة الثالثة من اتفاقية بودابست على انه التنصت أو نقل البيانات التي تتم داخل جهاز الحاسب او التي تتم عبر جهازين عن بعد عبر الشبكات المعلوماتية المختلفة، أو بترجمة الإنبعاثات الكهرومغناطيسية الصادرة من الحاسب يحمل هته البيانات أو التي تتم عبر الأجهزة اللاسلكية و ذلك عن طريق أي من الوسائل الفنية الغير علنية.

و لقد اشارت المذكرة التفسيرية لهذه الاتفاقية أن الهدف من هذه المادة هو حماية الحق في احترام نقل البيانات، و أن هذه الجريمة تمثل انتهاكا للحق في احترام الاتصالات مثل التنصت والتسجيل التقليدي للمحادثات التلفونية بين الأشخاص.

أما الاتفاقية العربية لمكافحة جرائم تقنية المعلومات فقد عرفتها في المادة السابعة على أنها: " الاعتراض المتعمد بدون وجه حق لخط سير البيانات بأي من الوسائل الفنية و قطع بث وإستقبال بيانات تقنية المعلومات".

كما أن الجريمة المنصوص عليها تطبق هذا المبدأ على كافة أشكال النقل الالكتروني للبيانات سواء تم هذا النقل عن طريق التلفون أو الفاكس أو البريد الالكتروني أو نقل الملفات[333].

لذلك فإن الاعتراض غير القانوني يشكل جريمة اعتراض طريق نظام المعلومات أو المعطيات المرسلة عن طريق النظم المعلوماتية بغرض التنصت عليها أو تسجيلها أو إعاقة سيرها، و أن هذه الجريمة تشكل جانبا من الاعتداء على حق الخصوصية و المتمثل في المساس بحرية الاتصالات و المراسلات، هذا الحق الذي نص عليه الدستور و الاعتداء عليه يشكل جريمة يعاقب عليها جزائيا[334].

و إذا كان مقررا وفقا للقواعد العامة آن القانون يقرر حماية المراسلات و المخابرات التلفونية، كما يكفل سريتها فإنه لا يجوز مراقبتها أو الاطلاع عليها إلا في الحالات الاستثنائية و المبينة في القانون و ذلك أيضا ينطبق على رسائل الاتصال الالكترونية و منها الرسائل المتداولة عبر البريد الالكتروني [335] و الاتصالات التي تتم عبر السكايب أو تطبيقات الاتصال الأخرى.

---

[333]– د. **هلالي عبد اللاه أحمد**، مرجع سابق، ص 78،79.

[334]– أنظر المواد 303 مكرر و ما بعدها **من قانون العقوبات الجزائري** المعدل و المتمم و المضافة بموجب القانون 06_23 الصادر بتاريخ 20 ديسمبر 2006، ج.ر عدد 84 ص 23.

[335]– د.**ضياء على أحمد نعمان**، الغش المعلوماتي، الظاهرة و التطبيقات، سلسلة الدراسات القانونية في المجال المعلوماتي، الطبعة الأولى، الوراقة الوطنية، مراكش– المغرب– 2011، ص 123.

و تتضح تلك الحماية في التشريع الجزائري من خلال ما جاء به المشرع من أحكام عامة واردة في المواد 303 مكرر و ما بعدها من قانون العقوبات و المادة 137 من نفس القانون، حيث أشار من خلال تعديله لسنة 2006 للجرائم التي تعد مساس بحرمة الحياة الخاصة و بأية تقنية كانت ما يلي:

- ✓ إلتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاه.
- ✓ إلتقاط او تسجيل أو نقل صورة لشخص في مكان خاص بغير إذن صاحبها أو رضاه.

و الاعتراض هو في مضمونه هو التقاط أو تنصت أو تسجيل أو مراقبة الاتصالات أو المراسلات التي تتم بوسائل تقنية أو الكترونية [336]، و بالتالي أي اعتراض لأي بيانات كانت مرسلة أو متداولة إلكترونيا و دون وجه حق يشكل جريمة تستحق العقاب.

هذا و إضافة إلى ذلك نجد قانون البريد و المواصلات السلكية و اللاسلكية رقم 2000-03 قد نص على هذا الشكل من الاعتداء من خلال المادة 127 و سيتم توضيح ذلك في العناصر التالية.

المطلب الثاني: أركان الاعتراض غير المشروع

تنشأ جريمة الاعتراض غير القانوني بكل فعل من شأنه إعاقة سير المعلومات أو التقاطها أو تسجيلها أو التنصت على الاتصالات أو ما هو مرسل عبر الشبكة أو أي وسيلة تناقل أو تراسل، و هذه الجريمة مثل كل جريمة لها أركانها نوضحها فيما يأتي:

الفرع الأول: الركن المادي لجريمة الاعتراض غير المشروع

يتمثل الركن المادي في جريمة الاعتراض غير القانوني للبيانات في فعل الاعتراض الذي يشمل أفعال التنصت أو الالتقاط [337] أو مراقبة الاتصالات أو إعاقة سير البيانات أو المعلومات الالكترونية المرسلة عبر الشبكة المعلوماتية أو عبر وسائل تقنية المعلومات أو قطع بثها أو استقبالها[338].

---

[336]- عرف المشرع الجزائري الاتصالات الالكترونية في القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من جرائم بتكنولوجيات الإعلام و الاتصال و مكافحتها في المادة 02 الفقرة و على أنها" أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية

[337]- عرفت ***الاتفاقية العربية لمكافحة جرائم تقنية المعلومات*** ، فعل الالتقاط من خلال المادة 8/2 على انه" مشاهدة البيانات أو المعلومات أو الحصول عليها"

[338]- المادة السابعة من **الاتفاقية العربية لمكافحة جرائم تقنية المعلومات** ، و كذا المادة الثامنة من **المرسوم السلطاني لسنة 2011** لسلطنة عمان سابق الإشارة إليهما

و هذه الأفعال بحسب ما جاء في اتفاقية بودابست و التشريعات السابق الإشارة إليها، يقوم بها الجاني بدون حق و باستعمال وسائل فنية غير علنية، لذلك فإنه لقيام هذا الركن لابد من توافر شروط معينة وفقا للمادة الثالثة من اتفاقية بودابست و المادة السابعة من الاتفاقية العربية مع إمكانية إضافة شروط أخرى في القوانين الداخلية للدول التي تعمل بهذه الاتفاقي ات و بحسب ما تراه ملائما لكيانها الداخلي:

البند الأول: استخدام وسائل فنية غير علنية لفعل الاعتراض

يشترط لقيام هذه الجريمة أن يتم اعتراض البيانات و المعلومات بإستخدام وسائل فنية معينة غير علنية تتعلق بالتصنت أو التحكم أو مراقبة محتوى الاتصالات، و الحصول على هذا الأخير قد يتم بطريقة مباشرة عن طريق الولوج إلى النظام المعلوماتي و استخدامه، أو بشكل غير مباشر عن طريق استخدام أجهزة التصنت، كما يمكن أن تشمل وسائل الاعتراض على تسجيل البيانات على أي من الأشرطة أو الدعامات المغناطيسية المعدة للتسجيل[339].

و أن نطاق الوسائل الفنية يمكن أن يمتد ليشمل حتى الأجهزة الفنية المتصلة بخطوط النقل أو الاتصال، مثل أجهزة تجميع و تسجيل الاتصالات اللاسلكية كما يمكن أن تشمل الكيانات المنطقية و كلمات المرور و الشفرات[340].

و أن جريمة الاعتراض غير القانوني وفقا لنص الاتفاقية السالف ذكرها تشترط أن تكون البيانات أو المعلومات محل الجريمة أن تكون قد نقلت بوسيلة من الوسائل الاتصال غير العلنية أي غير العمومية، بحيث يلاحظ أن مصطلح غير علنية صفة تتبع وسيلة النقل أو الاتصال من أجهزة و معدات و طرق معدة للنقل أو التسجيل أو التنصت أو لالتقاط البيانات و المعلومات [341]، و ليس طبيعة البيانات و المعلومات المرسلة في حد ذاتها، فهذه قد تكون متوفرة للناس كافة و لكن أصحاب المحادثة أو المراسلة يرغبون في الاتصال أو إرسالها بطريقة سرية، لاعتبارات معينة قد تكون شخصية أو اقتصادية أو تجارية أو سياسية...

---

[339]- **بلال أمين زين الدين** ، جرائم نظم المعالجة الآلية للبيانات في التشريع المقارن و الشريعة الإسلامية، دار الفكر الجامعي، الاسكندرية، 2008، ص 307

[340]– د.**هلالي عبد إللاه أحمد**، مرجع سابق، ص 80.

[341]– **بلال أمين زين الدين**، مرجع سابق، ص 307.

و لكن بالرغم من ذلك فإن مصطلح غير العلنية لا يستبعد الاتصالات في حد ذاتها التي تكون متاحة لأي من الأشخاص الذين يرغبون في إستعمال هذه الوسائل لهذه الغايات.

و ما يلاحظ كذلك على نص المادة الثالثة من اتفاقية بودابست و المادة السابعة من الاتفاقية العربية في تجريمهما لهذا السلوك لم تشترط نوعية معينة من البيانات أو المعلومات، فقد تكون هذه تخص امن الدولة أو معلومات سياسية أو عسكرية يتجسس عليها، أو إقتصادية، أو معلومات خاصة بشخص طبيعي أو معنوي أو غير ذلك، و بذلك يكون للمشرعين الوطنيين أن يحددوا شروطا معينة تتعلق بطبيعة المعلومات أو البيانات محل التجسس أو تبعيتها لجهة معينة.

و منه يمكن أن يكون النص عاما ليشمل كافة أنواع المعلومات و البيانات سواء كانت تابعة لجهة حكومية أو خاصة.

و هذا ما يلاحظ كذلك على بعض التشريعات العربية الحديثة [342] التي جرمت هذا السلوك في تشريعات خاصة بمكافحة جرائم تقنية المعلومات و التي لم تضع شروطا تتعلق بطبيعة البيانات و المعلومات محل التجسس و ما إذا كانت مالية أو شخصية أو غيرها.

البند الثاني: ان يكون الاعتراض غير مشروع

كما يشترط في هذا السلوك أن يكون بدون حق أو بصفة غير مشروعة، فهذه الجريمة قد تقع من أي شخص مهما كانت صفته سواء كان يعمل في مجال الأنظمة المعلوماتية [343] أم لا علاقة له بذلك، غير أنه يجب أن لا يكون الجاني من أولئك المصرح لهم بالحصول على تلك المعلومات.

فإذا كان المتهم بالقيام بالتصنت على المحادثات أو التقاط البيانات أو المعلومات المرسلة أو تسجيلها من من لهم الحق أو المصرح لهم مسبقا بذلك من أطراف المحادثة أو الاتصال، أو بناء على

---

[342]– نصت المادة 05 من ***القانون الاردني المؤقت رقم 30 لسنة 2010*** على أنه " كل من قام قصداً دون سبب مشروع بالتقاط أو باعتراض أو بالتصنت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أي نظام معلومات يعاقب بالحبس مدة لا تقل عن شهر ولا تزيد على سنة أو بغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) ألف دينار أو بكلتا هاتين العقوبتين"

و نصت كذلك المادة 08 من المرسوم السلطاني رقم 2011/12 السابق الإشارة إليه على انه " يعاقب بالسجن مدة لا تقل عن الشهر و لا تزيد عن السنة و بغرامة لا تقل عن خمسمائة ريال عماني و لا تزيد عن ألفي ريال عماني أو بإحدى هاتين العقوبتين، كل من إعترض عمدا و دون وجه حق بإستخدام وسائل تقنية المعلومات خط سير البيانات و المعلومات الالكترونية المرسلة عبر الشبكة المعلوماتية أو وسائل تقنية المعلومات أو قطع بثها أو استقبالها تصنت عليها"

[343]– ان العقوبة تكون اشد إذا كان الاعتراض من موظفي الاتصالات و المواصلات السلكية و اللاسلكية، وفق المادة 127 من ***قانون البريد و المواصلات رقم 2000_03*** المعدل و المتمم

ما له من حق استمده من سلطة معينة لها الحق بمراقبة الاتصالات، أو بناء على تصريح من الأطراف المعنية باختبار أجهزة الاتصالات و الحاسبات الشخصية و النظم المعلوماتية الخاصة بمؤسسة أو بشركة و الذي من خلاله تمكن من الاستماع إلى الأحاديث أو الاطلاع على البيانات و تسجيلها لإغراض تتعلق بالتجربة و اختبار الأجهزة و المعدات لوضع أفضل السبل الأمنية لحماية هذه البيانات و المعلومات[344] من أفعال الاعتداء عليها.

كما لا يعد فعل اعتراض غير مشروع إذا كان بناء على تصريح من جهات مختصة لاعتبارات تتعلق بالأمن القومي للدولة أو لإغراض التحقيقات و التحريات القضائية من أجل ضبط الأدلة و الوقائع الجرمية أو الأعمال التحضيرية التي تسبق الفعل الجرمي، و لدرء خاصة خطر المؤامرات التي تحاك ضد الدولة و أجهزتها، و مكافحة الإرهاب و غيرها من الاعتداءات التي تهدد أمن المجتمع، و هذا ما سنوضحه عند الحديث عن الجانب الإجرائي لهذه الجرائم.

في كل هذه الحالات يكون اعترض البيانات أو المعلومات بطريق مشروع إما بناء على اتفاق مسبق أو وفقا للحالات المستثنات بحكم القانون لوجود ضرورة ما.

الفرع الثاني: الركن المعنوي لجريمة الاعتراض غير المشروع

تقوم جريمة الاعتراض غير المشروع وفقا لما جاء في النصوص السابقة بتوافر القصد الجنائي العام بعنصريه العلم و الإرادة أما القصد الخاص فلم يستخلص من تلك النصوص حيث جاء في المادة الثالثة من اتفاقية بودابست أن يكون " الاعتراض عمدا و بدون حق.."، و كذلك الاتفاقية العربية لمكافحة جرائم تقنية المعلومات حيث جاء فيها " الاعتراض المتعمد بدون وجه حق..." [(345)].

و عليه يجب أن يعلم الجاني بأن حصوله على تلك المعلومات أو البيانات و أن التصنت على المحادثات أو تسجيل أو التقاط البيانات المعلوماتية تم بوجه غير مشروع و ضد إرادة صاحب الاتصال أو ضد رغبة صاحب السيطرة ؛

---

[344]– **بلال أمين زين الدين**، مرجع سابق، ص 309.

[345]– المادة 07 من **الاتفاقية العربية لمكافحة جرائم تقنية المعلومات** السابق الإشارة إليها، و نفس الأمر بالنسبة للمادة 05 من **القانون الأردني المؤقت** رقم 30 لسنة 2010، و المادة 08 من **المرسوم السلطاني رقم** 2011/12 المشار إليه سابقا.

أما إذا لم يتوفر فيه هذا العلم مثل من يعتقد أن أطراف الاتصال قد صرح ا له بذلك أو من سلطته مراقبة الاتصالات[346]على نحو فيه خطأ في تفسير حدود سلطته و إختصاصه أو أنه دخل إلى نطاق الاتصال على سبيل المصادفة فإنه في هذه الحالة عنصر العلم قد إنتفى و تبعا له ينتفي الركن المعنوي لهذه الجريمة.

هذا من جهة و من جهة أخرى لابد أن تتجه إرادة الجاني إلى إتيان هذا الفعل بمخالف ته للقانون و لإرادة صاحب المراسلة أو الاتصال، فإذا ما اجبر على ذلك من قبل أخريين لما قد يمتلكه من خبرة أو مهارة في إستعمال أجهزة التصنت و التسجيل مثلا، فإنه لا قيام للقصد الجنائي كذلك و بالتالي لا جريمة[347].

المطلب الثالث: الاعتراض غير القانوني في التشريع الجزائري

يعتبر التصنت على الاتصالات أو على ما هو مرسل عن طريق الشبكة المعلوماتية أو أي نظام معلوماتي أو بأية تقنية اعتداءا خطيرا على حرمة الحياة الخاصة و قدسيتها، و بالتحديد حرية الاتصال و المراسلات، هذه الحريات التي كفلها الإعلان العالمي لحقوق الإنسان [348](1948) و نص علي حمايتها الاتفاقية الأوروبية لحقوق الإنسان[349](1950).

كما أن هذه الحقوق كفلتها دساتير الدول و منها الدستور الجزائري حيث جاء فيه " سرية المراسلات و الاتصالات بكل أشكالها مضمونة"[350].

---

[346]– **بلال أمين زين الدين، مرجع** سابق، ص 310.

[347]- **بلال أمين زين الدين،** نفس المرجع، ص 310.

[348]– تنص المادة 12 من **الإعلان العالمي لحقوق الإنسان** ا لذي اعتمد ونشر بموجب قرار الجمعية العامة للأمم المتحدة 217 المؤرخ في 10 ديسمبر 1948: " لا يعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه وسمعته، ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات.

[349]– المادة 08 **اتفاقية حماية حقوق الإنسان** في نطاق مجلس أوروبا (روما في 4 نوفمبر 1950).

[350]– المادة 2/39 من **الدستور الجزائري** لسنة 1996 المعدل و المتمم.

و نص في قانون العقوبات المعدل بالقانون 06_23 على مادة جديدة تشمل الاعتداء على حرمة الحياة الخاصة جاء فيها أنه:" يعاقب....كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأي تقنية كانت و ذلك:

- ✓ بالتقاط أو تسجيل أو نقل مكالمات خاصة أو سرية بغير إذن صاحبها أو رضاه
- ✓ بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص، بغير إذن صاحبها أو رضاه..."[351].

و عليه لم يشر صراحتا المشرع الجزائري شأنه شأن المشرع الفرنسي عند إضافته قسم خاص بجرائم أنظمة المعالجة الآلية للمعطيات على حكم أو نص خاص بجريمة الاعتراض المعلوماتي، و لكن استدرك الأمر كونه قد حمى الاعتداء على الاتصالات و المراسلات بأية تقنية كانت و وسع من مجال حماية الاتصالات و المراسلات من خلال المادة 303 مكرر المضافة لقانون العقوبات 2006 و شملها ضمن حماية الحياة الخاصة.

و الأساس في جريمة الاعتراض غير المشروع هو حماية حرية الاتصالات و عدم إعاقة سيرها أو اعتراضها حتى و لو لم تكن المعلومات سرية و لكن أطراف الاتصال أرادوا أن تكون بوسيلة سرية أو غير علنية.

كما أن التشريعات التي نصت صراحة على جريمة الاعتراض غير المشروع في نصوص عقابية خاصة[352] كانت تهدف إلى تشجيع استخدام أنظمة المعلومات و الشبكات المعلوماتية و انتشارها من خلال حماية مستخدميها الذين يحرصون على ضمان السرية و الخصوصية و الحماية لمعلوماتهم المالية و الشخصية و غيرها.

و نجد أن المشرع كذلك قد جرم هذا الفعل من خلال تشريعات خاصة، مثل ما نجده في قانون البريد و المواصلات السلكية و اللاسلكية رقم 2000_03 المعدل و المتمم حيث جاء في المادة 127 ما يلي:" تطبق العقوبات المنصوص عليها في المادة 137 من قانون العقوبات على كل شخص مرخص له بتقديم خدمة البريد السريع الدولي أو كل عون يعمل لديه و الذي في إطار ممارسة مهامه، يفتح أو يحول أو يخرب البريد أو ينتهك سرية المراسلات أو يساعد في ارتكاب هذه الأفعال ،

---

[351]– المادة 303 مكرر من ***قانون العقوبات المعدل و المتمم***.

[352]– نجد من تلك التشريعات ***القانون الأردني و العماني***.

تسري نفس العقوبات على كل شخص مرخص له بتقديم خدمة مواصلات سلكية و لاسلكية وكل عامل لدى متعاملي الشبكات العمومية للمواصلات السلكية و اللاسلكية و الذي في إطار ممارسة مهامه و زيادة على الحالات المقررة قانونا، ينتهك و بأية طريقة كانت سرية المراسلات الصادرة أو المرسلة أو المستقبلة عن طريق المواصلات السلكية و اللاسلكية أو الذي أمر أو ساعد في ارتكاب هذه الأفعال.

يعاقب بالحبس من شهرين إلى سنة و بغرامة مالية من 50.000 دج إلى 1.000.000 دج أو بإحدى هاتين العقوبتين، كل شخص غير الأشخاص المذكورين في الفقرتين السابقتين، ارتكب أحد الأفعال المعاقب عليها بموجب هاتين الفقرتين ...." [353]

و عليه فقد حاول المشرع الجزائري الإحاطة بكل المعطيات لحماية البيانات و المعلومات المعالجة آليا أو المرسلة عبر شبكة المعلوماتية أو وسائل تقنية المعلومات و الاتصالات أو قطع سيرها و اعتراضها سواء في قانون العقوبات أو قوانين خاصة مثل قانون الاتصالات.

كما حدد حالات المراقبة غير المشروعة و الحالات التي أجاز فيها المراقبة الالكترونية القضائية لأغراض التحري و التحقيق أو للوقاية من الإخطار التي قد تمس أمن الدولة و مؤسساتها من خلال ما جاء به في القانون رقم 09_04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، و سيأتي الحديث مفصلا عن هذا الإجراء الخطير الذي يعد انتهاكا لحريات الأشخاص في مقابل الحفاظ على أمن الدولة وحماية المجتمع، و ذلك عند حديثنا عن الجوانب الإجرائية للسلامة المعلوماتية و خصوصية إجراءات التحقيق و التحري و الضبط في الجرائم المعلوماتية في الباب الأخير من هذه الرسالة.

أما بالنسبة للمشرع الفرنسي فقد أصدر القانون رقم 91-646 في 10 يوليو 1991 المنظم لمراقبة المحادثات و المعدل بموجب القانون رقم 669/2004، حيث نصت المادة الأولى منه على" سرية المراسلات التي يام نقلها بطريق الهاتف أو غيره من وسائل الاتصال الالكتروني يضمن القانون حمايتها". و يرد على هذه القاعدة إستثناء نصا عليه الفقرة الثانية من المادة الأولى بقولها: " لا يجوز

---

[353]- جرم كذلك المشرع الأردني فعل الاعتراض في **القانون المؤقت رقم 30 لسنة 2010** و من قبله في **قانون الاتصالات رقم 13 لسنة 1995 المعدل و المتمم لغاية 2011** حيث جاء في المادة 76 منه ما يلي: " كل من إعترض أو أعاق أو حور أو شطب محتويات رسالة بواسطة شبكة الاتصالات أو شجع غيره على القيام بهذا العمل يعاقب بالحبس مدة لا تقل عن الشهر و لا تزيد على ستة أشهر أو بغرامة لا تزيد عن (200) دينار أو بكلتا العقوبتين" .

الاعتداء على هذا السر إلا عن طريق السلطات العامة، في حالات الضرورة التي تبررها المصلحة العامة المنصوص عليها في القانون و في نطاق الحدود المبينة فيه"[354].

المبحث الرابع:

إساءة استخدام الحاسب أو الاستعمال غير المشروع للمعلومات

إن أي جريمة متعمدة قد تمر بمراحل متتالية أو قد تحتاج إلى حيازة و الحصول على ب عض الوسائل المساعدة أو المسهلة لارتكابها، و لما كانت جرائم الاعتداء على نظم المعالجة الآلية للمعطيات أكثر الجرائم خطورة و انتشارا في الوقت الراهن، خاصة منها ما تمس سرية المعلومات و سلامتها و إتاحتها، و أن الدول التي جرمت الأفعال الماسة بهذه العناصر قد تبنت سياسة جنائية تضمن الوقاية و الحماية و تحقق أهداف الأمن المعلوماتي و السلامة المعلوماتية من خلال تجريم أي فعل متوقع قبل و بعد تمام الجريمة أو الاعتداء على تلك العناصر.

و من شأن ذلك أن جاء في اتفاقية بودابست للإجرام المعلوماتي أنه:" يجب على كل طرف أن يتبنى الإجراءات التشريعية و أية إجراءات يرى أنها ضرورية لتجريم تبعا لقانونه الداخلي القيام عمدا و دون حق بما يلي:

أ. إنتاج أو بيع، أو الحصول من اجل الإستخدام، أو استيراد أو نشر، أو أي أشكال أخرى للوضع تحت التصرف.

1.أي جهاز يحتوي على برنامج معلوماتي مصمم أو موفق بشكل أساسي لغرض إرتكاب إحدى الجرائم المنصوص عليها وفقا للمواد من 2_5 السابق الإشارة إليها.

2. كلمة المرور، أو شفرة الدخول، أو أي بيانات مماثلة تسمح بالولوج إلى كل أو إلى جزء من نظام الحاسب، بنية إستخدامها لغرض إرتكاب جريمة من الجرائم المشار إليها في المواد من 2-5.

ب. حيازة أي عنصر من العناصر المشار إليها في البندين أ. 1، أ.2 بنية إستخدامه في إرتكاب أي جريمة من الجرائم الواردة في المواد 2_5.

---

[354]- **الموسوس عتو** ، حماية الحق في الخصوصية في القانون الجزائري في ظل التطور العلمي و التكنولوجي- دراسة مقارنة- اطروحة لنيل شهادة الدكتوراه في العلوم تخصص علوم قانونية، فرع قانون تجاري، جامعة جلالي ليابس، كلية الحقوق و العلوم السياسية، سيدي بلعباس، 2014، ص 299.

و يمكن لأي طرف أن يشترط في قانونه الداخلي وجود بعض هذه العناصر من أجل تقرير المسئولية الجنائية.."[355]

يتضح من هذه المادة أن الإتفاقية لم تقتصر على تحديد الأفعال التي تشكل إعتداء على المعلومات و النظم المعلوماتية، أو النص على السبل الرادعة لعقاب مرتكبي هذه الأفعال، و إنما ذهبت بهذه المادة إلى أبعد من ذلك بحث الدول على تجريم أي تصرف من شأنه أن يؤدي إلى إرتكاب الأفعال المحدد من المواد 2_5 من الاتفاقية أو كان الغرض منها المساس بعناصر الأمن المعلوماتي.

هذا و قد جاء في مذكرتها التفسيرية أن هذا النص يعتبر كجريمة جنائية منفصلة و مستقلة الارتكاب عمدا لأفعال غير مشروعة خاصة ترتبط ببعض الأجهزة أو بيانات الولوج من حيث إساءة إستخدامها بغرض إرتكاب الجرائم السابق الإشارة إليها ضد سرية و سلامة و عدم إتاحة نظم و بيانات الحاسب.

و كما يتطلب إرتكاب هذه الجرائم غالبا حيازة وسائل الولوج، مثال ذلك أدوات القرصنة أو أي أدوات أخرى، فإن هناك دافعا قويا للحصول عليها لأغراض إجرامية، الأمر الذي يمكن أن يؤدي في النهاية إلى خلق نوع من السوق السوداء لإنتاج و توزيع مثل هذه الأدوات[356].

و تضيف المذكرة التفسيرية كذلك أنه " من أجل وقاية أكثر فاعلية من هذه المخاطر، فإنه يجب على قانون العقوبات أن يحظر الأفعال راجحة الخطورة من المنبع، قبل إرتكاب الجرائم المشار إليها في المواد من 2_5 من هذه الاتفاقية.

و هذا ما فعله المشرع الجزائري حينما نص على هذه الجريمة من خلال المادة 394 مكرر2 حيث شدد العقاب لكل من يرتكب أحد الأفعال التي تسهل أو تؤدي إلى إرتكاب الجرائم الماسة بسرية و إتاحة و توافر المعلومات و النظم المعلوماتية و المشار إليها في القسم الخاص بجرائم المعالجة الآلية للمعطيات.

و هو بذلك حذا حذو المشرع الفرنسي الذي جاء بهذه الجريمة في المادة 323_3_1 المضافة إلى قانون العقوبات المعدل سنة 2004[357]، و هذا بعد أن صادقت فرنسا على إتفاقية بودابست التي أصبحت سارية المفعول إبتداءا من 2004 و باعتبار فرنسا دولة في الاتحاد الأوروبي.

---

[355]- المادة 06 من **اتفاقية بودابست** لسنة 2001 بشان الإجرام المعلوماتي.

[356]- د. **هلالي عبد اللاه أحمد**، مرجع سابق، ص 99-101.

[357] - **Art.323-3-1** du C.P.F ;(**inséré par Loi nº 2004-575 du 21 juin 2004 art. 46 I Journal Officiel du 22 juin 2004**) dispose que « Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les

غير أن موقف المشرع الجزائري في هذه الحالة كان أوسع من نظيره الفرنسي أو ما جاء في الاتفاقية الأوروبية حيث كان نطاق الحماية أشمل، و وضع في الحسبان كل احتمال قد ينجم عنه ارتكاب تلك الجرائم و وسع دائرة العقاب من خلال ما جاء به في الفقرة الثانية من المادة 394 مكرر 2 بقوله: " ...حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم..".

فهو بذلك يحمي المعطيات و المعلومات المتحصل عليها بطريقة غير مشروعة و رغبة منه في الحفاظ على ما تبقى من سريتها.

و لخطورة هذه الأفعال وضع المشرع نصا القانونيا رادعا و وقائيا لكل من يحوز وسائل تساعد في ارتكاب الجرائم المنصوص عليها أو يتعامل في معلومات متحصل عليها من إحدى تلك الجرائم السابق دراستها.

و الأمر نفسه نصت عليه الاتفاقية العربية بشأن مكافحة جرائم تقنية المعلومات من خلال المادة التاسعة[358].

و جريمة إساءة إستخدام الحاسب كما جاء في إتفاقية بودابست أو كما تسمى جريمة اساءة استخدام وسائل تقنية المعلومات في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات كغيرها من الجرائم يشترط لقيامها وجود أركان، ركن مادي(المطلب الأول) و ركن معنوي(المطلب الثاني) و نفصل في ذلك حسب الآتي:

المطلب الأول: الركن المادي

يتحقق الركن المادي بإتيان الجاني نشاط إجرامي، و وفقا لهذه الجريمة قد يتحقق هذا النشاط بصور مختلفة تنصب على محل معين لتحقيق نتيجة و نوضح ذلك كما يلي:

الفرع الأول: النشاط الإجرامي

---

articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée »

[358]- تنص المادة 09 من **الاتفاقية العربية لمكافحة جرائم تقنية المعلومات** على أنه:" 1- إنتاج أو بيع أو شراء أو استيراد أو توزيع أو توفير : أ) أية أدوات أو برامج مصممة أو مكيفة لغايات ارتكاب الجرائم المبينة في المادة السادسة إلى المادة الثامنة . ب) كلمة سر نظام معلومات أو شيفرة دخول أو معلومات مشابهة يتم بواسطتها دخول نظام معلومات ما بقصد استخدامها لأية من الجرائم المبينة في المادة السادسة إلى المادة الثامنة – 2 .حيازة أية أدوات أو برامج مذكورة في الفقرات أعلاه بقصد استخدامها لغايات ارتكاب أي من الجرائم المذكورة في المادة السادسة إلى المادة الثامنة".

بالرجوع إلى نص المادة 394 مكرر 2 عقوبات جزائري مقارنتا مع النص الفرنسي (323_3_1 عقوبات) و نص المادة 06 من اتفاقية بودابست، يتضح أن المشرع الجزائري حدد النشاط الإجرامي لجريمة التعامل في معلومات غير مشروعة في صورتين من خلال فقرتي المادة السابق الإشارة إليها، فأما الصورة الأولى بقوله " تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم" و هي نفسها منصوص عليها في القوانين المقارنة محل الدراسة، أما الصورة الثانية الواردة في فقرة الثانية من المادة 394 مكرر 2 أن " حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم" صورة تفرد بها المشرع الجزائري عن باقي المشرعين، لذلك سوف نحدد كل نشاط جرمي وفقا لتلك الصور:

البند الأول : التعامل في معلومات لإرتكاب جريمة

يتضح أن المشرع الجزائري إتخد الحيطة من خلال تجريم بعض الأفعال التي قد تشكل ازديادا في نسبة الجريمة ما لم يتم العقاب عليها، و تتمثل تلك الأفعال في التصميم أو البحث أو التوفير أو النشر أو الاستعمال، و متى توافر أي فعل من هته الأفعال يتشكل النشاط الإجرامي لجريمة التعامل في معلومات لإرتكاب أحد الجرائم المنصوص عليها في القسم السابع مكرر 1 المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات و هو ما ورد في الفقرة الأولى من المادة 394 مكرر 2 باستعمال المشرع لفظ " أو".

أولا: التصميم و البحث في معطيات مخزنة أو معالجة آليا

التصميم هو إعداد معلومات أو معطيات صالحة لارتكاب الجريمة من قبل أشخاص مختصين في هذا المجال مثل مصممي البرامج المعلوماتية [359] لغرض إرتكاب جرائم ضد سرية وسلامة و توافر النظم و البيانات المعلوماتية.

---

[359]- **رشيدة بوكر**، مرجع سابق الإشارة إليه، ص 281.

و قد ورد في إتفاقية بوداست مصطلح إنتاج بمعنى إنتاج أو صنع أي جهاز يحتوي على برنامج معلوماتي مصمم لغرض إرتكاب إحدى الجرائم المنصوص عليها في المواد من 02_05 من الاتفاقية ، و هو نفس ما ورد في الاتفاقية العربية.

أما البحث كلمة وردت في المادة 394 مكرر 2 من قانون العقوبات الجزائري و التي لا نجدها في نص المادة 06 من اتفاقية بودابست و إن جاء النص مفتوح و عام و يمكن لأي دولة أن تضيف أي شكل من الأشكال الأخرى للوضع تحت التصرف.

هي كلمة استعملها المشرع الجزائري ذات صياغة واسعة، فهل كان المقصود من ورودها في النص هو تجريم البحث عن كيفية تصميم المعلومات و إعدادها؟ أم تجريم مجرد البحث عن أي معلومات أو معطيات يمكن أن ترتكب بها جرائم المساس بأنظمة المعالجة الآلية للمعطيات؟

و بالتالي كل ما يقوم به الشخص من بحث عن معلومات و مواقع من خلال شبكة الانترنت و بواسطة محركات البحث، كالبحث عن كيفية القيام باختراق الأنظمة المعلوماتية يشكل جريمة؟.

إن الأخذ بالتفسير الواسع لهذه العبارة يوسع من نطاق دائرة التجريم و يشكل تهديدا، فليس كل من يبحث عن معلومات يمكن أن ترتكب بها جريمة يعد قد ارتكب جرما [360]، و إنما من يبحث عن معلومات لتصميم ما يمكن أن ترتكب به هذه الجرائم يكون قد إرتكب جريمة إساءة إستعمال معلومات أو تقنية المعلومات لإرتكاب جريمة، و لعل هذا ما جعل المشرع الجزائري يستتبع كلمة بحث بعد كلمة تصميم.

ثانيا: تجميع أو توفير معطيات مخزنة أو معالجة

جرم كذلك المشرع الجزائري شكل من أشكال الاستعمال غير المشروع للمعلومات و هو الحصول على قدر من المعلومات التي تشكل خطرا و جمعها لارتكاب إحدى جرائم الاعتداء على نظم المعالجة الآلية[361]، بما اصطلح عليه بالتجمع.

أما المشرع الفرنسي فقد ذكر مصطلح الحيازة" Détenir " و يبدو من ذلك تأثره باتفاقية بودابست التي ورد فيها ذات المصطلح.

---

[360]– **رشيدة بوكر**، نفس المرجع، ص 281.

[361]- نفس المرجع، ص 281.

إضافة إلى ذلك جرم المشرع الجزائري فعل التوفير و هو نفس ما أشار إليه المشرع الفرنسي في المادة 323_3_1 عقوبات[362]" التوفير أو الوضع تحت التصرف" أما إتفاقية بودابست فقد فتحت المجال تحت عبارة " أي أشكال أخرى للوضع تحت التصرف".

و مصطلح التوفير يقتضي إتاحة المعلومات و جعلها تحت تصرف الغير و في حيازته مثل توفير كلمات المرور، أو شفرات الدخول إلى كل أو جزء من نظام المعالجة الآلية، و قد توسع القضاء الفرنسي بخصوص تفسير معنى التوفير ليشمل أفعال الكشف أو الإفشاء العلني للثغرات الأمنية في النظام[363]، أي توفير كل ما من شأنه تسهيل إرتكاب جرائم المساس بأنظمة المعالجة الآلية للمعلومات مما يشكل انتهاكا للسلامة المعلوماتية و الامن المعلوماتي.

و لقد أشارت كذلك المذكرة التفسيرية لاتفاقية بودابست بشان الإجرام الالكتروني و السابق الإشارة إليها، معنى بعض المصطلحات من بينها الوضع تحت التصرف و التي تشير إلى وضع أجهزة على الخط on ligne ليتم استخدامها بواسطة الغير....[364].

ثالثا : النشر و الاتجار

ورد ذكر فعل النشر في المادة 394 مكرر 2 عقوبات جزائري و في فقرتيها الأولى والثانية و هي جريمة نشر معلومات صالحة لارتكاب إحدى الجرائم المعاقب عليها في المواد السابقة.

و ورد ذكرها كذلك في اتفاقية بودابست من خلال المادة 2/6، و المقصود بالنشر في هذه الجريمة هو إذاعة معلومات محل الجريمة و تمكين الغير من الاطلاع عليها و ذلك مهما كانت طبيعتها[365].

كما جاء في المذكرة التفسيرية لاتفاقية بودابست أن النشر la diffasion ينبغي أن يمتد ليشمل كل نشاط من شأنه نقل بيانات إلى الآخرين.

أما بخصوص المشرع الفرنسي فلا نجده قد أشار إلى هذا الفعل في المادة 323_3_1 الذي يمكن أن ترتكب به إحدى الجرائم السابقة، غير أنه ضيق من نطاق تجريم هذا الفعل و نص عليها فيما

---

[362] **Art** 323-3-1 De Code Pénal Français Modifié par LOI n°2013-1168 du 18 décembre 2013 - art. 25 ; dépose que « Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, **de céder ou de mettre à disposition** un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée »

[363] – **Nicolas ARPAGAIN**, op.cit, p 36,38.

[364]- د.**هلالي عبد اللاه أحمد**، مرجع سابق، ص 101.

[365]- د.**محمد خليفة** ، جرائم الحاسوب، مشار اليه لدى **رشيدة بوكر**، مرجع سابق، ص 283.

يخص إفشاء المعلومات و البيانات التي قد تضر أو تمس بحرمة الحياة الخاصة من خلال المادة 226-22[366] أو ما يتعلق بإفشاء البيانات الاسمية او الشخصية بالكشف والإفصاح عنها.

البند الثاني: التعامل في معلومات متحصل عليها من إحدى الجرائم

و هو ما ورد في الفقرة الثانية من المادة 394 مكرر 2 بقولها:"....حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم"

و هذه الصورة لا نجد المشرع الفرنسي قد نص عليها و لا نجدها في اتفاقية بودابست وإنما تفرد المشرع الجزائري بالتنصيص عليها، حيث نجده قد تدرج في تصور المراحل التي يتبعها المجرم المعلوماتي فمن اختراق أو البقاء في النظام المعلوماتي غشا إلى تخريبه أو تخريب معطياته إلى مرحلة اعتراض المعلومات و الحصول عليها لاستعمالها أو إفشائها أو الاتجار فيها .

كما أن الأفعال التي ورد ذكرها في المادة السابقة من النص الجزائري لا يشترط قيامها كلها حتى يتحقق النشاط الإجرامي بل يكفي تحقق فعل من هته الأفعال لقيام هذه الجريمة، ويتمثل النشاط الإجرامي في الأفعال الآتية:

أولا: الحيازة

الحيازة[367] هي سلطة واقعية يمارسها الحائز على الشيء أو وضع واقعي ينطوي على مباشرة الحائز سلطة فعلية على الشيء

و عرفها غارسون بأنها: سيطرة واقعية و إرادية للحائز على المنقول تخوله الانتفاع به تعديل كيانه، تحطيمه أو نقله، فهي إذا سيطرة إرادية للشخص على الشيء[368] .

---

[366] **-Art 226-22 du C.P.F** Modifié par ***Loi n°2004-801 du 6 août 2004 - art. 14 JORF 7 août 2004***
« Le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.

La divulgation prévue à l'alinéa précédent est punie de trois ans d'emprisonnement et de 100 000 Euros d'amende lorsqu'elle a été commise par imprudence ou négligence.

Dans les cas prévus aux deux alinéas précédents, la poursuite ne peut être exercée que sur plainte de la victime, de son représentant légal ou de ses ayants droit »

[367]- تقوم الحيازة على نية احتباس المعلومات و السيطرة عليها أبدا أو لمدة مؤقتة أو الاستمرار في السيطرة عليها

و بالتالي فان الحيازة سلطة واقعية يمارسها الحائز على المعلومات، أو وضع واقعي ينطوي على مباشرة الحائز سلطة فعلية على المعلومات المتحصل عليها.

فوجود المعلومات لدى الحائز الجاني و استعمالها و استغلالها طبقا لما تسمح به طبيعة المعلومات يكفي القول بتحقق السيطرة عليها سيطرة مستقلة لا يكون فيها خاضعا لسلطة شخص أخر، مثل العامل الذي تربطه علاقة عمل بالمعلومات، كما لا يسيطر عليها بنية الاحتباس ولا يقوم بأي عمل عليها بدون تصريح[369].

و من شروط الحيازة كذلك أن تكون السيطرة على المعلومات المتحصل عليها مستمرة لمدة معينة أو للأبد.

مع علم أن الحيازة في جريمة التعامل في معلومات غير مشروعة تكون حيازة غير مشروعة كون المعلومات المتحصل عليها هي ناتجة من إحدى الجرائم الماسة بنظم المعالجة الآلية للمعطيات طبقا لما جاء في المادة 394 مكرر 2 عقوبات جزائري.

ثانيا: الإفشاء و النشر

إن استعمال الوسائل الحديثة في نقل و تخزين و جمع المعلومات ساعد الدول والمؤسسات و الأشخاص على حد سواء في تنظيم شؤونها، إلا انه من جانب أخر كان لهذه الوسائل جانب مضر في فضح و إفشاء ما تحتويه في حالة اختراقها من قبل الهاكر [370] أو القراصنة لاستخدامها لأغراض شخصية أو للابتزاز أو لإفشائها و نشرها بحيث يطلع عليها غير أصحابها و مالكيها.

---

[368]- د.**محمد زكي أبو عامر**، قانون العقوبات، القسم الخاص، الدار الجامعية للطباعة و النشر، بيروت، 1990، ص 149، مشار اليه لدى **خليفة الملط**، مرجع سابق، ص 205.

[369]– **رشيدة بوكر**، مرجع سابق، ص 285.

[370]– **الهاكر**: هو الشخص الذي يقوم بإنشاء وتعديل البرمجيات والعتاد الحاسوبي. وقد أصبح هذا المصطلح ذا مغزى سلبي حيث صار يطلق على الشخص الذي يقوم باستغلال النظام من خلال الحصول على دخول غير مصرح به للأنظمة والقيام بعمليات غير مرغوب فيها وغير مشروعة .غير أن هذا المصطلح (هاكر) يمكن أن يطلق على الشخص الذي يستخدم مهاراته لتطوير برمجيات الكمبيوتر وإدارة أنظمة الكمبيوتر وما يتعلق بأمن الكمبيوتر.

و تجنبا لهذا الأمر الخطير قام المشرع الجزائري على خلاف المشرع الفرنسي، بتجريم إفشاء و نشر و بأية وسيلة[371] كانت المعلومات المتحصل عليها من إحدى جرائم الاختراق أو البقاء غير المصرح به أو جرائم الإتلاف المعلوماتي طبقا لما جاء في المادة 394 مكرر 2 عقوبات جزائري.

و فعل الإفشاء كالنشر لا يتم فيهما قصر المعلومة المتحصل من جريمة غير مشروعة على الجاني فقط أو حيازتها من طرفه فقط بل يفترض في ذلك انتقالها أو تقديمها لأشخاص آخرين[372].

هذه الأفعال التي سعى المشرع من ورائها إلى تضييق نطاق إنتهاك السرية و تجنب وصولها لغير أصحابها أو الاطلاع عليها.

ثالثا: الإستعمال

أما الاستعمال فهو أشد خطورة من الأفعال السابقة كون المتحصل على المعلومات من الجرائم المنصوص عليها في المواد من 394 مكرر إلى 394 مكرر 2 قد يستغلها لإغراض اشد خطورة مثل الابتزاز أو المنافسة أو غير ذلك.

و هذا ما يستفاد من تجريمه لهذا الفعل في المادة 394 مكرر 2 بقولها : " ...إستعمالها لأي غرض كان...."، و ذلك يعني حتى لو استعملت لأغراض مشروعة فإن الحصول عليها كان بطريق غير مشروع.

الفرع الثاني: محل النشاط الإجرامي

إن المشرع الجزائري من خلال المادة 394 مكرر 2 عقوبات جزائري قد حدد محل جريمة التعامل بمعلومات غير مشروعة في المعلومات أو المعطيات التي قد تكون في حالات عدة، ففي الفقرة الأولى من المادة السابقة نجده يتحدث عن " تجميع أو تصميم، بحث أو توفير أو الاتجار في معطيات.." غير أنه وسع نطاق التجريم بعدم حصره للحالة التي تكون عليها تلك المعلومات بقوله:" معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية.."

كما لم يحدد المشرع الجزائري كذلك طبيعة هته المعلومات، غير أنه أشار أن تلك المعلومات و في أي حالة كانت عليها يمكن أن ترتكب بها إحدى الجرائم المنصوص عليها سابقا، مما يعني أنه قد يتم

---

[371]– لم يحدد المشرع نوع الوسيلة التي قد يتم بها إفشاء أو نشر المعلومات المتحصل عليها من جرائم المساس بأنظمة المعالجة الآلية للمعطيات، مما يستفاد منه أن الجريمة تقع حتى ولو تم النشر أو الإفشاء بوسائل تقليدية.

[372]– مشار إليه لدى: **محمد خليفة الملط**، المرجع السابق، ص 223.

التعامل في تلك المعلومات أو المعطيات بجمعها أو تصميمها وغير ذلك و لكن قد لا تكون صالحة لارتكاب جريمة، بمعنى مجرد قيام تلك الأفعال عليها يعد فعلا غير مشروع و إذا قام بذلك متعمدا .

أما بخصوص الفقرة الثانية من المادة 394 مكرر 2 و التي تمثل الصورة الثانية من جريمة التعامل في معلومات غير مشروعة ، حيث أن محل النشاط الإجرامي هو المعلومات المتحصل عليها فقط من إحدى الجرائم المنصوص عليها في المواد من 394 مكرر إلى 394 مكرر 1 ، وليس أي جريمة هي محل اعتبار.

و على خلاف المشرع الفرنسي الذي لم يحصر محل هته الجريمة في المعلومات فقط بل شمل كل الأجهزة و الأدوات و البرامج المعلوماتية و حتى المعلومات، و لكنه من جهة أخرى ضيق نطاق هته الوسائل و الأدوات في أن جمعها أو حيازتها أو نشرها يكون معد خصيصا لارتكاب الجرائم المنصوص عليها في المواد من 323-1 إلى 323-3 عقوبات فرنسي[373].

و في هذا المجال قد يكون المشرع الفرنسي متأثر بإتفاقية بودابست لسنة 2001 التي جاء في مادتها السادسة فقرة أ/ 1:" أي جهاز يحتوي على برنامج معلوماتي مصمم أو موفق بشكل أساسي لغرض إرتكاب إحدى الجرائم المنصوص عليها....."

كما أشارت المذكرة التفسيرية لهذه الاتفاقية لطبيعة الأجهزة محل التجريم، و هل يشمل على الأجهزة المصممة خصيصا لارتكاب الجرائم المعلوماتية أو مظلة التجريم تتسع لتشمل حتى الأجهزة ذات الإستخدام المزدوج أي المشروع و غير المشروع وفقا لقصد الشخص من إستخدامها و توظيفه لها، فجاء فيها أنه سبق أن ناقش الفقهاء مسألة ما إذا كانت الاجهزة يجب أن تقتصر على تلك المصممة فقط أو بشكل خاص من أجل إرتكاب الجرائم، و بالتالي يتم إستبعاد الأجهزة ذات الاستخدام المزدوج.

و لكن أخذ على هذا الاتجاه أنه اتجاه ضيق للغاية،إذ أنه يخاطر في الواقع بخلق صعوبات منيعة فيما يتعلق بتقديم الدليل، في الإجراءات الجنائية مما يجعل النص غير قابل للتطبيق أو أنه يطبق فقط في حالات نادرة.

---

[373] -**Art.323-3-1 du code pénal français** (inséré par Loi nº 2004-575 du 21 juin 2004 art. 46 I Journal Officiel du 22 juin 2004). « Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée ».

كما تم أيضا استبعاد الرأي القائل بإدراج كل الأجهزة حتى تلك التي تم إنتاجها و نشرها بشكل مشروع، و لذا لا يتبقى من اجل تطبيق العقاب كما يرى الاتجاه الثالث إلا الاعتماد على العنصر الشخصي أي قصد ارتكاب جريمة معلوماتية، و هو نفس المسلك الذي سبق أن أخذ به في مجال تزييف العملة، و في مقام المفاضلة بين الاتجاهات الثلاثة تبنت الاتفاقية حلا ذا تسوية معقولة [374] و ذلك بتحديد نطاق تطبيق نص المادة السادسة السالفة الذكر على الأجهزة التي يمكن موضوعا القول أنها مصممة أساسا من أجل ارتكاب جريمة و بالتالي هذا النص يستبعد عادة الأجهزة ذات الاستخدام المزدوج .

الفرع الثالث: النتيجة الجرمية

جريمة التعامل في معلومات غير مشروعة تندرج ضمن الجرائم الشكلية التي يتمثل أثرها في الخطر الذي قد يهدد أمن و سلامة المعلومات و الأنظمة المعلوماتية ، و التي قد تتعدى مرحلة الخطر إلى حدوث أضرار أخرى إن لم يتم استدراك هته الأفعال أو ردعها أو بتجريمها ودمجها في نطاق العقاب .

إلا أن المشرع الجزائري و كغيره من المشرعين [375] لم يشترط حدوث نتيجة مادية أو ملموسة، بل سعى من خلال تجريمه لهذا الفعل الحد من تلك الأخطار المحتملة التي قد تهدد مصالح بالغة الأهمية، و ما موقف المشرع من هذا التجريم إلا لإدراكه تلك الأهمية للمصالح المراد حمايتها.

المطلب الثاني: الركن المعنوي

كون الأفعال التي تتم بها جريمة التعامل في معلومات غير مشروعة – أو كما يسميها البعض جريمة إساءة استخدام أجهزة الحاسب– أفعال شائعة الحدوث حيث يأتيها الكثير من مستخدمي الأنظمة المعلوماتية، و إن الركن المعنوي لهذه الجريمة أهمية كبيرة في تحققها خاصة و أن عمليات التصميم و البحث، التجميع، الحيازة، الإفشاء، الاستعمال و غيرها مما جاء بها النص لا يمكن تجريمها إلا إذا تحقق بشأنها القصد الجنائي.

و لما وجب توافر القصد الجنائي لقيام هذه الجريمة فقد اشترطت إتفاقية بودابست أن يتوافر القصد الخاص إلى جانب القصد العام [376]، أي أن القيام بتلك الأفعال غير المشروعة يكون عن علم و إرادة و بسوء نية بغرض الإضرار بالآخرين.

---

[374]-د. **هلالي عبد اللاه**، مرجع سابق، ص 101-103.

[375]– من ذلك المشرع الفرنسي الذي لم يتطلب حدوث نتيجة لقيام جريمة إساءة استخدام أجهزة الحاسب

و بناء على ما سبق بيانه نوضح في معرض الحديث عن الركن المعنوي لجريمة التعامل في معلومات غير مشروعة القصد الجنائي العام في هذه الجريمة (الفرع الأول) ثم نتطرق لمدى تطلب المشرع للقصد الجنائي الخاص(الفرع الثاني) على النحو الاتي:

الفرع الأول: القصد الجنائي العام

اعتبر المشرع الجزائري و غيره من المشرعين الذين جرموا هذا الفعل، أنه من الجرائم العمدية التي تقوم على القصد الجنائي العام و يلزم لقيام ذلك أن يعلم الجاني أن الأفعال التي يأتيها غير مشروعة و ليس له الحق في القيام بها، و أن تتجه إرادته إلى القيام بتلك الأفعال التي جاءت في النص التشريعي.

و عليه فان هذه الجريمة من الجرائم العمدية التي تقوم على القصد الجنائي العام بعنصريه العلم(أولا) و الإرادة(ثانيا).

البند الأول: عنصر العلم

يتوفر عنصر العلم و بحسب المبادئ العامة للقصد الجنائي بأن يحيط الجاني علما بكافة العناصر الداخلة في تشكيل الجريمة و ذات الأهمية القانونية في تكوينها، فيجب أن يعلم الجاني بأركان الجريمة و العناصر المكونة لها.

و بالتالي على الجاني أن يعلم و يدرك أنه يقوم بالتعامل في معلومات غير مشروعة، و أن يدرك خطورة الفعل الذي يقوم به على الحق محل الحماية القانونية.

و سواء كان من شأن المعلومات التي يتعامل فيها أن تستخدم في ارتكاب الجرائم بالنسبة للصورة الأولى من الجريمة المنصوص عليها في البند الأول من المادة 394 مكرر 2 عقوبات جزائري[377]، أو

---

[376]– جاء في **المذكرة التفسيرية لاتفاقية بودابست** انه :" و في كل الحالات يشترط في الجريمة التي ترتكب عمدا وبدون حق و من أجل..."

[377]- تقابلها المادة 323-3-1 **عقوبات فرنسي**.

Art 323-3-1 **de C.P.F** Modifié par **LOI n°2013-1168 du 18 décembre 2013 art. 25** ; « Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 3231 à 3233 est puni des peines prévues respectivement pour l'infraction elle même ou pour l'infraction la plus sévèrement réprimée ».

كان من شأن ذلك التعامل في معلومات متحصل عليها من إحدى جرائم المساس بنظم المعالجة الآلية تفاقم الضرر الذي ينتج عن تلك الجرائم و زيادته[378].

كما يجب أن يعلم الجاني بالصفة غير المشروعة للمعلومات المتعامل فيها إن كانت لارتكاب جريمة أو ناتجة عن جريمة من جرائم نظم المعالجة الآلية، و في حالة انتفاء العلم بالعناصر الموضحة سلفا انتفى معها القصد الجنائي[379] أو في حالة وقوع الجاني في خطأ.

البند الثاني: الإرادة

الإرادة الآثمة هي عنصر جوهري في القصد، و لما كانت جريمة التعامل في معلومات غير مشروعة من جرائم الخطر أو الجرائم الشكلية فإن الإرادة فيها تتجه نحو إتيان السلوك أو أحد الأفعال التي نص عليها المشرع الجزائري ، دون اتجاه الإرادة إلى إحداث النتيجة.

و عليه فإن هذا العنصر يتوفر باتجاه إرادة الجاني إلى تحقيق أحد المظاهر السلوكية المنصوص عليها في المادة 394 مكرر 2[380]عقوبات جزائري من ذلك حيازة أو اتجار في معلومات مع العلم بصفتها غير المشروعة.

و إضافة إلى ذلك فإن القصد الإجرامي لا يتوافر لدى المتعامل في تلك المعلومات إلا إذا كان حرا[381]، و إذا ثبت انه كان تحت طائلة الإكراه أو انه في حالة ضرورة فان القصد الجرمي يكون منتفيا لديه.

الفرع الثاني: القصد الجنائي الخاص

إذا كان القصد الجنائي العام يتحقق بإنصراف إرادة الجاني نحو فعل ما يعلم أن القانون ينهي عن إتيانه، فإن القصد الجنائي الخاص يتمثل في الغاية [382] التي يقصدها الجاني من وراء ارتكاب تلك الجريمة فضلا عن إدراكه الواعي لمخالفة القانون.

و لقد تطلبت اتفاقية بودابست بشأن الإجرام المعلوماتي ضرورة وجود القصد الجنائي الخاص في جريمة إساءة إستخدام أجهزة الحاسب، و يتضح ذلك من خلال العبارات الواردة في النص السادس من

---

[378]- **رشيدة بوكر**، مرجع سابق، ص 296.

[379]- **محمد خليفة الملط**، مرجع سابق، ص 212.

[380]- تقابلها في ذلك المادة 06 من **اتفاقية بودابست**، و المادة 323-3-1 **عقوبات فرنسي**.

[381]– **رشيدة بوكر**، مرجع سابق، ص 296.

[382]– الغاية هي الغرض النهائي الذي يرمي الجاني إلى تحقيقه من وراء إرتكابه الجريمة

الاتفاقية من ذلك قولها: " لغرض إرتكاب إحدى الجرائم المنصوص عليها" أو " بنية استخدامها لغرض ارتكاب جريمة"، كما نصت في الفقرة الثانية من المادة السادسة على أنه:" يجب أن لا تفسر على أنها تفرض مسئولية جنائية حينما يكون إنتاج أو بيع أو الحصول.."

و كذلك الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في مادتها التاسعة بقولها:" لغايات ارتكاب الجرائم المبينة في المادة السادسة إلى المادة الثامنة".

الفصل الثاني:

الجرائم المتصلة بالحاسب الآلي

تعتبر هذه الطائفة من أهم الجرائم التي تتصل بالمعلوماتية و أكثرها إثارة للمشكلات القانونية، حيث يشكل الحاسب الآلي في هذه الجرائم الأداة الرئيسية لارتكاب العمل الإجرامي نظرا لما يحتويه من معلومات و أصول، فالحاسب الآلي لا يعد هنا مجرد وسيلة لتبسيط وتسهيل العمل الإجرامي وتحقيق النتيجة، وإنما ما يحتويه من معلومات وبيانات يشكل الدافع الرئيسي على ارتكاب الجريمة.

ويهدف الجاني من وراء هذا النوع من الجرائم الحصول إلى تحقيق ربح مادي بطرق غير قانونية، وتشتمل هذه الطائفة من الجرائم على الجرائم التقليدية ولكن في شكلها الجديد، مما أدى إلى صعوبة تطبيق القوانين التقليدية عليها في ثوبها الجديد، وهذا ما وضحته المذكرة التفسيرية لاتفاقية بودابست بشأن الجرائم الالكترونية، بأنها جرائم عادية سبق للدول أن جرمتها غير أن التشريع قد لا يكون مرنا لاستيعاب هذا النوع من الجرائم وبشكل كافي، لذلك ومن أجل وضع هذه المواد موضع التنفيذ يجب على الدول أن تفحص قوانينها الداخلية، لتحديد ما إذا كانت تنطبق على مواقف مرتبطة بنظم أو بيانات الحاسب، بحيث إذا كانت الجرائم الموجودة تغطي مثل هذه الأفعال، فإنه لا تكون ثمة ضرورة لتعديل الجرائم الموجودة أوسن جرائم جديدة، ومن هذه الجرائم وحسب ما ورد في اتفاقية بودابست و الاتفاقية العربية لمكافحة جرائم تقنية المعلومات نجد التزوير المعلوماتي (مبحث أول) والغش أو الاحتيال المعلوماتي(مبحث ثاني)، وعلى هذا الأساس ندرس هذا النوع من الجرائم وفقا لهذه الاتفاقيات وما جاء فيها من مواد صريحة ، وكذا حسب ما جاء في التشريع الجزائري والتشريعات المقارنة السابق الإشارة إليها، ونقسم هذا الفصل على النحو الآتي:

المبحث الأول:

التزوير المعلوماتي

إن ظهور وسائل تكنولوجية حديثة مثل طابعات الليزر والماسحات الضوئية قد ساعد بكثير في عمليات التزوير، ومع انتشار استخدام الحاسبات الآلية، وزيادة الاعتماد عليها في معالجة وتخزين المعلومات التي قد تكون لها أهمية قانونية، مثل بيانات شهادات الميلاد أو بيانات جواز السفر [383]، كان من اللازم حمايتها من التلاعب بها.

ولقد احتلت الدعامات المادية للحاسب الآلي مكان المحررات والمستندات الورقية لأهمية و خطورة ما تحتويه من بيانات، مما قد يعتبر محلا للاعتداء بتغيير حقيقتها بقصد الغش في مضمونها وجعلها غير صحيحة، وفي هذا الشأن جاءت المادة السابعة [384] من اتفاقية بودابست بغرض إنشاء جريمة موازية لجريمة تزوير المستندات الورقية، و كذا المادة العاشرة من الاتفاقية العربية بشأن جرائم تقنية المعلومات، واستكمال النقص الذي يشوب قوانين العقوبات بشأن التزوير التقليدي، الأمر الذي يتطلب سهولة القراءة المرئية للمحرر والتي قد لا تنطبق مع البيانات المسجلة على دعامات إلكترونية، ذلك أن التلاعب بالبيانات المسجلة يمكن أن يؤدي إلى نفس النتائج الوخيمة للأفعال التقليدية للتزوير.

و شهد التزوير في مجال نظم المعالجة الآلية للمعلومات بوصفه أحد أنماط الغش المعلوماتي تزايدا سريعا في الفترة الأخيرة؛ مثل تزوير المستخرجات الإلكترونية، و تزوير عمليات السحب على الجوائز– و ذلك بالقدر الذي تحتل فيه الدعامة المعلوماتية محل السندات في جميع المجالات[385].

و لخطورة الأمر سارعت بعض الدول ووسعت في مفهوم المحرر الذي يقع عليه التزوير وشملت بالحماية حتى المحرر المعلوماتي، ومنها القانون الفرنسي الذي قام بتعديل القانون قانون العقوبات وأدرج تعريفا للتزوير في نص المادة 441 منه، بحيث أضحت تشمل كل صور التزوير ومهما كانت الوسيلة التي تم بها أو الدعامة التي تتضمنها.

---

[383]- **نائلة عادل محمد فريد قورة**، المرجع السابق، ص 270.

[384]– تنص **المادة السابعة** من **اتفاقية بودابست بشان الجرائم الالكترونية** على أنه:" يجب على كل طرف أن يتبنى الإجراءات التشريعية وأية إجراءات أخرى يرى أنها ضرورية لتجريم وفقا لقانونه الداخلي، الإدخال، الإدخال الإتلاف، المحو، او الطمس العمدي، وبدون حق للبيانات المعلوماتية، الذي يتولد عنه بيانات غير صحيحة، بقصد أخدها بالحسبان أو استخدامها لأغراض قانونية كما لو كانت صحيحة، بصرف النظر عما كانت إذا كانت سهلة القراءة مباشرتا أو واضحة أم لا، ويمكن لأي طرف ان يشترط في قانونه الداخلي نية الغش أو أية نية إجرامية مشابهة من اجل تقرير المسئولية الجنائية"

[385] - **Chamoux(F)**, La loi sur la fraude informatique, de nouvelles incrimination, J.C.P, 1998-1-3321,n°10.
مشار إليه لدى: د. **عمر أبو الفتوح عبد العظيم الحمامي** ، الحماية الجنائية للمعلومات المسجلة إلكترونيا– دراسة مقارنة – دار النهضة العربية، القاهرة، 2010، ص 873.

أما بخصوص المشرع الجزائري فانه لم يستحدث أي نص خاص بالتزوير المعلوماتي، و أن النصوص الواردة في قانون العقوبات تجرم التزوير الذي يرد على محرر العادي و بحيث لا يمكن إخضاع التزوير المعلوماتي إلى النصوص العامة للتزوير، مما يتطلب تدخلا تشريعيا لاستدراك الأمر.

وترتيبا لما تقدم و لتوضيح أكثر نتطرق لمفهوم التزوير المعلوماتي، وإلى صوره و أركان هذه الجريمة على النحو الأتي:

المطلب الأول: مفهوم التزوير المعلوماتي

إن تعريف التزوير المعلوماتي يستوجب بيان مفهومه ومحل الجريمة، أو محل الحماية الجنائية.

الفرع الأول: تعريف التزوير المعلوماتي

التزوير في مفهومه العام يعني تغيير الحقيقة أيا كانت وسيلته بالقول أو بالكتابة، و هذا المفهوم هو شامل لجميع أنواع الغش بما في ذلك الاحتيال و إساءة الائتمان، مما حدا بالمشرعين إلى التضييق من نطاق هذا المفهوم[386] و قصره على التزوير في المحررات و تقليد الأختام و الأوراق الرسمية كما فعل المشرع الجزائري .

و عرف التزوير في الفقه الجنائي [387] على انه تغيير الحقيقة بقصد الغش في سند أو وثيقة أو أي محرر أخر بإحدى الطرق المادية أو المعنوية التي يبينها القانون، تغييرا من شأنه إحداث ضررا بالمصلحة العامة أو مصلحة شخص من الأشخاص.

أو هو تغيير الحقيقة في محرر بإحدى الطرق التي حددها القانون، تغييرا من شأنه أن يرتب ضررا للغير، وذلك بنية إستعمال هذا المحرر فيما أعد له[388].

و على ذلك ينصب التزوير على وثيقة ما بتحويل معناها و مفهومها و الذي لا يمت إلى الحقيقة بصلة، مثل ما عرفته الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في المادة العاشرة منها.

أما التزوير المعلوماتي فهو أي تغيير للحقيقة يرد على مخرجات الحاسب الآلي سواء تمثلت في مخرجات ورقية مكتوبة كتلك التي تتم عن طريق الطابعة وكانت مرسومة عن طريق الرسم ويستوي في

386– د. **عمر أبو الفتوح عبد العظيم الحمامي**، مرجع سابق، ص 875.

387- **محمد زكي أبو عامر وسليمان عبد المنعم**، قانون العقوبات (القسم الخاص)، منشورات الحلبي الحقوقية، بيروت – لبنان، 2006 ص 524،

388– د.**سليمان أحمد الفضل** ، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، القاهرة، 2007، ص115.

المحرر المعلوماتي أن يكون مدوناً باللغة العربية محفوظة على دعامة لبرنامج منسوخ على اسطوانة وبشرط أن يكون المحرر المعلوماتي ذا أثر إثبات حق أو اثر قانوني معين[389].

و التزوير المعلوماتي يشكل اعتداء على منتوجات نظام المعالجة الآلية، أي التلاعب بالمعلومات المعالجة أليا أو بعبارة أصح التلاعب بالمستند المعلوماتي بخصائصه وما يحتويه من معلومات بهدف إحداث تغيير في حقيقة المستند واستخدامه والاستفادة منه فيما زورا لأجله.

و على هذا الأساس ومن اجل عدم الخلط بين جريمة التلاعب بالمعلومات المدخلة إلى النظام الآلي أو مخزنة فيه، وبين التلاعب بالمستند المعلوماتي واستخدامه من اجل فائدة معينة، نجد المشرع الفرنسي قد تدارك الأمر حين عدل قانون العقوبات الجديد، بعد أن كان قد استحدث بموجب قانون الغش المعلوماتي رقم 19/88 قسما خاصا يرمي إلى حماية النظام وحماية نتاج هذا النظام على صعيد واحد من خلال المواد 2/462 إلى 9/462 التي تناول فيها نوعين من الاعتداءات، الأولى هي الاعتداءات على نظام المعالجة أما الصورة الثانية تتمثل في المساس بمنتجات نظام المعالجة الآلية وتجسد هذا المساس في فعل التزوير، هذا التزوير يختلف عن التزوير المعروف في قوانين العقوبات التقليدية وتحديدا ما جاء في المادتين 462-5 و462-6 [390]من هذا القانون حيث خصص في الأولى جريمة تزوير المستندات المعالجة أليا، وفي الثانية لاستعمال تلك المستندات.

فإنه بتعديل قانون العقوبات الفرنسي بموجب القانون رقم 92- 1336 المؤرخ في 16 ديسمبر 1992 المعدل والمتمم لقانون العقوبات الذي أصبح ساريا مند عام 1994، اخرج جريمة تزوير الوثيقة المعلوماتية و استعمالها من نطاق جرائم الاعتداء على نظم المعالجة الآلية وأدرجها ضمن جريمة التزوير العادية، و تجسيدا لذلك تم إلغاء المادتين السابقتين (462-5، 462-6) ودمجهما ضمن المادة 441-1[391] بعد تعديلها.

---

[389]– **عبد الفتاح بيومي حجازي**، الدليل الجنائي والتزوير في جرائم الكومبيوتر والانترنت ، مرجع سابق، ص 170.

[390]- **Art** 462-5 du C.P.F dispose que ; « quiconque aura procédé à 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 20000 f à 2000000 f ».

- **Art**. 462-6 du C.P.F dispose que « quiconque aura sciemment fait usage des documents informatisé vise à l'article 462-5 sera puni d'un emprisonnement d'un an à cinqs ans et d'une amende de 20 000 f à 2000 000 f ou de l'une de ces deux peines ».

[391] - Article 441-1 Modifié par Ordonnance n°2000-916 du 19 septembre 2000 - art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002

و بالتعديل الذي جاء به التشريع الفرنسي و الذي أصبح يستوعب حالات التزوير التقليدي إلى جانب تزوير الوثيقة المعلوماتية حيث جاء في المادة 441-1 عقوبات فرنسي " ou tout autre support" أي في أي دعامة أخرى تحتوي تعبير عن الفكر...، و بالتالي شمل تغيير الحقيقة في محرر أو أي دعامة أخرى لتشمل حتى المحرر أو الوثيقة المعلوماتية سواء خضعت للمعالجة الآلية أم لا، و حتى كل صور التزوير التي يمكن أن تظهر مستقبلا كون النص جاء مرنا عاما ليشمل أي دعامة أو وثيقة.

و حسن فعل المشرع الفرنسي حينما أخرج جريمة تزوير المستندات المعالجة أليا من جرائم الاعتداء على نظم المعالجة الآلية، إذ يعتبر ذلك آمر منطقي لاختلاف المصلحة المحمية بالقانون والتي تقف وراء تجريم كل منهما [392]، و بذلك يكون المشرع قد فصل بين تغيير الحقيقة في المكونات غير المادية في نظام المعالجة الآلية للمعطيات (المساس بسلامة المعلومات أو التلاعب بالمعلومات المخزنة بالنظام المعلوماتي) في المادة 323-3[393] وبين تغييرها في محررات نظام المعالجة أو مستخرجاته (الاعتداء على أصالة المعلومات)[394] التي شملها بالمادة 441-1.

أما بالنسبة للمشرع الجزائري فإن الأمر يتعلق بالتزوير التقليدي ورغم التعديل الذي جاء به في قانون العقوبات بشأن الجرائم الماسة بأنظمة المعالجة الآلية، إلا انه أغفل الجرائم الماسة بمنتجات أنظمة المعالجة الآلية، ولازالت جريمة التزوير جريمة تقليدية خاضعة للمواد من 214 إلى 229 عقوبات، ودون أن يقدم على أي خطوة يوسع ضمنها مفهوم التزوير ليشمل كافة المحررات [395]، مما يستدعي تدخلاً تشريعيا جديد لتحديد مفهوم التزوير ليشمل مختلف الوسائل والمحررات الحديثة.

« Constitue un faux toute altération frauduleuse de la vérité, de nature à causer un préjudice et accomplie par quelque moyen que ce soit, dans un écrit ou tout autre support d'expression de la pensée qui a pour objet ou qui peut avoir pour effet d'établir la preuve d'un droit ou d'un fait ayant des conséquences juridiques.

Le faux et l'usage de faux sont punis de trois ans d'emprisonnement et de 45000 euros d'amende » .

[392]-د. **عبد الفتاح بيومي حجازي** ، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، مرجع سابق، ص 142،143/ كذلك: **عفيفي كامل عفيفي وفتوح الشاذلي**، المرجع السابق، ص 246.

[393]- تقابلها المادة 394 مكرر 1 **عقوبات جزائري**

[394]- أ. **رشيدة بوكر**، مرجع سابق، ص 265.

[395]- في حين نجد المشرع الجزائري قد وسع من مفهوم الكتابة من خلال تعديله للقانون المدني سنة 2005 وأضاف المادة 324 م مكرر التي تنص على أنه:" ينتج الإثبات بالكتابة من تسلسل حروف أو أرقام أو أوصاف أو أية علامات أو رموز ذات

و خاصة و أن الجزائر صادقت مؤخرا على الاتفاقية العربية بشأن مكافحة جرائم تقنية المعلومات، و التي نصت على جريمة الاحتيال المعلوماتي في المادة العاشرة منها.

وجريمة التزوير المعلوماتي كما سبق وأن قلنا أنها جريمة تمس أو متعلقة بمنتجات نظام المعالجة الآلية للمعطيات لذا يفترض التعرض لمفهوم منتجات النظام المعلوماتي قبل التطرق لأركانها.

الفرع الثاني: مفهوم منتجات نظام المعالجة الآلية للمعطيات

أن التعرض لمفهوم منتجات نظام المعالجة الآلية للمعطيات يقتضي التفرقة بين مفهومين كما يلي:

البند الأول : المستند أو الوثيقة المعالجة أليا

يقصد بالمستند في الاصطلاح القانوني كل دعامة مادية (مكتوب أو أي شيء) تصلح لأن يدون عليها المعلومات أو الآراء والتي هي غير مادية، أو الشيء المادي الذي يصلح أن يدون عليه شيء المعنوي، أما في مجال المعلوماتية فيقصد بالمستند كل شيء مادي متميز (قرص أو شريط ممغنط أو غير ذلك) يصلح لآن يكون دعامة أو محلا لتسجيل المعلومات المعالجة بواسطة نظام معالجة أليه[396].

فالمستند المعالج أليا هو كل دعامة مادية مهيأة لاستقبال المعلومات والتي تسجل المعطيات عليها من خلال تطبيق إجراءات المعالجة الآلية أومن خلال نظام المعالجة الآلية للمعطيات.

البند الثاني: المستند أو الوثيقة المعلوماتية

هي تلك الوثيقة غير المعالجة آليا، حيث تعد المستندات المعلوماتية دعامات أو الأوراق المعدة لتسطير المعلومات عليها، والأقراص الممغنطة التي لم يسجل عليها شيء بعد، وكذلك البطاقات البنكية التي لم تدخل الخدمة بعد [397]، وهذه وإن كان مسجل عليها معلومات مكتوبة بخط اليد أو مطبوعة أو محفورة، إلا أنه لم يتم معالجتها بعد، بل تعتبر في مرحلة الإعداد فقط.

معنى مفهوم، مهما كانت الوسيلة التي تتضمنها وكذا طرق إرسالها" أضيفت بموجب **القانون رقم 10/05 المؤرخ في 20 يونيو2005 جريدة رسمية عدد44 ص 24.**

396- د.**عفيفي كامل عفيفي وفتوح الشاذلي**، مرجع سابق، ص 150.

397– **نهلا عبد القادر مومني**، المرجع السابق، ص 135.

المطلب الثاني: أركان التزوير المعلوماتي

التزوير المعلوماتي شأنه شأن بقية الجرائم يتكون من ركنين هما الركن المادي المتمثل في تغيير الحقيقة والركن المعنوي المتمثل في القصد الجنائي، وهذا ما سيتم بحثه فيما يأتي.

الفرع الأول: الركن المادي

لتحقق الركن المادي في جريمة التزوير المعلوماتي لابد من نشاط يباشره الجاني يتمثل في تغيير الحقيقة في سند أو محرر أو وثيقة بأي طريقة يقرها القانون وباستخدام الحاسب الآلي ، وكذا حدوث ضرر للغير أو احتمال حدوثه من جراء ذلك، ومن هذا يتضح أن الركن المادي في الجريمة محل البحث يتكون من عناصر الآتية:

البند الأول: تغيير الحقيقة

يقصد بتغيير الحقيقة هو إبدالها بغيرها أو بما يخالفها، وإذا انتفى هذا التغيير انتفى التزوير حتى ولو توهم الجاني أنه يغير الحقيقة [398]، وتغيير الحقيقة في التزوير المعلوماتي يتم بأي طريقة يقرها القانون المعالج لهذه الجريمة كإدخال بعض البيانات أو المعلومات إلى برنامج أو الإتلاف أو المحو للمعلومات أو طمس للبيانات المعلوماتية، والذي ينشأ عنه بيانات غير صحيحة بقصد استخدامها لأغراض قانونية كما لو كانت صحيحة، بصرف النظر عما إذا كانت سهلة القراءة مباشرة و واضحة أم لا[399].

فالتزوير المعلوماتي يتكون من خلق أو تعديل غير مصرح به للبيانات المسجلة بطريقة من شأنها أن تحوز هذه البيانات قيمة دامغة، مختلفة عن سياق المعاملات القانونية، والتي تكون مؤسسة على صحة المعلومات المستخرجة من خلال هذه البيانات [400]، وبالتالي يمكن أن تكون موضوعا لخداع المصالح القانونية المحمية و أن إمكانية تشغيل البيانات الإلكترونية يمكن أن تكون بها عواقب على العلاقات القانونية.

---

[398]- د. **هشام محمد فريد رستم** ، قانون العقوبات ومخاطر تقنية المعلومات،مكتبة الآلات الحديثة، أسيوط- مصر، 1992، ص 325.

[399]- وذلك حسب ما جاء في المادة 7 من **اتفاقية بودابست للإجرام المعلوماتي** لسنة 2001.

[400]- د. **هلالي عبد الله أحمد**، مرجع سابق، ص 109.

و عليه فإن تغير الحقيقة كعنصر 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 سواء كانت صورا أم رموز أم علامات.

البند الثاني: المحرر أو السند

محل جريمة التزوير هو المحرر بحسب ما يتطلبه القانون، و حيث لا يعد تغيير الحقيقة تزويرا إلا إذا وقع في أو على محرر، لذا قد يثار التساؤل حول طبيعة السند أو المحرر أو الوثيقة التي يقع عليها فعل التزوير، هل ينصب على المحرر بمفهومه التقليدي المتعارف عليه؟ أم انه يقع على محرر له مفهوم خاص لاسيما وأننا في إطار جريمة لا تنطبق عليها النصوص التقليدية لجريمة التزوير؟.

المحرر في مضمونه كتابة مركبة من حروف أو علامات تعبر عن معنى أو فكرة معينة، مع إمكانية القراءة البصرية لمحتواه، وهو ما تفترضه نصوص التزوير التقليدية، ويتسم المحرر بثلاثة خصائص هي:

أ –أن يتخذ المحرر شكلا كتابيا: فيجب أن يكون مكتوبا كتابة مفهومة، وإذا استحال قراءته فلا يصلح وسيلة للإثبات ولا عقاب على ما احتواه من تغيير.

ب أن تكون الكتابة منسوبة لشخص معين معروف أو يمكن معرفته

ج– أن يحدث المحرر أثر قانونيا

أما المحررات الاليكترونية فهي سجل أو مستند الكتروني يتم إنشاءه أو تخزينه أو استخراجه أو نسخه أو إرساله أو إبلاغه أو استلامه بوسيلة الكترونية على وسيط ملموس أو على أي وسيط اليكتروني أخر ويكون قابلاً للاسترجاع بشكل يمكن فهمه [401]، من قبيل المحررات الإلكترونية الأقراص اللينة والمضغوطة أو أية وسائط اليكترونية أخرى.

وبالتالي ما مدى انطباق النصوص التقليدية للتزوير على السندات المعالجة أليا؟

بالنسبة للمستندات الصادرة عن النظام الآلي أو المستخرجة منه متى تعرضت لفعل تغيير الحقيقة، فإنها تحقق التزوير المعاقب عليه، ويكون المسئول عن ذلك هو من أمد النظام الآلي بالمعلومة غير الصحيحة، أو الذي قام بتعديل هذه المعلومات حذفا أو إضافة من ذاكرة النظام الآلي حتى تخرج المستندات والأوراق بهذا الشكل المغاير للحقيقة[402].

401- مثل ما جاء في **المادة الثانية** من **قانون المعاملات الالكترونية الاردني**

402- **سليمان أحمد فضل**، مرجع سابق، ص 118.

لذلك ينبغي التمييز بين تغيير الذي يطرأ على المعلومات أو البيانات المختزنة في ذاكرة النظام، وبين إثبات هذه المعلومات الكاذبة في أوراق أو مستندات صادرة عن النظام الآلي.

فبالنسبة للتلاعب في المعلومات في بأي صورة سواء كانت ثابتة في ذاكرة الحاسب أم كانت تمثل جزء من نظام المعالجة الآلية أم مخزنة فيه، فإن ذلك لا يمثل التزوير في المحررات ويصعب العقاب عليه وفقا للقانون، ذلك أن البرنامج أو الشريط أو الاسطوانة الممغنطة المسجل عليها تلك المعلومات لا تحقق وصف المحرر بالمعنى الذي تتطلبه نصوص التزوير التقليدية[403].

أما في حالة إثبات المعلومات الكاذبة في المحررات الصادرة أو المستخرجة من النظام المعلوماتي، فانه يتحقق فيها وصف المحرر وبالتالي من السهل إخضاعها لنصوص التزوير العادي.

و على هذا الأساس فإن يمكن تصور وقوع التزوير في شكل جديد من خلال تغيير الحقيقة في الشرائط و منتوجات النظام المعلوماتي، ولضيق مجال النصوص التقليدية بشأن التزوير، عمدت تشريعات بعض الدول إلى الأخذ بهذه التفرقة و من بينها التشريع الفرنسي كما سبق أن أشرنا، الذي ميز بين تغيير الحقيقة في معلومات نظام المعالجة الآلية للمعطيات، و المعلومات المختزنة فيه، حيث قام بتعديل نصوص التزوير وجاء بمفهوم عام و موسع للتزوير من خلال المادة 441-1 بأن شمل تغيير الحقيقة في المحرر أو أي دعامة أخرى لتشمل بذلك كافة أشكال وصور التزوير ومنها التزوير المعلوماتي.

أما تغيير الحقيقة في المعلومات المختزنة بالنظام المعلوماتي فلقد افرد لها نص خاص متعلق بالتلاعب بمعلومات نظام المعالجة الآلية(المادة 323-2 عقوبات فرنسي)[404].

البند الثالث: طرق التزوير

لا يكفي تغيير الحقيقة في المستند، وإنما يشترط القانون إضافة إلى ذلك أن يتم وفقا للطرق المحددة قانونا، ولذلك يتعين قبل إصدار الحكم بالإدانة بالتزوير أن يتضمن بيانا للطريقة التي توصل بها الجاني لتغيير الحقيقة، و إلا كان قاصر التسبيب متعينا نقضه[405].

---

[403]- د. **نائلة عادل محمد فريد قورة**، مرجع سابق، ص 271.

[404]- كانت تقابلها المادة 462-4 من **قانون الغش المعلوماتي الفرنسي** رقم 88-19 السابق الإشارة إليه.

[405]- د. **سليمان أحمد الفضل**، المرجع السابق، ص 121.

و يستوي أن يكون التغير ماديا[406] أو معنويا[407] و إذا لم يشترط في تغيير الحقيقة التقليدية أن تكون بطريقة معينة [408] فانه يشترط في تغير الحقيقة في التزوير المعلوماتي أن تتم باستخدام النظام المعلوماتي بغرض غير مشروع و لغرض تمييزها عن جريمة التزوير التقليدية.

و عليه يشترط تحقق العنصر الثالث من عناصر الركن المادي لجريمة التزوير المعلوماتي الذي يتم بتغير الحقيقة في محررات ذات صفة اليكترونية على اعتبار أن التزوير التقليدي يختلف عن التزوير المعلوماتي ذلك أن الأول جريمة عادية و الثاني جريمة اليكترونية يشترط لارتكابها استخدام الحاسب الآلي استخدام غير مشروع، و لكن هذا لا يمنع من إمكانية أن يتم تغيير الحقيقة في التزوير المعلوماتي على محررات عادية إذا كان للحاسب الآلي دور فيه حتى و ان كان له دور ضئيل.

البند الرابع: الضرر

يعتبر الضرر شرطا أساسيا في جريمة التزوير المعلوماتي، إذ لا يعد تغيير الحقيقة في محرر أو سندا أو وثيقة بإحدى الطرق المحددة قانونا تزويرا إلا إذا ترتب عنه ضرر أو كان من شأنه إحداث ضرر مادي، و لا يشترط القانون وقوعه فعلا بل يكفي أن يكون الضرر محتمل الحدوث مستقبلا، أو ضرر معنويا [409] ، و هذا ما وضحته الاتفاقية العربية في المادة العاشرة بقولها"...تغييرا من شأنه إحداث ضرر".

الفرع الثاني: الركن المعنوي

التزوير هو من الجرائم العمدية، ومنها التزوير المعلوماتي الذي يشترط لقيامه توفر القصد الجنائي بعنصريه العلم و الإرادة أي أن يكون الجاني عالماً بأنه يرتكب فعل مجرم أو سلوك غير مشروع معاقب عليه في التشريعات العقابية ومع ذلك أقدم على ارتكابه، بمعنى أنه يجب أن يكون عالما بأن إدخال المعلومات والبيانات إلى مضمون المحررات أو محو تلك المعلومات أو تحويرها أو إتلافها أو القيام بأية أفعال أخرى من شانها أن تؤدي إلى التأثير على المجرى الطبيعي لمعالجة البيانات، ولا يكفي هذا بل لابد من أن يثبت إدراك الجاني وأن تكون إرادته متوجهة إلى إحداث النتيجة الجريمة من جراء

406– **التزوير المادي** هو تغيير الحقيقة بطريقة مادية تترك أثر يدركه البصر.

407– **التزوير المعنوي** هو تغيير الحقيقة في معنى المحرر أو مضمونه أو محتواه دون أن يمس ذلك شكله أو مادته وهو صعب الإثبات عنه بالنسبة للتزوير المادي.

408- طرق تغيير الحقيقة التقليدية تتمثل في تزوير المحررات و النقود و الأختام ومنصوص عليها في المواد 197 –231 **عقوبات جزائري.**

409– أ. **بن وارث**.م، مذكرات في القانون الجزائي الجزائري (القسم الخاص)، الطبعة الرابعة، دار هومة، الجزائر، 2009، ص60.

سلوكه غير المشروع وهي الإضرار بالغير [410] سواء كان إضرارا معنويا أم ماديا أو أي ضرر من الأضرار التي تصيب المصلحة العامة أو بمصلحة شخص من الأشخاص .

و يمكن تصور وقوع التزوير المادي و المعنوي في الجرائم المستخدم فيها أجهزة أو أنظمة أو برامج الحاسب الآلي و ملحقاته، فيتصور التزوير بأسلوب الاصطناع من خلال الحاسب الآلي بما يمكن اعتباره تزويرا معلوماتيا عن قصد و بتوافر علم و إرادة مستخدم هذا الجهاز الالكتروني، و في ذات الوقت قد ينسب صدور هذه البيانات و المعلومات إلى شخص ما أو جهة ما ذلك لأن الاصطناع هو خلق محرر بأكمله و نسبته إلى غيره [411] ، و ليس هناك صعوبة في عملية إدخال عناصر المحرر المراد تزويره إلى جهاز الحاسب سواء أكان عن طريق الماسح الضوئي، أو عن طريق لوحة المفاتيح، بل و عن طريق استخراج المعلومات و البيانات من الشبكة المعلوماتية و صياغتها في شكل المحرر المزور الذي يريده الجاني و يقوم بطبعه في شكله الجديد المخالف للحقيقة الواقعية و استعماله.

لذلك فإن وقوع جريمة التزوير المعلوماتي بهذا السلوك الإجرامي مستخدما التقنية التكنولوجية هو أمر ممكن و جائز الحدوث في ظل التقدم التقني لأنظمة المعالجة الألية.

وعليه إذا كان الجاني جاهلاً بأن الفعل الذي يرتكبه غير مشروع فلا يتحقق لديه القصد الجرمي وكذلك الحال إذا انتفى علم الجاني بأي ركن من أركان الجريمة فلا يترتب عليه توافر القصد الجنائي لأنه يفترض بالفاعل أن يكون عالما بكافة أركان جريمته. كما يجب كذلك على الجاني في جريمة التزوير المعلوماتي، أن تتجه نيته إلى التزوير بقصد الغش أي اتجهت إلى استعمال الوثيقة المعلوماتية فيما زورت لأجله، أي إلى الاحتجاج به كما لو كان صحيحا [412] وفي حالة تخلف هذه النية تنتفي جريمة التزوير لانتفاء القصد الجنائي.

كما أن المشرع الفرنسي عاقب على التزوير واستعمال المستند المزور بنفس العقوبة بحسب نص المادة 441-2/1 عقوبات فرنسي[413].

410– د. **عبد الفتاح بيومي حجازي**، الحماية الجنائية للتجارة الالكترونية، مرجع سابق، ص 90.

411– **راشد محمد المري**، مرجع سابق، ص 72-73.

412– د. **سليمان أحمد الفضل** ، مرجع سابق، ص 123./ كذلك: د. **عبد الفتاح بيومي حجازي** ، الحماية الجنائية للتجارة الالكترونية، المرجع السابق، ص 91.

413 - Article 441-1/2 de C.P.F Modifié par Ordonnance n°2000-916 du 19 septembre 2000 - art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002 ; « Le faux et l'usage de faux sont punis de trois ans d'emprisonnement et de 45000 euros d'amende ».

نخلص إلى أن المشرع الفرنسي خرج من الباب الواسع عندما وسع من مفهوم التزوير بقوله أن تغيير الحقيقة يكون على محررات أو أية دعامة أخرى، وبذلك ينصرف وصف الدعامة إلى المستندات المعلوماتية أو أي دعامة أخرى ناتجة عن التقدم التكنولوجي وتصلح أن تكون محررا يحتوي في مضمونه معلومات ويكون قابل للتزوير، وسواء كانت مطبوعة على ورق أو على أي وسيلة أو دعامة أخرى.

فالقانون الفرنسي تطور في هذه المسألة وحسم الأمر بالنسبة لهذه الجريمة خاصة وأنها تعد من أخطر صور الغش في مجال المعلوماتية وذلك بسبب خطورة الدور الذي يقوم به الحاسب الآلي في الوقت الحاضر واقتحامه مختلف المجالات، حيث أصبح يتم من خلاله عمليات هائلة ترتب أثار قانونية خطيرة ومع ذلك في تشريعات أخرى لا يصدق عليها وصف المحرر أو المستند أو الصك في القانون المدني[414] وكذلك القانون الجنائي[415] الأمر الذي يشكك في قيمتها كدليل في الإثبات.

إضافة إلى ذلك فإن جريمة التزوير تفترض إمكانية استخدام الوثيقة المزورة كوسيلة إثبات، ومن المعلوم أن الوثائق المعلوماتية لها قيمة ضعيفة في الإثبات في التشريع الجزائري.

لذلك نرى أن الحاجة توجب على المشرع الجزائري التدخل من جديد لأن النصوص التي جاء بها فيما يخص جرائم المساس بأنظمة المعالجة الآلية سنة 2004 غير كافية لتجريم الأفعال الواقعة على منتجات نظم المعالجة الآلية، وإتيان نصوص خاصة تتواءم مع التزوير المعلوماتي كما فعل المشرع الفرنسي، و ما جاء في الاتفاقية العربية.

المبحث الثاني:

الاحتيال المعلوماتي

لقد انتشرت جريمة الغش المعلوماتي انتشارا كبيرا، خاصة بعد اتساع مجالات استخدام الحاسب الآلي و شبكة الانترنت بحيث أصبح الاحتيال يقع عبر هته الشبكة كالنصب والاحتيال من خلال البريد الإلكتروني، كما تضاعفت نسب الإحتيال المعلوماتي نتيجة لظهور البنوك الإلكترونية و التحويل

---

[414]- بالنسبة لمفهوم المحرر نجد المشرع الجزائري قد وسع من مفهوم الكتابة في الماد المدنية من خلال تعديل **القانون المدني** وإضافته للمادة 323 مكرر لتشمل المحررات العادية و الالكترونية .

[415]– أما بالنسبة لجريمة التزوير في **القانون الجنائي الجزائري** فإنها لا تنطبق إلا على المحررات الورقية أو الكتابة الورقية ولا يهم إذا تمت معالجتها بطريقة آلية وتمت طباعتها أم لا.

الإلكتروني للاموال، و يتم في الوقت الراهن توظيف الأنظمة المعلوماتية و في المصارف و المؤسسات النقدية لعمليات التحويل بشكل يومي، إلا أن الإجراءات الأمنية التي تحيط بالمعلومات و أنظمة معالجتها قد توجد بها ثغرات يتم إستغلالها من المخترقين لتحقيق أهدافهم .

ولقد ورد ذكر هذه الجريمة في المادة الثامنة من اتفاقية بودابست بشأن الجرائم الالكترونية، والمادة الحادية عشر من الاتفاقية العربية و هناك عدة وسائل و أنواع للإحتيال المعلوماتي، من خلال هذا المبحث سوف نتطرق إلى مفهوم جريمة الغش المعلوماتي، وصورها و أركانها.

المطلب الأول: مفهوم الغش المعلوماتي

يراد بالغش المعلوماتي الاحتيال عبر الانترنت ونحدد مفهومها أو تعريفها من عدة نواحي:

الفرع الأول: التعرف اللغوي لجريمة الاحتيال

الاحتيال في اللغة العربية مأخوذ من الفعل الثلاثي حيل، والحيلة إسم من الاحتيال، وجريمة الاحتيال تعرف في اللغة الأجنبية بـ fraude التي ورد معناها في مصطلحات العدالة الجنائية على أنها" الحصول على النقود أو أي شيء أخر له قيمة عن طريق المظاهر الكاذبة والخداعة"[416].

وفي الاصطلاح وبوجه عام يقصد به الغش والخداع الذي يعمد إليه الشخص للحصول من الغير وبدون وجه حق على فائدة أو ميزة، ووصفه بالمعلوماتي يشير إلى صورة له مستحدثة تقوم على إساءة إستخدام الحاسبات والتلاعب في نظم المعالجة الآلية للمعلومات، للحصول بغير حق على أموال أو أصول أو خدمات[417].

الفرع الثاني: تعريف الفقه القانوني لجريمة الاحتيال

هناك عدة تعريفات وردت بشان جريمة الاحتيال، فهناك من عرفها بأنها:" كل كذب مصحوب بوقائع خارجية أو أفعال مادية يكون من شأنها توليد الاعتقاد لدى المجني عليه، بصدق هذا الكذب بما يدفعه إلى تسليم ما يراد منه تسليمه طواعيتا واختيارا"[418].

أما الاحتيال عبر الانترنت فيقصد به: "أي سلوك احتيالي ينتهج منهج الحوسبة بنية الحصول على امتياز مالي"[419].

---

[416]- مشار إليه لدى: على عدنان الفيل، الإجرام الالكتروني، طبعة أولى، منشورات زين الحقوقية،صيدا، لبنان، 2011 ص 15.

[417]- د. **هشام فريد رستم**، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق الذكر، ص 45،46.

[418]– **علي عدنان الفيل**، المرجع السابق، ص 16.

[419]– **سليمان أحمد الفضل**، المرجع السابق، ص 197.

الفرع الثالث: التعريف التشريعي لجريمة الاحتيال

الأصل أن التشريعات لا تأتي بتعريفات إلا إذا أريد بها معنى أو أمر محدد، لذلك نجد أغلب التشريعات العقابية تتجنب إيراد تعريفات، أما بالنسبة لجريمة الإحتيال المعلوماتي أو عبر الانترنت، فقد اختلفت التشريعات في تجريمها والنص عليها، فمنها من جعلها خاضعة للأحكام العامة لجريمة الاحتيال من ذلك التشريع الجزائري، ومنها من أورد لها نص خاص كجريمة مستحدثة، ومن ذلك القانون الاتحادي الإماراتي لمكافحة جرائم تقنية المعلومات .

كما أن التشريعات العربية اختلفت في تسميتها لهذه الجريمة، فهناك من يطلق عليها تسمية "النصب" كالقانون الجزائري والمصري [420]، و هناك من إستخدم تسمية "الاحتيال" كالقانون الأردني والعماني[421].

إن الاحتيال أو الغش المعلوماتي ورد تعريفه في المادة الثامنة من إتفاقية بودابست على أنه: "التسبب في إحداث ضرر للغير عن طريق:

أ –الإدخال، الإتلاف، المحو، الطمس لبيانات الحاسب.

ب كل شكل من الاعتداء على وظيفة الحاسب، بنية الغش أو أية نية إجرامية مشابهة، من أجل الحصول دون حق على منفعة اقتصادية له أو للغير"

كما أشارت المذكرة التفسيرية لاتفاقية بودابست إلى أنه مع حدوث الثورة التكنولوجية، تضاعفت إمكانية إرتكاب جرائم إقتصادية كالغش وبالأخص النصب ببطاقات الائتمان، كما أنا الأصول الممثلة أو المتداولة عن طريق النظم المعلوماتية، كالأموال الالكترونية أو الودائع أصبحت هدفا للتلاعبات بنفس الأشكال التقليدية.

كما ورد تعريف الاحتيال المعلوماتي في المادة الحادية عشر من الاتفاقية العربية بقولها:" التسبب بإلحاق الضرر بالمستفيدين و المستخدمين عن قصد و بدون وجه حق بنية الاحتيال لتحقيق المصالح و المنافع بطريقة غير مشروعة للفاعل أو للغير عن طريق....".

و بالتالي فإن جريمة الاحتيال المعلوماتي أو عبر الانترنت ومن خلال ما سبق تحديده، هي جريمة تنصب على الأموال المادية أو المعنوية ولكن في شكل جديد وعبر وسائل جديدة تستخدم فيها أنظمة المعالجة الآلية، بهدف الاستيلاء على أموال أو خدمات وبدون وجه حق.

---

[420]– المادة 372 من **قانون العقوبات الجزائري المعدل والمتمم**، المادة 336 من قانون العقوبات المصري

[421]– أنظر المادة372 من قانون **العقوبات الأردني**، والمادة 288 من **قانون الجزاء العماني**.

ولقد حددت المادة الثامنة من اتفاقية بودابست الأفعال التي تدخل في الاحتيال المعلوماتي، سواء كانت التلاعب الاحتيالي يقع على المكونات المعنوية أو المادية للنظام المعلوماتي، وسبب ضررا اقتصاديا مباشرا للغير[422].

المطلب الثاني: أركان جريمة الاحتيال

تشتمل على ركنين مثل كل جريمة وهي:

الفرع الأول: الركن المادي

يمثل الركن المادي في جريمة الاحتيال الوسيلة التي يلجأ إليها النصاب أو المحتال بقصد الاستيلاء لنفسه أو للغير على مال منقول[423]، ومن ذلك يتبين أن عناصر الاحتيال المعلوماتي تتمثل في:

البند الأول : السلوك الاجرامي

إن كل أسلوب يؤدي إلى الخداع يمكن أن يعد طريقة احتيالية، ولقد تعددت الاساليب التي ترتكب بها أفعال الاحتيال والغش المعلوماتي، ولكنها كلها تجتمع في التعدي على البرامج والمعلومات المخزنة أليا، والتلاعب فيها للحصول على أموال أو أصول أو خدمات، وتحقيق أغراض إجرامية أخرى.

فأي طريقة من شأنها إيهام المجني عليه وخداعه وإيقاعه في دائرة النصب والاحتيال تعد طريقة إحتيالية.

كما أنا أساليب الاحتيال المعلوماتي أو عبر الانترنت هي أساليب متنوعة ومتعددة وهي تساير التقدم التكنولوجي.

غير انه وبالرجوع إلى إتفاقية بودابست و الاتفاقية العربية نجده ما قد حددت الأساليب التي تقع بها هذه الجريمة بقولهما: "التسبب في إحداث ضرر ... عن طريق....."

مع ملاحظة أن العناصر المكونة لمصطلحات الإدخال أو الإتلاف أو المحو أو الطمس لها نفس المعنى الوارد في المواد السابقة [424]، كما جاء في المذكرة التفسيرية لهذه الإتفاقية، ومن هذه الأساليب نجد ما يلي:

---

[422]- د.**هلالي عبد اللاه أحمد**، المرجع السابق الإشارة اليه، ص 114.

[2]– **علي عدنان الفيل**، الإجرام الالكتروني، المرجع السابق، ص 23،24.

[424]- لقد سبق شرح هذه الصور والأساليب في جريمة التزوير المعلوماتي السابق بيانها.

أولا: التعدي على المعلومات والبيانات

يتم التعدي على البيانات أو المعلومات بالتلاعب فيها إما بالإدخال أو الإتلاف للمعلومات الموجودة بنظام المعالجة الآلية، أو بإدخال معلومات مصطنعة.

و يتم هذا الأسلوب عادة من طرف الشخص المسئول عن القسم المعلوماتي، والذي يسند إليه على وجه الخصوص وظيفة الحاسب والمعاملات المالية، وتتحقق هذه الصورة في عدة أشكال منها:

– ضم مستخدمين غير موجودين في الواقع ليتم صرف رواتبهم

– الإبقاء على مستخدمين تركو الوظيفة بالفعل.

ثانيا: إتلاف المعلومات الموجودة بالنظام المعلوماتي

يتم ذلك بإتلاف معلومات معينة لها علاقة بالحسابات أو صرف الأموال.

حيث يمكن للمسئولين عن تخزين المعلومات وحفظها أن يغيروا أو يتلفوا المعلومات والبيانات المكلفين بحفظها داخل جهاز الحاسب الآلي أو النظام المعلوماتي.

ومن بين تلك الأفعال استبدال رقم حساب بأخر، أو إحلال بطاقة ائتمان محل أخرى[425].

وتعتبر هذه الأفعال من أخطر الجرائم خاصة إذا استمرت لزمن طويل حتى يتم إكتشافها.

ثالثا: التعدي على برامج التطبيق ونظم التشغيل و المواقع

يتم ذلك من خلال تعديل نظم أو برامج التطبيق، أو تعديل نظم التشغيل، منها التعديل الذي يتم عن طريق المداخل المتميزة وعي عبارة عن ممرات خالية متروكة في البرامج أو القيام بتعديلات في شفرة هذا البرنامج والمنافذ الوسيطة، أو اصطناع برنامج كامل ومخصص فقط لارتكاب فعل الغش المعلوماتي[426].

وعليه فإن هذه الأساليب وحسب ما جاء في الاتفاقية السابقة والتي على أساسها تبنت الدول الأطراف أو أي دولة تريد المصادقة عليها أن تأتي في قوانينها الداخلية أساليب مشابهة.

غير أنه بالرجوع للقانون الفرنسي، فإنه فيما يخص الاحتيال المعلوماتي فإن المشرع لم يورد نصا خاصا به، بل إكتفى بتجريمه بنص عام في المواد 313–1 إلى 313–3 من قانون العقوبات، حيث

---

[425]– د. **محمد محمود المكاوي**، مرجع سابق، ص 323–326.

[426]– د. **محمد محمود المكاوي**، نفس المرجع، ص 324.

جاء فيها أن الاحتيال هو: القيام بإسم كاذب أوصفة كاذبة أو بالتعسف بصفة حقيقية أو بإستعمال مناورات....."[427].

أما القضاء الفرنسي، فقد طبق النص التقليدي على الحالات التي يتم فيها التلاعب ببيانات داخل نظام المعالجة الآلية، من أجل إجراء تحويل لإلكتروني غير مشروع للأموال[428].

و نفس الأمر بالنسبة للمشرع الجزائري لم يورد لها نص خاص، شأنها شأن التزوير المعلوماتي، مما يستوجب التدخل و إعادة النظر في نصوص العقوبات وضم الجرائم الماسة بمنتوجات نظم المعالجة الآلية.

أما بخصوص القضاء فلم نلحظ أي حكم بشأن الاحتيال المعلوماتي، بالرغم من أن هذه الأساليب موجودة في الواقع.

أما بالنسبة للمشرع الأردني فلقد جاء بنص عام [429] في قانون المعاملات الالكترونية [430]، حيث جرمت المادة 38 منه إرتكاب الجرائم التقليدية بوسائل إلكترونية بقولها:" يعاقب كل من إرتكب فعلا يشكل جريمة بموجب التشريعات النافدة بواسطة إستخدام وسائل إلكترونية، بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد عن عشرة ألاف دينار، أو بكلتا هاتين العقوبتين، ويعاقب بالعقوبة الأشد إذا كانت العقوبات المقررة في تلك التشريعات تزيد على العقوبة المقررة في هذا القانون"

و عليه فإن النص قد يسعف القضاء الأردني لمواجهة بعض الجرائم التقليدية في صورتها أوحلتها الجديد والتي ترتكب بوسائل إلكترونية مثل الاحتيال والتزوير المعلوماتي.

البند الثاني: وجود نظام معلوماتي

لقد سبق وأن وضحنا ما المقصود بالنظام المعلوماتي ونظام المعالجة الآلية للمعطيات، بحيث تشمل الحاسب الآلي والبرامج وحتى شبكة الانترنت، حيث تعد هذه الأخيرة عنصرا أساسيا في إرتكاب جريمة الاحتيال في مختلف أشكالها، سواء الاحتيال عبر البريد الالكتروني أو عبر بطاقات الإئتمان

427– د. **محمد طارق عبد الرؤوف الخن**، جريمة الاحتيال عبر الانترنت، مرجع سابق، ص 109.

428– محكمة إستئناف باريس في حكم لها سنة 1990، مشار إليه لدى: د.**محمد طارق عبد الرؤوف الخن** ، نفس المرجع، ص 109،110./ كذلك: **راشد محمد المري**، مرجع سابق، ص 90، 92.

429- لقد نصت بعض التشريعات على هذه الجريمة بموجب نص خاص منها التشريع العماني، السعودي، الاماراتي :أنظر في ذلك: **محمد طارق عبد الرؤوف**، المرجع السابق، ص 113-115.

430– **قانون المعاملات الالكترونية** الأردني رقم 58 لسنة 2001.

التي تستخدم في شراء المنتجات عبر الانترنت، وحيث يتم الاستلاء على المبالغ قد تصل إلى مئات الماليين[431]، خاصة عندما يمنح أحد الضحايا رقم حسابه المصرفي لشخص عبر البريد الالكتروني.

البند الثالث: النتيجة الجرمية

إذا ما أقدم الجاني على إتيان فعل من الأفعال الاحتيالية وكان عن طريق نظام للمعالجة الآلية، فلكي تكتمل الجريمة لا بد من أن يتم إنتقال المال من المجني عليه إلى الجاني أو غيره دون وجه حق، ذلك كون الاحتيال من الجرائم التي تقع على المال ويتم الاستيلاء فيها على مال الغير وبالتالي فإن التلاعبات المعلوماتية الاحتيالية تكون مجرمة إذا سببت مباشرة للغير ضررا إقتصاديا أو ماديا أو حتى بنية الحصول على منفعة إقتصادية غير مشروعة للجاني أو لغيره.

و مصطلح الضرر الاقتصادي أو المادي له مفهوم واسع جدا ليشمل النقود الالكترونية، والأشياء المادية وغير المادية[432] ذات القيمة الاقتصادية، وهذا ما نص عليه المشرع الفرنسي من خلال المادة 313 الفقرة 1 من قانون العقوبات[433].

وفي هذه الجريمة تتحقق النتيجة أو يتحقق تسليم المال إما عن طريق أحد المصارف أو عن طريق إحدى شركات تحويل النقود أو باستعمال بطاقة الاعتماد الممغنطة، إذ لا يمكن أن يتم تسليم المال باليد، وإلا كانت جريمة تقليدية أو جريمة احتيال عادية.

أما في حالة ما إذا وقع فعل من الأفعال أو الأساليب الاحتيالية ولم تتحقق النتيجة أو خاب فعل الجاني لسبب خارج عن إرادته فإنه يعاقب على الشروع في هذه الجريمة، وحيث ألزمت اتفاقية بودابست الدول الموقعة ضرورة تجريم الشروع بالاحتيال والعقاب عليه بموجب المادة 2/11.

البند الرابع: العلاقة السببية

---

[431]– للمزيد فيما يخص صور الاحتيال عبر الانترنت والبريد الالكتروني لدى: د. **عدنان علي الفيل** ، الإجرام الالكتروني، المرجع السابق، ص 27.

[432]- اختلفت التشريعات في تحديد طبيعة المال محل جريمة الاحتيال، فقد يكون مال مادي منقول أو أي منقول أخر له قيمة اقتصادية، أو مال منقول غير مادي كالمنافع والخدمات مثل طلبات الاستشارة عن طريق الانترنت وإيهام المستشار بسداد قيمة الاستشارة من خلال بطاقة الاعتماد الائتمانية وعدم تسديدها...لمزيد من الأمثلة لدى: علي **عدنان الفيل**، المرجع نفسه، ص 31.

[433] -**Art 313** alinéa 1 du **C.P.F** ; « L'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge ».

يكتمل الركن المادي بقيام الرابطة السببية بين طريقة الاحتيال التي استخدمها الجاني في النصب على المجني عليه، وبين النتيجة المتمثلة في تسلم المال أو المنفعة محل الجريمة، أي أن المال أو الخدمة كان نتيجة منطقية للطريقة الخادعة أو الاحتيالية.

الفرع الثاني: الركن المعنوي

جريمة الاحتيال المعلوماتي، جريمة عمدية تستلزم توافر القصد الجنائي العام والقصد الجنائي الخاص حتى تتحقق هذه الجريمة، فالقصد الجنائي العام يتجه إلى التلاعب بالنظام المعلوماتي على نحو يسبب خسارة للغير.

و يقوم القصد الجنائي العام على عنصرين أولهما العالم وثانيهما الإرادة، فيجب أن يكون المحتال على علم بالأفعال التي يقترفها على أنها مجرمة قانونا، ومن شأن سلوكاته وأساليبه خداع المجني عليه وحمله على تسليم المال، وأن يعلم الجاني أن المال سوف يتسلمه دون وجه حق وانه مال مملوك للغير [434] .

كما ينبغي أن تتجه إرادته إلى استعمال أحد الأساليب الاحتيالية المجرمة، وان تتجه أيضا إلى تحقيق النتيجة الجرمية[435].

أما القصد الجنائي الخاص فهو تلك الصورة من القصد الجنائي التي لا يكتفي فيها القانون بهدف الإرادة القريب وهو الغرض، يل يعتد بهدفها البعيد وهو الغاية[436].

و القصد الجنائي الخاص في جريمة الاحتيال المعلوماتي، يتمثل في نية الجاني غير الشريفة في الحصول على مكسب إقتصادي له أو لغيره [437]، أي اتجاه نية المحتال إلى الاستيلاء على مال الغير وتملكه دون وجه حق.

و لقد جاء في المذكرة التفسيرية لاتفاقية بودابست أنه يجب أن ترتكب الجريمة عمدا، والعنصر العام للقصد ينطبق على التلاعب أو التدخل المعلوماتي الذي يسبب ضررا إقتصاديا أو ماديا للغير، وعلاوة

434- **علي عدنان الفيل**، المرجع السابق، ص 37.

435– المرجع نفسه، ص 37.

436– د. **جلال ثروت**، النظرية العامة لقانون العقوبات، الطبعة 1، مؤسسة الثقافة الجامعية، الاسكندرية، ص 209، 210: مشار إليه لدى علي عدنان الفيل، الإجرام الالكتروني،المرجع نفسه، ص 37.

437– د. **محمد طارق عبد الرؤوف الخن**، مرجع سابق، ص 122.

على ذلك تتطلب الجريمة نية خاصة هي نية الغش أو نية غش خاصة، أو بتعبير أخر نية غير أمينة أو غير شريفة بغرض الحصول على منفعة إقتصادية لنفسه أو للغير[438].

[438]- د. **هلالي عبد الإله أحمد**، المرجع السابق، ص 115.

الفصل الثالث:الجرائم المتصلة بالاعتداءات الواقعة على الملكية الفكرية والحقوق المجاورة

إن نظام الملكية الفكرية، نظام تتشابك عناصره و موضوعاته حتى ببنائه التقليدي و قبل أن يطاله تأثير تقنية المعلومات، و بازدهار الإبداعات التقنية و اتساع أثرها على النظم القانونية، وبظهور أنماط جديدة من المبتكرات الإبداعية كان لها قيمة و أهمية فرضت ضرورة توفير الحماية لها و تعزيز أنظمة الملكية الفكرية و إعادة بنائها على كافة المستويات الوطنية والدولية، و في هذا الإطار نعمد إلى تحديد المصنفات المعلوماتية في البيئة الرقمية و على شبكة الانترنت المحمية بموجب أنظمة الملكية الفكرية و الحقوق المجاورة (المبحث الأول) والتي كانت محل جدل كبير في الساحة القانونية، مع بيان الحماية القانونية التي وفرها المشرع الجزائري لحماية حقوق المؤلفين و المبدعين في البيئة الرقمية، و معرفة مدى مواكبة النص القانوني الجزائري للتكنولوجيا الحديثة و تأثيرها على الملكية الفكرية و حقوق المؤلف خاصة؟

و هو ما يقتضى الإيجاز السريع حول هذه النقاط مع ضرورة تحديد الجرائم و الانتهاكات الواقعة على الملكية الفكرية و الحقوق المجاورة (المبحث الثاني) في إطار الأمن المعلوماتي باعتباره احد السبل لحماية الملكية الفكرية، إذ أن التعامل مع الانترنت و تقديم الخدمة المعلوماتية قد يتعارض مع حقوق الملكية الفكرية و حمايتها لمصنفات البيئة الالكترونية و هذا ما استدعى سن تشريعات جديدة لحماية برامج الحاسب و قواعد البيانات خاصة مع إحداث توازن بين مصلحة المنتج و مستهلكي المعلومات على حد سواء و حفاظا على حقوق المبدعين و المؤلفين و المنتجين لهته الوسائط و ذلك على النحو الأتي:

المبحث الأول:

المصنفات المحمية بموجب حقوق الملكية الفكرية في البيئة الرقمية

من بين أهم الإشكالات المطروحة في مجال الأمن المعلوماتي تلك المتعلقة بنشر و استعمال الأدوات المرقمنة، فحماية الملكية الفكرية لجميع المصنفات الناتجة عن التطور التكنولوجي تعتبر من القضايا القانونية المطروحة للنقاش، نظرا لتأثرها بالتقنية الحديثة بعدما تم طرح العديد من الإشكالات التي تعرض لها أمن المعلومات و حمايتها في البيئة الرقمية.

فما هي المصنفات المحمية بموجب القانون (مطلب أول) ؟ و ما الشروط التي تتطلبها الأنظمة القانونية و المشرع الجزائري لتوفير تلك الحماية (مطلب ثاني) ؟

المطلب الأول: تحديد المصنفات المعلوماتية

يقتضي الأمر و قبل تحديد المصنفات الرقمية، أن يتم تحديد مفهوم المصنف و المصنف الرقمي (فرع أول) ثم الحديث عن أنواع المصنفات في البيئة الرقمية و على شبكة الانترنت (فرع ثاني):

الفرع الأول: مفهوم المصنف

عرف المشرع الجزائري المصنف أو المؤلف في المادة الأولى من الأمر رقم 73-14[439] بأنه: " كل إنتاج فكري مهما كان نوعه و نمطه و صورة تعبيره، و مهما كانت قيمته ومقصده وأن يخول لصاحبه حقا يسمى حق المؤلف يجري تحديده و حمايته طبقا لأحكام هذا الأمر".

و لم يعرفه المشرع الجزائري في الأمر رقم 03-05[440] و إنما ذكر ما يماثله في ذلك من المصنفات من خلال المادتين 04 بقولها :" تعتبر على الخصوص كمصنفات أدبية أو فنية محمية ما يأتي....." و 05 منه بقولها:" تعتبر أيضا مصنفات محمية الأعمال الآتية....." .

حيث نجد المشرع الجزائري قد عدد صور و أنواع المصنفات و لكن على سبيل المثال وليس الحصر، باعتبار أن التطور العلمي و التكنولوجي قد يطرح أشكال جديدة من المصنفات ولكن بتوفرها على نفس شروط المصنفات و بالتالي تطالها الحماية القانونية و هذا ما يستشف من نص المادة 3 من

-الأمر رقم 73-14 المؤرخ في 03 ابريل 1973 ***المتضمن حق المؤلف،*** الجريدة الرسمية عدد 29 بتاريخ 10 ابريل 1973، ص 434[439].

[440]- الأمر رقم 03-05 المؤرخ في 19 يوليو 2003 **المتعلق بحقوق المؤلف و الحقوق المجاورة**، الصادر بالجريدة الرسمية عدد 44 بتاريخ 23 يوليو 2003، ص 3.

الأمر رقم 03-05 بقولها:" يمنح كل صاحب إبداع أصلي لمصنف أدبي أو فني الحقوق المنصوص عليها في هذا الأمر.
تمنح الحماية مهما يكن نوع المصنف و نمط تعبيره و درجة استحقاقه و توجيهه، بمجرد إبداع المصنف سواء أكان المصنف مثبت أم لا بأية دعامة تسمح بإبلاغه للجمهور".

و قد عرفته المادة الثانية من اتفاقية برن بأنه: " تشمل عبارة «المصنفات الأدبية والفنية» آل إنتاج في المجال الأدبي والعلمي والفني أيا كانت طريقة أو شكل التعبير عنه....."[441].

و يعرفه الفقه على أنه كل إنتاج ذهني مكتوب أو مرسوم أو محفور أو مخطوط أو مذاع بواسطة الإذاعة أو التلفزيون، أو معبر عنه بالحركة، و تمتد الحماية إلى عنوان المصنف طالما أن له طابع ابتكاري متميز "[442]

و من خلال التعريفات السابقة فإن المصنف هو كل إنتاج ذهني ينطوي على شيء من الابتكار و الأصالة يقدم في أي شكل يبرز فيه إلى الوجود.

أما **المصنف الرقمي** أو المعلوماتي فإن التشريعات المتعلقة بالملكية الفكرية لم تقدم أي تعريف له و ترك الأمر للفقه القانوني الذي واجه صعوبة في تحديد مفهومه حيث ثار الخلاف بشأنه بسبب حداثة المصطلح في الحقل القانوني [443]، و إجتهد البعض في إعطاء تعريف للمصنف الرقمي على أنه:" مصنف إبداعي عقلي ينتمي إلى بيئة تقنية المعلومات، إذ يضم برامج الحاسوب و قواعد البيانات و الدوائر المتكاملة و أسماء النطاقات و مواقع الانترنت ....."[444].

و نفس التعريف تقريبا بكونها مصنفات إبداعية عقلية و التي تنتمي إلى تقنية المعلومات و يتم التعامل معها بشكل رقمي و تتمثل في برنامج الحاسب الآلي و قواعد البيانات وطبوغرافيا الدوائر المتكاملة" [445].

---

[441]- إتفاقية برن **لحماية المصنفات الأدبية والفنية وثيقة** باريس المؤرخة 24 يوليو 1971 والمعدلة في 28 سبتمبر 1979

[442]– المركز القومي للبحوث الاجتماعية و الجنائية، " حق المؤلف و الحقوق المجاورة في إطار الملكية الفكرية"، المجلة الجنائية القومية، العدد 01 بتاريخ مارس– جويلية 1999، ص 03 عن د. **رقية عواشرية** : مقال الحماية القانونية للمصنفات المنشورة إلكترونيا في ضل معاهدة الويبو لحقوق المؤلف 1996– دراسة تقيمية– مجلة جيل حقوق الإنسان، العدد 01 ، فيفري 2013، لبنان، ص 104.

[443]– **د. رقية عواشرية**، نفس المرجع، ص 105./ **راضية مشري**: الحماية الجزائية للمصنفات الرقمية في ظل قانون حق المؤلف، مجلة التواصل لكلية الحقوق، جامعة 08 ماي 45، قالمة، عدد 34، جوان 2013، 137.

[444]– **راضية مشري**، نفس المرجع، ص 137، عن **ميلود العربي بن حجار**، تشريعات الملكية في حقل البرمجيات في الجزائر، مقال منشور بالمجلة الالكترونية " cybrarians journal " العدد 26 ، سبتمبر 2011 على الموقع http://www.journal.cybrarians.org/index اطلع عليه بتاريخ 2015/03/18

[445]– د. **محمد حماد مرهج الهيتي**: مقال نطاق الحماية الجنائية للمصنفات الرقمية– دراسة مقارنة في القوانين العربية لحماية حق المؤلف– مجلة الشريعة و القانون، العدد 48، كلية الحقوق، جامعة المملكة، مملكة البحرين، اكتوبر 2011، ص 105.

و يتضح من التعاريف السابقة أنها ركزت على الطابع الإبداعي العقلي للمصنفات و هو الأمر الذي تتطلبه القوانين بصفة عامة، إلا أن تلك التعاريف بتحديدها للمصنفات الرقمية التي تنتمي إلى تقنية المعلومات قد أعطته مدلولا واسعا.

الفرع الثاني: تحديد المصنفات المعلوماتية

من خلال مفهوم المصنف الرقمي ابتداء و لغاية الآن تم تحديد ثلاثة أنواع من المصنفات الرقمية و التي شملت البرمجيات و قواعد البيانات و طبوغرافيا الدوائر المتكاملة، ثم ظهرت أنماط جديدة من المصنفات تثير حاجتها إلى الحماية القانونية و هي أسماء النطاقات أو الميادين أو المواقع على الشبكة، و عناوين البريد الالكتروني، و قواعد البيانات على الخط التي تتضمنها مواقع الانترنت، و مادة أو محتوى مواقع الانترنت من نصوص و رسوم وأصوات و مؤثرات حركية أو ما يطلق عليها بالوسائط المتعددة.

و بالتالي قد يطرح التساؤل حول مدى القدرة على حماية حقوق الملكية الفكرية على ما تتضمنه المواقع أو ما يتم نشره الكترونيا، و الذي قد يكون علامة تجارية أو اسما أو نموذجا صناعيا أو رسما أو صورتا...؟ يتم تحديد المصنفات المعلوماتية إلى نوعين كالآتي:

البند الأول: مصنفات الرقمية في بيئة الحاسوب

و تشتمل على برامج الحاسوب و قواعد البيانات و طبوغرافيا الدوائر المتكاملة:

أولا: برامج الحاسوب

البرمجيات هي الكيان المعنوي لنظام الكمبيوتر دونها لا يكون ثمة أي فائدة للمكونات المادية من الأجهزة والوسائط وهي بوجه عام تنقسم من الزاوية التقنية إلى برمجيات التشغيل المناط بها إتاحة عمل مكونات النظام مع توفير بيئة عمل البرمجيات التطبيقية، وتمثل البرمجيات التطبيقية النوع الثاني من أنواع البرمجيات وهي التي تقوم بمهام محددة كبرمجيات معالجة النصوص أو الجداول الحسابية أو الرسم أو غيرها، وقد تطور هذا التقسيم للبرمجيات باتجاه إيجاد برمجيات تطبيقية ثابتة وأنواع مخصوصة من البرمجيات تتزاوج في مهامها بين التشغيل والتطبيق، أما من ناحية الدراسات والتشريعات القانونية فقد أثير فيها عدد من المفاهيم المتصلة بأنواع البرمجيات أبرزها برمجيات المصدر و برمجيات الآلة والخوارزميات ولغات البرمجة وبرامج الترجمة[446] .

تعد برامج الحاسوب أول واهم المصنفات المعلوماتية أو تقنية المعلومات التي حظيت باهتمام كبير من حيث وجوب الاعتراف بها والتي أثارت جدلا قانونيا بشأن توفير الحماية القانونية لها من حيث طبيعتها وموضع حمايتها من بين تشريعات الملكية الفكرية.

---

[446]- **ميلود، العربي بن حجار**، تشريعات الملكية الفكرية في حقل حماية البرمجيات بالجزائر –.Cybrarians Journal –. ع 26، سبتمبر 2011 متاح في http://www.journal.cybrarians.org/index

إلا أن الاتجاه التشريعي الغالب اعتبرها أعمالا أدبية تحمى بموجب تشريعات حق المؤلف حيث اعتبرتها معاهدة الويبو مصنفات أدبية في المادة الرابعة بقولها: " تتمتع برامج الحاسوب بالحماية باعتبارها مصنفات أدبية بمعنى المادة 2 من اتفاقية برن ، وتطبق تلك الحماية على برامج الحاسوب أياً كانت طريقة التعبير عنها أو شكلها " [447] كما نصت المادة العاشرة من اتفاقية تربس على أن البرمجيات محل للحماية.

كذلك المشرع الجزائري حسم الأمر بشأن براج الحاسوب و شملها بالحماية ضمن المصنفات الأدبية المنصوص عليها في المادة 04 من الأمر 03-05 المتضمن حقوق المؤلف.

ثانيا: قواعد البيانات

تعرف قواعد البيانات من الناحية التقنية بأنها عبارة عن مجموعة منظمة من ملفات تحتوي على معلومات تختص بموضوع معين، و هذه الملفات تتفرغ بدورها إلى سجلات تتفرغ بدورها إلى حقول[448]، و تعرف من الناحية الفقهية بأنها تجميع لكمية كبيرة من المعلومات أو البيانات و عرضها بطريقة أو بأكثر تسهل عملية الاستفادة منها، لكونها موضوعة بطريقة منظمة بحيث يمكن الوصول إليها بسهولة و إجراء العمليات المختلفة عليها[449].

و يقصد بها كذلك كل النصوص، و الصور و الأصوات المحفوظة رقميا و التي بذل فيها جهد فكري و مادي في جمعها و تنسيقها، و هي عبارة عن بيانات و معطيات تخص موضوعا معين تم تجميعها، ترتيبها و تصنيفها بطريقة مبتكرة يتم تخزينها و يمكن استرجاعها و الاستفادة منها عند الحاجة[450].

فقاعدة البيانات هي البيانات المجمعة المبتكرة و هذه الأخيرة هي مناط الحماية.

و تحمى قواعد البيانات في التشريع الجزائري ضمن قانون حق المؤلف حيث جاء في المادة 2/5 من الأمر 05/03 المشار إليه سابقا أنه:" تعتبر مصنفات محمية كذلك الأعمال الآتية... المجموعات و المختارات من المصنفات، مجموعات...و قواعد البيانات سواء كانت مستنسخة على دعامة قابلة

---

[447]- **معاهدة الويبو** بشأن حق المؤلف كما اعتمدها المؤتمر الدبلوماسي في 20 ديسمبر 1996.

[448]- الحقل عبارة عن جزء من السجل الذي يتمثل في مجموعة كاملة من المعلومات عن شيء معين.

[449]-د. **محمد حماد مرهج الهيتي**، نطاق الحماية الجنائية للمصنفات الرقمية، مرجع سابق، ص 405.

[450]- **نايت أعمرعلي** ، الملكية الفكرية في إطار التجارة الالكترونية مذكرة ماجستير فرع قانون دولي للأعمال، مدرسة دكتوراه للقانون و العلوم السياسية، كلية الحقوق و العلوم السياسية، جامعة مولود معمري، تيزي وزو نوقشت بتاريخ 15 مارس 2014 ، ص13، عن **عبد الرءوف طالب حسينات** ، الحماية المدنية لحق المؤلف، في التشريعين المصري والأردني، رسالة دكتوراه، جامعة القاهرة، 2006، ص 197.

للاستغلال بواسطة آلة أو بأي شكل من الأشكال الأخرى، و التي تتأتى أصالتها من انتقاء موادها أو ترتيبها".

و الابتكار لا يستمد من طبيعة البيانات نفسها و إنما من طريقة ترتيبها أو إخراجها أو تجميعها أو استرجاعها، وفسر القضاء الفرنسي الابتكار بالنسبة لقواعد البيانات بأنه يقتضي توافر جهد جاد في البحث والاختيار والتحليل والذي عندما يقارن بمجرد التوثيق تظهر أهمية الجهد المبتكر للعمل ، وفي الاجتهاد القضائي قضت محكمة النقض الفرنسية في قضية (MICROFOR-LEMONDE) بأن قيام شركة MICROFOR الكندية بجمع الصحف الفرنسية وتنظيمها وفهرستها وخزنها بالحاسب و وضعها في متناول الجمهور يعد جهدا فكريا يقوم على مصنف محمي بقانون حق المؤلف[451].

و بالرجوع إلى الاتفاقيات الدولية نجد اتفاقية حقوق الملكية في إطار المنظمة العالمية للتجارة" تريبس" قضت في المادة 02/10 أنه: " تتمتع بالحماية البيانات المجمعة أو المواد الأخرى سواء كانت في شكل مقروء آليا أو أي شكل أخر إذا كانت تشكل خلقا فكريا نتيجة انتقاء أو ترتيب محتواها"[452]

و من جهة أخرى فقد نصت المادة 05 من معاهدة " الويبو" بشأن حق المؤلف المؤرخة في 20 ديسمبر 1996 على أنه" تتمتع مجموعات البيانات أو المواد الأخرى بالحماية بصفتها هذه ، أياً كان شكلها ، إذا كانت تعتبر ابتكارات فكرية بسبب اختيار محتوياتها أو ترتيبها، ولا تشمل هذه الحماية البيانات أو المواد في حد ذاتها، و لا تخل بأي حق للمؤلف قائم في البيانات أو المواد الواردة في المجموعة"[453].

ثالثا: طوبوغرافيا الدوائر المتكاملة

و يطلق عليها طوبوغرافيا الدوائر المدمجة و تعرف أيضا باسم التصميمات التخطيطية و هي عبارة عن دائرة كهربائية تصمم بطريقة مصغرة على رقائق أو شرائح، و من خلال إنتاج ا+لأجزاء الإلكترونية بشكل مصغر للغاية ، فان ذلك يسمح بدمجها في أجهزة مختلفة تكون ذات حجم صغير أيضا مثل الحاسبات الآلية أو التليفونات المحمولة لدرجة إمكانية وضعها في الحافظات أو في أجهزة أو معدات

---

[451]– مشار إليه لدى **ياسين بن عمر** ، جرائم تقليد المصنفات الأدبية و الفنية و آليات مكافحتها في التشريع الجزائري، مذكرة ماجستير، كلية الحقوق و العلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2011/2010، ص 23،24.

[452]– المادة 10 فقرة 2 من الجزء الثاني ، القسم الأول من اتفاقية تريبس

[453]- **معاهدة الويبو** بشأن حق المؤلف 1996 السابق الإشارة إليها.

يمكن برمجتها وفقا لذاكرة محددة، و تستخدم في العديد من الأجهزة حيث تعتبر بمثابة الدعامة الرئيسية للصناعات الالكترونية الحديثة[454] .

و وفقا لتعريف الدائرة المدمجة الواردة في اتفاقية الملكية الفكرية اتفاقية EPIC فان الدائرة المدمجة هي "منتج في هيئته النهائية أو الوسيطة يتضمن مكونات–أحدها على الأقل يكون عنصرا نشطا– و تشكل مع بعض الوصلات أو كلها ،كيانا متكاملا على قطعة من مادة عازلة بهدف تحقيق وظيفة الكترونية محددة"[455] .

أما المشرع الجزائري فقد عرفها في المادة الثانية من الأمر رقم 03–08 على أنها: " الدائرة المتكاملة: : "منتوج في شكله النهائي أو في شكله الانتقالي يكون أحد عناصره على الأقل عنصرا نشطا و كل الارتباطات أو جزءا منها هي جزء متكامل من جسم و/أو سطح لقطعة من مادة، و يكون مخصصا لأداء وظيفة إلكترونية".

التصميم الشكلي نظير الطبوغرافيا :" كل ترتيب ثلاثي الأبعاد، مهما كانت الصيغة التي يظهر فيها، لعناصر يكون أحدها على الأقل عنصرا نشيطا و لكل وصلات دائرة متكاملة أو لبعض منها أو لمثل ذلك الترتيب الثلاثي الأبعاد المعد لدائرة متكاملة لغرض التصنيع"[456].

البند الثاني: المصنفات الرقمية في بيئة الانترنت

من المشكلات القانونية التي أثيرت من وراء استخدام الانترنت ما يتعلق بكيفية حماية مصنفات الأدبية و الفنية المتاحة عبر شبكة الانترنت، و نظرا لقصور التشريعات حيث أنها لم تعالج إشكالية النشر الالكتروني للمصنفات الفنية و الأدبية أو المصنفات الموجودة على الشبكة ، فقد تطلب الأمر إيجاد حلول لمواجهة ما طرحه التقدم التكنولوجي في عرض المصنفات على شبكة الانترنت، و اتجهت الجهود الدولية التي بدلت تحت مظلة الويبو، خاصة و أن المادة 20 من اتفاقية برن أجازت للدول الأعضاء في إتحاد برن [457] أن تبرم فيما بينها اتفاقيات خاصة طالما أن تلك الاتفاقيات تمنح للمؤلفين حقوقا تفوق الحقوق المنصوص عليها في اتفاقية برن.

454– **عبد الرحمن ألطاف** ، تحديات حماية الملكية الفكرية للمصنفات الرقمية، أطلع عليه في الموقع http://www.f-law.net/law/threads/28525 بتاريخ 2015/03/18.

455– عبد الرحمن ألطاف، نفس المرجع المشار إليه.

456– **الأمر** رقم 03–08 المؤرخ في 19 يوليو 2003 يتعلق **بحماية التصاميم الشكلية للدوائر المتكاملة** ، الصادر بالجريدة الرسمية عدد 44 بتاريخ 23 يوليو 2003، ص 35.

457– " **إتحاد برن**" يقصد به الاتحاد الدولي الذي أنشأته اتفاقية برن.

وقد اسفرت الجهود الدولية في نهاية الأمر عن إصدار اتفاقية خاصة تطبيقا لحكم المادة 20 من اتفاقية برن وهي معاهدة الويبو بشأن حق المؤلف 1996 ، كما أبرمت اتفاقية أخرى تتوافق معها هي معاهدة الويبو بشأن فناني الأداء ومنتجي التسجيلات الصوتية[458] 1996 (WPPT).

و كذلك هناك مشكلات تتصل بأمن المعلومات بالنسبة لمواقع الانترنت أو المستخدمين، وعليه سوف نحاول تحديد نطاق المصنفات الرقمية في بيئة الانترنت من خلال العناصر الآتية:

أولا: أسماء نطاقات (عناوين الانترنت)

اسم النطاق أو الموقع[459] هو في الحقيقة عنوان على شبكة الانترنت يسمح بتحديد ذلك الموقع وتمييزه عن غيره من المواقع الأخرى، ولا يمكن الدخول إلى الموقع إلا عن طريق اسم الدومين[460].

لكل موقع على شبكة الإنترنت عنوان دال عليه يمكن للمستخدم بمجرد وضعه في مكان العناوين بعد الدخول للشبكة أن يصل إلى الموقع أياً كان موقع أنظمة الكمبيوتر المستضيفة له أو الموقع الجغرافي الفعلي لصاحب الموقع أو مزودات الموقع بالمواد المنشورة، و تتميز عناوين المواقع بسمات معينة، فالمواقع التجارية بوجه عام تنتهي بالاختصار (com) أما عناوين مواقع المنظمات فتنتهي بالاختصار (org) والمواقع الحكومية بالاختصار (gov) والجامعات بالاختصار (edu)، و بالنسبة للعناوين المرتبطة بدول معينة فتنتهي برمز أو اختصار الدولة، مثالها:- fr فرنسا،dz الجزائر و هكذا.

وحتى الآن لا توجد ثمة تشريعات شاملة ناظمة لمسائل أسماء النطاقات [461] و ما أثارته من إشكالات قانونية خاصة عندما يكون الاسم مطابقاً أو مقارباً أو مشابهاً لاسم تجاري أو علامة تجارية[462] .

إلا أن القضاء الأوروبي وتحديداً في فرنسا تصدى لنظر عدد من الدعاوى بهذا الخصوص، لكن مناط التطبيق بشأنها كان قوانين العلامات التجارية وقواعد حماية العلامات التجارية وليس قواعد قانونية خاصة بأسماء النطاقات[463].

ثانيا: النشر الالكتروني – محتوى مواقع الانترنت–

---

[458]– و يطلق على هاتين الاتفاقيتين **باتفاقيتي الانترنت**

[459]- و يطلق عليه أيضا " أسماء الدومين " Le Non De Domaine، " أسماء المجال"، " أسماء الحقل".

[460]– **كوثر مازوني**، الشبكة الرقمية و علاقتها بالملكية الفكرية، دار هومة، الجزائر، 2008، ص187.

[461]– **نايت أعمر علي**، مرجع سابق، ص 21، 22.

[462]– تفاصيل أكثر عن الموقع الالكتروني و تشابهه بالعلامة التجارية، مشار إليها لدى: **أ.خليفي مريم**، الرهانات القانونية للتجارة الإلكترونية، رسالة دكتوراه في القانون الخاص، كلية الحقوق و العلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، 2012/2011، ص 283–292.

[463]– م. **يونس عرب**، المرجع نفسه، ص 22.

اختلفت الآراء حول تحديد مفهوم النشر الالكتروني، حيث قيل بأنه: "عبارة عن العملية التي يتم من خلالها إعادة الوسائط المطبوعة كالكتب و الأبحاث العلمية بصيغة يتم استقبالها وقراءتها عبر شبكة الانترنت"، كما عرف على انه:" نقل و توزيع و استخدام المعلومات عن طريق الوسائط الالكترونية الرقمية مثل شبكات الاتصال و أجهزة الأقراص المضغوطة"[464].

و بالتالي النشر الالكتروني أو محتوى مواقع الإنترنت قد يتضمن معلومات عن إعلان تجارى والبث المرئي، والتسجيل الصوتي و الرسومات و الصور و غير ذلك..، فلا شك أن الانترنت كعالم افتراضي تحمل في طياتها العديد من المصنفات الرقمية و الالكترونية، منها ما تم حمايته قانونا و منها ما لم يتم حمايته بعد، مما يثير التساؤلات حول مدى القدرة على حماية حقوق الملكية الفكرية على ما تتضمنه المواقع؟ .

و ليس ثمة إشكال يثار في حالة كان محتوى الموقع مصنفاً أو عنصراً من عناصر الملكية الفكرية الذي يحظى بالحماية بشكل مجرد بعيداً عن موقع الإنترنت، كعلامة تجارية لمنتجات شركة ما تتمتع بالحماية استخدمتها الشركة على موقعها على الإنترنت، فما ينشر على الموقع هو بالأساس محل حماية بواحد أو أكثر من تشريعات الحماية في حقل الملكية الفكرية، لكن الإشكال يثور بالنسبة للمواد والعلامات والأشكال والرسومات التي لا يكون ثمة وجود لها إلا عبر الموقع، وبشكل خاص عناصر وشكل تصميم الموقع والمواد المكتوبة التي لا تجد طريقاً للنشر إلا عبر الإنترنت.

و لا تزال هذه الإشكاليات في مرحلة بحث واسع من قبل خبراء القانون والملكية الفكرية في مختلف الدول، خاصة بعد شيوع مسائل التجارة الإلكترونية و قواعد الأمن المعلوماتي وإنجاز قوانين التي تنظم الجرائم المتصلة بها، باعتبار إن أحد تحديات الأمن المعلوماتي مسائل الملكية الفكرية.

أما بالنسبة للوسائط المتعددة المستخدمة في ميدان بناء ومحتوى مواقع الإنترنت، فإنه يقصد بها وسائل تمثيل المعلومات باستخدام أكثر من نوع من الوسائط مثل الصوت والصورة والحركة

ويتميز هذا المصنف بمزج عدة عناصر: نص، صورة، صوت، وتفاعلها معاً، عن طريق برنامج من برامج الكمبيوتر، وتسوق تجارياً عن طريق دعامة مادية مثل الديسك أو السي دي (CD) أو يتم توزيعها أو إنزالها عن طريق خط الاتصال بشبكة الإنترنت

ويرى جانب من الفقه أن هذه المصنفات محمية بموجب القواعد العامة لحماية المصنفات الأدبية دون حاجة لإفراد قواعد جديدة، باعتبارها – لدى البعض – تتميز بتدخل برنامج كمبيوتر يسمح بالتفاعل بين

---

[464]- مشار إليه لدى **نايت أعمر علي**، مرجع سابق، ص 17

وسائل التعبير المتعددة (وبرنامج الكمبيوتر محل حماية) أو لأنها بمفرداتها محل حماية باعتبار هذه المفردات من المصنفات الأدبية أصلا [465](المواد المكتوبة، المواد السمعية والمرئية، الأداء...)و كلما توفر فيها عنصر الابتكار تحقق شرط الحماية المطلوب لحماية المصنفات الأدبية.

المطلب الثاني: الشروط القانونية لحماية المصنفات الرقمية

أي مصنف يجب أن يكون مشمولاً بالحماية القانونية، بأن يكون مبتكراً أو مبتدعا، و معبر عنه في شكل معين، فهل تتوافر هذه الشروط في المصنفات الرقمية ؟

إن المصنفات الرقمية المحمية بنصوص الملكية الفكرية و التي نص عليها المشرع الجزائري صراحة، تمثلت في برامج الحاسب الآلي و قواعد البيانات و الدوائر المتكاملة كما سبق بيانه، و حتى تحضا هذه المصنفات بالحماية لابد من توفر الشروط الآتية:

الفرع الأول: الإبتكار

لاحظ المشرع الجزائري أهمية التطور التكنولوجي و من ثم ضرورة حماية حق صاحب المصنفات المتعلقة بالبيئة الالكترونية، حيث ذكرت المادتين 04 و 05 من الأمر 05/03 صراحة حماية برامج الحاسوب و قواعد البيانات ، و لكن بما أن المشرع الجزائري اعتبرها مصنفات و من ثم إنتاجا ذهنيا أي يشترط شرط الابتكار لحمايتهم، و ما يمكن إثارته بهذا الخصوص هل يشترط الابتكار بمفهومه التقليدي لحماية المصنفات الرقمية في بيئة الحاسوب و الانترنت؟ أم بمفهومه الحديث الذي يتلاءم و طبيعة هذه المصنفات؟

يقصد بالابتكار " الأصالة " [466] أي أن يتميز المصنف بطابع أصيل سواء في إنشائه أو التعبير عنه، بحيث يكون الإنتاج الذهني يتميز بطابع معين يبرز شخصية صاحبه في مضمون و جوهر الفكرة أو مجرد الطريقة التي اتبعها لعرض الفكرة[467].

و لقد تعرض المشرع الجزائري لهذا الشرط بموجب أحكام المادة 01/03 من الأمر 03-05 السالف الذكر، غير أم مفهوم شرط الابتكار بالنسبة للمصنفات المعلوماتية كان محل جدل من قبل الفقه و القضاء الأوروبي خاصة القضاء الفرنسي.

---

[465]- **حسام الدين الأهواني** ، حماية الملكية الفكرية في مجال الانترنت، الدليل الالكتروني للقانون العربي، ص 03 على الموقع: www.arablawinfo.com

[466]– يفضل البعض مصطلح الأصالة على الابتكار كون ه ذا الأخير ينطبق أكثر على الملكية الصناعية: كوثر مازوني، مرجع سابق، ص 158.

[467]– **راضية مشري**، مرجع سابق، 138.

فا بالنسبة للابتكار في برامج الحاسب الآلي فقد تبنت المحاكم الفرنسية في قراراتها مفهوما موسعا و معيارا موضوعيا لشرط الأصالة،لأن المفهوم التقليدي أصبح لا يتلاءم مع الابتكارات المعلوماتية، إذ أعتبر أنه يكفي لتوافره أن يحمل البرنامج السمة التي تدل على المجهود الشخصي الذهني لصاحبه[468] حيث قضت محكمة إستئناف باريس في 07 مارس 1986 بأن:" مؤلف برنامج الحاسب الآلي يجب أن يقيم الدليل على أنه قد بذل مجهودا ذاتيا و ذلك خارج إطار ما يفترضه الحاسب الآلي من وجود عمل يتم دون إسهام ذاتي خلاق، و أن وضع هذا الجهد الذاتي موضع التطبيق يجب أن يكمن في تدخل شخصي من المؤلف"[469].

و قد تم تطبيق هذا المفهوم على قواعد البيانات، إذ أن الابتكار لا يستمد فيها من طبيعة البيانات نفسها و إنما كذلك من طريقة ترتيبها أو إخراجها أو تجميعها أو استرجاعها، فالابتكار لا يتحقق إلا إذا عكست قاعدة البيانات سمات شخصية[470] لصاحبها.

و هذا ما أشار له المشرع الجزائري في المادة 02/05 من الأمر 03-05 بقوله:" ...و التي تأتي أصالتها من انتقاء موادها أو ترتيبها ".

كما فسر القضاء الفرنسي الابتكار بالنسبة لقواعد البيانات بأنه يقتضي توافر جهد جاد في البحث و الاختيار و التحليل و الذي عندما يقارن بمجرد التوثيق تظهر أهمية الجهد المبتكر للعمل[471].

و عليه إذا كانت قاعدة البيانات عبارة عن تجميع لبيانات و أن هذه قد تعبر عن فكرة، فإن الفكرة لا تكون محلا للحماية لذاتها أو لتلك البيانات و إنما ينسحب أمر الحماية إلى طريقة الترتيب و الاختيار أو الانتقاء و الاسترجاع و التي تبرز الميزة الشخصية للمؤلف و هي التي تعطي قاعدة البيانات طابع الابتكار.

---

[468]- **بن عمر ياسين**، جرائم تقليد المصنفات الأدبية و الفنية و آليات مكافحتها في التشريع الجزائري، مذكرة ماجستير تخصص قانون جنائي، كلية الحقوق و العلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2010-2011، ص 22. و كذا: راضية مشري، مرجع سابق، ص 138.

[469] - "que l'auteur des logiciels avait fait preuve d'un effort personnalisé allant au- de la simple mise en œuvre d'une logique automatique et contraignante et que la matérialisation de cet effort résidait dans une structure individualisée". حكم محكمة باريس في 07 مارس 1986 مشار إليه **لدى كوثر مازوني**، مرجع سابق، ص 142 عن د. **أشرف وفا محمد** ، تنازع القوانين في مجال الحقوق الذهنية للمؤلف، ط 1، دار النهضة العربية، القاهرة، 1999، ص 18.

[470]- **راضية مشري مرجع سابق**، ص 139.

[471]- **بن عمر ياسين**، مرجع سابق، ص 23،24 .

و هي النتاج الذهني الذي يستحق الحماية في نطاقها دون قصر الحماية على جمع المعلومات أو البيانات فقط[472]، و هذا ما أكدته التشريعات السابق الإشارة إليها و من بينها التشريع الجزائري، و كذا ما جاء في المادة 2/10 من اتفاقية تريبس:" تتمتع بالحماية البيانات المجمعة أو المواد الأخرى ، سواء أكانت في شكل مقروء آليا أو أي شكل آخر ، إذا كانت تشكل خلقا فكريا نتيجة انتقاء أو ترتيب محتوياتها وهذه الحماية لا تشمل البيانات أو المواد في حد ذاتها ولا تخل بحقوق المؤلف المتعلقة بهذه البيانات أو المواد ذاتها "[473].

أما فيما يتعلق بأصالة تصاميم الدوائر المتكاملة_ لتحقيق وظيفة الكترونية– فإن المادة 03 من الأمر 03–08 قد نصت على ذلك بقولها:" يمكن بموجب هذا الأمر حماية تصاميم الشكلية لدوائر المتكاملة الأصلية.

يعتبر التصميم الشكلي أصليا إذا كان ثمرة مجهود فكري لمبتكره، و لم يكن متداولا لدى مبتكري التصاميم الشكلية وصانعي الدوائر المتكاملة..."

و يلاحظ أن المشرع الجزائري قصر شرط الأصالة في تعبير التصميم الشكلي عن الجهد الفكري الشخصي لمبتكره و تفرده بعدم تداوله لدى مبتكري و صانعي الدوائر المتكاملة.

و تتطلب المادة (35) من اتفاقية تربس أن تقوم الأعضاء بمنح الحماية للتصميمات المدمجة ، و هذه الحماية فقط إذا كانت مجموعة العناصر و الطبوغرافية بشكل متكامل تستوفى شروط الأصالة و ليست معروفة لدى مبتكري و مصنعي الدوائر المتكاملة

هذا ما تم إدراكه لشرط الابتكار بالنسبة للمصنفات المعلوماتية في بيئة الحاسوب و التي كان موقف الفقه و القضاء و حتى التشريع واضحا منها، يبقى الإشكال بالنسبة للمصنفات المعلوماتية في بيئة الانترنت فكيف يكون الابتكار شرطا لحمايتها؟

إن الابتكار في بيئة الانترنت ليس شرطا لحماية المصنفات الالكترونية فقط، بل هو عنصرا رئيسيا في وجودها، حيث يظهر الابتكار مثلا في وجود المواقع الالكترونية و تحقيق نجاحها لما تقدمه من أعمال أو خدمات و قدرتها على المنافسة.

472– د.**حماد مرهج الهيتي**، نطاق الحماية الجنائية للمصنفات الرقمية،دراسة مقارنة في القوانين العربية لحماية حق المؤلف، مرجع سابق، ص 407–408.

473– ***اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية (تربس)***

كما يظهر الابتكار في تصميم الموقع على صفحات الويب، و ما يتضمنه من رسومات أو ما يصاحبه من موسيقى أو عناصر حركية، بقصد جدب انتباه مستخدمي الانترنت[474].

و فيما يتعلق بالنشر الالكتروني أو المصنفات التي تتمثل في الوسائط المتعددة فانه و كما سبق الإشارة إليه تحمى بموجب القواعد العامة لحماية المصنفات الأدبية، و على الرغم من أنه لا يمكن الإطلاع على مضمونها إلا بوسيلة الكترونية، فإن هذا لا يعني أنها أخذت وصف المصنف الرقمي و بالتالي ينبغي أن تأخذ حكمه إنما ستضل هذه المصنفات محتفظة بطبيعتها بحسبانها مصنفات تخضع للتقييم و بالتحديد في نطاق الابتكار [475] المتطلب كشرط لحماية المصنف بمضمون أفكاره أو محتواه، و إذا ما كان هذا المضمون يشكل ابتكارا أم لا؟

و ننوه في هذا المقام إلى أن تشريعات الملكية الفكرية لم تنص صراحة إلا على المصنفات في بيئة الحاسوب، و انه لا توجد تشريعات خاصة بحماية مصنفات بيئة الانترنت التي قد تتعرض إلى انتهاكات متعددة دون أن يعاقب مرتكبيها مما يستدعي ضرورة التدخل لبسط الحماية القانونية لها.

الفرع الثاني: الإيداع و التسجيل

يمكن حماية المصنفات بما فيها المصنفات الرقمية باللجوء إلى عملية إيداعها في المكان الذي يحدده القانون، و يقصد بالإيداع القانوني للمصنف إلزام صاحب الحق على المصنف بتسليم نسخة أو أكثر من المصنف لإحدى السلطات الحكومية أو إحدى المكتبات الوطنية التي يحددها القانون لهذا الغرض[476].

و لقد اشترط المشرع الجزائري إضافة إلى الابتكار و أصالة المصنف أن يتم إيداعه و ذلك مهما يكن نوع المصنف أو نمط تعبيره و درجة إستحقاقه و وجهته، و سواء أكان المصنف مثبتا أم لا بأي دعامة تسمح بإبلاغه للجمهور و ذلك بموجب أحكام المادة 02/03 من الأمر 05/03.

فالمشرع الجزائري كغيره من المشرعين اعترف بإمكانية إيداع برامج الحاسب الآلي وقواعد البيانات للحصول على الحماية الممنوحة لحق المؤلف من أي اعتداء، لكن هذا الإجراء و إن كان يمنح هذه

---

[474]– **حسام الدين الأهواني**، مرجع سابق، ص 3.

[475]– د. **حماد مرهج الهيتي** ، نطاق الحماية الجنائية للمصنفات الرقمية،دراسة مقارنة في القوانين العربية لحماية حق المؤلف، مرجع سابق، ص 411.

[476]- م. **عماد محمد سلامة**، الحماية القانونية لبرامج الحاسب الآلي و مشكلة قرصنة البرامج، الطبعة الأولى، دار وائل للنشر، عمان، الاردن، 2005، 149.

المصنفات الحق المعترف به قانونا، إلا أن ذلك لا يشكل إلا قرينة على الملكية، بحيث تقبل إثبات العكس بموجب المادة13 من نفس القانونن و هو مجرد شرط شكلي وقائي.

و بحسب الأصل يكون الشخص مالكا للمؤلف بعد التصريح بالمصنف لدى الديوان الوطني لحقوق المؤلف و الحقوق المجاورة[477].

و فيما يخص تصاميم الدوائر المتكاملة فإنه وفقا للأمر 03-08 اشترط المشرع كذلك الإيداع و التسجيل لدى مصالح مختصة حتى يحضا هذا المصنف بالحماية[478].

بالنسبة لأسماء النطاقات أو العناوين الالكترونية فإن تسجيلها يكون حسب نوع الموقع إذا ما كان دوليا عاما(g LTD)[479] أو وطنيا محليا (cc LTD)[480]، أما عن تسجيل العناوين الالكترونية العامة فتشرف عليه منظمة الأيكان " ICANN"[481] و التي تفوض العديد من الشركات التابعة لها بحسب موقعها الجغرافي و التي لها فروع تتولى عملية التسجيل في كل من أوروبا و أسيا و أمريكا[482].

وتسجيل العناوين الالكترونية الوطنية قد يتطلب الحضور الشخصي لصاحب الطلب أمام الجهة المختصة بالتسجيل، و يتحقق من عدم أسبقية التسجيل مع تعبئة الطلب و دفع نفقات التسجيل.

و بالتالي لا يمكن أن تتطابق العناوين الالكترونية بهذا الإجراء و تكون من حق من قام بتسجيلها أولا، حيث يمكن الوصول بواسطتها و بكل سهولة إلى المواقع الإلكترونية على شبكة الانترنت.

تنص المادة الرابعة من معاهدة المنظمة العالمية للملكية الفكرية (ويبو) والمعتمدة في سنة 1996 على أنه "تتمتع برامج الحاسوب بالحماية باعتبارها مصنفات أدبية في معنى المادة الثانية من اتفاقية برن، وتطبق تلك الحماية على برامج الحاسوب أياً كانت طريقة التعبير عنها أو شكلها.

---

[477]- يكفل الديوان الوطني لحقوق المؤلف و الحقوق المجاورة حماية المصنف لمالكه طبقا للمادة 131 من الأمر 03-05 السابق الإشارة إليه.

[478]- حددت المواد من 11-18 من الأمر 03-08 المتضمن ***حماية التصاميم الشكلية للدوائر المتكاملة*** الصادر في 19 يوليو 2003، إجراءات و شكليات إيداع و تسجيل و نشر التصاميم الشكلية للدوائر المتكاملة، جريدة رسمية عدد 44 بتاريخ 23 يوليو 2003، ص 35.

[479]- اختصار بالانجليزية لـ : Génériques Top Level Domain Name

[480]- اختصار بالانجليزية لـ : Country Code Top Level Domain Name

[481]- منظمة الايكان اختصار بالانجليزية لـ : Internet Corporation For Assigned Names & Numbers و هي عبارة عن منظمة أمريكية تكونت سنة 1998 تمثل جهة تنظيمية و تنسيقية فيما يتعلق بتسجيل أسماء النطاق وعناوين الانترنت كما تضطلع بوضع القواعد الخاصة المطبقة على المنازعات المتعلقة بأسماء عناوين النطاقات.

[482]- د. **مريم خليفي**، مرجع سابق، ص 287.

و تنص المادة الخامسة على أنه تتمتع مجموعات البيانات أو المواد الأخرى بالحماية بصفتها هذه أياً كان شكلها إذا كانت تعتبر ابتكارات فكرية بسبب اختيار محتوياتها أو ترتيبها.

المبحث الثاني:

صور الإعتداء على المصنفات الرقمية

مما سبق توضيحه في المبحث الأول فإن الأصل في حماية حقوق الملكية الفكرية بشقيها هي حماية الحقوق المترتبة لأصحابها على المصنفات، متى توافرت فيها الشروط القانونية لحماية المصنف، ولا شك ان هذه الحماية تمتد حتى فيما يخص استغلال هذه الإبداعات والمصنفات على شبكة الانترنت و بثها رقميا أو عبر الأنظمة المعلوماتية، و يترتب على ذلك أنه لا يجوز استغلال أو استعمال أي من المصنفات بما فيها الرقمية أو المنشورة الكترونيا دون الحصول على إذن أو ترخيص مسبق من أصحابها أو من لديهم حق على ذلك المصنف.

و حيث تعتبر الاعتداءات على حقوق الملكية الفكرية و على وجه الخصوص حق المؤلف من بين الانتهاكات الأكثر انتشارا على الانترنت، الأمر الذي يهم كل من أصحاب الحقوق و مستعملي الشبكة خاصة مع غياب القوانين في هذا المجال و انتشار التجارة الالكترونية و ضعف الرقابة، الأمر الذي يشكل مساسا بمسائل الأمن المعلوماتي و باعتبار الانتهاكات الواقعة على الملكية الفكرية خاصة في البيئة المعلوماتية تشكل إحدى و أهم تحدياته.

و ما يهمنا في هذا الإطار هو الاعتداءات التي تقع على حقوق المؤلفين داخل الشبكة المعلوماتية أو بواسطة نظام معلوماتي، بما فيها جنحة التقليد و الأفعال الأخرى الملحقة بها و المنصوص عليها في قوانين الملكية الفكرية.

من بين المصنفات الرقمية التي شملها التشريع الجزائري بالحماية كما تم بيانه نجد حماية قانون المؤلف و الحقوق المجاورة لبرامج الحاسب الآلي و قواعد البيانات كما حدد الجرائم الواقعة على هذه المصنفات، لذلك و من خلال العناصر التي سيتم توضحها فيما يخص الجرائم الواقعة عليها من خلال المطالب الآتية :

المطلب الأول: الاعتداء المباشر على المصنف

إن المبدأ العام لحماية حقوق الملكية الفكرية سواء كانت أدبية أو فنية أو حقوق الملكية الصناعية، هو حماية الحقوق المترتبة لأصحابها على مصنفات أو إبتكارات مهما كانت ومتى تميزت بالأصالة

بالنسبة لحقوق التأليف و متى تميزت بطابع الابتكار و قابليتها للتطبيق الصناعي و إستفاء الشروط الشكلية بالنسبة للبراءة و الرسوم و النماذج الصناعية، أما بالنسبة للعلامات فمتى توفرت فيها الشروط الموضوعية و الشروط الشكلية[483].

ولا شك أن هذا المبدأ يمتد حتى فيما يخص استغلال هذه الابتكارات و المصنفات عبر الأنظمة المعلوماتية المختلفة أو بثها الكترونيا، بحيث لا يجوز إستغلال أو استعمال من هذه المصنفات بأي طريق أو بأي شكل يؤثر على حق صاحب المصنف دون إذن أو تصريح مسبق عن أصحابها، و إلا أعتبر اعتداءا على تلك الحقوق يعاقب عليه القانون.

و لقد نبهت المذكرة التفسيرية لإتفاقية بودابست 2001 إلى إنتهاكات حقوق الملكية الفكرية و على وجه الخصوص حق المؤلف و التي تعتبر من بين الجرائم الأكثر انتشارا على الانترنت[484].

غير ما يمكن الإشارة إليه فيما يخص اتفاقية بودابست و ما جاء في مادتها العاشرة بشأن تلك الانتهاكات و ما جاء في مذكرتها التوضيحية، أن تجريم تلك الانتهاكات يجب أن يكون متطابق مع التشريع الداخلي للدول المعنية بالاتفاقية، و أنها تستبعد تطبيق الاتفاقية على انتهاكات حقوق براءات الاختراع و العلامات التجارية.

و بالتالي يقتصر التجريم على انتهاكات حقوق المؤلف و الحقوق المجاورة و إذا ما تم ارتكابها عن طريق نظام معلوماتي و على نطاق تجاري.

كما أن الاتفاقية العربية لمكافحة لجرائم تقنية المعلومات المحررة بالقاهرة 2010، نصت كذلك على تجريم الانتهاكات المتعلقة بحقوق المؤلف و الحقوق المجاورة في المادة 17 منها [485].

و أما المشرع الجزائري فلقد تعرض بصفة عامة للجرائم الواقعة على حقوق المؤلف ممثلة في جريمة التقليد في الأمر 03-05 في الفصل الثاني تحت عنوان أحكام جزائية.

---

[483]- **كوثر مازوني**، مرجع سابق، ص 76.

[484]- د.**طارق إبراهيم الدسوقي عطية**، مرجع سابق، ص 332.

[485]- تنص المادة 17 من **الاتفاقية العربية بشأن مكافحة جرائم تقنية المعلومات** المحرر بالقاهرة 2010: " انتهاك حق المؤلف كما هو معرف حسب قانون الدولة الطرف، وذلك إذا ارتكب الفعل عن قصد ولغير الاستعمال الشخصي، وانتهاك الحقوق المجاورة لحق المؤلف ذات الصلة كما هي معرفة حسب قانون الدولة الطرف، وذلك إذا ارتكب الفعل عن قصد ولغير الاستعمال الشخصي".

و بخصوص المشرع الفرنسي فإنه من هذا الجانب قد أحدث قوانين جديدة لكل ما يتعلق بحقوق الملكية الفكرية في البيئة الرقمية و على شبكة الانترنت مسايرا في ذلك التطور التكنولوجي و ما ينجر عنه من مهددات، و كالعادة دائما سباق في سن التشريعات[486].

و بالتالي فإن كل استنساخ أو تمثيل أو نشر بكل وسيلة ما لمصنف ذهني يعتبر خرق لحقوق المؤلف، و من ثم يشكل تقليدا، و يعتبر ذلك احد أشكال الإجرام المعلوماتي متى تم بواسطة نظام معلوماتي[487].

و من هذا المنطلق يمكن دراسة جريمة التقليد و التي لا تقوم إلا بتوافر أركانها الأساسية، ركن مادي (فرع أول) و ركن معنوي(فرع ثاني) على النحو الأتي:

الفرع الأول: الركن المادي

يتحقق الركن المادي لجريمة التقليد و كسائر الجرائم بتوافر نشاط إجرامي و نتيجة و علاقة سببية بينهما، أما محل النشاط فقد تم التطرق إليه في المبحث الأول.

و لتحقق الفعل الإجرامي يجب أن يقع الاعتداء على الحق المالي أو الأدبي لمؤلف المصنف، كما يجب أن يقع الاعتداء بواسطة نظام معلوماتي و بدون إذن المؤلف، و بالرجوع لاتفاقية بودابست فإنها استثنت بموجب المادة العاشرة الاعتداءات الواقعة على الحق المعنوي أو الأدبي و اقتصرت على الحق المالي فقط، لكن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لم تحدد ذلك و إنما جرمت كل إعتداء على حق المؤلف كما هو معرف حسب قانون الدولة الطرف.

رجوعا إلى التشريع الجزائري فإن صور الاعتداء على حق حق المؤلف كما ورد في المادة 151 و ما بعدها من الأمر 03-05 السالف الذكر.

البند الأول: الاعتداء على الحق الأدبي لمؤلف المصنف

---

[486]- **القانون** رقم 2009-1311 بتاريخ 28 اكتوبر 2009 بشأن **الحماية الجنائية للملكية الأدبية و الفنية على شبكة الانترنت** ، والقانون رقم 2012-278 بتاريخ 01 مارس 2012 **بشأن الاستغلال الرقمي للكتب غير المتوفرة الصادرة في القرن العشرين** وغيرها من التشريعات ذات العلاقة

[487]- بالرغم من إحداث المشرع الاردني **لقانون خاص بمكافحة جرائم تقنية المعلومات** لسنة 2010، إلا انه لم يأتي بنص صريح حول الجرائم المعلوماتية المتعلقة بالملكية الفكرية، غير أن المادة 14 منه أحالت فيما لم يرد بشأنه نص صريح و تم ارتكابه بستخدام الشبكة المعلوماتية أو أي نظام معلوماتي إلى تطبيق نفس الأحكام و لا حاجة لتكرار النص:" كل من ارتكب جريمة معاقب عليها بموجب أي تشريع نافذ باستخدام الشبكة المعلوماتية أو أي نظام معلومات أو اشترك أو حرض إلى ارتكابها يعاقب بالعقوبة المنصوص عليها في ذلك التشريع" .

لم ينص المشرع الجزائري على جميع الاعتداءات الواقعة على كل حقوق المؤلف و إنما جرم البعض منها ضمن أحكام المادة 151 من قانون المؤلف و الحقوق المجاورة و تمثلت تلك الاعتداءات في ما يلي:

أولا: الكشف غير المشروع للمصنف

لمؤلف المصنف الحق وحده في الكشف عن مصنفه بإسمه الخاص أو باسم مستعار، كما يمكن له تحويله إلى الغير، و يعود هذا الحق إلى ورثته بعد وفاته طبقا للمادة 22 من الامر 03-05، و عليه أي عملية للكشف عن المصنف و إظهارها للعن من قبل الغير الذي ليس له هذا الحق، يعد اعتداء غير مشروع و يدخل ضمن نطاق التجريم المنصوص عليه في القانون الداخلي.

و بهذا الخصوص أدانت المحكمة الإصلاحية لمدينة ميتز METZ الفرنسية شابين قرصانين بسبب قيامهما بالهندسة العكسية و النسخ لبرمجيات ألعاب، و كشفهما عنها في ذات اليوم الذي كانت الشركة المنتجة قد قررت الإطلاق التجاري لها[488].

ثانيا: المساس بسلامة المصنف

حق تعديل أو تغيير أو حذف أو إضافة في مصنف ما يكون كذلك للمؤلف وحده [489]، و لا يمكن للغير الاعتراض على ذلك ما لم يكن فيه إخلال أو مساس بمصالحهم [490]، فمن يرتكب أحد الأفعال السابقة يتوفر في حقه النشاط الإجرامي لجريمة التقليد.

البند الثاني: الاعتداء على الحقوق المالية لمؤلف المصنف

تقع أفعال الاعتداء على الحق المالي لمؤلف المصنف باستغلاله أيا كانت صورة هذا الاستغلال سواء بالنسخ أو الاستعمال أو الترجمة، و سواء وقع النسخ كليا أو جزئيا، و يقع جرم النسخ أيضا سواء تم نسخ المصنف باسم مؤلفه الحقيقي أو باسم شخص أخر، أو باسم الجاني نفسه أو بإسم خيالي[491].

و يدخل في حكم الاستنساخ تثبيت البرمجية في جهاز أخر غير المرخص به للتثبيت في الاستنساخ غير المشروع، و من ذلك ما قضت به المحكمة الإصلاحية لمدينة Cusset الفرنسية في قضية شركة

488- حكم مشارا ليه لدى: **مسعود خثير**، مرجع سابق، ص 90

489- حسب ما جاء في المادة 89 من **الأمر 03-05** السابق الإشارة إليه.

490- **خثير مسعود**، مرجع سابق، ص 91.

491- **راضية مشري**، مرجع سابق، ص 142.

قام رئيسها رفقة أحد مديريه بتثبيت برمجية مرخص بها لجهاز واحد في باقي أجهزة المؤسسة، و تمت إدانته بناء على تفتيش من فرقة الدرك الفرنسية المختصة[492].

فإذا كان من حق المؤلف أو من له الحق المالي على المصنف هو وحده المخول بإجراء النسخ و بأي شكل أو وسيلة كانت، إلا أن المشرع الجزائري لم يعطه هذا الحق على إطلاقه، ويظهر ذلك من خلال الاستثناءات الواردة في الأمر 03-05 فيما يخص المواد 41-51 منه، و كذا فيما يخص استنساخ برامج الحاسب الآلي دون إذن من مؤلفها بموجب المادتين 52 و53 من نفس الأمر.

البند الثالث: قيام الفعل بدون موافقة صاحب المصنف

لا يكفي توافر النشاط أو السلوك الإجرامي لأفعال التقليد بل يشترط إلى جانب ذلك عدم موافقة صاحب المصنف على تلك الأفعال.

و لقد اشترط المشرع الجزائري ضرورة الإذن الكتابي من المؤلف يتنازل به عن حقوقه المادية و ذلك طبقا للمادة 62 من الأمر 03-05، إذ تعتبر كتابة الإذن شرط وجود لقيام التصرف لا شرط إثبات، كما أن الإذن اللاحق على عملية الاستنساخ أو التقليد لا يمكن أن يأخذ حكم الإذن السابق، و بالتالي موافقة صاحب المصنف بعد تمام الجريمة لا تحول دون متابعته[493].

كما أن المذكرة التفسيرية لاتفاقية بودابست أشارت إلى أن إعادة إنتاج أو بث الأعمال المحمية دون موافقة حائز حق المؤلف هو أمر شائع للغاية، و هذه الأعمال المحمية تشمل على وجه الخصوص: الأعمال الأدبية و التصويرية و الموسيقية و السمعية البصرية.

البند الرابع: وقوع الاعتداء بواسطة نظام معلوماتي

لاعتبار الاعتداءات الواقعة على حقوق الملكية الفكرية و الحقوق المجاورة كشكل من أشكال الإجرام المعلوماتي، يشترط أن تتم بواسطة نظام معلوماتي[494]، و هذا الشرط مفترض حتى و إن لم يتم النص عليه صراحة ذلك أن النظام المعلوماتي أو الشبكة المعلوماتية جزء من الجريمة المعلوماتية.

و قد نصت عليه اتفاقية بودابست بقولها في المادة العاشرة:" ...إذا ما ارتكبت هذه الأفعال عمدا و على نطاق تجاري و بواسطة نظام معلوماتي..."

---

[492]- مشار إليه لدى: **خثير مسعود**، مرجع سابق، ص 93.

[493]- **راضية مشري**، مرجع سابق، ص 142.

[494]- د. **طارق إبراهيم الدسوقي عطية**، مرجع سابق، ص 332، 333.

يستهل من ذلك أن جرائم الملكية الفكرية تحكمها القواعد العامة الخاصة بها، ولا تأخذ حكم الجرائم معلوماتية إلا إذا وقعت بنظام معلوماتي، و أن تلك الجرائم تدخل في هذا النطاق خاصة عند استخدام التكنولوجيا الرقمية التي تسهل أفعال النسخ غير المصرح به، نطاق يتم بمقتضاه إعادة الإنتاج و التوزيع عبر الشبكات المعلوماتية، مما يفرض وضع جزاءات لحماية المصنفات في البيئة الرقمية.

كما أن الاتفاقية العربية بشأن مكافحة تقنية جرائم المعلومات لم تحدد هذا الشرط صراحة في النص الذي يجرم الانتهاكات الواقعة على حق المؤلف و الحقوق المجاورة، و إنما اشترطت أن يكون التجريم وفقا لما جاء في القانون الداخلي للدولة الطرف.

و بالرجوع إلى التشريع الجزائري نجد أن المشرع وسع من دائرة التجريم لصور جنحة التقليد من خلال ما نص عليه في المادة 152 من الأمر 03-05 بقولها:" يعد مرتكب لجنحة التقليد كل من ينتهك الحقوق المحمية بموجب هذا الأمر فيبلغ المصنف أو الأداء عن طريق .....أو بأي وسيلة نقل أخرى لإشارات تحمل اصواتا أو صورا و أصواتا أو بأي منظومة معالجة آلية"

و أعتبر أن تبليغ المصنف بدون إذن صاحبه أو من له الحق عليه بأي وسيلة بما فيها منظومة المعالجة الآلية يشكل جريمة تقليد و تخضع لجزاء جرائم الملكية الفكرية.

الفرع الثاني: الركن المعنوي

جريمة التقليد من الجرائم العمدية لا يكفي الركن المادي بعناصره لقيامها، بل يقوم إلى جانبه القصد الجنائي العام بعناصره، العلم و الإرادة و بالتالي يكفي أن يعلم الجاني أنه يعتدي على مصنف لشخص أخر بواسطة نظام معلوماتي، و أن تتجه إرادته إلى ذلك الفعل من أجل تقرير مسؤوليته الجنائية.

المطلب الثاني: صور و أشكال الاعتداء غير المباشر على المصنف

حدد المشرع الجزائري الجرائم الملحقة بجريمة التقليد في المادة 151 الفقرات الثالثة والرابعة و الخامسة من الأمر 03-05، نتطرق إليها باعتبارها جريمة مكونة من ركنين مادي(فرع أول) و معنوي(فرع ثاني):

الفرع الأول: الركن المادي

يتحدد الركن المادي للجرائم الملحقة لجريمة التقليد من خلال توفر مجموعة من السلوكيات نحاول التطرق إليها باختصار على النحو الآتي:

البند الأول: إستراد أو تصدير مصنفات مقلدة

جرم المشرع الجزائري في الفقرة الثالثة من المادة 151 السالفة الذكر، أفعال التصدير أو الإستراد لمصنفات أو أداءات مقلدة من و إلى الجزائر، و بالتالي التوسيع من صور جريمة التقليد.

و بالتالي متى كانت الأفعال المتابع بشأنها تعد من أعمال الاستراد و التصدير لمصنفات مقلدة أعتبر ذلك جريمة تقليد.

كما يعتبر تقليدا مجرد عرض المصنفات المقلدة المستوردة أو إعدادها بغرض تصديرها، سواء تعلق الأمر بمصنفات وطنية أو أجنبية[495].

البند الثاني: بيع أو تأجير أو وضع رهن التداول لمصنفات مقلدة

البيع المجرم بموجب التشريع هو الذي يتم بمقتضاه نقل حق إستغلال مصنف مقلد إلى المشتري مقابل ثمن [496]، أما التأجير فهو وضع المصنف المقلد أو نسخ منه لدى الغير قصد تمكينه من استعمالها و الانتفاع منها لمدة معينة مقابل دفع أجر مالي[497].

و تقوم جريمة التقليد حتى بتداول المصنف المقلد، بإعطائه لشخص ما لمشاهدته حتى ولو لم يكن ذلك بثمن[498].

البند الثالث: رفض إعطاء مكافأة المستحقة للمؤلف أو لصاحب الحق

انفرد المشرع الجزائري بهذه الصورة من جرائم التقليد عن باقي التشريعات و أخضعها لنفس عقوبة التقليد المباشرة، و الأصل في استغلال المصنف أن يكون بمقابل مادي أو بما يسمى بالمكافأة المستحقة لصاحب المصنف عن حق من حقوقه المادية سواء كليا أو بصفة مؤقتة، و في حالة إمتناع الشخص المكلف بدفع المكافأة المستحقة يقوم الركن المادي للجريمة[499].

و ما يمكن ملاحظته كذلك على تفرد المشرع الجزائري بهذه الصورة، أنه لم يولي اهتماما لصور أخرى قد تشكل إعتداءات أو إنتهاكا لحق المؤلف في ظل الثورة التكنولوجية، من بينها القيام بفك أو تعطيل أو إزالة عن قصد أو بسوء نية لأي حماية يستخدمها صاحب المصنف أو الأداء لتشفير

---

[495]- **راضية مشري**، مرجع سابق، ص 143.

[496]- **عفيفي كامل عفيفي**، مرجع سابق، ص 95.

[497]- **مسعود خثير**، مرجع سابق، 98.

[498]- **عماد محمد سلامة** ، الحماية القانونية لبرامج الحاسب الآلي و مشكلة قرصنة البرامج،ط 1، دار وائل للنشر، عمان- الأردن، 2005، ص 167.

[499]- **خثير مسعود**، مرجع سابق، ص 98.

مصنفه الموجود على شبكة الانترنت أو أي نظام معلوماتي بقصد حمايتها من صور التقليد، مما يستوجب التدخل التشريعي من جديد لتدارك مثل هذه الأفعال.

و بطبيعة الحال إذا ما ارتكبت هذه الأفعال بواسطة نظام معلوماتي، قد تشكل جريمة معلوماتية تقع على مصنفات الملكية الفكرية، أو تدخل في نطاق جرائم التقليد في البيئة الرقمية.

الفرع الثاني: الركن المعنوي

يتمثل في القصد الجنائي العام و هو يقتضي أن يكون الجاني عالما بأن ما قام ببيعه أو تاجيره أو تداوله هو مصنف مقلد مع اتجاه إرادته لذلك، و الركن المعنوي في هذه الجريمة مفترض بمجرد توفر الركن المادي[500].

و كخلاصة لهذا الفصل و مما تم تحديده في العناصر السابقة، أن حقوق المكية الفكرية والحقوق المجاورة محمية بموجب التشريعات الدولية و الداخلية لكل دولة و مخصصة لهذا الغرض، غير أن التطور التكنولوجي أظهر الارتباط بين تشريعات الملكية الفكرية و جرائم تقنية المعلومات، ذلك أن حماية حق صاحب المصنف مهما كان نوعه أو شكله أو طريقة التعبير عنه للوجود سواء في دعامة مادية أو بطريقة أخرى أو عبر أنظمة معلوماتية مما يقتضي، و أن هذه الطريقة قد تسهل من أفعال الاعتداء على تلك الحقوق، مما يقتضي وجود تشريعات مرنة تتلاءم مع كل تطور تكنولوجي وتحمي كل مصنف تم تقليده و على نطاق واسع، و ليس بشكل مجرد وفقا للقوانين التقليدية لحماية الملكية الفكرية.

---

[500]– **عفيفي كامل عفيفي**، مرجع سابق، ص 96.

الباب الثاني:
مجالات الوقائية و الإجرائية لقواعد الأمن المعلوماتي

الباب الثاني

الجوانب الوقائية و الإجرائية لقواعد الأمن المعلوماتي

بعد دراسة الجوانب الموضوعية للسلامة المعلوماتية متمثلة في إبراز الجانب الموضوعي لجرائم الاعتداء على نظم المعالجة الآلية للمعطيات وبعض الجرائم الماسة بمنتوجات الحاسب الآلي، وما تشتمل عليه من مخاطر تهدد أمن وسلامة المعلومات والأنظمة المعلوماتية، ومما يستوجب التدخل القانوني وتوفير المقومات البشرية والمادية لمواجهة ومكافحة هذا النوع من الإجرام وأخطاره التي تهدد الأمن والأمان المعلوماتي.

و مما يستوجب اتخاذ كل الإجراءات والتدابير الوقائية والعلاجية لمواجهة هذا الخطر، ونعني بالإجراءات والتدابير الوقائية تحديد العقوبات المناسبة لجرائم الاعتداء على نظم المعالجة الآلية والجرائم ذات الصلة، باعتبار انه لا جريمة ولا عقوبة ولا تدابير امن إلا بنص، حيث يعد تحديد الجرائم والعقوبات المقررة لها احتراما لمبدأ الشرعية.

حيث تعد العقوبة الإطار الوقائي والرادع لكل الجرائم المحددة، أما في حالة عدم وجودها فإن الأمر صعب خاصة إذا ترتب على تلك الأفعال خسائر مادية أو معنوية، و حتى مع وجود نصوص قانونية تعاقب على تلك الأفعال إلا أنه يلاحظ صعوبة تطبيقها نظرا لحداثة هذا النوع من الإجرام و عدم تمكن رجال القانون من تكييف هذه الجرائم مع النص الملائم لها خاصة مع عدم وجود نصوص تنظيمية مكملة لتلك القوانين.

و نظرا للخسائر التي قد تسببها هته الجرائم و سعيا لتجنب وقوعها يستوجب على المشرع الجزائري و غيره من المشرعين التدخل و فرض العقاب المناسب حتى يتحقق الهدف الوقائي والردعي لهذه الجرائم، كما يستوجب استحداث قواعد وتدابير وقائية وعلاجية أكثر ملائمة وانسجاما مع الطبيعة التقنية التي تقع عليها هذه الجرائم.

فإن حدث ووقعت الجريمة حسب الشكل القانوني لها، يكون بذلك للدولة حق الاقتضاء ومعاقبة الجاني واتخاذ الإجراءات اللازمة والمقررة قانونا للكشف عن الجريمة والمجرمين وتثبيت الإدانة، لذلك يجب أن تتوافق كذلك القواعد الإجرائية مع المسرح المستحدث للجريمة و البيئة الرقمية؛

ذلك أن القواعد الإجرائية التقليدية لجمع أدلة الإثبات قد لا تكون كافية في البيئة الرقمية لكشف الجريمة، و لكون هذه البيئة تتصف بالتعقيد والتشابك لكثرة الاتصالات وطرق بث ونقل المعلومات، و أن الدليل فيها يختلف عن الدليل في الجريمة التقليدية، وأنا تحديث القواعد العقابية لتتماشى مع الجرائم المستحدثة غير كافي ما لم يسايرها القانون الإجرائي فيما يخص تقنيات التحري والضبط والتفتيش...

إضافة إلى صعوبات أخرى قد تطرح فيما يتعلق بقبول الدليل الالكتروني و مدى اقتناع القاضي به كوسيلة من وسائل الإثبات؟ و خاصة أن هذا الدليل له طبيعة خاصة تميزه عن الدليل العادي، إضافة إلى انه دليل يمكن تغييره أو محوه أو تزييفه مما يجعل قبوله والاعتراف به أمر صعب؟

لذلك ومن خلال هذا الفصل سوف أحاول الإجابة على بعض الإشكالات المتعلقة بالجوانب الوقائية والعلاجية للسلامة و الأمن المعلوماتي متمثلة فيما يلي:

ما مدى كفاية العقوبة للوقاية والردع من الجرائم المعلوماتية؟ وهل هناك تدابير أخرى للوقاية من الجريمة قبل وقوعها؟

ما مدى ملائمة القواعد الإجرائية التقليدية للكشف عن الجريمة في البيئة الرقمية؟

ما مدى قبول الدليل التقني من القاضي الجزائي؟ وما هي شروط قبوله كدليل إثبات؟.

و عليه يتم التطرق في هذا الباب إلى الإجراءات الوقائية للأمن المعلوماتي متمثلة في العقوبات المقررة في التشريع الجزائري و التشريعات المقارنة(فصل أول) و إلى الإجراءات العلاجية في حالة وقوع الجريمة(فصل ثاني) و كذا إلى سبل مكافحة الجريمة المعلوماتية و إجراءات التعاون على المستوى الإقليمي و الدولي كحلول لدعم الأمن المعلوماتي (فصل ثالث) كالآتي:

الفصل الأول

الإجراءات الوقائية للأمن المعلوماتي

إن المشكلة في مجال الوقاية ومكافحة الإجرام المعلوماتي هو قلة القوانين المختصة التي تحول دون ارتكاب هذا الإجرام، إذ القوانين الموجودة أغلبها متعلقة بالجرائم التقليدية و كون الجرائم المتعلقة

بالحاسبات ونظم المعالجة تعد شكلا جديدا مقارنتا بسابقتها، ومع ازدياد انتشارها ظهرت الحاجة إلى وضع نصوص قانونية لردع و معاقبة مرتكبيها و محاربة و مكافحة وقوعها.

و أن الأخطار و الخسائر الناجمة عنها أكثر من تلك الناجمة عن الجريمة التقليدية، كونها تكلف الأشخاص والشركات مبالغ مالية باهظة، وتهدد أمنهم وخصوصياتهم مما يستدعي وضع تشريعات أكثر صرامة، قد تردع بعض ضعيفي النفوس من القيام بأعمال غير شريفة[501].

و في هذا انقسم الفقه القانوني في نظر الطريقة المناسبة لردع هذا الإجرام و الوقاية منه إلى اتجاهين:

اتجاه يعتقد فيه رجال القانون أن العقوبة يجب أن تتناسب مع تأثير الجريمة، فالعقوبة تكون أخف إذا كان هدف الجاني مجرد التطفل والتسلية، وتكون العقوبة أشد إذا كان الجاني يهدف إلى سرقة أموال أو معلومات أو إتلافها فالعقوبة هنا تكون قاسية.

أما أصحاب **الاتجاه الثاني** يرون أنه في أي حالة من حالات التجاوز يجب أن يعاقب عليها القانون ويشدد في ذلك دون النظر إلى تأثيرها ودوافع القائمين بها[502].

و من خلال ذلك سوف نبحث عن موقف المشرع الجزائري في الوقاية والردع لهذا النوع من الإجرام وما هي الطرق التي اتبعها؟ ومدى كفاية العقوبة؟ مقارنة مع التشريعات الأخرى[503].

---

[501]- **د.دلال صادق الجواد ود. حميد ناصر الفتال**، أمن المعلومات، دار اليازوري، عمان الأردن، 2008، ص142.

[502]– نفس المرجع، ص 142.

[503]– منها التشريع الفرنسي والأردني

المبحث الأول

دور العقوبة في في تحقيق الأمن المعلوماتي

إن الدور الأهم في العقوبة هو الجزاء القانوني الرادع لكل من يشارك أو يقوم بالاعتداء على المعلومات و عناصر نظم المعالجة الآلية للمعطيات، و كذا ضمان الأمن واسترجاع الحقوق في حالة الاعتداء عليها.

وهذا ما أكدته اتفاقية بودابست بشأن الجرائم الالكترونية، وعلى ضرورة تكريس عقوبات فعالة ملائمة ورادعة تتناسب و خطورة الأفعال الواقعة على نظم المعالجة الآلية للمعطيات.

حيث أشارت هذه الاتفاقية على ضرورة أن يكون كل فعل مجرم تم النص عليه فيها مستحق لجزاءات عقابية والتي يجب أن تكون فعالة وملائمة ورادعة، وذلك للحيلولة دون حدوث نتائج خطيرة[504]، وهذا ما وضحته بموجب المادة 13 تحت عنوان الجزاءات والإجراءات.

و هذا التأكيد نابع من خطورة هذه الجرائم و خسائرها على الاقتصاد الوطني، وانتشار الوعي بهذا الأمر، و أنا صعوبة التصدي لهذا الخطر والتهديد نابع من صفة بعض الأشخاص قد يطلق عليهم تسمية" المتطفلين الأذكياء"[505] و الذين يمكن تسخيرهم من قبل الجهات والحكومات للحصول على ما هو أثمن وأخطر، سواء من أجل المنافسة أومن أجل امتلاك مركز القوة، فمن يمتلك المعلومة يمتلك القوة كما سبق بيانه .

كما أن هذه الأخطار لا ترتكب من قبل أشخاص معينين، بل من قبل جميع الأشخاص والفئات والطبقات، وذلك نتيجة انتشار التكنولوجيا وتبسيط وسائل الاتصال، وانتشار الانترنت، حيث أشارت الإحصائيات إلى أن عدد مقاهي الانترنت في الجزائر وصلت في سنة 2011 إلى أكثر من 6000 نادي انترنت انتشرت عبر أنحاء الوطن مقابل 3500 موقع إلكتروني فقط[506]، ضف إلى ذلك دخول الجزائر في السنوات الأخيرة تكنولوجيا الجيل الثالث و الرابع، وعلى الرغم من التأخر التكنولوجي في الجزائر وضآلة نتائج التطور مقارنة مع الدول العالم، إلا أنها ليست بمعزل عن الأخطار المعلوماتية التي أصبحت تهدد امن أكبر دول العالم.

---

[504]- د. **هلالي عبد اللاه أحمد**، مرجع سابق، ص 154،155.

[505]– لتفاصيل أكثر لدى: د.**دلال صادق الجواد ود.حميد ناصر الفتال**، مرجع سابق، ص 141

[506]– أ. **رشيدة بوكر**، المرجع السابق، ص 315.

و من اجل ذلك سارع المشرع الجزائري إلى إدخال تعديلات على قانون العقوبات في الفصل الثالث المتضمن الجنايات والجنح ضد الأموال، وإضافة قسم سابع مكرر متعلق بأنظمة المعالجة الآلية للمعطيات بموجب القانون رقم 04_15 وتعديله من جديد في 2006 بموجب القانون رقم 06-23[507] حيث شدد فيه عقوبة الغرامة دون المساس بالنصوص التجريمية الواردة بشان المساس بأنظمة المعالجة الآلية.

و نفس الأمر بالنسبة للمشرع الفرنسي، وبناء على الوضع القائم قام بتعديل قانون العقوبات وفي كل مرة يشدد فيها العقاب على الجرائم المتعلقة بالمعالجة الآلية للمعطيات، من تلك التعديلات نجد تعديل سنة 2004 بموجب القانون 2004-575 المؤرخ في 21 جوان والمتعلق بالثقة في الاقتصاد الرقمي[508] الذي جاء فيه تشديد عقوبة الحبس والغرامة المقررة لهذه الجرائم وذلك بموجب المادة 45 الفصل الثاني منه بعنوان مكافحة الجرائم الفضاء المعلوماتي.

حيث يثبت تدخل المشرع وتشديده العقاب على هذه الجرائم إدراكا منه بخطورة الوضع وضرورة وجود عقاب رادع.

أما بالنسبة للمشرع الأردني فإنه أصدر قانونا في سنة 2010 بشان جرائم أنظمة المعلومات، قانون متأخر و مؤقت مقارنة مع تشريعات الدول الأخرى، ولكنه يشمل العقاب على مختلف الجرائم المعلوماتية.

---

[507]- القانون رقم 23/06 المعدل لقانون العقوبات المؤرخ في 20 ديسمبر 2006

[508] **-Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique,** JORF n°0143 du 22 juin 2004 page 11168 texte n° 2. Chapitre II : Lutte contre la cybercriminalité Art 45 : Art 45 ;

I. - L'article 323-1 du code pénal est ainsi modifié :

1° Au premier alinéa, les mots : « d'un an » sont remplacés par les mots : « deux ans » et la somme : « 15 000 EUR » est remplacée par la somme : « 30 000 EUR » ;

2° Au second alinéa, les mots : « deux ans » sont remplacés par les mots : « trois ans » et la somme : « 30 000 EUR » est remplacée par la somme : « 45 000 EUR ».

II. - A l'article 323-2 du même code, les mots : « trois ans » sont remplacés par les mots : « cinq ans » et la somme : « 45 000 EUR » est remplacée par la somme : « 75 000 EUR ».

III. - A l'article 323-3 du même code, les mots : « trois ans » sont remplacés par les mots : « cinq ans » et la somme : « 45 000 EUR » est remplacée par la somme : « 75 000 EUR ».

و السؤال الذي يمكن طرحه في هذا المقام هو هل العقوبات الواردة بهذه النصوص هي كافية لردع هذه الأفعال أو للحد و الوقاية من جرائم تقنية المعلومات؟ آم لا بد من احتياطات واستراتجيات أخرى؟ نحاول معرفة ذلك خلال العناصر الآتية:

المطلب الأول: مضمون و نطاق العقاب

إن العقاب الجنائي رادع سواء بالنسبة للأشخاص الطبيعية بفرض عقوبة الحبس والغرامة، وكذا بالنسبة للأشخاص المعنوية تنشأ مسؤوليتها وتكون خاضعة لجزاءات نوضحها بحسب ما جاء في التشريع الجزائري و التشريعات المقارنة كما يأتي:

الفرع الأول: العقوبات بالنسبة للأشخاص الطبيعية

أوضحت النصوص القانونية سواء في التشريع الجزائري أوفي التشريعات المقارنة العقوبات الأصلية المقررة لمختلف الجرائم المعلوماتية، وإضافة إلى ذلك عقوبات تكميلية.

البند الأول: العقوبات الأصلية

العقوبات الأصلية هي كل عقوبة لا توقع إلا إذا نطق بها القاضي وحدد نوعيتها ومقدارها وهي السجن أو الحبس أو الغرامة المالية التي تكون كافية بذاتها لتحقيق معنى الجزاء وهي العقاب الأساسي للجريمة[509].

يحدد القانون لكل جريمة عقوبة، وتشدد العقوبة إذا اقترنت بظرف من ظروف التشديد المنصوص عليها، لذلك سوف أحاول توضيح العقوبات التي تخضع لها كل جريمة من الجرائم التي تم التطرق إليها في الباب الأول من هذه الدراسة، سواء كانت تخضع لعقوبة بسيطة أم مشددة، مع التطرق إلى تشريعات مقارنة لتوضيح أكثر.

أولا: عقوبة الجرائم ضد سرية وسلامة المعلومات والنظم المعلوماتية

و هي تشمل العقاب على الجرائم الآتية:

1: عقوبات جريمة الدخول أو البقاء غير المصرح بهما:

---

[509]- **راضية مشري** ، مرجع سابق، ص 144.

تختلف العقوبة في هذه الجريمة وبحسب ما ترتب أولم يترتب عن الدخول أو البقاء أضرار مست المعلومات وأنظمة المعالجة الآلية في التشريع الجزائري والتشريعات المقارنة محل الدراسة وفقا لما يلي:

أ –**العقوبة في التشريع الجزائري:** نصت عليها المادة 394 مكرر من قانون العقوبات و التي حدد عقوبة هذه الجريمة في صورتها البسيطة والمشددة، و عليه تكون العقوبة الحبس من ثلاثة(03) أشهر إلى سنة و الغرامة من خمسون ألف(50000) إلى مائة ألف (100000) دينار جزائري كحد اقصى في حالة الدخول أو البقاء غير المصرح بها، و لم ينشأ عن ذلك أي ضرر أو إفساد أو تعطيل للنظام المعلوماتي المخترق أو للمعلومات المتضمنة فيه، و لا شك أن هدف المشرع من وراء تشديد و مضاعفة الحد الأقصى للغرامة هو مكافحة و محاولة الحد من انتشار جرائم الإختراق المعلوماتي خاصة و الجريمة المعلوماتية عامة، لاسيما إذا تم اختراق نظام يحتوي على معلومات سرية أو تتعلق بأمن الدولة و مؤسساتها [510] مما يشكل خطورة على الأشخاص و على الدولة الجزائرية التي تتوجه مؤخرا نحو إرساء حكومة إلكترونية [511] تقيدا بمبدأ العصرنة و التوجه نحو التكنولوجيا الرقمية و الانفتاح عليها.

أما إذا ترتب على فعل الدخول أو البقاء أضرار تمس المعلومات أو النظام فإن المادة 394مكرر من قانون العقوبات المعدل و في فقرتيها الثانية و الثالثة تنص على أنه"...تضاعف العقوبة إذا ترتب على حذف أو تغيير لمعطيات المنظومة؛ و إذا ترتب على الأفعال المذكورة أعلاه تخريب إشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين و الغرامة من 50.000 دج إلى 150.000 دج".

و ما هو ملاحظ في هذه الصورة لجريمة الدخول و البقاء المرتب لنتيجة، أن جعل المشرع الضرر الناتج عن ذلك الفعل ظرفا لتشديد العقوبة في حالتين اثنتين و هما:

---

[510]- و هذا ما أكد عليه المشرع الجزائري و أخذه بعين الاعتبار، عندما لم يقصر الحماية على المعلومات بمختلف أنواعها و بغض النظر عن الجهات التي تنتمي إليها، بتشديده للعقوبة إذا كانت المعلومات التي تم الاعتداء عليها تتعلق بالدفاع الوطني أو الهيئات و المؤسسات الخاضعة للقانون العام و ذلك بموجب المادة 394 مكرر3 من **قانون العقوبات** المعدل.

[511]– يظهر توجه الجزائر نحو تفعيل الحكومة الالكترونية من خلال إصدار تشريعات للتواصل في المسائل الإدارية و غيرها مع المواطنين من خلال القانون رقم 15–03 مؤرخ في أوّل فبراير سنة 2015 **يتعلق بعصرنة العدالة** ، و القانون رقم 15–04 مؤرخ في أوّل فبراير سنة 2015 يحدد **القواعد العامة المتعلقة بالتوقيع والتصديق الإلكتروني**، ج.ر عدد 06 بتاريخ السادس من فبراير 2015، ص 4–6.

* **إذا ترتب عن الدخول أو البقاء حذف أو تغيير لمعلومات المنظومة** : فإن العقوبة تضاعف عن تلك المقررة لعقوبة الدخول أو البقاء المجرد ليصبح الحبس في حده الأدنى (06) ستة أشهر و في حده الأقصى (02) سنتين، و الغرامة لتتراوح بين (100000) مائة ألف دينار جزائري إلى (200000) مائتي ألف دينار جزائري.

* **إذا ترتب عن فعل الدخول أو البقاء تخريب نظام اشتغال المنظومة:** و في هذه الحالة تكون عقوبة الحبس من (06) ستة أشهر إلى (02) سنتين، أما الغرامة فتكون بين (50000) دينار جزائري إلى احدها الأقصى (150000) ثلاثمائة ألف دينار جزائري.

و الملاحظ أن المشرع لم يعطي للقاضي الفاصل في المنازعة الحكم بإحدى العقوبتين الحبس أو الغرامة باستعمال حرف "واو" الربط بدلا من " أو" الاختيارية دون ترك المجال للسلطة التقديرية للقاضي في إمكانية الجمع من عدمه، و يكون المشرع الجزائري في ذلك قد جانب الصواب، لأنه يمكن للقاضي الحكم بإحدى العقوبتين مما قد يجعل العقاب أقل ردعا، و بإمكان القاضي أن يحكم بجعل الحبس أو الغرامة أو كلاهما معا موقوفة النفاذ طبقا لنص المادة 592 قانون إجراءات جزائية[512]، فضلا عن إمكانية تطبيق عقوبة العمل للنفع العام بدلا من الحبس طبقا للمادة 05 مكرر 1 من قانون العقوبات، و يكون للقاضي سلطة تقديرية في الحكم بالعقوبات بين الحد الأدنى والحد الأقصى بحسب ما تتطلبه كل حالة الاختراق.

ب –**العقوبة في التشريع الفرنسي:** حدد المشرع الفرنسي عقوبات مختلفة و عدلها في كل مرة بتشديدها بداية من أول قانون لسنة 1988 المتعلق بالغش المعلوماتي و إدخاله في قانون العقوبات سنة 1992 وبدأ العمل به بداية من 1994[513]، وكذا التعديل الذي جاء في 2004 و2012، و العقاب عليها في صورتها البسيطة والمشددة.

فكانت عقوبة الدخول أو البقاء غير المشروع في صورتها البسيطة في أول قانون للغش المعلوماتي رقم 88–19 تقدر بـ (02) شهرين حبس إلى (01) سنة أو بغرامة من (2000)

---

[512]– المادة 592 من الأمر رقم ***المتضمن قانون الإجراءات الجزائية الجزائري*** تقضي:" يجوز للمجالس القضائية وللمحاكم، في حالة الحكم بالحبس أو غرامة إذا لم يكن المحكوم عليه قد سبق الحكم عليه بالحبس لجناية أو جنحة من جرائم القانون العام، أن تأمر بحكم مسبب بالإيقاف الكلي أو الجزئي لتنفيذ العقوبة الأصلية" معدلة بموجب القانون رقم 04–14 المؤرخ في 10 نوفمبر 2004، ج.ر عدد 71، ص 06 .

[513] - **Loi n° 92-683 du 22 juillet 1992**, portant réforme du code pénal, texte origine au 01 mars 1994.

ألفين فرك فرنسي إلى (50000) خمسين ألف فرك فرنسي [514]، فكان الحد الأدنى و الأقصى منخفضا مع ترك السلطة التقديرية للقاضي في تقدير عقوبة ما بين الحدين مع حريته في الحكم بإحدى العقوبتين فقط.

ليأتي المشرع الفرنسي بقانون العقوبات الجديد سنة 1994 و يجعل عقوبة هذه الجرائم في حد واحد سواء كانت الحبس لمدة (01) سنة و بغرامة (15000) خمسة عشر ألف يورو ليسلب القاضي سلطته التقديرية في التحرك بالعقوبة[515].

و مرات أخرى و لأن جرائم المعالجة الآلية للمعطيات في انتشار و تطور مستمر تبعا لتطور التقنية الرقمية، و كذا لنمو و ازدياد الخسائر الناجمة عنها خاصة أن التقارير الأخيرة توضح تأثر فرنسا من ضمن الدول الأوروبية بهته الجرائم، و كذا قيامها بكل الإجراءات و التدابير لدراسة واقع الجريمة الإلكترونية و لمكافحة جرائم الانترنت لحماية شعبها من هذا الخطر المتلون و غير المحدود، إضافة إلى تشجيعها القيام بحملات تحسيسية و توعية من قبل مهنيين و متخصصين في هذا المجال، وضع برامج و خطط إستراتيجية و من ذلك تقديم تقرير حول" حماية مستخدمي الانترنت "[516] الذي قام به فريق عمل وزاري تحت إشراف مارك روبرت النائب العام لمحكمة استئناف ريوم.

و الملاحظ أن المشرع الفرنسي لم يدخر أي جهد في مكافحته لجرائم أنظمة المعالجة الآلية في كل فرصة تسمح بالتعديل، فقد بدأ مبكرا في مواجهته لهذه الجرائم، و لم يتأخر [517]عن أي إجراء تعديلي كلما تطلب الأمر ذلك.

---

[514] -**Art** 462-2 du A.C.P.F dispose que ; « quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement automatisé de données sera puni d'un emprisonnement de deux mois à un an et d'une amende de 2000 f à 50000 f ou de l'une de ces deux peines… »**Loi n°88-19** du 05 janvier 1988 relative à **la fraude informatique**, JORF du 06 janvier 1988, P 231.Sur le site ; www.legifrance.gouv.fr

[515] **-Art** 323-1 ; « le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 100 000 f d'amende… » **Loi n° 92-683** du 22 juillet 1992, portant réforme **du code pénal**, texte origine au 01 mars 1994.

[516] **-Remise du Rapport** « Protéger les Internautes » remettre par **Marc Robert**, Procureur général prées la cour d'appel de Riom, le rapport du group de travail interministériel sur la lutte contre la cybercriminalité, communiqué de presse, N° 185, Paris, le 30 juin 2014,sur le site ; www.presse.justice.gouv.fr

[517]- **رشيدة بوكر**، مرجع سابق، ص 319.

و قام المشرع الفرنسي مرة أخرى بتشديد العقوبة، و ذلك بموجب المادة (45) من الفصل الثاني من القانون رقم 2004-575 المتعلق بالثقة في الاقتصاد الرقمي لتصبح العقوبة ضعف عما كانت عليه: الحبس(02) سنتين و الغرامة(30000) ثلاثون ألف يورو.

أما عقوبة الدخول أو البقاء غير المصرح به و في صورته المشددة، حيث جعل المشرع ما يترتب عن الدخول أو البقاء بدون قصد من أضرار كظرف مشدد، فكانت في قانون الغش المعلوماتي لسنة 1988 محدد ب الحبس لمدة من (02) شهرين إلى (02) سنتين و بغرامة من (10000) عشرة ألاف فرك فرنسي إلى (100000) مائة ألف فرك فرنسي و ذلك في حالة ترتب عن الدخول أو البقاء حذف أو تعديل للبياناتاو تعطيل النظام[518].

و كذا في قانون العقوبات الجديد لسنة 1994 ليحتفظ بالحد الأقصى لعقوبة الحبس و رفع الغرامة إلى (30000) ثلاثون ألف يورو، أما قانون العقوبات لسنة 2004 كذلك زاد من عقوبة الحبس إلى (03) ثلاثة سنوات و الغرامة لتصبح (45000) خمسة و أربعون ألف يورو[519].

ليأتي المشرع الفرنسي في سنة 2012 بفقرة جديدة من نفس المادة، و يتفرد بها على غرار المشرع الجزائري و غيره من المشرعين، و يعاقب بعقوبة أشد إذا كان الدخول أو البقاء سواء في صورته البسيطة أو المشددة يرتكب على نظام معالجة آلية للبيانات الشخصية التي تنفذها الدولة[520].

ج- العقوبة في التشريع الأردني: نص المشرع الأردني على جريمة الدخول غير المصرح وحدد عقوبته في صورته البسيطة دون المشددة من خلال المادة 03 من القانون رقم 30 المتعلق بجرائم أنظمة المعلومات لسنة 2010، ولم يحدد أو ينص على عقوبة البقاء غير المصرح مما يستدعي التدخل من جديد ووضع عقاب رادع لهذا الفعل دون ترك الجناة بغير جزاء، و حتى لا يتحجج الجاني بدخوله خطأ و يبقى في النظام المعلوماتي.

---

[518] **-Art** 462-2/2 ; « Lorsqu'il en sera résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, l'emprisonnement sera de deux mois à deux ans et l'amende de 10000 F à 100000 F » **la loi n° 88-19** précédente.

[519] - **Art** 323-1 alinéa 2, « 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 45 000 euros d'amende » **Du code pénal français** modifié par la **loi n° 2004-575** du juin 2004 pour **la confiance dans l'économie numérique**, art 45, JORF n°0143 du 22 juin 2004, P11168, texte n°02.

[520]- **Art** 323-1 alinéa 3 **de code pénal** ; « Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 75 000 € d'amende » Modifié par **LOI n°2012410** du 27 mars 2012 art 9,

فكانت عقوبة الدخول غير المصرح به و المجرد هي الحبس مدة لا تقل عن أسبوع و لا تزيد على (03) ثلاثة أشهر أو بغرامة لا تقل عن(100) مائة دينار و لا تزيد على (200) مائتي دينا أو بكلتا هاتين العقوبتين.

و قد أعطى بذلك سلطة تقديرية للقاضي في الحكم بالعقوبتين معا أو بإحداهما و كذا بين الحدين الأقصى و الأدنى على حسب ظروف كل قضية مع ملاحظة أنا العقوبة غير رادعة أو غير كافية لردع هذا النوع من الإجرام مقارنتا بحجم العقوبات المقررة في التشريع الجزائري و الفرنسي.

أما عقوبة الدخول في صورتها المشددة لم ينص عليها المشرع الأردني بالصيغة التي نص عليها كل من المشرع الجزائري و الفرنسي، و إنما جاء في الفقرة الثانية من المادة الثالثة أنه إذا كان الدخول بهدف إلغاء أو حذف...." بما يعني إذا كان القصد من الدخول وقوع أفعال أخرى مثل إتلاف أو انتحال صفة إلى غير ذلك، فالقصد هنا متوفر منذ البداية و ليس كما رأينا في الدخول غير المصرح به و المرتب لنتيجة جرمية، فإن قصد ترتيب تلك النتيجة لم يكن منذ البداية و إنما جاء نتيجة أو بعد الدخول دون أن يقصد حدوثه، و مع ذلك إذا ترتب عنه أضرار تشدد العقوبة و هته الحالة غير متوفرة في القانون الأردني مما يستوجب إعادة النظر في هذا الأمر.

إضافة إلى ذلك فإن المشرع الأردني يعاقب على الدخول غير المصرح به إلى موقع إلكتروني او نظام معلومات بأي وسيلة كانت بهدف الإطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني، فإن العقوبة تضاعف بالحبس مدة لا تقل عن أربعة أشهر و بغرامة لا تقل عن (500) خمسمائة دينار و لا تزيد على (50000) خمسة ألاف دينار[521].

2:عقوبة جريمة الإتلاف المعلوماتي

أ –**في التشريع الجزائري:** اخضع المشرع الجزائري لمن تعمد مند البداية الإضرار بمعلومات المتضمنة في نظم المعالجة الآلية لعقوبة أشد عن من دخل أو بقي بدون تصريح و ترتب عن ذلك ضرر وفقا للمادة 394 مكرر 1، و لا شك أن المشرع قد شدد العقوبة في هـ ذه الصورة عن العقوبة في الصورة الأولى لجريمة الاختراق المعلوماتي و ذلك راجع إلى توفر عنصر القصد منذ بداية ارتكاب فعل الإتلاف، فحددت العقوبة بـ (06) ستة أشهر حبس

---

[521]- **المادة 11/** أ من **القانون الأردني رقم 30 لسنة 2010** السابق الإشارة إليه.

إلى (03) ثلاثة سنوات و غرامة من (500000) خمسمائة ألف إلى (2.000.000) اثنان مليون دينار جزائري لكل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش، ولم ينص على إتلاف أو تخريب نظام اشتغال منظومة المعالجة الآلية للمعطيات مكتفيا بنص المادة 394 مكرر عقوبات، إن كان إدخال معلومات فيها مثل بعض الفيروسات قد يترتب عنه تعطيل اشتغالها.

ب -**في التشريع الفرنسي:** كذلك المشرع الفرنسي نص على عقوبات إتلاف المعطيات والمعلومات المتضمنة في أنظمة المعالجة الآلية، وعلى إتلاف أو تعطيل تلك الأنظمة بموجب المادتين462-3 و 462-4 من القانون 88-19 فكانت عقوبة إتلاف أو تعطيل نظام للمعالجة الآلية للمعلومات هي الحبس من (03) ثلاثة أشهر إلى (03) ثلاثة سنوات و غرامة (10000) عشرة ألاف فرك إلى (100000) مائة ألف فرك فرنسي أو بإحدى العقوبتين[522].

و عقوبة إتلاف معلومات متضمنة في نظام معلوماتي هي بالنسبة للحبس نفس عقوبة تعطيل النظام الحبس من (03) ثلاثة أشهر إلى (03) ثلاثة سنوات و الغرامة اقل منها مقارنتا بسابقتها بالنسبة لحدها الأدنى و الضعف خمس مرات بالنسبة لحدها الأقصى و هي (2000) ألفين فرك إلى (500000) خمسمائة ألف فرك فرنسي أو بإحدى هاتين العقوبتين[523] .

و بعد تعديله لقانون العقوبات الجديد الذي أصبح ساريا بدايتا من مارس 1994، جعل العقوبات في حدها الأقصى فقط و هي واحدة سواء بالنسبة لإتلاف المعلومات أو إتلاف النظام و تعطيله ، بأن أصبحت عقوبة الحبس (03) ثلاثة سنوات و بغرامة (45000) خمس و أربعون ألف يورو دون أن تكون للقاضي سلطة تقديرية بين العقوبتين و ذلك بموجب المادتين 232 -2 و323-3 عقوبات فرنسي المعدل والمتمم.

---

[522] -**Art 462-3** ; « quiconque aura intentionnellement et au mépris des droits d'autrui, entravé ou faussé le fonctionnement d'un système de traitement automatisé de données sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 10 000 F à 100 000 F ou de l'une de ces deux peines **». Loi n°88-19** précédente.

[523] **- Art 462-4** ; « quiconque aura intentionnellement et au mépris 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 500000 F ou de l'une de ces deux peines » **Loi n°88 -19**

ليعود المشرع الفرنسي من جديد و يستجيب للمستجدات بتعديله لهته المواد بموجب القانون رقم 2004-575 و يرفع العقوبات السابقة بالنسبة لجريمة الإتلاف سواء بالنسبة للمعطيات أو البيانات او بالنسبة لتشغيل النظام بأن يعاقب على ذلك بالحبس لمدة (05) خمس سنوات و غرامة (75000) خمس و سبعون ألف يورو.

و لقد فسر تقارب العقوبتين بالنسبة لصور الإتلاف المعلوماتي من قبل الجمعية الوطنية الفرنسية بالتقارب الكبير بين الجريمتين، و يتعذر التمييز بينهما في بعض الأحيان، كما فسر أن فعل إعاقة النظام يكون نتيجة إدخال معلومات و هي صورة من صور إتلاف أو التلاعب بالمعلومات[524].

و في 2012[525] و مؤخرا في 2014 ليعدل المادة 233-3[526] و يضيف المشرع الفرنسي في المادتين323-2 و 323-3 زيادة عقوبة الحبس (07) سبع سنوات و غرامة (100000) مائة ألف يورو إذا وقع الإتلاف المعلوماتي أو جريمة التلاعب المعلوماتي على نظام المعالجة الآلية للبيانات الشخصية التي تنفذها الدولة.

جـ- في التشريع الأردني:

بالنسبة للمشرع الأردني نفرق بين جريمتين يترتب عنها إتلاف أو تعطيل نظام معلوماتي أو موقع الكتروني، و ذلك من خلال نص المادة 03 فقرة ب التي تعاقب بالحبس لمدة لا تقل عن (03) ثلاثة أشهر و لا تزيد عن (01) سنة أو بغرامة لا تقل عن (200) مائتي دينار ولا تزيد عن (1000) ألف دينار أو بكلتا هاتين العقوبتين، و ذلك في حالة ما كان الدخول قصدا إلى موقع إلكتروني أو نظام معلوماتي بهدف تحقيق غاية و هي إلغاء أو حذف أو إضافة أو تدمير

---

[524]- محمد خليفة، مرجع سابق، 192.

[525] **-Art 323-2 alinéa 2** du **C.P.F**; « Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 100 000 € d'amende »

Art 323-3 alinéa 2 ; « Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 100 000 € d'amende **» Loi n° 2012-410** du 27 mars 2012 précédente.

[526] **-Art 323-3** ; « Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende.

Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 100 000 € d'amende » modifie par **LOI n°2014-1353** du 13 novembre 2014 **renforçant les dispositions relatives à la lute contre le terrorisme**, art. 16, JOPF n° 0263 du 14 novembre 2014, P 19162, texte n°5.

أو إتلاف أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات، أو توقيف أو تعطيل عمل نظام أو تغيير موقع إلكتروني أو إلغائه أو إتلافه تعديل محتوياته أو إشغاله.

و جاء في المادة الرابعة من القانون رقم 30 لسنة 2010 ليعاقب على جريمة الإتلاف المعلوماتي و التي يتم فيها إدخال أو نشر أو استخدام برنامج عن طريق الشبكة المعلوماتية أو بإستخدام نظام معلوماتي و ذلك بهدف إلغاء أو حذف أو إضافة أو تدمير أو إتلاف أو... إعاقة أو تشويش أو إيقاف أو تعطيل عمل نظام معلومات ...أو تغيير موقع إلكتروني أو إلغائه أو إتلافه أو تعديل محتوياته دون تصريح أو بما يجاوز أو يخالف التصريح بعقوبة نفس الجريمة السابقة و هي الحبس لمدة لا تقل عن (03) ثلاثة أشهر و لا تزيد عن (01) سنة أو غرامة لا تقل عن (200) مائتي دينار و لا تزيد على (1000) ألف دينار أردني أو بكلتا هاتين العقوبتين.

و عليه فإن المشرع الأردني و علا خلاف المشرع الجزائري و الفرنسي قد وسع من صور جريمة الإتلاف المعلوماتي سواء كان الإتلاف ناتج عن جريمة الدخول غير المصرح و الذي يكون بهدف تحقيق غاية أو ناتج عن إدخال برنامج مثل الفيروسات بهدف تحقيق إتلاف المعلومات أو النظام و حتى المواقع الإلكترونية، مع إعطاء لكلا الصورتين و بمختلف أشكالها نفس العقوبة و للقاضي سلطة تقديرية في تحديد العقاب بحسب كل ظروف جريمة من خلال الحد الأدنى و الأقصى لكل عقوبة مع إمكانية عدم الجمع بين العقوبتين.

و بطبيعة الحال إذا كان الإتلاف متعلق بالدخول قصدا و دون تصريح إلى موقع إلكتروني أو نظام معلومات بأي وسيلة كانت بهدف إلغاء بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني أو إتلافها أو تدميرها فإن الفاعل يعاقب بالأشغال الشاقة المؤقتة و بغرامة لا تقل عن (1000) ألف دينار و لا تزيد على (5000) خمسة ألاف دينار[527].

3: عقوبة جريمة التعامل في معلومات غير مشروعة

هذه الجريمة نص عليها كل من التشريع الجزائري والفرنسي أما المشرع الأردني فلم ينص عليها صراحة في القانون المتعلق بجرائم أنظمة المعلومات.

---

[527]- بموجب المادة 11/ب **من القانون الأردني المؤقت رقم 30 لسنة 2010** السابق الإشارة إليه.

أ -**التشريع الجزائري:** عاقب على هذه الجريمة بالحبس من(02) شهرين إلى (03) ثلاثة سنوات و بغرامة من (1.000.000) مليون دينار إلى (5.000.000)خمسة ملايين دينار جزائري و ذلك بموجب المادة 394 مكرر 2 الفقرة 1 عقوبات المعدل و المتمم و يلاحظ أن عقوبة هذه الجريمة مقارنتا مع الجريمتين السابقتين، أن المشرع خفض من الحد الأدنى لعقوبة الحبس بداية من شهرين و رفع من عقوبة الغرامة كحد أقصى هو خمسة ملايين دينار جزائري، و قد يرجع السبب في ذلك إلى أن الأضرار المترتبة عن جريمة التعامل بمعلومات غير مشروعة قد تفوق بكثير الأضرار المترتبة عن الجريمة الأولى و الثانية.

ب -**التشريع الفرنسي:** يعاقب عليها المشرع الفرنسي بموجب المادة 323-3-1 عقوبات المضافة بموجب القانون 2004-575 المتعلق بالثقة في الاقتصاد الرقمي، و المعدلة بموجب القانون رقم 2013-1168 و أن العقاب على هذه الجريمة يكون بنفس العقوبة المقررة للجريمة نفسها أي العقوبة المقررة لجريمة الدخول أو البقاء غير المصرح بهما أو جريمة إتلاف المعلومات، أو نظم المعالجة الآلية التي يمكن أن تؤدي البرامج و الأجهزة والوسائل المتعامل فيها إلى ارتكابها أو بعقوبة أشد[528].

اعتبر المشرع الفرنسي و هو ما لم يقم به المشرع الجزائري، أن هذه الجريمة من الأعمال التحضيرية لجريمة أخرى قد تكون للتحضير للقيام بدخول غير مصرح أو إتلاف معلوماتي لذلك عاقب بنفس عقوبة الجريمة المحضر لها، أو بعقوبة أشد و حسن فعل المشرع الفرنسي.

4: عقوبة جريمة الاعتراض المعلوماتي:

أ -**في التشريع الجزائري:**

[528] -**Art 323-3-1 de C.P.F** « Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée » Modifié **par Loi n° 2013-1168** du 18 décembre 2013 relative **à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale**, JORF n°0294 du 19 décembre 2013 page 20570 texte n° 1

إن المشرع الجزائري لم يشر إليها صراحة بموجب مواد القسم السابع المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات المضاف إلى قانون العقوبات سنة 2004 ، و لكن استدرك الأمر كونه قد حمى الاعتداء على الاتصالات و المراسلات بأية تقنية كانت و وسع من مجال حماية الاتصالات و المراسلات من خلال المادة 303 مكرر المضافة لقانون العقوبات سنة 2006 [529] و شملها ضمن حماية الحياة الخاصة.

و منه يعاقب بالحبس من (06) ستة أشهر إلى (03) ثلاثة سنوات و بغرامة من (50.000) خمسون ألف دينار إلى (300.000) ثلاثمائة ألف دينار جزائري كل من تعمد المساس بحرمة الحياة الخاصة و بأية تقنية كانت و ذلك بإلتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاه، و هذا يخص إعتراض المراسلات و الاتصالات السرية أو بما يسمى خصوصية الإتصالات.

غير أنه في جريمة الإعتراض لا يشترط أن تكون المعلومات سرية و إنما وسيلة إرسالها سرية ذلك أن الأساس في جريمة الاعتراض غير المشروع هو حماية حرية الاتصالات و عدم إعاقة سيرها أو اعتراضها حتى و لو لم تكن المعلومات سرية و لكن أطراف الاتصال أرادوا أن تكون بوسيلة سرية أو غير علنية.

كما أن التشريعات التي نصت صراحة على جريمة الاعتراض غير المشروع في نصوص عقابية خاصة[530] كانت تهدف إلى تشجيع استخدام أنظمة المعلومات و الشبكات المعلوماتية وانتشارها من خلال حماية مستخدميها الذين يحرصون على ضمان السرية و الخصوصية ولحماية لمعلوماتهم المالية و الشخصية و غيرها.

و نجد أن المشرع كذلك قد جرم هذا الفعل من خلال تشريعات خاصة، مثل ما نجده في قانون البريد و المواصلات السلكية و اللاسلكية رقم 2000_03 حيث جاء في المادة 127 ما يلي:" تطبق العقوبات المنصوص عليها في المادة 137 من قانون العقوبات على كل شخص مرخص له بتقديم خدمة البريد السريع الدولي أو كل عون يعمل لديه و الذي في إطار ممارسة مهامه، يفتح أو يحول أو يخرب البريد أو ينتهك سرية المراسلات أو يساعد في ارتكاب هذه الأفعال ، تسري نفس العقوبات على كل شخص

---

[529]- **القانون رقم 06-23** المؤرخ في 20 ديسمبر 2006 **المعدل لقانون العقوبات**، ج.ر عدد 84 بتاريخ 24 ديسمبر 2006، ص 11.

[530]– نجد من تلك التشريعات القانون الأردني و العماني.

مرخص له بتقديم خدمة مواصلات سلكية و لاسلكية و كل عامل لدى متعاملي الشبكات العمومية للمواصلات السلكية و اللاسلكية و الذي في إطار ممارسة مهامه و زيادة على الحالات المقررة قانونا، ينتهك و بأية طريقة كانت سرية المراسلات الصادرة أو المرسلة أو المستقبلة عن طريق المواصلات السلكية و اللاسلكية أو الذي أمر أو ساعد في ارتكاب هذه الأفعال.

يعاقب بالحبس من شهرين إلى سنة و بغرامة مالية من 50.000 دج إلى 1.000.000 دج أو بإحدى هاتين العقوبتين، كل شخص غير الأشخاص المذكورين في الفقرتين السابقتين، ارتكب أحد الأفعال المعاقب عليها بموجب هاتين الفقرتين ...." [531].

في التشريع الفرنسي : لم يشر إليها صراحة المشرع الفرنسي عند إضافته قسم خاص بجرائم أنظمة المعالجة الآلية للمعطيات ولكن نص على حكم خاص بجريمة الاعتراض المعلوماتي أو جريمة التنصت على المراسلات ضمن الجرائم الحياة الخاصة، بعقاب كل من يقوم وبسوء نية بإعتراض أو تحويل أو إستخدام أو الكشف عن المراسلات الواردة أو المرسلة عن طريق إلكتروني أو بتركيب المعدات المصممة للقيام بمثل هذه الإعتراضات، و ذلك بموجب الأحكام الخاصة بالمادة 226–15 عقوبات المعدل و التي تحدد العقوبة بالسجن لمدة سنة واحدة و غرامة (45.000) خمسة و أربعون ألف يورو [532].

ج. في التشريع الأردني

نص عليها صراحة المشرع الأردني وحدد عقوبتها من خلال المادة 05 من قانون جرائم أنظمة المعلومات رقم 30 لسنة 2010، و ذلك بمعاقبة كل من قام قصدا بإلتقاط أو اعتراض أو بالتنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أي نظام معلومات بالحبس مدة لا تقل عن شهر و لا تزيد على سنة أو بغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) ألف دينار أو بكلتا هاتين العقوبتين.

531- جرم كذلك المشرع الأردني فعل الاعتراض في القانون المؤقت رقم 30 لسنة 2010 و من قبله في قانون الاتصالات رقم 13 لسنة 1995 المعدل و المتمم لغاية 2011 حيث جاء في المادة 76 منه ما يلي: " كل من إعترض أو أعاق أو حور أو شطب محتويات رسالة بواسطة شبكة الاتصالات أو شجع غيره على القيام بهذا العمل يعاقب بالحبس مدة لا تقل عن الشهر و لا تزيد على ستة أشهر أو بغرامة لا تزيد عن (200) دينار أو بكلتا العقوبتين" .

532 - **Art 226-15** de **code pénal français** ; « Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45 000 euros d'amende. Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie électronique ou de procéder à l'installation d'appareils de nature à permettre la réalisation de telles interceptions » Modifié par **Loi n°2013-1168** du 18 décembre 2013 art. 23

وكذلك بموجب المادة 76 و80 من قانون الاتصالات المعدل والمتمم سنة 2011 [533].

ثانيا: عقوبات الجرائم المتصلة بالحاسب الآلي

هذه الجرائم من الجرائم التقليدية العادية ولكن ترتكب بواسطة الحاسب وأنظمة المعالجة الآلية، لذلك قد عمدت بعض التشريعات إلى جعل نصوص وقواعد القانون الجنائي مرنة لدرجة استيعاب أي تطور تكنولوجي وتطبيق نفس العقاب على هذه الجرائم في شكلها وبيئتها الجديدة وهي كالآتي:

1: عقوبة جرائم التزوير المعلوماتي

أ -**في التشريع الجزائري:** لا يزال العقاب على تزوير المحررات في التشريع الجزائري ينطبق على جرائم التزوير التقليدية، و لم تستوعب نصوصه جريمة التزوير المعلوماتية أو المستندات المعالجة آليا، كون محل هذه الجريمة في القانون الجزائري يشترط المحررات الورقية دون المحررات الالكترونية أو المستند المعلوماتي مما يستدعي النظر من جديد في أحكام التزوير و جعل نصوصه مرنة تستجيب لأي تطور بشأن محل الجريمة.

غير أن تغيير الحقيقة في البيانات أو المعطيات المسجلة في ذاكرة الحاسب الآلي أو المحفوظة بالنظام المعلوماتي فهي تخضع لحكم نص المادة 394 مكرر 1 من قانون العقوبات تحت جريمة التلاعب بالمعطيات بطريق الغش في نظام معلوماتي أو بتعديلها و يعاقب الجاني بنفس عقوبة جريمة الإتلاف كون التعديل شكل أو صورة من صور الإتلاف و هي ستة أشهر إلى ثلاثة سنوات و بغرامة من 500.000 دج إلى 2.000.000 دج.

ب -**في التشريع الفرنسي:** دخلت المستندات الإلكترونية أو المعالجة آليا نطاق الحماية الجنائية في التشريع الفرنسي منذ صدور قانون الغش المعلوماتي رقم 88-19 السالف الذكر الذي جرم و عاقب على أفعال تزوير المستندات المعالجة آليا واستخدام تلك المستندات بموجب المادتين 462-5 و 462-6 منه.

فكان العقاب على جريمة تزوير المستندات المعالجة آليا و أيا كان شكلها و بما يؤدي إلى حدوث ضرر للغير بالحبس لمدة تتراوح بين(01) سنة واحدة و (05) خمس سنوات و

533- قانون **الاتصالات الأردني** رقم 13 لسنة 1995 الجريدة الرسمية رقم 4072 ، بتاريخ 1/ 10 / 1995 ، الصفحة2939 ، المعدل بموجب **القانون رقم** 21 لسنة 2011 والصادر بالجريدة الرسمية بتاريخ 2011/04/21 على الصفحة 5156.

غرامة التي تتراوح بين (20.000) عشرون ألف فرك إلى (2.000.000) مليونين فرك فرنسي.

أما العقاب على جريمة إستخدام مستند معلوماتي مزور فكانت نفس عقوبة جريمة التزوير، غير أن المشرع كان قد أعطى القاضي سلطة تقديرية في أن يحكم بإحدى العقوبتين فقط [534]، وهذه كانت كخطوة أولى من قبل المشرع الفرنسي يتم فيها معالجة جريمة التزوير المعلوماتي.

و بصدور قانون العقوبات الفرنسي الجديد لسنة 1994 أورد المشرع الفرنسي نصا جديدا هو المادة 441–1 التي عاقبت على تغيير الحقيقة في محرر أو أي دعامة أخرى بأي طريقة كانت و على إستعمال المزور بالحبس (03) ثلاثة سنوات و غرامة (45000) خمس و أربعون ألف يورو.

و ما بين النص القديم و الجديد نلاحظ أن المشرع سحب السلطة التقديرية للقاضي بين الحد الأدنى و الأقصى لجريمة التزوير، في الحكم بإحداهما في جريمة إستعمال المستند المزور في قانون الغش المعلوماتي و جعل للقاضي طبقا لقانون العقوبات الجديد عقوبة واحدة ليس له فيها سلطة تقديرية سواء في جريمة التزوير أو في إستعمال المستند المزور.

و عليه فإن نصوص القانون الفرنسي اتسعت لتشمل التزوير في شتى أشكاله و صوره ومنها التزوير المعلوماتي، حيث عاقب عليه في المادة 1/441 عقوبات و نفس العقوبة على إستعمال المحرر المزور.

ت -**في التشريع الأردني:** و نفس الأمر بالنسبة للمشرع الأردني الذي يعاقب على التزوير في شكله التقليدي و الذي يقتصر على صك أو محرر مخطوط طبقا لما جاء في المادة 260 من قانون العقوبات [535] و يعاقب بنفس العقوبة لمن استعمل المزور بموجب المادة 261 من نفس القانون.

بينما يدخل تغيير أو تعديل معطيات داخل نظام معلوماتي عن طريق الشبكة المعلوماتية أو باستخدام نظام معلومات ضمن العقاب المقرر في المادة 04 من القانون رقم 30 لسنة 2010.

---

[534] - **Art.462-6 du la loi n°88-19** dispose ; « 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 20000 F à 2.000.000 F ou de l'une de ces deux peines ».

[535]- عرفت **المادة 260** التزوير على أنه" التزوير، هو تحريف مفتعل للحقيقة في الوقائع و البيانات التي يراد إثباتها بصك أو مخطوط يحتج بهما نجم أو يمكن أن ينجم عنه ضرر مادي أو معنوي أو إجتماعي" من ***قانون العقوبات الأردني رقم 16/ 1960***، ج.ر بتاريخ 1960/01/01 و المعدل بأخر قانون رقم 2011/8 في الجريدة الرسمية رقم 5090 بتاريخ 2011/05/02.

غير أن المشرع الأردني و تلافيا لتكرار النصوص و الأحكام قام بإدراج المادة 14 من القانون رقم 30 لسنة 2010 السالف الذكر، و التي نص بمقتضاها على معاقبة كل أرتكب أي جريمة معاقب عليها بموجب أي تشريع نافذ باستخدام الشبكة المعلوماتية أو أي نظام معلومات أو اشترك أو تدخل أو حرض على ارتكابها، يعاقب بالعقوبة المنصوص عليها في ذلك التشريع.

و بالتالي عقوبة تزوير مستندات و إستعماله في قانون العقوبات الأردني هي الأشغال الشاقة المؤقتة لمدة (05) خمس سنوات على الأقل طبقا لحلات التزوير الواردة في المواد 262-265 من نفس القانون.

2: عقوبات الاحتيال المعلوماتي

أ -**في التشريع الجزائري:** الأمر نفسه كما في جريمة التزوير المعلوماتي لا تزال النصوص العقابية عادية ولا تستوعب هذه الصورة الجديدة .

ب **في التشريع الفرنسي:** المشرع الفرنسي لم يورد نص خاص بالاحتيال المعلوماتي، غير أن القضاء طبق النص التقليدي على التلاعب ببيانات داخل نظام المعالجة الآلية من أجل إجراء تحويل إلكتروني غير مشروع للأموال.

و تعاقب المادة 313-1 من قانون العقوبات جريمة الاحتيال ب (05) خمس سنوات حبس و غرامة تقدر (375.000) ثلاثمائة و خمس و سبعون ألف يورو[536].

ت -**في التشريع الأردني** : عاقب المشرع الأردني على جريمة الاحتيال في صورتها التقليدية في المادة 417 من قانون العقوبات بالحبس من(03) ثلاثة أشهر إلى (03) ثلاثة سنوات و بغرامة من(100) مئة إلى (200)مائتي دينار أردني.

و عاقب على جريمة الاحتيال المعلوماتي كل من استخدم عن طريق الشبكة المعلوماتية أو أي نظام معلومات على بيانات أو معلومات تتعلق ببطاقات الائتمان أو البيانات و المعلومات التي تستخدم في تنفيذ المعاملات المالية أو المصرفية الإلكترونية للحصول لنفسه أو لغيره على بيانات أو معلومات أو أموال أو خدمات تخص الآخرين بالحبس لمدة لا تقل عن سنة و بغرامة لا تقل عن (1000) ألف

---

[536] - **Art 313-1 du C.P.F** ; « L'escroquerie et le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge.

L'escroquerie est punie du cinq ans d'emprisonnement et de 375 000 euro d'amende ».

دينار و لا تزيد على (5000) خمسة ألاف دينار أردني و ذلك بموجب الفقرة (ب) من المادة 06 من القانون رقم 30 لسنة 2010 السالف الذكر، وهي تطبيق من التطبيقات الخاصة لجريمة الاحتيال المعلوماتي.

بل إن المشرع الأردني عاقب كذلك على مجرد الحصول دون تصريح و بإستعمال الشبكة المعلوماتية أو أي نظام معلوماتي على بيانات أو معلومات تتعلق ببطاقة الائتمان أو التي تستخدم في المعاملات المالية أو المصرفية الالكترونية بالحبس مدة لا تقل عن (03) ثلاثة أشهر و لا تزيد على (02) سنتين أو بغرامة لا تقل عن (500) خمسمائة دينار و لا تزيد على (2000) ألفي دينار أو بكلتا هاتين العقوبتين و ذلك بموجب الفقرة (أ) من المادة السادسة من القانون رقم 30 لسنة 2010.

و الملاحظ فيما يخص التشريع الأردني أن المشرع قد جرم الأفعال التي تتضمنها الفقرة (أ) من المادة 6 و ركز على فكرة أن المعلومات التي تتضمنها بطاقة الائتمان لا تقل عن البطاقة ذاتها، و قد جعل مجرد الحصول على تلك المعلومات و بدون وجه حق باستخدام أنظمة معلوماتية يشكل جريمة في حد ذاتها تستوجب العقاب و لا يشترط استخدام الجاني لتلك المعلومات حتى يطبق العقاب بحقه، و هذا طبعا من اجل الحفاظ على استقرار المعاملات المالية الإلكترونية التي انتشرت في الفترة الأخيرة خاصة في إطار التجارة الإلكترونية و العمل على تشجيعها.

فلا شك أن يكون العقاب اشد إذا تم استغلال تلك المعلومات من اجل النصب و الإحتيال من أجل الحصول على معلومات أو أموال أو خدمات من الغير و دون وجه حق و هذا ما عاقب عليه في الفقرة (ب) من المادة نفسها.

ثالثا: عقوبات الجرائم المتصلة بالاعتداءات الواقعة على الملكية الفكرية والحقوق المجاورة

لقد حصر المشرع الجزائري الأفعال التي تشكل تعديا على حقوق المؤلف و الحقوق المجاورة، مهما كان نوع المصنف في المواد 151 إلى 159 من الأمر 05/03، كما وضع عقوبة واحدة لهذه الجرائم، إذ نصت المادة 153 من الأمر 03/05 على العقوبات الأصلية لجنحة التقليد و هما الحبس من (06) ستة أشهر إلى (03) ثلاث سنوات وبغرامة من (500.000) خمسمائة ألف دينار إلى (1.000.000) مليون سواء كان النشر قد حصل في الجزائر أو في الخارج.

البند الثاني: العقوبات التكميلية

نص القانون على عقوبات تكميلية يحكم بها إلى جانب العقوبات الأصلية و المتمثلة في المصادرة و الغلق و هو ما سيتم شرحه كما يأتي:

أولا: المصادرة

يتم مصادرة الأشياء التي يتم حيازتها واستخدامها لأغراض إجرامية حيث تشمل الأجهزة و البرامج و الوسائل المستخدمة في إرتكاب جريمة من الجرائم الماسة بأنظمة المعالجة الآلية، و لقد نص المشرع الجزائري في المادة 394 مكرر 6 على أنه : "مع الاحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الأجهزة و البرامج والوسائل المستخدمة"

وكذلك المشرع الفرنسي نص على عقوبة مصادرة الأشياء التي استخدمت في ارتكاب جرائم المعالجة الآلية بموجب المادة 323-5 الفقرة الثالثة من قانون العقوبات الفرنسي[537].

ونفس الأمر بالنسبة للمشرع الأردني نص على هذه العقوبة في المادة 12/ج من قانون جرائم أنظمة المعلومات بحيث يكون للمحكمة المختصة الحكم بمصادرة الأجهزة والأدوات والوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها أو يشملها هذا القانون و مصادرة الأموال المتحصلة من تلك الجرائم.

ثانيا: الغلق

إلى جانب عقوبة المصادرة نص المشرع على عقوبات تكميلية أخرى وهي الغلق، ويقصد بها وفقا لما جاء في المادة 394 مكرر 6: "إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على ذلك إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها".

غير أن المشرع لم يحدد مدة الغلق و هل يكون الغلق نهائيا؟

و بالنسبة للمشرع الفرنسي نص عليها في المادة 323-5 الفقرة 4 على "الغلق لمدة (5) خمس سنوات أو أكثر للمؤسسات أو لواحد أو أكثر من فروع المشروع الذي أستخدم في ارتكاب الجريمة" و إضافة إلى عقوبة الغلق والمصادرة، نص المشرع الفرنسي على عقوبات أخرى تكميلية وجوبية وبحسب طبيعة كل جريمة وظروفها بموجب نفس المادة[538].

---

[537] **-Art 323-5 alinéa 3 du C.P.F** : « Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes :

3° La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ; »

[538] **-Art 323-5 du C.P.F** « Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes :

1° L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26 ;

كذلك المشرع الأردني حينما نص في المادة 12/ج من القانون رقم 30 على توقيف أو تعطيل عمل أي نظام معلومات أو موقع إلكتروني مستخدم في ارتكاب أي من الجرائم المنصوص عليها، والحكم بإزالة المخالفة على نفقة مرتكب الجريمة.

الفرع الثاني: العقوبات بالنسبة للأشخاص المعنوية

كرس القانون مبدأ المسئولية الجزائية للشخص المعنوي، وقرر له عقوبات، حيث أقر المشرع الجزائري بذلك بموجب المادة 51 مكرر من قانون العقوبات واستثنى الدولة والجماعات المحلية والأشخاص المعنوية الخاضعة للقانون العام كونها هي الحامية للمجتمع وتحافظ على أمن وسلامة الأشخاص.

و يكون الشخص المعنوي مسئولا عن الجرائم التي ترتكب لحسابه من طرف أجهزته أو ممثليه الشرعيين عندما ينص القانون على ، و نص المشرع في المادة 394 مكرر 4 على الحد الأقصى للعقوبة المقررة للشخص المعنوي وهي غرامة تعادل (05) خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.

أما إذا ارتكبت إحدى الجرائم السابقة من شخص معنوي على إحدى الجهات العامة أو إستهدفت الجريمة الدفاع الوطني أو الهيئات و المؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد حسب المادة 394 مكرر 3 عقوبات، وبالتالي تضاعف العقوبة مرتين إذا كانت من شخص معنوي ضد شخص معنوي أو أحد الجهات العامة، و بذلك يكون مجموع الغرامة 10 مرات أضعاف الغرامة المقررة للشخص الطبيعي.

أما بخصوص المشرع الفرنسي، نجده قد ضاعف الغرامة إلى 05 أضعاف ما يفرض على الشخص الطبيعي بموجب الفقرة الأولى من المادة 323-6 والتي أحالت في تحديد العقوبات وكيفيتها إلى مواد أخرى من قانون العقوبات[539].

2° L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ;

4° La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés;

5° L'exclusion, pour une durée de cinq ans au plus, des marchés publics ;

6° L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ;

7° L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35

[539] **-Art 323-6 de C.P.F** Modifié par LOI n°2009-526 du 12 mai 2009 - art. 124 : «

و بالنسبة للمشرع الأردني فإنه لم ينص على عقوبة الشخص المعنوي في القانون رقم 30 المتعلق بجرائم أنظمة المعلومات، لذلك يتم الرجوع إلى الأحكام العامة بخصوص المسئولية الجزائية للشخص المعنوي والعقوبات المقررة له قانونا.

المطلب الثاني: نطاق العقوبة

قد يتطلب ارتكاب بعض الجرائم البدء في القيام بنشاط إجرامي يؤدي مباشرة إلى إرتكاب الجريمة، أو القيام ببعض الأعمال لتنفيذ تلك الجريمة، و على ذلك لم تكتفي بعض التشريعات على تجريم أفعال قد تمس امن المعلومات المعالجة أو أمن أنظمتها المعلوماتية بل عاقبت حتى على الاتفاق السابق على تلك الجرائم أو الشروع فيها، و عملا بالأحكام العامة فإن الأفعال التي تسبق البدء في التنفيذ فلا عقاب عليها، و لكن نظرا لخطورة هذه الجرائم قد يخرج المشرع عن ذلك الأصل رغبتا منه لزرع الرهبة و الردع في نفوس مجرمي هذا الشكل من الإجرام، و كذا الحيلولة دون ارتكاب تلك الجرائم، و بغرض تقرير نوع من الحماية الوقائية المبكرة، و ذلك بتقرير نص خاص يعاقب على مجرد الأعمال التحضيرية أو ما يعرف في التشريع الجزائري بجمعيات الأشرار[540].

و فضلا عن تقريره العقاب على المرحلة التي تتبع الأعمال التحضيرية إذا كانت الجريمة تشكل جنحة، نجده وسع من نطاق العقوبة نظرا لخطورة الجرائم الماسة بأنظمة المعالجة الآلية، لتشمل الأشخاص الذين يشاركون في التحضير لهذه الجرائم في إطار الاتفاق الجنائي أو أعمال البدء و الشروع.

ومن ثم فإننا نلمس مدى رغبة المشرع الجزائري في مكافحة هذه الجرائم و الوقاية منها، فالعقاب على الاتفاق الجنائي أو الشروع يغلق باب كل الأفعال سواء الماسة بأنظمة المعالجة الآلية للمعطيات أو بالأمن المعلوماتي لذا ارتأينا التطرق إلى كل من المعاقبة على الاتفاق و الشروع على الشكل الأتي:

الفرع الأول: المعاقبة على الاتفاق في الجرائم الماسة بالأمن المعلوماتي

Les personnes morales déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre encourent, outre l'amende suivant les modalités prévues par l'article 131-38, les peines prévues par l'article 131-39.
L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise ».

[540]- أ. **رشيدة بوكر**، المرجع السابق، ص 339.

حدد قانون العقوبات[541] أنه يعد اتفاقا جنائيا كل اتفاق بين شخصين أو أكثر على ارتكاب جناية أو جنحة، سواء كانت هذه الجرائم معينة أو غير معينة أو على الأفعال المجهزة أو المسهلة لارتكابها متى ما كان هذا الاتفاق منظما و مستمرا ولو لمدة قصيرة.

كما لجأت العديد من المشرعين [542] إلى تجريمه و من بينهم المشرع الجزائري بإعتباره جريمة مستقلة بذاتها من جهة و من جهة أخرى كونها تعاقب على مجرد الأعمال التحضيرية، و قبل الفصل في موقف المشرع الجزائري و التشريعات المقارنة من تقرير عقوبة الاتفاق الجنائي، نتطرق أولا إلى الجدل الفقهي الذي ثار حول مدى ملائمة تجريم المشرع للإتفاق الجنائي من عدمه حيث ظهر هناك اتجاهان كالأتي:

فذهب اتجاه[543] إلى القول أن الاتفاق الجنائي عزم إجرامي، و تجريمه لا يعتبر استثناء يرد على قاعدة "عدم العقاب على مجرد العزم الإجرامي" ، و يستند هذا الرأي إلى أن المشرع لا يعاقب على الاتفاق الجنائي كخطوة للجريمة المتفق عليها و إنما يعاقب عليه في حد ذاته كجريمة خاصة تامة، و حجة تبرير المعاقبة عليه أنه في الاتفاق الجنائي يظهر العزم الإجرامي الجماعي بمظهر خارجي مادي لأن كل عضو فيه يعلن عزمه إلى سائر الأعضاء فتتحد إرادتهم على ارتكاب الجريمة، و بذلك يكون الاتفاق معلوما و يمكن إثباته، و من جهة ثانية الاتفاق الجنائي ظاهرة خطير تهدد الأمن العام تهديدا فعليا، كما أن هدف المشرع من العقاب على الاتفاق هو الوقاية حيث أن إحباط الاتفاق الجنائي نتيجته هي الحيلولة بين الجناة و بين تحقيق خططهم الإجرامية.

و يرى أصحاب هذا الإتجاه أنه لا مجال للاعتراض على تجريم الإتفاق الجنائي بحجة أن في ذلك حث للجناة على الإقدام على ارتكاب الجرائم المتفق عليها مادام أن العقاب يقع لأول مبادرة بدرت منهم

---

[541] – المادة 176 من ***قانون العقوبات الجزائري المعدل و المتمم.***

[542]– جرم المشرع الفرنسي الاتفاق الجنائي في قانون العقوبات بموجب المادة 450-1 من الباب الخامس من الكتاب الرابع تحت عنوان " المشاركة في جمعيات الأشرار " de la participation à une association de malfaiteurs.

[543] - **XAVIER** Linant de bellefonds et **ALAIN** hollande ,Pratique du droit de l'informatique, 4e éd, DELMAS, 1998, p 239.

مشار إليه لدى: **محمد خليفة**، مرجع سابق، ص 113.

و هي اتفاقهم، و أن باب العدول الفردي مفتوح و ذلك بالتبليغ و الإخبار و ما يتبعه ذلك من إعفاء من العقاب[544].

في حين يرى اتجاه آخر[545] أن تجريم مجرد الاتفاق فقط ستكون له انعكاسات سلبية، ذلك لما يخلقه من دفع للمجرمين بإتمام ما تم الاتفاق عليه نظرا لأن اتفاقهم قد تم تجريمه حيث أن العدول عن هذا الاتفاق وفقا للرأي السابق لا يمنع من تقرير العقوبة، لأن الاتفاق حسبهم جريمة مستقلة بذاتها لذلك ذهب هذا الاتجاه للقول بأن حجج الرأي السابق غير قويمة ويكفي لدحضها جميعا المقارنة بين خطورة الاتفاق الجنائي على نحو ما صوره أصحاب الاتجاه السابق، و بين خطورة الأعمال التحضيرية التي تصدر عن شخص يسعى إلى ارتكاب الجريمة بمفرده، فالاتفاق الجنائي في مرحلة مبكرة بالنسبة للتحضير للجريمة إذ أنها ترد إلى المرحلة النفسية أي إلى مرحلة اتخاذ القرار و عقد العزم على ارتكاب الجريمة، بينما يعقب التحضير للجريمة هذه المرحلة النفسية لهذا– يضيف أصحاب هذا الاتجاه– أنه لو صحت خطورة الاتفاق الجنائي تبريرا لمعاقبة المتفقين في هذه المرحلة المبكرة من المراحل التي تمر بها الجريمة، لوجب على المشرع أن يجرم مرحلة التحضير للجريمة من باب أولى.

ذلك ما تنبه له كل من المشرع الجزائري و الفرنسي من خلال اشتراطهما أن يكون التحضير مجسدا بأفعال مادية، و ليس مجرد العزم و التصميم على الإعداد لجرائم الاعتداء على نظم المعالجة الآلية، أي تجنب المشرع العقاب على المرحلة النفسية، و هو ما يستفاذ بوضوح من نص المواد 394 مكرر 5 عقوبات جزائري و المادة 323–4 من قانون العقوبات الفرنسي المعدل و المتمم.

و للإلمام أكثر بجريمة الاتفاق الجنائي في مجال جرائم الاعتداء على نظم المعالجة الآلية للمعطيات، نتطرق إلى الأركان المكونة لها و الجزاء المقرر لهذه الجريمة من خلال النقاط الآتية:

البند الأول: الركن المادي للاتفاق الجنائي

من خلال المادة 394 مكرر 5 عقوبات جزائري يتضح أن الركن المادي لهذه الجريمة يشتمل على ثلاث عناصر تتمثل في فعل الاتفاق و تعدد المتفقين و موضوع الاتفاق.

أولا: فعل الاتفاق

الأصل العام في الاتفاق هو اجتماع إرادتين أو أكثر على موضوع معين، و لقد جاء في المادة 176عقوبات جزائري انه : " كل جمعية أو اتفاق مهما كانت مدته وعدد أعضائه تشكل وتؤلف بغرض الإعداد لجناية أو أكثر، أو لجنحة أو أكثر، معاقب عليها بخمس(05) سنوات حبس على الأقل، ضد الأشخاص أو الأملاك تكون جمعية أشرار، و تقوم هذه الجريمة بمجرد التصميم المشترك على القيام

---

[544]- يستفيد من العذر المعفى وفقا للشروط المقررة في **المادة 52** من يقوم من الجناة بالكشف للسلطات عن الاتفاق الذي تم أو عن وجود الجمعية و ذلك قبل أي شروع في الجناية موضوع الجمعية أو الاتفاق و قبل البدء في التحقيق و ذلك طبقا للمادة ***179 من قانون العقوبات الجزائري المعدل و المتمم .***

[545]– مشار اليه لدى: **محمد خليفة**، مرجع سابق، ص 113

بالفعل " غير أن المشرع الجزائري لم يخضع فعل الاتفاق في جرائم المساس بأنظمة المعالجة الآلية للمعطيات للحكم العام لهذه المادة و إنما أخضع الفعل لنص المادة 394 مكرر 5 عقوبات.

و عليه قضت المادة 176 عقوبات جزائري أن فعل الاتفاق هو انعقاد أو تلاقي إرادتين أو أكثر واجتماعهما على ارتكاب الجريمة، أما المادة 394 مكرر 5 عقوبات لم تكتف بمجرد الاتفاق بل اشترطت أن يكون التحضير أو الاتفاق مجسدا بفعل أو عدة أفعال مادية، حيث تنصت 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 يعاقب بالعقوبات المقررة للجريمة ذاتها "

و هذه المادة تقابلها المادة[546] 323-4 عقوبات فرنسي،حيث يشترط المشرع الفرنسي كذلك ضرورة توافر أعمال مادية تحضيرية تعقب الاتفاق، إلا أن المشرع الفرنسي لم يقصر تجسيد ذلك الاتفاق في أفعال مادية لارتكاب جرائم الماسة بأنظمة المعالجة الآلية و إنما وسع من نطاق الاتفاق و اشترط نفس الأمر حتى في الحكم العام للاتفاق الجنائي على خلاف المشرع الجزائري و ذلك بموجب المادة 450-1 من نفس القانون.[547]

و قد أثار مفهوم المادية جدلا فقهيا و في ما مدى اعتبار الأعمال المادية قد تتحقق فقط في صورة بدء تنفيذ الأعمال التحضيرية؟

إن جانب من الفقه الفرنسي[548] قال أنه من الواجب إعطاء مفهوم أوسع للمادية حيث أن مجرد تبادل المعلومات في صورة مناسبة بحيث يؤدي ذلك إلى تحقيق الجرائم المنصوص عليها، يعد كافيا لقيام هذه الجريمة، ومن أمثلة الأعمال التحضيرية في مجال المعلوماتية تبادل المعلومات الهامة لارتكاب الجريمة كالكشف عن رمز الاستخدام أو عبارات الدخول إلى نظام معلوماتي.

ثانيا: تعدد المتفقين أو الجناة

---

[546] **-Art 323-4 de C.P.F** ; « La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée » Modifié par ***Loi n°2004-575 du 21 juin 2004 - art. 46 JORF 22 juin 2004***

[547] **-Art 450-1 de C.P.F** ;« Constitue une association de malfaiteurs tout groupement formé ou entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'un ou plusieurs crimes ou d'un ou plusieurs délits punis d'au moins cinq ans d'emprisonnement.Lorsque les infractions préparées sont des crimes ou des délits punis de dix ans d'emprisonnement, la participation à une association de malfaiteurs est punie de dix ans d'emprisonnement et de 150 000 euros d'amende.

Lorsque les infractions préparées sont des délits punis d'au moins cinq ans d'emprisonnement, la participation à une association de malfaiteurs est punie de cinq ans d'emprisonnement et de 75 000 euros d'amende » Modifié par ***Ordonnance n°2000-916 du 19 septembre 2000 - art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002***

[548]- مشار اليه لدى: د.**عمر أبو الفتوح عبد العظيم الحمامي**، مرجع سابق، ص 1021.

جريمة الاتفاق تتطلب تعددا ضروريا للجناة و أن تكون إرادتهم جادة و كلا منها محلا لاعتداد القانون بها[549]، إضافة إلى ذلك و لقيام جريمة الاتفاق يتعين أن تتجه إرادة المتفقين إلى نفس جرائم الاعتداء على نظم المعالجة الآلية و أن تتلاقى عنده متحدتاً و إلا لا قيام للجريمة.

و الحد الأدنى لهذا التعداد هو شخصان بينما لا يرد قيد على الحد الأقصى حسب نص المادة 176 عقوبات جزائري، و المادة 394مكرر 5 أو من المادة 323-4 عقوبات فرنسي .

و المهم في ذلك أن يتم الاتفاق بين شخصين على الأقل، فإذا ارتكب العمل التحضيري المادي شخص واحد بمفرده و بمعزل عن غيره فلا يعاقب في هذه الحالة، فالعقاب لا يتقرر إلا في حالة اجتماع شخصين أو أكثر.

ثالثا: موضوع الاتفاق

يكتسي الاتفاق صفته الإجرامية من موضوعه فإذا لم تكن لموضوعه صفة إجرامية أي كان فعلا مشروعا و لم تكن له صلة بجريمة ما، فلا يعد الاتفاق جريمة[550]، و الملاحظ أن نص المادة 176 من قانون العقوبات الجزائري، التي نصت على الاتفاق الجنائي العام في الجنايات أو الجنح ضد الأشخاص أو الأملاك تجرم الاتفاق المنصب على ارتكاب جريمة أو الإعداد لها، و لا شك أن جرائم الإعتداء على نظم المعالجة الآلية تعد جنح ترتكب ضد الأملاك، و هو ما يجعل البعض يتساءل عن سبب نص المشرع لحكم خاص بها في المادة 394 مكرر5 مادام النص العام قد يشملها؟

إن المتمعن بنص المادة 176 السالفة الذكر قد يلاحظ أن موضوع الاتفاق يستهدف الإعداد للجنايات و الجنح المعاقب عليها بخمس(05) سنوات حبس على الأقل، بينما اقتصر نص المادة394 مكرر 5 تجريم الاتفاق في جرائم المساس بأنظمة المعالجة الآلية للمعطيات حيث لا يتجاوز الحبس فيها ثلاثة(03) سنوات كحد أقصى، و هذا ما تفطن له المشرع و استدركه بنص خاص لتجريم الاتفاق الجنائي.

و الجنح التي يشكل تحضيرها هدف الاتفاق المنصوص عليه بالمادة 394 مكرر 5 قانون العقوبات هي فقط الجنح الماسة بأنظمة المعالجة الآلية للمعطيات، و عليه لا يعاقب استنادا إلى هذا النص الاتفاق بهدف ارتكاب جنح أخرى غير المنصوص عليها في المواد من 394 مكرر إلى 394 مكرر 2 كالسرقة أو التزوير المعلوماتي.

الأمر نفسه بالنسبة للمشرع الفرنسي بخصوص موضوع الاتفاق يجب أن يتمثل في أعمال التحضير والإعداد للجرائم المنصوص عليها من المواد 323-1 إلى 323-3-1 عقوبات فرنسي.

و عليه متى كان موضوع الاتفاق يتمثل في التحضير و الإعداد للجرائم محل الدراسة والمحدد بالنصوص القانونية السالفة الذكر، فان الاتفاق يكتسب صفته الإجرامية حتى ولو كانت الأعمال في

---

[549]– **رشيدة بوكر**، مرجع سابق، ص 345.

[550]– **محمد خليفة**، مرجع سابق، ص 115.

ذاتها مشروعة، فالاتفاق على تعليم كيفية تصميم المعطيات وتجميعها ونشرها هو مشروع في الأصل لكنه يصبح غير مشروع إذا كان الاتفاق على تعليم ذلك بغية استعماله في الإجرام[551] خاصة الأفعال التي نصت عليها المواد من 394 مكرر 394 مكرر عقوبات جزائري، و المواد 323-1 إلى 323-3-1 عقوبات فرنسي.

كما انه لا يشترط أن يكون موضوع الاتفاق الجنائي هو الإعداد لعدة جرائم من الجرائم السابقة، بل يكفي أن يشمل موضوعه على واحدة منها و هذا ما يستفاد من نص المادة 394 مكرر بقولها " ... لجريمة أو أكثر....."

البند الثاني: الركن المعنوي للاتفاق الجنائي

الاتفاق جريمة عمدية يشترط لقيامها توافر قصد جنائي و هذا الأخير يقوم على عنصرين هما العلم و الإرادة.

أولا: العلم

يلزم لتوافر القصد الجنائي ان يعلم كل عضو في الجماعة بماهية الفعل أو الأفعال موضوع الاتفاق، و بما لها من خصائص يعتمد عليها المشرع في إضفاء الصفة الإجرامية عليها [552]، أي توافر العلم لدى كل منهم بأنه عضو في جماعة إجرامية و أن الغرض من الاتفاق هو ارتكاب جنح الاعتداء على نظام المعالجة الآلية أو التحضير لها، أما من جهل الغرض من ذلك لا يعد القصد الجرمي متوفرا من جانبه؛

كما إذا انضم عضو إلى الاتفاق معتقدا انه الاتجار في برامج معلوماتية أو معلومات عادية، فإذا به للاتجار في برامج غير مشروعة أو برامج خبيثة مثل البرامج الفيروسية، أو البرامج الإختراق [553] فبانتفاء علمه بموضوع الاتفاق لا يتوفر القصد الجنائي لديه، ولكنه يتوافر فيه القصد إذا علم هذا

---

551 – **طعباش أمين**، الحماية الجنائية للمعاملات الإلكترونية، رسالة ماجستير في القانون العام تخصص علم اللإجرام و علم العقاب، كلية الحقوق و العلوم السياسية، جامعة الحاج لخضر، باتنة، 2013/2012، ص149/ لئذا: **محمد خليفة**، مرجع سابق، ص 115.

552– **احمد خليفة**، مرجع سابق، ص 117.

553 – **رشيدة بوكر**، مرجع سابق ص348.

العضو بعد دخوله الاتفاق بموضوعه غير المشروعية ومع ذلك بقي في الاتفاق[554]، و عليه يلزم وعي الشخص بمشاركته باتفاق بغرض الإعداد لارتكاب إحدى الجرائم الماسة بأنظمة المعالجة الآلية.

ثانيا: الإرادة

إضافة إلى علم كل عضو من أعضاء الاتفاق بموضوع الاشتراك فيه فانه لابد أن تتجه كذلك إرادة كل عضو إلى تحقيق نشاط إجرامي معين يتمثل في العمل التحضيري لتلك الجرائم المنصوص عليها[555].

وعليه فانه يجب أن تتوفر الإرادة الجادة لشخصين على الأقل للدخول في الاتفاق، أي إرادة كل واحد و يكون طرفا في هذا الاتفاق، و أن يقوم بالدور الذي سيعهد به إليه، فإذا لم تكن الإرادة جادة [556] و كان دخول الاتفاق لمجرد الوثوق بأعضاء المجموعة أو لمجرد الاطلاع على أمرهم دون الانضمام إليهم أو كان لمجرد العبث، فانه ينتفي عنه القصد الجنائي لانتفاء الإرادة الجادة.

و لا شك أن تجريم المشرع الجزائري للاتفاق الجنائي بغرض الإعداد لجريمة من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات قد يكون من ورائه حكمة، ذلك أن مثل هذه الجرائم تتم عادة في إطار مجموعات لتبادل و جمع المعلومات ، إضافة إلى رغبة المشرع في توسيع نطاق العقوبة فأخضع حتى الأعمال التحضيرية التي تسبق البدء في تنفيذ هذه الجرائم إلى العقاب.

البند الثالث:عقوبات الاتفاق الجنائي

---

[554] – **محمد خليفة**، مرجع سابق، ص117/ **طعباش أمين**، مرجع سابق، ص151

[555]– **سوير سفيان**، جرائم المعلوماتية ، مذكرة ماجستير في العلوم الجنائية و علم الإجرام، كلية الحقوق و العلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2011/2010، ص102 .

[556]– د.**علي عبد القادر القهوجي**، مرجع سابق، ص 129/ **احمد خليفة**، مرجع سابق، ص117.

حسب ما جاء في المادة 394 مكرر 5– فان المشرع[557]يعاقب على الاشتراك في الاتفاق الجنائي بنفس عقوبة الجريمة التي تم الإعداد والتحضير لها و ذلك ما يظهر بوضوح من العبارة الواردة في المادة السابقة "....يعاقب بالعقوبات المقررة لجريمة ذاتها..."

وما يمكن ملاحظته من ذلك أيضا أن المشروع لم يحدد العقوبة في حالة تم التحضير و الإعداد لارتكاب عدة جرائم من الجرائم الماسة بأنظمة المعالجة الآلية كإعداد لارتكاب جريمة الدخول أو البقاء غير المصرح و كذلك التلاعب بالمعطيات وأنظمة المعالجة الآلية أو نشر المعلومات المتحصل عليها من اختراق النظام.

و في هذه الحالة يمكن الرجوع إلى الأحكام العامة في حالة تعدد الجرائم من فاعل واحد و بذلك تطبق عليه العقوبة الأشد.

و هذا ما أقره المشرع الفرنسي صراحة و أورده في أخر عبارة من المادة 323–4 بقوله ".....او بعقوبة الجريمة الأشد": "Ou pour l'infraction la plus sévèrement réprimée"

و تطبق العقوبة حتى في حالة عدم إتمام الجريمة التي تم الإعداد لها، ذلك أن جريمة الاتفاق جريمة مستقلة بذاتها عن الجرائم الأخرى و تقوم بمجرد الاتفاق[558].

الفرع الثاني: المعاقبة على الشروع في الجرائم الماسة بالأمن المعلوماتي

نصت على الشروع المادة 11 من اتفاقية بودابست للإجرام الالكتروني[559]، و تبناه كذلك المشرع الجزائري في نص المادة 394 مكرر 7 من قانون العقوبات.

---

[557]– بالرجوع إلى الأحكام العامة الواردة بشان العقاب على الاتفاق الجنائي العام فان المشرع حدد العقوبات على أساس خطورة الجريمة من خلال ا**لمادة 177 قانون العقوبات الجزائري المعدل و المتمم** و التي جاء فيها "يعاقب على الاشتراك في جمعية الأشرار بالسجن المؤقت من خمس (5) سنوات إلى عشر (10) سنوات و بغرامة من 500.000 دج إلى 1.000.000 د.ج، إذا تم الإعداد لارتكاب جنايات.

و تكون العقوبة الحبس من سنتين(2) إلى خمس (5) سنوات و الغرامة من 100.000 دج إلى 500.000 دج إذا تم الإعداد لارتكاب جنح ".

[558] – **عمر ابو الفتوح عبد العظيم الحمامي**، مرجع سابق، ص 1022.

[559]– ورد التنصيص على الشروع كذلك في **الإتفاقية العربية لمكافحة جرائم تقنية المعلومات** الموقعة بالقاهرة و المصادق عليها مؤخرا من طرف الجزائر، في المادة **2/19** مع حق الدول الأطراف في عدم تطبيق هذه الفقرة جزئيا أو كليا.

ويراد بالشروع "tentative" في الجريمة ذلك السلوك الذي يهدف به صاحبه إلى ارتكاب جريمة معينة، كانت لتقع بالفعل لو لا تدخل عامل خارج عن إرادة الفاعل حال دون وقوعها في أخر لحظة **(560)** .

إن الأصل في المعاقبة على المشروع يكون في مجال الجنايات فقط آما الجنح فلا يكون إلا بنص صريح و في الجنح الخطيرة منها، و لقد تطرق المشرع الجزائري للشروع في قانون العقوبات تحت مسمى المحاولة، من خلال المادة 30 منه و التي تنص بأنه: " كل محاولة لجناية تبتدئ بالشروع في التنفيذ أو بأفعال لا لبس فيها تؤدي مباشرة إلى ارتكابها تعتبر كالجناية نفسها إذا لم توقف أو لم يخب أثرها إلا نتيجة لظروف مستقلة عن إرادة مرتكبها.."

و كذلك ما جاء في نص المادة 31 من نفس القانون "المحاولة في الجنح لا يعاقب عليها إلا بناء على نص صريح في القانون والمحاولة في المخالفة لا يعاقب عليها إطلاقا".

و بالتالي إذا كان المشرع قد جرم و عاقب على مرحلة الاتفاق الجنائي في الأعمال التحضيرية بصفتها مرحلة تسبق مرحلة الشروع، فمن المنطقي تجريم مرحلة الشروع بوصفها مرحلة البدء في التنفيذ.

ونفس الآمر يقال بشأن المشرع الفرنسي حيث عاقب على الشروع بموجب المادة 323-7 عقوبات فرنسي**(561)**.

تعتبر الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات من الجنح الخطيرة التي أخضعها التشريع الجزائري و التشريعات المقارنة[562] لنظام الاتفاق الجنائي المجسد بأعمال مادية ثم لنظام الشروع أيضا، و لهذا الأخير كذلك أركان محددة و عقوبة مقررة نستشف ذلك من خلال العناصر الآتية:

البند الأول: الركن المادي

يقوم الركن المادي في الشروع في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات على عنصرين اثنين هما:

---

[560] – **د.طارق ابراهيم الدسوقي عطية**، مرجع سابق، ص184.

[561]- **Art 323-7 Du C.P.F** ; « La tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines » Modifié ***par Loi n°2004-575 du 21 juin 2004*** art. 46 JORF 22 juin 2004.

[562]– إن المشرع الأردني رغم وضعه لقانون مؤقت لجرائم أنظمة المعلومات إلا أنه على خلاف المشرع الجزائري و الفرنسي لم يعاقب على الشروع في هذه الجرائم.

أولا: البدء في التنفيذ

البدء في التنفيذ مرحلة تأتي بعد التفكير في ارتكاب جريمة من الجرائم الماسة بقواعد الأمن المعلوماتي أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، و مرحلة التحضير لها إذ يبدأ الجاني في تنفيذ الجريمة بالقيام بفعل مادي في سبيل تنفيذها، و يكون بذلك قد دخل في نطاق الشروع، غير أن الإشكال الذي ثار كان بشان تحديد مرحلة بدئ التنفيذ عن المراحل التي تسبقها و خاصة ان المرحلة التحضيرية لا عقاب عليها إلا إذا اتخذت مظهرا ماديا وفق ما سبق بيانه حيث اختلف الفقه حول تحديد معيار البدء في تنفيذ و انقسم إلى مذهبان:

المذهب المادي أو الموضوعي طبقا لهذا المذهب فان البدء في التنفيذ هو أن يكون الفاعل قد حقق عملا للبدء في الركن المادي للجريمة، فاذا لم يدخل الجاني بفعله الى الركن المادي، فلا يعتبر سلوكه بدء في التنفيذ ولا شروعا في الجريمة ولا يناله العقاب[563]، فلا يعد الشخص مثلا شارعا في السرقة إذا لم يكن قد وضع يده على المال الذي يريد أن يختلسه[564] .

و قد أخذ على هذا المذهب أنه يترك بدون عقاب جناة هم أهل العقاب رغم خطورة أفعالهم.

المذهب الشخصي : يذهب أنصاره و على رأسهم الفقيه " Garraud " إلى القول بأن الشروع هو سلوك يؤدى حالا و مباشرة إلى الركن المادي للجريمة، كما وصفها نموذجها في القانون، ولو لم يكن السلوك قد حقق بالفعل بداية هذا الركن.

و لا يلزم على ذلك اعتبار شخص ما شارعا في السرقة أن يكون قد حاز بالفعل المال المنقول المقصود بالسرقة، و إنما يكفي أن يكون قد بلغ في السلوك حدا يؤدي حالا و مباشرة إلى هذه الحيازة [565] و بالتالي عليه الإتيان بفعل يؤدي مباشرتا إلى النتيجة المقصودة.

و قد انتقدت صياغة هذا المذهب من قبل الأستاذ " Roux " من ناحية أن الفعل قد لا يؤدي في الحال إلى الركن المادي للجريمة و إنما قد يستغرق في سبيل بلوغ هذا الركن مدة من الوقت أو أياما، و من ثم الاكتفاء في تعريف الشروع بأنه:" العمل المؤدى مباشرة إلى ارتكاب الجريمة"[566]

قد استقر القضاء الفرنسي على الأخذ بالمذهب الشخصي و على ترديد صياغته في التعريف بالشروع [567] .

---

[563]- **عمر أبو الفتوح عبد العظيم الحمامي**، مرجع سابق ص 1007.

[564]- د.**طارق إبراهيم الدسوقي عطية**، مرجع سابق، ص186.

[565] – نفس المرجع، ص 186.

[566] – **رشيدة بوكر**، مرجع سابق، ص 354/د.**طارق ابراهيم دسوقي عطية**، مرجع سابق ص187.

أما عن موقف المشرع الجزائري فقد تأثر في ذلك بالاتجاه الغالب في معظم التشريعات و في مقدمتها التشريع الفرنسي الذي اعتمد المذهب الشخصي، كما استفاد من العبارة ذاتها المكرسة من قبل القضاء الفرنسي و يظهر ذلك من خلال العبارات الواردة بالمادة 30 عقوبات جزائري "...بالشروع في التنفيذ أو بأفعال لا لبس فيها تؤدي مباشرة إلى ارتكابها...".

من ثم فان الشروع في تنفيذ وهو العمل المؤدي مباشرة الى ارتكاب الجريمة.

وتطبيقا لذلك هل يمكن تصور الشروع في نطاق الجرائم الماسة بقواعد الأمن المعلوماتي بصافة عامة و جرائم المساس بأنظمة المعالجة الآلية للمعطيات كما جاء بها المشرع الجزائري؟

أن موقف المشرع الجزائري كان جليا فيما يخص الشروع في الجريمة بصفة عامة، و على خلاف ذلك بالنسبة لجرائم المساس بأنظمة المعالجة الآلية للمعطيات، حيث جرم المشرع الجزائري معظم الأعمال التحضيرية لهذه الجرائم نظرا لخطورتها و باعتبارها جرائم مستقلة قائمة بذاتها و ذلك من خلال المادة 394 مكرر 2 عقوبات.

غير أنه لا يتصور دائما الشروع في جميع جرائم الاعتداء على النظم، من ذلك جريمة الدخول غير المصرح به و على اعتبار أنها من الجرائم الشكلية فإنه وفقا للأحكام العامة لا يمكن الحديث عن الشروع فيها، فلكي يكون هناك مجال للقول بخيبة الأثر لابد أن يكون هناك نتيجة، أو عدم تحققها لظروف خارجة عن إرادة الفاعل، و بالتالي فالجرائم الشكلية إما أن تقع بوقوع الفعل فتعتبر جريمة تامة و إما أن لا تقع أبدا.

و عليه إذا كان موقف المشرع الجزائري واضحا بشان تجريم الشروع في كل الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بدون استثناء إلا انه من الصعب تصوره في كل تلك الجرائم، و مع ذلك نجده قد ختم في المادة 394 مكرر بعبارة" ...أو يحاول ذلك".

وهذا ما تنبهت له اتفاقية بودابست بإشارتها إلى صعوبة تصور الشروع في بعض عناصر الجرائم التي تستهدف امن ألمعلومات, وتأسيسا على ذلك فان الأطراف الموقعة على الاتفاقية لا يلزمون بتجريم

---

[567] -**عمر أبو الفتوح عبد العظيم الحمامي**، مرجع سابق، ص1008.

الشروع إلا في الجرائم المحددة في بعض المواد، كما انه ليس ملزم بتجريم الشروع المرتكب في كل جريمة منصوص عليها في هذه الاتفاقية[568]

ومن الجرائم التي استثنت الاتفاقية بودابست عدم تجريم الشروع فيها نظرا لصعوبته، نجد جريمة الدخول غير مصرح و لعل ذلك يرجع إلى صعوبة معرفة أو تحديد الأفعال التي تدخل في نطاق البدء في التنفيذ وتميزها عن الأعمال التحضيرية الغير معاقب عليها من محاولة الدخول إلى النظام المعلوماتي.

و الأمر ذاته بالنسبة للاتفاقية العربية بشان مكافحة جرائم تقنية المعلومات و ما جاءت به الفقرة الثالثة من المادة 19 من ذات الاتفاقية.

ثانيا: خيبة اثر الجريمة نتيجة ظروف خارجة عن إرادة الفاعل.

حسب المادة 30 من قانون العقوبات جزائري فإنه للحديث عن الشروع فانه لا يكفي البدء في التنفيذ وإنما يتطلب الأمر وقف التنفيذ أو خيبة اثر الفعل لأسباب خارجة عن الفاعل لا دخل لإدارته فيها بقولها "... إذا لم توقف أو لم يخب أثرها إلا لظروف مستقلة عن إرادة مرتكبها..."

و إذا كان تحديد الشروع المعاقب عليه تعترضه بعض الصعوبات حيث لا يوقف الفاعل في إتمام سلوكه الى النهاية لتدخل عوامل خارجة عن إرادته حالت دون ذلك، فانه لا صعوبة في ذلك التحديد في حالة كان الفاعل قد مضى في سلوكه إلى النهاية و بدون عائق غير أن الحدث الذي كان يراد تحقيقه هو الذي تأثر بالعامل الذي حال دون وقوعه[569].

وفي الحالتين لا تحدث الجريمة على الصورة الكاملة المطابقة لنموذجها وعلى ذلك نفرق بين الجريمة التامة و الشروع في الجريمة.

نقول أن الجريمة تامة عندما تكتمل جميع أركانها وعناصرها المحددة بالنص القانوني المعاقب عليها، فيتحقق الركن المادي والمعنوي والنتيجة التي يريدها الجاني إذا كان من الجرائم المادية، أما

568- **هلالي عبد الله احمد**، مرجع سابق ص 146-147.

569- هناك فرق بين الجريمة الناقصة أو الشروع التام والجريمة الموقوفة أو الناقصة، في الأصل لا تتحقق الجريمة على الصورة الكاملة المطابقة لنموذجها الموصوف في القاعدة الجنائية إذ لا يتوفر منها سوى السلوك، و في الحالة الثانية أو في الجريمة الموقوفة لا يتوفر منها سوى جزء من السلوك اللازم لارتكابها، و من اجل ذلك يطلق على الشروع في الحالتين اسم الجريمة الناقصة: لمزيد من التفاصيل لدى **د.طارق ابراهيم الدسوقي عطية**، مرجع سابق، ص190.

الشروع فيختلف عن الجريمة في تحقيق النتيجة، حيث إذا لم تتوفر هذه الأخيرة رغم تحقق العناصر الأخرى اعتبر الأمر شروعا في الجريمة[570]

الأصل في القواعد العامة التقليدية انه لا شروع في الجرائم الشكلية غير أننا نجد المشرع الفرنسي و تبعه في ذلك المشرع الجزائري قد خرج عن هذه القواعد كما سبق بيانه ، وعاقب على الشروع في الجرائم الشكلية في نطاق الماس بأنظمة المعالجة الآلية للمعطيات و ذلك ما يستفاد من 323-7 قانون العقوبات فرنسي و المادة 394 مكرر 05 عقوبات جزائري[571].

البند الثاني: الركن المعنوي

الشروع جريمة عمديه[572] يتخذ فيها الركن المعنوي صورة القصد بعنصريه العلم و الإرادة و لا يختلف هذا الركن الخاص بجريمة الشروع عن الركن المعنوي في الجريمة التامة و هو ما يقتضي اتجاه الإرادة إلى ارتكاب الجريمة لا إلى مجرد الشروع فيها.

و على ذلك يكون سلوك الجاني إراديا، و ان يتوافر علمه بكافة العناصر الجوهرية اللازمة قانونيا لقيام الجريمة، و ان تتوفر لديه نية تحقيق النتيجة[573].

مع الإشارة إلى انه إذا كانت جريمة الشروع من الجرائم القصد الخاص، فلا بد أن يتوافر لدى الجاني هذا القصد.

البند الثالث: المعاقبة على الشروع:

وفقا للمادة 30 من قانون العقوبات السابقة الذكر، فإن المشرع الجزائري جعل الشروع في الجناية كالجناية نفسها، و بالتالي يعاقب عليها بنفس العقوبة المحددة قانونا للجناية، أما بالنسبة للجنح فانه لا عقاب على الشروع فيها إلا بنص صريح [574]، و هذا ما استدركه فيما يخص الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بالعقاب على الشروع فيها بالعقوبات المقررة للجنحة ذاتها، ولا شك أن تقرير

---

570 – **عمر أبو الفتوح عبد العظيم الحمامي**، مرجع سابق ص 1009.

571 – بعض التشريعات العربية و منها **التشريع الأردني** على خلاف **المشرع الجزائري** لم تنص على المعاقبة على الشروع في هذا النوع من الجرائم

572– وهذا مانصت عليه المادة 2/11 من اتفاقية بودابست

573– **طارق ابراهيم دسوقي عطية**، مرجع سابق، ص 193.

574– المادة 1/31 من **قانون العقوبات الجزائري** المعدل والمتهم.

المشرع الجزائري العقاب على الشروع في هذا النوع من الجرائم قد يرجع إلى إدراكه لخطورتها وخصوصيتها، و إلى ما قد تؤدي إليه من خسائر في حالة إتمامها.

وهو ما اقره المشرع الفرنسي كذلك و ذلك بموجب المادة 323-7 عقوبات.

غير أن الفرق بين التشريعين أن المشرع الجزائري من خلال المادة 394 مكرر 7 [575]عاقب على الشروع في كل الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بما في ذلك المادة التي تعاقب على الاتفاق الجنائي و وسع بذلك من نطاق العقاب على الشروع ليشمل حتى الاتفاق الجنائي، أما بالنسبة للمشرع الفرنسي فقد أخرجه من دائرة العقاب على الشروع من خلال المادة 323-7[576] و التي اقتصرت العقاب على الشروع في الجرائم المنصوص عليها في المواد من 323-1 إلى 323- 3-1.

المبحث الثاني:

دور مراقبة الاتصالات الإلكترونية في تحقيق الأمن المعلوماتي

قد تكون هناك وسائل عدة لتحقيق أمن معلوماتي أو السلامة معلوماتية من الناحية القانونية، وذلك بوضع قواعد جزائية رادعة لمن يعتدي على سلامة المعلومات والنظم المعلوماتية.

كما يمكن كذلك إتباع إجراءات فنية أو تقنية حرصا و تيقظا من وقوع أي إعتداء على نظم المعالجة الآلية للمعطيات، إضافة إلى إتباع إرشادات ونصائح الخبراء في مجال الأمن المعلوماتي.

---

[575]– تنص المادة 394 مكرر 7 عقوبات جزائري على أنه:: يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها".

[576] **-Art 323-7 Du C.P.F** dispose que : « La tentative des délits prévus par les articles 323-1 à 323-3--1 est punie des mêmes peines ».

غير أن التكنولوجيا في تطور مستمر وقد تستخدم في أغراض غير مشروعة، وبالتالي فإن التحكم في المجال المعلوماتي وجعله أمنا أمر نسبي، إذ ليس من السهل تحديد المخاطر والثغرات و الاعتداءات و التحكم فيها.

و كون هذه الجرائم تتم في عالم إفتراضي حيث يتم تبادل المعلومات والمراسلات عبر وسائل إلكترونية وخدمات الاتصال المفتوحة التي يصعب فيها الرقابة كما هي في المجالات العادية، مما دعت الحاجة إلى وضع إطار قانوني وفني ينسجم مع هذا النوع من الأفعال والاعتداءات التي تقع على المعلومات و نظم المعالجة الآلية، و ذلك بتضمين قواعد تسمح بالرصد المبكر للاعتداءات المحتملة و التدخل السريع لتحديد مصدرها و التعرف على مرتكبيها ، ومن تلك القواعد لاسيما مراقبة الاتصالات الالكترونية مع مراعاة خطورة التهديدات المحتملة و أهمية المصالح المحمية، و من خلال هذا العنصر سوف نحدد ما المقصود بالرقابة الالكترونية والحالات التي تجوز فيها هذه الرقابة كونها إجراء خطير و حساس قد يمس بحريات الأشخاص؟

المطلب الأول: المقصود بالرقابة الالكترونية

تطرق المشرع الجزائري إلى الرقابة الالكترونية من خلال المادة الرابعة من القانون رقم 09-04 بشأن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، غير أنه لم يحدد المقصود بمراقبة الاتصالات الالكترونية[577]، شانه في ذلك شان التشريعات المقارنة، غير أن الفقه تناولها بالتعريف حيث قيل إنها: "العمل الذي يقوم به المراقب بإستخدام التقنية الالكترونية لجمع المعطيات والمعلومات عن المشتبه فيه سواء كان شخصا أو مكانا أو شيئا حسب طبيعته مرتبط بالزمن (التاريخ والوقت) لتحقيق غرض أمني أو لأي غرض أخر"[578]

ومن هذا التعريف يتضح أن المراقبة الالكترونية تتم بالاطلاع أو مراقبة الاتصالات والمراسلات التي تتم عبر وسائل الاتصال، وهذا قد يشكل مساسا بحق محمي دستوريا وهو سرية

---

[577]- لقد عرف المشرع الجزائري الاتصالات الالكترونية بموجب الفقرة (و) من المادة 02 **من القانون رقم 09-04** على أنها: "أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية "، وكذلك المشرع الفرنسي عرفها في **قانون البريد والاتصالات الالكترونية لسنة 1980**.

[578]– د. **مصطفى محمد موسى** ، المراقبة الالكترونية عبر شبكة الانترنت– دراسة مقارنة– مشار إليه لدى: أ. **رشيدة بوكر** ، مرجع سابق، ص 370.

المراسلات والاتصالات والحق في الخصوصية [579]، لذلك يجب تحديد نطاق المراقبة الالكترونية، والحالات التي يجوز فيها ذلك على النحو الآتي:

المطلب الثاني: نطاق المراقبة الالكترونية

إن مراقبة الاتصالات الالكترونية الخاصة أمر محظور كونها وكما سبق ذكره أنها تتعلق بحق الإنسان في خصوصية مراسلاته و اتصالاته، و هو حق مكفول دستوريا في مختلف التشريعات [580]، غير أنه أصبح مهددا بالخرق بواسطة التكنولوجيا الحديثة التي يمكن من خلالها اختراق الاتصالات والتنصت على كافة الاتصالات السلكية واللاسلكية، و حتى على الاتصالات والمراسلات التي تتم عن طريق الانترنت (مثل البريد الالكتروني)[581].

غير أن المشرع الجزائري قد أجاز مراقبة الاتصالات السلكية واللاسلكية بما فيها تلك التي تتم عبر الوسائل الالكترونية، إذا ما كانت هناك ضرورة تستدعي الوقاية قبل وقوع بعض الجرائم، ولا يجوز المراقبة في كل الحالات، حيث كفل حرية الإنسان وسرية مراسلاته واتصالاته وحدد الحالات والكيفيات التي تتم فيها الرقابة من خلال المادة 04 من القانون المتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بقوله" يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 3 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 الاقتصاد الوطني.

ج. لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية

ت. في إطار تنفيذ طلبات المساعدة القضائية الدولية...".

وعليه فإن المشرع الجزائري قد أظهر محاولته في مكافحة جرائم تقنية المعلومات بصفة عامة من خلال تعديلاته لقانون العقوبات بهدف تطوير القاعدة الجزائية وجعلها تتفاعل وتتواءم مع صور الإجرام

---

[579]– المادة **39** من **الدستور الجزائري لسنة 1996 المعدل والمتمم**

[580]– حضر **الدستور الجزائري لسنة 1996 المعدل و المتمم** التنصت و إعتراض المراسلات و الاتصالات الخاصة بمختلف اشكالها من خلال المادة 39 منه.

[581]– **عفيفي كامل عفيفي وفتوح الشاذلي**، مرجع سابق، ص 265،266.

الحديث، وكذا إصداره للقانون رقم 09-04 للوقاية ومكافحة هذه الجرائم وأهم ما جاء فيه هو عنصر المراقبة الالكترونية[582]، الذي فرضته الظروف الواقعية والتي جعلت المشرع مخيرا بين حق الإنسان في الخصوصية وحق الدولة والمجتمع في الأمن.

الفصل الثاني:

الإجراءات العلاجية لجرائم الأمن المعلوماتي

إن وضع قواعد موضوعية للتصدي و مكافحة الجرائم الماسة بالأمن المعلوماتي أو جرائم العالم الافتراضي لا يكون له أثر إلا إذا ما استكمل بقواعد إجرائية، ذلك أن الجانب الموضوعي الجنائي يبقى قاصرا و غير مفعل ما لم تكمله قواعد إجرائية بقدر ذلك التحدي الذي يفرزه التطور التكنولوجي في المجال الجنائي.

و من الحقائق المسلم بها أن التقدم العلمي له تأثيره البالغ على القانون و على الواقع الذي يطبق عليه هذا القانون؛ و لكي تتحقق الفائدة المرجوة من هذا التقدم، فإن القانون يجب ألا ينفصل عن الواقع الذي يفرزه و يطبق عليه ، بل يجب أن يكون متجاوبا معه ومتطورا بتطوره .

فالتطور الحالي الذي انعكس أثره على قانون العقوبات، قد انعكس أثره أيضا على قانون الإجراءات الجنائية، بحيث أن هذا القانون الأخير قد لا يطبق بسبب عجز القانون الأول عن استيعاب الجرائم

---

[582]- من نماذج وتقنيات المراقبة الالكترونية، نجد تقنية كارنفور وتقنية كشف وجمع الأدلة والقرائن من الرسائل الالكترونية والبريد الالكتروني، وتقنية البريد الالكتروني: لمزيد من التفاصيل لدى:د. **نبيلة هبة هروال** ، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الإسكندرية، 2006، ص 203/202./ كذلك لدى: **فهد عبد الله العبيد العازمي**، مرجع سابق، ص 205،206.

المستحدثة التي ترتكب بالوسائل الإلكترونية، كما و أن الإثبات الجنائي وهو احد الموضوعات الهامة لهذا القانون قد تأثر بدوره بالتطور الهائل الذي لحق الأدلة الجنائية بسبب تطور طرق ارتكاب الجريمة، الأمر الذي يتعين معه تغير النظرة إلى طرق الإثبات الجنائي لكي تقترب الحقيقة العلمية في واقعها الحالي من الحقيقة القضائية .

فإثبات الجرائم التي تقع على العمليات الإلكترونية بإستخدام الوسائل الرقمية سيتأثر بطبيعة هذه الجرائم، وبالوسائل العلمية التي قد ترتكب بها، مما قد يؤدي إلى عدم اكتشاف العديد من الجرائم في زمن إرتكابها، أو عدم الوصول إلى الجناة الذين يرتكبون هذه الجرائم، أو تعذر إقامة الدليل اللازم لإثباتها مما يترتب عليه إلحاق الضرر بالأفراد و بالمجتمع.

كما أن جرائم الأمن المعلوماتي و التي تمس القواعد و المبادئ الأساسية التي يقوم عليها مثلها مثل غيرها من الجرائم تقوم على أركان محددة، و تسير بشأنها دعوى جنائية و بنفس مراحل و خطوات الجرائم التقليدية.

و لقد أكدت المذكرة التفسيرية لإتفاقية بودابست على ذلك حيث جاء فيها أن ثورة التكنولوجية دخلت دائرة قانون العقوبات و قانون الإجراءات الجزائية، و أنها فتحت أفاقا جديدة للإجرام لذلك فإن القواعد العقابية الموضوعية فقط لا تكفي إذا ما تماشت مع هذه لجرائم، بل يجب أن يشمل هذا التطور أيضا قوانين الإجراءات الجنائية و تقنيات التنقيب و التحري، و بنفس الطريقة يجب اتخاذ احتياطات تسمح بأن تكون لها تأثير على البيئة التكنولوجية الجديدة و على تطوير سلطات الإجراءات الجديدة[583].

لذلك إذا ما حدث و أن وقعت الجريمة في نطاق المساس بأمن المعلوماتي، أو جرائم المساس بأنظمة المعالجة الآلية للمعطيات كما جاء في التشريع الجزائري و التشريعات المقارنة فإن العقاب عليها لن يكون إلا بكشفها و تثبيت الدليل عليها، مما يستدعي تكريس قواعد مناسبة لبيئة الجريمة الحديثة، كونها تختلف عن البيئة التقليدية للجرائم العادية، و كون الدليل فيها له ذاتيته و خصائصه تجعله مميزا مما قد يشكل صعوبة في تحديده و الحصول عليه، وإضافة إلى صعوبة تحديد الفاعل وتقييم مدى و أثر الجريمة.

و بالتالي حتى و لو وجدت إجراءات تقليدية للكشف عن الجريمة في بيئة رقمية و عالم افتراضي، فإنه لا شك قد لا تكفي و انه ستختلف إجراءات الكشف عن الجريمة في عالم افتراضي عنها في

---

[583]- د. **هلالي عبد الإله أحمد**، مرجع سابق، ص 160.

الجريمة في البيئة التقليدية، حيث أن مسرح الجريمة سيتغير [584] فيكون للدليل خصوصية(مبحث أول)، وستحتاج إلى نوع خاص من إجراءات جمع الأدلة من معاينة وضبط وتفتيش، وكذلك لا بد من أن يتأثر مجال الخبرة الفنية في الكشف عن الجريمة المعلوماتية وحيثياتها حيث تزداد أهميتها في هذه الجرائم(مبحث ثاني)، و سيختلف دور السلطات المختصة في القيام بعمليات الاستدلال والتحقيق، وسيحتاج القضاة أن يتعاملوا بشكل مختلف مع هذا النوع من الإجرام(مبحث ثالث).

و من خلال هذا الفصل سوف نوضح تلك العناصر وعلى النحو الآتي:

المبحث الأول

خصوصية الدليل التقني

إن قواعد الإثبات جاءت لتنظيم و إقامة الدليل على وقوع الجريمة، ونسبتها لفاعل معين حتى تتمكن الدولة من إقتضاء سلطتها بعقاب المجرمين، ومن هنا تبرز أهمية الإثبات، فعند وقوع أي جريمة يكون هدف السلطات المختصة الكشف عن الحقيقة و الوصول إلى ما حدث؛

و إن إثبات الجريمة في مجال الأمن المعلوماتي من العقبات التي يعمل الخبراء على كسرها من أجل إيجاد وسائل لإثباتها فهي تتطلب خبرة فنية عالية و اعتماد أسلوب واضح لتحقيق، ومما لا شك فيه أن التكنولوجيا الحديثة في مجال نظم المعلومات لم تؤثر فقط على نوعية الجرائم و إنما أثرت على الإثبات الجنائي و طرقه، بحيث أن الطرق التقليدية أصبحت عقيمة بالنسبة لإثبات هذا النوع من الجرائم الحديثة و ذلك لظهور نوع خاص من الأدلة في إثبات الجريمة في العالم الافتراضي، لذا يتطلب الأمر أن نبين نوعية الدليل في هذه الجرائم فما هو هذا الدليل التقني؟ و ما هي طبيعته؟

المطلب الأول: ماهية الدليل التقني

---

[584]– **هناء جميل عبد الحافظ أبو حمدية** ، الإثبات الالكتروني في الدعوة الجزائية في الأردن، رسالة ماجستير، كلية الدراسات العليا،الجامعة الأردنية، 2006 ، ص 54.

ثارت إشكالات إجرائية في مجال الأمن المعلوماتي تتعلق بطرق الإثبات الجنائي و كيفيه كما سبق و أن اشرنا، و يرجع ذلك للبيئة التي تتم فيها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تكنولوجيا الاتصالات و المعلومات فهي بيئة افتراضية و الجريمة التي ترتكب فيها في الغالب لا يكون لها اثر ملموس كما في الجريمة التقليدية التي قد يترك فيها الجاني أثرا ماديا[585] .

و أن الاعتماد على تقنيات المعلومات والاتصال في مختلف مجالات التعامل والإرسال والبحث لم تؤثر في نمط الأفعال الإجرامية المرتكبة في نطاق الأمن المعلوماتي أو أنظمة المعالجة الآلية للمعطيات، بل أثرت كذلك على أدلة الإثبات الجنائي، إذا أصبحت أدلة الإثبات التقليدية عاجزة عن إثبات هذا النوع من الجرائم الحديثة.

فقد أنتج الصراع المعلوماتي في مجال تقنية أنظمة المعلومات و الاتصالات مظهرا جديدا لإثبات الجنائي، و طرح العديد من التساؤلات في موضوعات الدراسات القانونية الجنائية التي تناولت البحث في مدى إمكانية تجاوب وسائل الإثبات العادية (التقليدية) مع التقنيات التكنولوجية في الاتصال و الأنظمة المعلوماتية؛

و البحث في الإثبات في المسائل الجزائية في إطار اتفاقها مع التقنية الحديثة غير ذي معنى إذا لم يكن مدعما بتوفيق من التقنية ذاتها مع كل ما يتم إثباته في هذا الشأن [586] ، كما بدأ الاهتمام يتزايد بعلم الأدلة الجنائية المعلوماتية، التي تهدف إلى التعرف على الأدلة الرقمية وحفظها و تحليلها و تقديمها بطريقة مقبولة، أو بمفهوم أخر [587] هو العلم الذي يضم خليطا من تخصصي القانون و علوم تقنية الحاسوب و دوره هو جمع و تحليل البيانات من أنظمة الحاسب و الشبكات و الاتصالات و أجهزة التخزين الرقمية بمختلف أنواعها م تقديم هذه البيانات كدليل يعتد به في الحالات القانونية.

و عليه هناك مفهوم حديث يربط بين الظاهرة الرقمية ذات الطبيعة الالكترونية و بين الإثبات الجنائي و هو ما اصطلح عليه الدليل الرقمي أو الالكتروني(فرع أول) الذي اتصف بخصوصية استمدادها من طبيعة الجريمة في المجال أنظمة المعالجة الآلية للمعطيات جعلت منه دليلا صعبا ومعقدا و متميزا عن الدليل العادي(فرع ثاني)، و ليس من السهل الحصول عليه بإتباع الإجراءات

---

[585]– **الأثر المادي:** "علامة ظاهرة أو غير ظاهرة بمسرح الجريمة أو عالقة بالمتهم أو المجني عليه، تساعد على كشف الحقيقة من حيث إثبات وقوع الجريمة وتحديد مرتكبيها وظروف ارتكابها، وهو كل ما يعثر عليه المحقق في مسرح الجريمة.

[586]– **فتحي محمد أنور عزت**، الأدلة الالكترونية في المسائل الجنائية و المعلومات المدنية و التجارية، دار الفكر والقانون، المنصورة، مصر 2010، ص581.

[587]- **فهد عبد الله العبيد العازمي**، مرجع سابق، ص 354.

التقليدية في استخلاص و جمع الأدلة ، و كذا لتنوعه (فرع ثالث) و هذا ما سندرسه بمناقشة المسائل الآتية:

الفرع الأول: تعريف الدليل الالكتروني

الدليل بصفة عامة في اللغة هو المرشد وما يتم به الإرشاد، وما يستدل به، والدليل هو الدال أيضا، و الجمع أدلة ودلالات[588].

و في الاصطلاح هو: ما يلزم من العلم به على علم شيء أخر و غايته أن يتوصل العقل إلى التصديق اليقيني بما كان يشك في صحته، أي التوصل به إلى معرفة الحقيقة [3].

أما الدليل في البيئة الرقمية فقد تعددت التعريفات التي قيلت بشأنه و تباينت بين التوسيع والتضييق ، فقد قيل بأنه "معلومات يقبلها المنطق و العقل و يعتمدها العلم، يتم الحصول عليها بإجراءات قانونية و علمية بترجمة البيانات الحسابية المخزنة في أجهزة النظم المعلوماتية وملحقاتها و شبكات الاتصال و يمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بجريمة أو جان أو مجني عليه" [589].

أو أنه:" الدليل الذي يجد له أساسا في العالم الإفتراضي و يقود إلى الجريمة" [590].

و لعلى التعريف الاشمل و الأوضح هو الذي يعرف الدليل الإلكتروني أو الرقمي على أنه: " هو ذلك الدليل المشتق من أو بواسطة النظم البرامجية المعلوماتية الحاسوبية، و أجهزة و معدات و أدوات الحاسب الآلي، أو شبكات الاتصالات من خلال إجراءات قانونية و فنية لتقديمها للقضاء بعد تحليلها

588– **منصور عمر المعايطة**، الأدلة الجنائية والتحقيق الجنائي، ط1، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2009،ص.27

3– **محمد حماد مرهج الهيتي**، التحقيق الجنائي والأدلة الجريمة، ط1، دار المناهج للنشر والتوزيع، عمان الأردن، 2010، ص16.

589– د. **محمد الأمين البشري**، التحقيق في جرائم الحاسب الآلي و الانترنت، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004، ص 233.

590– د.**ابو بكر بن يونس**، الجرائم الناشئة عن استخدام الانترنت، مرجع سابق، ص 969.

علميا أو تفسيرها في شكل نصوص مكتوبة، أو رسومات أو صور و أشكال و أصوات لإثبات وقوع الجريمة و لتقرير البراءة و الإدانة فيها[591].

و بعد استعراض التعريفات التي قيلت بشأن الدليل الرقمي و مدى تقاربها من بعضها، إلا انه يجب ملاحظة أن عبارة الرقمي" Digital " لا تشير إلى وضعية مميزة لنوعية أو طبيعة الدليل في هذا المجال، و إنما هي تفسير يحمل على تطوير ظهر تحديدا مع عام 2000م في مرجعيات القواعد الإرشادية الأمريكية، فمرجعية رقمي المضافة إلا الدليل هو التحول نحو تفسير الدليل الرقمي لكي يكون له مفهوما أكثر إتساعا بحيث يشمل كافة أشكال الرقمية و إستخداماتها مثل الهواتف المحمولة و الفاكس الرقمي و الفديو الرقمي...[592].

و مهما كانت التعريفات التي قيلت بشأن الدليل الإلكتروني كدليل جنائي حديث، فلا شك أن له دور و أهمية كبيرة في معرفة و اكتشاف الجريمة الماسة بقواعد الأمن المعلوماتي و كيفية حدوثها، و كذا من أجل إثباتها و معرفة مرتكبيها حتى يطالهم العقاب، و لا شك كذلك أن الدليل الرقمي يستمد من البيئة الرقمية التي يتناسب معها في شكلها و مضمونها.

الفرع الثاني: خصائص الدليل التقني

إن البيئة التي تحتوي الدليل الإلكترونية بيئة إفتراضية غير محدودة و لا منتهية، فهي تتضمن أنواع متعددة من البيانات الإلكترونية و العناصر الرقمية التي قد تصلح لكي تكون دليلا رقميا، و قد انعكس هذا العالم الافتراضي على طبيعة الدليل مما جعله يتميز بمجموعة من الخصائص تمثلت فيما يلي:

البند الأول: الدليل الإلكتروني دليل علمي

الأدلة الرقمية تتكون من بيانات ومعلومات ذات هيئة إلكترونية غير ملموسة، لا تدرك بالحواس العادية، بل يتطلب إدراكها الاستعانة بأجهزة ومعدات وأدوات الحاسبات الآلية (Hardware)، واستخدام نظم برامجية حاسوبية(Software) [593].

---

[591]. د. **عبد الناصر محمد محمود فرغلي، و د.محمد عبيد سيف سعيد المسماري** : الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية و الفنية– دراسة تطبيقية مقارنة، بحث مقدم للمؤتمر العربي الأول لعلوم الأدلة الجنائية و الطب الشرعي، جامعة نايف العربية للعلوم الأمنية، الرياض، في 12–2007/11/14، ص 13.

[592]- **أميرة محمود بدوي الفقي** ، الإثبات الجنائي للجرائم المرتكبة عبر الانترنت، رسالة لنيل درجة الدكتوراه، جامعة عين شمس، كلية الحقوق، مصر، 2013، ص 127.

[593]– د. **عمر محمد ابو بكر بن يونس**، الجرائم الناشئة عن استخدام الانترنت، مرجع سابق، ص 977.

ذلك أن الدليل الرقمي لا يمكن الحصول عليه أو الإطلاع على فحواه سوى بإستخدام الأساليب العلمية.

البند الثاني: الأدلة الرقمية ليست أقل مادية من الدليل المادي فحسب، بل تصل إلى درجة التخيلية في شكلها و حجمها ومكان تواجدها غير المعلن وذلك لأن مصطلح الدليل الرقمي يشمل كافة أشكال وأنواع البيانات الرقمية الممكن تداولها رقميا، بحيث يكون بينها وبين الجريمة رابطة من نوع ما، وتتصل بالضحية على النحو الذي يحقق هذه الرابطة بينها وبين الجاني، فهي تمتاز بالسعة التخزينية العالية.

البند الثالث: سهولة التلاعب بالدليل التقني

من ميزات الدليل التقني كذلك انه يسهل التلاعب به سواء بالإتلاف أو التعديل أو إدراجه في ملفات أو مستندات أو معلومات رقمية أخرى بسرعة متناهية[594].

البند الرابع: دليل قابل للنسخ

يمكن استخراج نسخ من الأدلة الجنائية الرقمية مطابقة للأصل و لها ذات القيمة العلمية والحجية الثبوتية الشيء الذي لا يتوافر في أنواع الأدلة الأخرى (التقليدية).

مما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل ضد الفقد، والتلف، والتغيير، عن طريق عمل نسخ طبق الأصل من الدليل [595]، مثل نسخ المواد المخزنة في نظم المعالجة الآلية للبيانات بقصد عرضها على الجهات القضائية.

البند الخامس: الأدلة الرقمية يمكن استرجاعها بعد محوها، وإصلاحها بعد إتلافها و إظهارها بعد إخفائها، مما يؤدي إلى صعوبة الخلاص منها وهي خاصية من أهم خصائص الدليل الرقمي بالمقارنة بالدليل التقليدي، فهناك العديد من البرامج الحاسوبية التي وظيفتها استعادة البيانات التي تم حذفها أو إلغائها، سواء تم ذلك بالأمر Delete و حتى لو تم عمل إعادة تهيئة أو تشكيل للقرص الصلب بإستخدام الأمر Format و البرامج التي تم إتلافها أو إخفائها، سواء كانت صورا أو رسوماً أو كتابات أو غيرها[596]، مما يعني صعوبة إخفاء الجاني لجريمته أو التخفي منها، عن أعين الأمن والعدالة، طالما تم علم ضباط البحث و التحقيق الجنائي بوقوع الجريمة .

البند السادس : الأدلة الجنائية الرقمية ذات طبيعية ديناميكية فائقة السرعة تنتقل من مكان لأخر عبر شبكات الاتصال متعدية لحدود الزمان و المكان.

---

[594]- **رشيدة بوكر**، مرجع سابق، ص 388.

[595]- **عبد الناصر محمد محمود فرغلي**، مرجع سابق، ص 15.

[596]- **عبد الناصر محمد محمود فرغلي**، نفس المرجع ص 16.

البند السابع : يمكن من خلال الدليل الرقمي رصد المعلومات عن الجاني وتحليلها في ذات الوقت فالدليل الرقمي يمكنه أن يسجل تحركات الفرد، كما أنه يسجل عاداته و سلوكياته و بعض الأمور الشخصية عنه[597]، لهذا فإن البحث الجنائي قد يجد غايته بسهولة أيسر من الدليل المادي.

إضافة إلى خصائص أخرى قد يتميز و ينفرد بها الدليل الرقمي أو التقني.

الفرع الثالث: صور الدليل التقني

الدليل التقني له صور مختلفة و متنوعة و ذلك قد يرجع إلى طبيعته التي تقتضي ضرورة توافقه مع الواقعة الإجرامية و مع أماكن تواجده، و هي نفس الأماكن التي يمكن الحصول أو استخراج الدليل الرقمي منها، و على ذلك تقسم الأدلة الإلكترونية إلى:

قسمها البعض[598] إلى الأقسام الرئيسية الآتية:

- أدلة رقمية خاصة بأجهزة الحاسب الآلي و شبكاتها
- أدلة رقمية خاصة بالشبكة العالمية" الانترنت"
- أدلة رقمية خاصة ببروتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات[599].

و بتنوع الدليل الإلكتروني يفيد أن طرق الحصول عليه كذلك متنوعة بتنوع البيئة التي يوجد بها، و أن الحصول عليه يتطلب فحص الأنظمة المعلوماتية بإستعمال تطبيقات و برامج [600] معينة مخصصة لهذا الغرض.

المطلب الثاني: إجراءات جمع الدليل التقني

تمثل قواعد الإثبات أهمية خاصة، إذ إن الحق موضوع التقاضي يتجرد من كل قيمة إذا لم يقم الدليل عليه و هذا الأخير هو النتيجة التي تحققت باستعمال وسائل الإثبات على الواقعة التي يستند إليها، فالدليل هو جوهر الواقعة.

---

[597]- **رشيدة بوكر**، مرجع سابق، ص 388.

[598]– د. **عبد الناصر محمد محمود فرغلي، و د.محمد عبيد سيف سعيد المسماري**، مرجع سابق، ص 14.

[599]– **أميرة محمود بدوي الفقي**، مرجع سابق، ث 156.

[600]– **عائشة بن قارة مصطفى**، مرجع سابق، ص 57.

و الإثبات المراد به في محل دراستنا هو القواعد المتعلقة بالبحث عن الأدلة و إقامتها أمام القضاء وتقديرها و بالتالي فإن الإثبات في المواد الجنائية ما هو إلا كافة الأدلة التي تؤكد وقوع الجريمة، و تحقق حالة اليقين لدى القاضي لإدانة المتهم، أو ترجح حالة الشك لديه فيقضي بالبراءة.

وحتى يتحقق الدليل اللازم للإثبات فإنه لا بد من جمع عناصر التحقيق و الدعوى، وتقديم هذه العناصر إلى سلطة التحقيق الابتدائي، فإذا أسفر هذا التحقيق عن دليل أو أدلة ترجح معها إدانة المتهم قدمته إلى المحكمة، ومرحلة المحاكمة هي أهم المراحل لأنها مرحلة الجزم بتوافر دليل أو أدلة يقتنع بها القاضي بإدانة المتهم و إلا قضى ببراءته.

إن التطور التقني في أنظمة المعالجة الآلية و في البيئة الرقمية لا شك أنه سيؤدي إلي تغيير كبير، إن لم يكن كليا في المفاهيم السائدة حول الدليل و إجراءات جمعه و الحصول عليه، الأمر الذي سيستدعي إلى إعادة النظر في بعض المفاهيم و إجراءات التقليدية المحددة في قانون الإجراءات الجزائية كالتفتيش و معاينة بيئة الجريمة(فرع أول)، خاصة و أن بيئة الدليل التقني تختلف عن البيئة التقليدية، هذا فضلا عن استحداث إجراءات تتلاءم و ضبط الدليل الرقمي (فرع ثاني)، و يقود مثل هذا القول في الحقيقة إلى إعادة تطوير قواعد الإثبات الجنائي لمواجهة جرائم التطور التقني، و ضرورة الاستعانة بالمختصين و أصحاب خبرة في مجال النزاع.

الفرع الأول: الإجراءات التقليدية للاستدلال و دورها في جمع الدليل التقني

يصعب حتى هذا الوقت و في غالبية الأنظمة القانونية أن نحدد إلى أي مدى تكفي الأساليب التقليدية لإجراءات جمع الأدلة من أجل مباشرة تحقيقات ناجحة في مجال الجرائم الأمن المعلوماتي، و لا تقف صعوبة إثبات جرائم المساس بقواعد الأمن المعلوماتي عند تعذر الوصول إلى الأدلة التي تكفي لإثباتها، وإنما تمتد هذه الصعوبة لتشمل إجراءات الحصول على هذه الأدلة، فإذا كان من السهل على جهات التحري أن تتحرى عن الجرائم التقليدية عن طريق المشاهدة والتتبع والمساعدة فإنه قد يصعب عليها القيام بهذا التحري وبهذه الطرق بالنسبة للجرائم التي ترتكب بالوسائل الإلكترونية و عبر وسائل الاتصال الحديثة؛

فلا شك أن المجرمين الذين يرتكبون جرائمهم بالوسائل الإلكترونية الحديثة من فئة الأذكياء الذين يضربون سياجا أمنيا على أفعالهم غير المشروعة قبل إرتكابها لكي لا يقعوا تحت طائلة العقاب، فهم قد يزيدون من صعوبة إجراءات التفتيش التي يتوقع حدوثها للبحث عن الأدلة التي قد تدينهم بإستخدام

كلمات السر التي لا تمكن غيرهم من الوصول إلى البيانات المخزنة إلكترونياً أو المنقولة عبر شبكات الاتصال، وقد يلجأ هؤلاء المجرمون أيضا إلى استخدام الرمز أو التشفير لتعمية البيانات و المعلومات المستخدمة في أفعالهم بحيث قد يستحيل على غيرهم الاطلاع عليها ويتعذر على جهات التحري والضبط الوصول إلى كشف أفعالهم غير المشروعة .

إضافة إلى صعوبات كثيرة قد تعترض الحصول على الأدلة التقنية أو الالكترونية، و من ذلك انه قد يتعذر اتخاذ إجراءات التفتيش لضبط هذه الجرائم عندما يكون الحاسب الآلي متصلا بحاسبات أخرى قد تكون في أماكن متعددة داخل الوطن أو خارج الدولة، ويكون تفتيش هذه الحاسبات ضروري لكشف الستار عما تشتمله من جرائم، وهذا يثير مشكلات عديدة مثل تتبع الاتصالات الإلكترونية من طرف سلطات التحقيق لأجل إقامة الدليل على الجرائم التي ترتكب في مجال فضاء الإنترنت.

و قد يكون اختلاف التشريعات فيما بينها فيما يتعلق بشروط قبولها للأدلة و تنفيذ بعض الإجراءات مثل التفتيش عبر الحدود يثير مشكلات عديدة قد تعوق اتخاذ الإجراءات اللازمة لضبط هذا النوع من الجرائم العابرة للحدود، فعلى الرغم من أن الثورة التكنولوجية في مجال الاتصالات عن بعد قد أفرزت العديد من الجرائم ذات الطبيعة الخاصة، إلا أن إجراءات البحث عن هذه الجرائم وضبطها لزالت تتم في إطار النصوص الإجرائية التقليدية التي وضعت لكي تطبق على الجرائم التقليدية ، الأمر الذي ستترتب عليه الكثير من المشكلات بالنسبة لضبط هذه الجرائم المستجدة ذات الكيان المعنوي و التي قد تتعدد أماكن ارتكابها داخل الدولة الواحدة، أو يمتد نطاقها ليشمل الكثير من الدول عبر شبكة الإنترنت، فيتعذر تبعا لذلك اتخاذ إجراءات جمع الدليل بالنسبة لها، أو قد تلحق عدم المشروعية بهذه الإجراءات.

و مما لا شك فيه أن المشرع لم يجز استخلاص الدليل من غير ضوابط تحكم ذلك عن طريق قواعد إجرائية معينة أهمها: المعاينة، الخبرة، التفتيش وضبط الأشياء ، إلا أنها قد تكون بحاجة إلى تطوير لكي تتناسب مع الطبيعة الخاصة لجرائم المساس بأنظمة المعالجة الآلية للمعطيات وطبيعة الدليل الذي يصلح لإثباتها و هو ما سوف نعرفه من خلال الإجراءات التالية:

البند الأول: المعاينة التقنية

يقصد بالمعاينة إثبات حالة الأماكن و الأشياء و الأشخاص، و كل من يعتبر في كشف الحقيقة[601]، و المعاينة بهذا المعنى تستوجب الإنتقال إلى محل الواقعة أو إلى محل أخر توجد به أشياء أو أثار يرى المحقق لها صلة بالجريمة.

---

[601]- **د. خيرت علي محرز**، التحقيق في جرائم الحاسب الآلي، دار الكتاب الحديث، القاهرة، 2012، ص 59.

و هي إجراء يمكن اللجوء إليه في كافة الجرائم و يرى البعض [602] أن أهمية المعاينة تتضاءل في الجريمة المعلوماتية وذلك لندرة تخلف آثار مادية عند ارتكاب الجريمة المعلوماتية، كما أن طول الفترة بين وقوع الجريمة أو ارتكابها و بين اكتشافها قد يكون له تأثير سلبي على الآثار الناجمة عنها بسبب العبث أو المحو أو التلف لتلك الآثار.

و في كل الأحوال عند تلقي بلاغ عن وقوع إحدى الجرائم الماسة بقواعد الأمن المعلوماتي أو المساس بأنظمة المعالجة الآلية للمعطيات و بعد التأكد من البيانات الضرورية في البلاغ يتم الانتقال إلى مسرح الجريمة لمعاينته، ولا شك أن مسرح الجريمة المستحدثة يختلف عن مسرح الجريمة التقليدية كالقتل والسرقة.

و الجريمة المعلوماتية قد تكون جريمة مستمرة كما في حالة الجرائم الاقتصادية – السرقة والاحتيال– و قد يكون مسرحها كالجرائم الأخرى كما في التزوير و إتلاف البرامج و تفجير المباني والمنشآت، ففي حالة الجريمة المستمرة ذات الأهداف الاقتصادية تكون المعاينة هدفها المداهمة و ضبط الأدلة على الطبيعة، و في الحالة الثانية و بعد وقوع الجريمة فالأمر متوقف على اعترافات المتهمين متى تم القبض عليهم و كذلك شهادة الشهود و القرائن غير أنه عند إجراء المعاينة بعد وقوع الجريمة في المجال الإلكتروني فيجب مراعاة الضوابط[603] التالية:

1) تصوير الحاسب و الأجهزة الطرفية المتصلة به، على أن يتم تسجيل وقت و تاريخ و مكان التقاط كل صورة.
2) إخطار الفريق الذي سيتولى المعاينة قبل موعدها بوقت كاف حتى يستعد من الناحية الفنية و العملية، وذلك لكي يضع الخطة المناسبة لضبط أدلة الجريمة حال معاينتها
3) إعداد خطة المعاينة، موضحة بالرسومات مع تمام المراجعة التي تكفل تنفيذها على الوجه الأكمل

1 -العناية بالطريقة التي تم بها إعداد النظام.

602- **د.هشام فريد رستم** – الجوانب الإجرائية للجرائم المعلوماتية، مرجع سابق، ص 59/د. **خيرت علي محرز** ، نفس المرجع، ص60.

603- د. **هلالي عبد اللاه أحمد** ، تفتيش نظم الحاسب الألي و ضمانات المتهم المعلوماتي، مرجع سابق، ص 45، 47/ د. **طارق إبراهيم دسوقي عطية** ، مرجع سابق، ص367./ **عبد الناصر محمد محمود فرغلي** ، مرجع سابق، ص 17./ **علي حسن محمد الطوالبة**، التفتيش الجنائي على نظم الحاسوب و الأنترنت، دراسة مقارنة، ط 1، عالم الكتب الحديثة، أربد– الأردن، 2004، ص 11.

كذلك: **أميرة محمود بدوي الفقي**، مرجع سابق، ص 592–596.

2 - ملاحظة و إثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عمليات المقارنة والتحليل حين عرض الأمر فيما بعد على المحكمة.

و المعاينة و إن كانت واردة في كل الجرائم، إلا أن أهميتها تتضاءل في بعض الجرائم مثل جريمة السب و الشتم فإن المعاينة فيهما غير ذات جدوى، أما معاينة الجرائم التقليدية والاطلاع على مسرح الجريمة فيها فيكون ذا أهمية متمثلة في تصور كيفية وقوع الجريمة وظروف وملابسات ارتكابها و توفر الأدلة المادية التي يمكن تجميعها عن طريق هذه المعاينة، لكن هذه المعاينة لا تؤدي ذات الدور في كشف غموض الجرائم الماسة بقواعد الأمن المعلوماتي و ضبط الأشياء التي قد تفيد في إثبات وقوعها ونسبتها إلى مرتكبها.

البند الثاني: التفتيش في البيئة الالكترونية

يجمع الفقه الجنائي على أن التفتيش هو إجراء من إجراءات التحقيق يباشر من موظف مختص يهدف إلى البحث عن أدلة مادية لجناية أو جنحة، تحقق وقوعها في محل يتمتع بحرمة المسكن أو الشخص، وذلك من أجل إثبات ارتكابها أو نسبتها إلى المتهم وفقا للضمانات والقيود القانونية المقررة [1].

و أن ضبط الأدلة هو النتيجة الطبيعية التي ينتهي إليها التفتيش والتي يتم الحصول عليها أثناءه.

و على ذلك فإنه يتضح أن هذين الإجرائيين ما هما إلا وسيلة للإثبات المادي، ذلك أن التفتيش يستهدف ضبط أشياء مادية تساعد في إثبات وقوع الجريمة وإسنادها إلى المتهم المنسوب إليه ارتكابها.

من أجل هذا فإن تفتيش نظم المعالجة الآلية يعد من أخطر المراحل حال اتخاذ الإجراءات الجزائية ضد مرتكب جرائم ضد الأمن المعلوماتي، لكون محل التفتيش فيها هو نظام المعالجة الآلية ذو الطابع غير المادي، ولا يعدو أن يكون إلا معلومات إلكترونية ليس لها أي مظهر مادي محسوس، فما مدى صلاحية مكونات نظام المعالجة الآلية لأن تكون محلا يرد عليه التفتيش و ما هي الأشياء المضبوطة في ظل التفتيش في عالم افتراضي؟.

أولا: قابلية الشبكات و مكونات الحاسب للتفتيش

يثور التساؤل حول إمكانية تطبيق القواعد العامة للتفتيش على صورة تفتيش نظم الحاسوب و الإنترنت، ذلك أن هذا الإجراء يهدف إلى جمع الأدلة المادية [604]، في حين أن النظم المعلوماتية عبارة

---

[604]- د. **علي حسن محمد الطوالبة**، نفس المرجع، ص 07.

عن كيان معنوي و لا تتوافر له صفة المادة سواء تعلق ذلك ببرامج حاسوب أم ما يشمل عليه من بيانات.

و من المعروف أن نظم المعالجة الآلية للمعطيات تتكون من عناصر مادية و أخرى غير مادية و ترتبط بغيرها عبر شبكات إتصال عن بعد على المستوى المحلي أو الدولي كما سبق بيانه في الفصل التمهيدي من هذه الدراسة.

و إذا كان التفتيش هو التنقيب في وعاء السر بقصد ضبط ما يفيد من الأسرار في كشف الحقيقة، و أن جوهره هو كشف نقاب السرية عما تحويه نظم المعالجة الآلية من خفايا و أسرار إجرامية، و بالتالي إزاحة ستار الكتمان عنها للاستفادة منها في معرفة الحقيقة[605].

و إذا كان هذا المعنى لا يتقيد بالكيان المادي لوعاء السر، فإن الأمر يتطلب منا البحث في مسألة المحل الذي ينصب عليه هذا الإجراء التحقيقي في مجال الإجراءات العلاجية لتحقيق الأمن المعلوماتي.

ثانيا: محل التفتيش

المحل في القانون عموما هو المال محل الحماية و الذي ينصب الفعل الإجرامي عليه [606]، و على ذلك يمكن وضع صورة للمحل الإلكتروني الذي هو موضوع جرائم أنظمة المعالجة الآلية للمعطيات أو المحل الذي بواسطته تتم الاعتداءات أو الجرائم المعلوماتية.

و عليه يمكن أن يعرف المحل الإلكتروني بأنه المال الموجود على الحاسب الآلي سواء في صورة معلومات أو بيانات إلكترونية، كذلك أي شكل يكون فيه موجودا سواء على أقراص صلبة أو اسطوانات تكون في طريقها للإدخال على الحاسب الآلي، فالمحل الإلكتروني هو أي مدخلات إلكترونية قابلة للتعامل و لها من القيمة المادية ما يجعلها قابلة للتملك و تكتسب الحماية القانونية[607].

و لا شك أن تفتيش أي محل مهما كانت طبيعته يخضع لما هو مقرر بنصوص قانون العقوبات و قانون الإجراءات الجزائية، حيث كفلت تلك النصوص ضمان بعض الخصوصية و حماية أسرار أصحابها من الكشف عنها.

---

[605]- **سعيداني نعيم** ، اليات البحث و التحري عن الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماجستير في العلوم القانونية تخصص قانون جنائي، كلية الحقوق و العلوم السياسية، جامعلة الحاج لخضر، باتنة، 2012-2013، ص 144.

[606]- **د.هشام فريد رستم**، مرجع سابق، ص 227، 228.

[607]- **ناير نبيل عمر** ، الحماية الجنائية للمحل الإلكتروني في الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، الإسكندرية- مصر، 2012، ص 32، 33.

و بالتالي كيف يكون التفتيش في المكونات المادية للمحل الإلكتروني و المكونات المعنوية له؟ نوضح ذلك فيما يأتي:

1 -**تفتيش العناصر المادية للمحل الإلكتروني:**

إن التفتيش الواقع على المكونات المادية للنظام المعالجة الآلية لا توجد فيه أي مشكلة في التنفيذ لإمكانية ذلك وسهولته، مع الأخذ بعين الاعتبار الإجراءات الخاصة بضبط هذه الأجهزة لحساسيتها وإمكانية إتلافها، و تأتي سهولة هذا التفتيش لأنه يرد على أشياء مادية لا خلاف حول خضوعها للتفتيش طبقا لقواعد قانون الإجراءات الجزائية الخاصة بإجراء تفتيش الأشياء و ذلك طبقا لنص المادة 44 من قانون الإجراءات الجزائية، حيث ورد فيها أن التفتيش يرد على الأشياء، وهي كلمة تنصرف في الأرجح على المكونات المادية و نفس القول ينصرف على ما جاءت به المادة 64 من نفس القانون بنصها:" ... لا يجوز تفتيش المساكن ... و ضبط الأشياء".

و على ذلك فإنه لا يوجد مانع قانوني من أن ينصب التفتيش على المكونات المادية للحاسوب وملحقاته أو معداته، و ذلك تبعا لطبيعة المكان الذي يتواجد فيه الحاسوب و هذه الملحقات، سواء من الأماكن العامة أو من الأماكن الخاصة، إذ أن لصفة المكان أهمية خاصة في مجال التفتيش، فإذا كانت خاصة كمسكن المتهم أو أحد ملحقاته كانت لها حكمه فلا يجوز [608] تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه و بنفس الضمانات المقررة قانونا.

إلا أن المشرع الجزائري بمناسبة التعديل الذي ألحقه على قانون الإجراءات الجزائية بالقانون 22/06 لسنة 2006 استثنى بموجب الفقرة الثالثة من المادة 45 و كذا الفقرة الثالثة من المادة 47 والفقرة الثالثة من المادة 64 تطبيق هذه الضمانات عند إجراء التفتيش بمناسبة تحقيق مفتوح بخصوص جرائم المساس بأنظمة المعالجة الآلية للمعطيات.

ويفهم من استقراء هذه المواد أن المشرع استثنى تطبيق ضمانات التفتيش على طائفة من الجرائم من بينها جرائم المساس بأنظمة المعالجة الآلية، و بذلك لا يشترط حضور الشخص الذي يشتبه في أنه

---

[608]– و هذا ما يستشف من نص **المادة 64 من ق إ ج** أنه:" لا يجوز تفتيش المساكن و معاينتها و ضبط الأشياء المثبتة للتهمة إلا برضا صريح من الشخص الذي ستتخذ لديه هذه الإجراءات....." و فضلا عن تطبيق ما ورد في المواد من **44 إلى 47** من نفس القانون.

ساهم في إرتكاب الجريمة عند تفتيش مسكنه [609]، و أنه يجوز القيام بإجراء التفتيش في كل ساعة من ساعات النهار أو الليل[610] و ودون حاجة إلى رضائه عند القيام بهذا الإجراء[611].

و إذا كان المشرع الجزائري قد استثنى تلك الضمانات في مجال هذا النوع من الجرائم التي قد تمس قواعد الأمن المعلوماتي إلا انه أخضع إجراء التفتيش و أباحه في هذه الحالة إلى صدور إذن من وكيل الجمهورية المختص.

و الملاحظ أن المشرع في هذه الحالة قد غلب المصلحة العامة في تحقيق القصاص على حريات الأفراد، و مرد ذلك قد يرجع إلى اعتبارين[612]:

- ذاتية الجريمة المعلوماتية المتمثلة في إمكانية اختفائها بسرعة فائقة.

- افتراض كون الدليل الرقمي هو الدليل الوحيد في الدعوى الجزائية ومن ثم ارتكاز كل العملية الإثباتية على وجوده.

2 -**تفتيش العناصر المعنوية للمحل الإلكتروني:**

أثار الضبط الذي يترتب على أعمال التفتيش و الذي يقع على مكونات وشبكات الحاسب الآلي مشكلات كثيرة، ذلك أن هذا الضبط و إن كان يتصور وقوعه بالنسبة لمكونات الحاسب المادية، وبالنسبة لشبكات الحاسب حيث يمكن رصد الاتصالات التي تتم خلالها وتسجيل محتوياتها إلا أن اتخاذه سيكون في منتهى الصعوبة بالنسبة للعناصر المعنوية للحاسب الآلي .

إذا كان الأمر قد حسم بشأن صلاحية المكونات المادية للنظم المعلوماتية كمحل يرد عليه التفتيش، فإن امتداد ذلك إلى مكوناته غير المادية هو محل جدل كبير حول مدى صلاحيتها لأن تكون موضوعا للتفتيش تمهيدا لضبط الأدلة، فالخلاف حاصل في مسألة أن التفتيش التحقيقي وسيلة للبحث عن الأدلة المادية، إذ هو إجراء يسعى إلى ضبط الأدلة المتعلقة بالجريمة لتقديمها إلى المحكمة

---

[609]- و ذلك بحسب ما جاء **في الفقرة الاخيرة من المادة 45 من *قانون الإجراءات الجزائية*** بقولها:" إذا وقع التفتيش في مسكن شخص يشتبه أنه ساهم في إرتكاب الجناية فإنه يجب أن يحصل التفتيش بحضوره.....لا تطبق هذه الأحكام إذا تعلق الأمر بجرائم المخدرات و الجريمة المنظمة عبر الوطنية و جرائم المساس بأنظمة المعالجة الآلية للمعطيات...."

[610]- بحسب ما جاء كذلك في ا ***لمادة 47 ف 3 من الأمر 155/66*** :" عندما يعلق الأمر بـ.....أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات .....فإنه يجوز إجراء التفتيش..... في كل محل مسكن أو غير سكني في كل ساعة من ساعات النهار أو الليل..."

[611]- المادة 64 من نفس الأمر"لا يجوز تفتيش الأماكن و معاينتها أو ضبط الأشياء المثبة للتهمة إلا برضا صريح من الشخص الذي ستتخذ لديه هذه الإجراءات ..... وتطبق فضلا عن ذلك أحكام ***المواد 44 إلى 47 من هذا القانون*** " أي عدم تطبيق الضمانات الواردة بهذه المادة بخصوص التفتيش المتعلق بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

[612]- **رشيدة بوكر**، مرجع سابق، ص 396.

المختصة كدليل إدانة، لذلك يثور الشك والتساؤل حول إمكانية إعتبار البحث عن أدلة الجريمة المعلوماتية في نطاق العناصر المعنوية للنظم المعلوماتية نوعا من التفتيش؟ باعتبار أن البيانات الإلكترونية أو البرامج في حد ذاتها ليس لها مظهر مادي محسوس في المحيط الخارجي و يستشعر الفقه صعوبة المسألة نظرا لغياب الطبيعة المادية للمعلومات في ذاتها مجردة من دعامتها المادية[613].

و لقد أختلف الرأي بشأن ضبط الأشياء المعنوية من مكونات الحاسب الآلي إلى اتجاهين، **فذهب رأي** إلى جواز ضبط البيانات الإلكترونية بمختلف أشكالها، ويستند هذا الرأي في ذلك إلى أن القوانين الإجرائية عندما تنص على إصدار الإذن بضبط "أي شيء" فإن ذلك يجب تفسيره بحيث يشمل بيانات الحاسب المحسوسة وغير المحسوسة؛

و أن برامج الحاسوب يمكن أن تنطبق عليها خصائص وسمات المادة، و بالتالي تدخل في نطاق الأشياء المادية[614] و يستوي في ذلك أن تكون برامج نظام أو برامج تطبيقات، و بناءا عليه فإن الكيان المنطقي للحاسوب أو البرنامج يشغل حيزا ماديا في ذاكرة الحاسوب ويمكن قياسه [615] بمقياس معين هو البايت (Byte) والكيلوبايت (kb) والميغابايت(MB)، و بذلك يكون هذا الإتجاه قد وسع من مفهوم الشيء ليشمل الأشياء المادية و غير المادية.

بينما **ذهب رأي** آخر و تمثلت فكرته في عدم إمكانية إنسجام وتطابق أحكام التفتيش في القانون الجنائي الإجرائي مع ما قد يتطلبه كشف الحقيقة في الجرائم المعلوماتية من بحث وتنقيب عن الأدلة

---

[613]- **موسى مسعود أرحومة** ، الإشكالات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، بحث مقدم إلى المؤتمر المعاربي الأول حول المعلوماتية و القانون، المنعقد بتاريخ 28-29 من شهر أكتوبر 2009، أكادمية الدرسات العليا، طرابلس، ليبيا، ص 08.

[614]- يذهب رأي فقهي إلى أنه في تحديد مدلول الشيء بالنسبة لمكونات الحاسب الآلي يجب عدم الخلط بين الحق الذهني للشخص على البرامج والكيانات المنطقية وبين طبيعة هذه البرامج والكائنات، وإنما يتعين الرجوع في ذلك إلى تحديد مدلول كلمة المادة في العلوم الطبيعية، فإذا كانت المادة تعرف بأنها كل ما يشغل حيزا ماديا في فراغ معين وأن الحيز يمكن قياسه والتحكم فيه، و كانت الكيانات المنطقية أو البرامج تشغل حيزا ماديا في ذاكرة الحاسب الآلي ويمكن قياسها بمقياس معين، و أنها أيضا تأخذ شكل نبضات إلكترونية تمثل الرقمين صفر أو واحد، فإنها تعد طبقا لذلك ذات كيان مادي وتتشابه مع التيار الكهربائي الذي اعتبره الفقه والقضاء في فرنسا من قبيل الأشياء المادية.

ولقد ذهبت محكمة باريس الإبتدائية إلى ذلك عندما قضت بأنه لا يوجد اختلاف في الطبيعة بين مستخرجات البرامج وبين البرامج المستغلة:" Il n y Pas de différence de nature entre les programmes produits et les programmes d' exploitation"

TGI Paris, 1re ch., 21 août 1983, voir **Hubert Bitan ,** Droit des créations immatérielles: logiciels, bases de données, autre œuvres sur la web, Ed Lamy, France, 2010, P352.

[615]- د.**هلالي عبد اللاه أحمد** ، تفتيش نظم الحاسوب الآلي وضمانات المتهم المعلوماتي- دراسة مقارنة، دار النهضة العربية، القاهرة-مصر، 2006 ، ص 75،76 و 201.

في برامج الحاسوب و بياناته، ذلك أن التشريعات الإجرائية قد حددت هدف التفتيش في البحث عن الأشياء وضبطها، وهذا الشيء يقتصر بمفهومه على المال المادي المحسوس و لا يمتد في نطاق شموله إلى الكيانات المنطقية [616]، أو إلى عدم انطباق المفهوم المادي على بيانات الحاسب غير المرئية أو غير الملموسة، و لذلك فإنه يقترح مواجهة هذا القصور التشريعي بالنص صراحة على أن تفتيش الحاسب الآلي لا بد أن يشمل "المواد المعالجة عن طريق الحاسب الآلي أو بيانات الحاسب الآلي"، بحيث تصبح الغاية الجديدة من التفتيش بعد التطور التقني الذي حدث بسبب ثورة الإتصالات عن بعد تتركز في البحث عن الأدلة المادية أو أي مادة معالجة بواسطة الحاسب أو أنظمة المعالجة الآلية.

وقد عملت بعض الدول التي أخذت بهذا الاتجاه إلى حماية هذه الكيانات المنطقية عبر قوانين الملكية الفكرية[617].

بيد أن النصوص القانونية التي وضعت القواعد التي تحكم التفتيش تم سنها قبل ظهور و إنتشار النظم المعلوماتية، لكن تقدم الفكر البشري و التطور الذي رافقه أظهر للوجود قيما إقتصادية و أشياء غير مادية ليس لها حيز محسوس، لذلك فأيا كانت المبررات التي ساقها معتنقوا المساواة بين الكيان المادي و نقيضه فإن طبيعة البيانات والمعطيات المعالجة تتطلب قواعد خاصة تحكمها بدلا من محاولة تطويع القواعد التقليدية وتوسيع نطاقها، و هذا يتأتى من خلال إجراء تعديل عليها و تضمينها نصوص صريحة من شأنها توسيع نطاق الأشياء التي تكون مشمولة بالتفتيش وتضمينها من الأحكام بما يتلاءم ومتطلبات هذه التقنية الجديدة.

و هذا ما عمل به المشرع الجزائري كغيره من المشرعين حينما أجاز تفتيش هذه النظم من خلال ما جاء به في المادة 05 من القانون رقم 09-04 السالف الذكر و المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها، التي نصت على أنه يجوز للسلطات القضائية المختصة و كذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية.... الدخول بغرض التفتيش و لو عن بعد إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها و كذا منظومة تخزين معلوماتية .

---

[616]- د. **عبد الله حسين علي محمود** ، سرقة المعلومات المخزنة في الحاسب الآلي، ط 4، دار النهضة العربية، القاهرة- مصر، بدون تاريخ ، ص 362-365.

[617]- مشار إليه لدى، **علي حسن محمد الطوالبة**، مرجع سابق، و **رشيدة بهكر**، مرجع سابق، ص 397.

إلى جانب المشرع الجزائري نجد المشرع الفرنسي الذي نص على هذا الإجراء و قام بتعديل النصوص التي تحكم التفتيش من خلال المادة 94 من قانون الإجراءات الجزائية[618] بموجب المادة 42 من القانون رقم 545/2004 المؤرخ في 21/06/2004 المتعلق بالثقة في الإقتصاد الرقمي ليصبح نص هذه المادة 94 على النحو التالي:" يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء أو معطيات معلوماتية يكون كشفها مفيدا لإظهار الحقيقة ".

و هذا ما كانت قد نصت عليه إتفاقية بودابست بشأن الإجرام المعلوماتي و التي أقرت ذلك بموجب المادة 19 على أنه يجب على كل دولة طرف أن تتبنى الإجراءات التشريعية و أية إجراءات يرى أنها ضرورية من أجل تخويل سلطاتها المختصة سلطة التفتيش أو الولوج بطريقة مشابهة:

– لنظام معلوماتي أو لجزء منه و كذلك للبيانات المعلوماتية المخزنة فيه و على أرضه.

– لدعامة تخزين معلوماتية تسمح بتخزين البيانات معلوماتية...[619]

و يمكن التعقيب على ما سبق في أن المشكلة التي تثيرها الجرائم التي تقع على الكيان المعنوي للحاسب الآلي أو أنظمة المعالجة الآلية للمعطيات قد تتعلق بإثبات الجرائم التي تقع عليها، فالضبط الذي قد يقع بسبب التفتيش لا يتصور وقوعه إلا إذا تبين أن هناك جريمة قد ارتكبت، ولذلك فإن الجرائم التي ترتكب على الكيانات المادية يسهل اكتشافها و ضبطها، و أما الجرائم التي تقع على الكيانات المعنوية فإنه يصعب اكتشافها إذا ظلت على صورتها المعنوية في شكل نبضات أو ذبذبات إلا بمحض الصدفة في غالب الأحيان.

3 -**التفتيش عن بعد :** تعرف الشبكة المعلوماتية بأنها مجموعة مكونة من إثنين فأكثر من أجهزة الحاسوب و المتصلة ببعضها اتصالا سلكيا أو لا سلكيا[620] .

و قد تكون الأجهزة موجودة في نفس الموقع وتسمى بالشبكة المحلية، و قد تكون موزعة في أماكن متفرقة يتم ربطها عن طريق خطوط الهاتف تسمى بالشبكة بعيدة المدى و مع التطور التكنولوجي لثورة الاتصالات لم يعد نطاق الإتصالات محدودا في إقليم دولة واحدة، بل إمتد ليشمل كل أرجاء العالم بعد ظهور شبكة الأنترنات والتي هي عبارة عن منظومة واسعة جدا من شبكات المعلومات

---

[618] -**Art** 42 du L.C.E.N dispose que ; « A l'article 94 du code de procédure pénale, après les mots ; « des objets » sans insérés les mots « ou des données informatiques ».

[619]- د. **هلالي عبد اللاه أحمد**، الجوانب الموضوعية و الإجرائية لجرائم المعلوماتية، مرجع سابق، ص 225–227.

[620]– **علي حسن محمد الطوالبة**، المرجع السابق.، ص 34 .

الحاسوبية المتصلة مع بعضها البعض بطريقة لا مركزية، ويدخل في تركيب هذه الشبكة ملايين الحواسيب الموزعة عبر مختلف دول العالم.

و السؤال المطروح في هذا الصدد يتعلق بمدى خضوع شبكات نظام المعالجة الآلية للتفتيش و هي مسألة على درجة كبيرة من الخطورة تتعلق بالتفتيش عن بعد و ذلك نتيجة للطبيعة التكنولوجية الرقمية التي تسمح بتوزيع المعلومات التي تحتوي أدلة عبر شبكات حاسوبية في أماكن مجهولة بعيدا تماما عن الموقع المادي للتفتيش، فقد يكون الموقع الفعلي للشبكات داخل إختصاص قضائي آخر وحتى في بلد آخر، وهو ما يزيد المسألة تعقيدا بإعتبار أن الشبكة المعلوماتية ممتدة في أرجاء العالم تقريبا، وبالتالي فإن الحاسوب أو النهاية الطرفية التي يمكن أن ترتكب عليها أو بواسطتها الجريمة المعلوماتية تخضع للقانون الإجرائي الخاص بتلك المنطقة.

لذلك يثار التساؤل حول أثر تفتيش الأنظمة المعلوماتية المتصلة بالنظام المأذون بتفتيشه إذا تواجدت في دوائر اختصاص مختلفة؟ ونستطيع أن نميز في هذه الصورة بين احتمالين على النحو التالي:

1/3. **إتصال حاسب المشتبه فيه أو المتهم بحاسب آخر أو نهاية طرفية موجودة في مكان آخر داخل الدولة:** و هنا يثور التساؤل حول مدى إمكانية إمتداد الحق في التفتيش إلى أجهزة الحاسوب المتصلة بجهاز المشتبه فيه أو المتهم.

وفي هذه الحالة عمدت بعض التشريعات الإجرائية إلى حل هذه المشكلة من خلال نصها على إجازة تفتيش نظم المعلومات المتصلة بالحاسوب الذي يجرى تفتيشه أي الشبكة و ما يتصل بها، وتسجيل كل البيانات اللازمة كأدلة إثبات لإدانة المتهم أمام المحكمة.

و يعتبر المشرع الجزائري من بين هذه التشريعات حين نصت الفقرة الثانية من المادة الخامسة من القانون 09/04 بأنه في حالة تفتيش منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها إذا كانت هناك أسباب تدعو للإعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى و أن هذه المعطيات يمكن الدخول إليها إنطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك... ".

إلى جانب المشرع الجزائري نجد كذلك المشرع الفرنسي من قبله قد فصل في هذه المسألة بإضافته للمادة 57-1 إلى قانون الإجراءات الجزائية و ذلك بموجب المادة 17-1 من القانون رقم 2003-

239 بشأن الأمن الداخلي، حيث أجاز المشرع لرجال الضبط القضائي الدخول من الجهاز الرئيسي على المعلومات التي تهم البحث و التحري، و في إطار التفتيش المنصوص عليه الدخول عن طريق الأنظمة المعلوماتية المثبة في الأماكن التي يتم فيها التفتيش على المعطيات التي تهم التحقيق و المخزنة في النظام المذكور أو أي نظام معلوماتي أخر[621]

و قبل ذلك نصت اتفاقية بودابست لعام 2001 على هذا الأمر و أجازت للدول الأعضاء أن تمد نطاق التفتيش الذي كان محله جهاز كومبيوتر معين إلى غيره من الأجهزة المرتبطة به في حال الاستعجال[622] إذا كان يتواجد به معلومات يتم الدخول إليها في هذا الجهاز من خلال الجهاز محل التفتيش

2/3.إتصال بحاسب المشتبه فيه أو المتهم بحاسب آخر أو نهاية طرفية موجودة في مكان آخر خارج الدولة: من المتصور طبقا لهذا الإحتمال أن يقوم مرتكبوا الجرائم بتخزين بياناتهم و معلوماتهم في أنظمة معلوماتية خارج الدولة عن طريق شبكات الإتصال الدولية و إحاطتها بالحماية الفنية بهدف إعاقة محاولة الوصول إليها و عرقلة سلطات التحقيق في جمع الأدلة[623].

و هذه من المشاكل الحقيقية التي تواجه جهات التحقيق في جمع الأدلة، إذ يتطلب إمتداد الإذن بالتفتيش إلى خارج الإقليم الجغرافي للدولة التي صدر عن جهاتها المختصة الإذن بالتفتيش، ودخوله في النطاق الجغرافي لدولة أخرى، وهو ما يسمى بالتفتيش العابر للحدود، وقد يتعذر القيام به بسبب تمسك كل دولة بسيادتها وحدودها الإقليمية..

إن جانبا من الفقه يرى أن التفتيش الإلكتروني العابر للحدود ينبغي أن يتم في إطار إتفاقيات تعاون خاصة ثنائية أو دولية تجيز هذا الإمتداد، و أنه لا يجوز القيام به في ظل غياب تلك الإتفاقيات[624].

---

[621] - **Art 57-1 alinéa 1 de C.P.P.F** dispose que ; « Les officiers de police judiciaire ou, sous leur responsabilité, les agents de police judiciaire peuvent, au cours d'une perquisition effectuée dans les conditions prévues par le présent code, accéder par un système informatique implanté sur les lieux où se déroule la perquisition à des données intéressant l'enquête en cours et stockées dans ledit système ou dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial… » Créé par ***Loi n° 2003-239 pour la sécurité intérieure 2003-03-18 art. 17 1° JORF du 19 mars 2003.***

[622]- حسب ما جاء في الفقرة الثانية من المادة 19 من اتفاقية بودابست للإجرام المعلوماتي لسنة 2001.

[623]– **عبد الله حسين علي محمود،** مرجع سابق، ص338.

[624]– مشار إليه لدى: **رشيدة بوكر**، مرجع سابق، ص 404.

عمل المشرع الجزائري على مواجهة هذا الأمر حيث قد أجاز تفتيش الأنظمة المتصلة حتى و لو كانت متواجدة خارج الإقليم الوطني، و هو ما أورده بالفقرة الثالثة من نص المادة 05 من القانون09/04 بقولها: ".... إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها إنطلاقا من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للإتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل".

و لعل هذه الفقرة مأخوذ نصها من الفقرة الثانية(2) من المادة 57-1 من قانون الإجراءات الجزائية الفرنسي[625].

و لكن طالما أن التفتيش عن بعد يمتد إلى إقليم بلد أجنبي فإن الأمر يستلزم بالضرورة الدخول في إطار بحث هذا الإختراق المباشر على مستوى الدول كافة بإعتباره إجراء عابرا للحدود كما سبق بيانه، و هو الأمر الذي لا يخلو من ضرورة التوصل إلى إتفاق دولي يضمن التعاون الدولي فيما بين السلطات المختصة، و القول بغير ذلك يجعل من هذا الإجراء تهديدا لسيادة الدول، و هذا ما نصت عليه الإتفاقية العربية بشأن مكافحة جرائم تقنية المعلومات المحررة بالقاهرة سنة 2010 و التي صادقت عليها الجزائر في 2014 من أجل المساعدة المتبادلة بين الدول العربية المصادقة على هذه الإتفاقية.

كذلك فإن الاتفاقية الأوروبية الخاصة بالإجرام المعلوماتي أجازت إمكانية الدخول بغرض التفتيش إلى أجهزة و شبكات تابعة لدولة أخرى بدون إذ منها في حالتين

- إذا تعلق التفتيش بمعلومات أو بيانات مباحة للجمهور.
- إذا رضي صاحب أو حائز هذه المعلومات بهذا التفتيش[626].

ثالثا: شروط التفتيش في البيئة الرقمية

---

[625] - Art 57-1 alinéa 2 de C.P.P.F dispose que ; « S'il est préalablement avéré que ces données, accessibles à partir du système initial ou disponibles pour le système initial, sont stockées dans un autre système informatique situé en dehors du territoire national, elles sont recueillies par l'officier de police judiciaire, sous réserve des conditions d'accès prévues par les engagements internationaux en vigueur.. » » Créé par ***Loi n° 2003-239 pour la sécurité intérieure 2003-03-18 art. 17 1° JORF du 19 mars 2003***

[626]- **المادة 32 من إتفاقية بودابست** لسنة 2001 بشأن الإجرام المعلوماتي المشار إليها سابقا.

يعد التفتيش من الإجراءات الماسة بحق الخصوصية و تقيدا للحرية الفردية، لذلك عمدت القوانين الإجرائية على إحاطة هذا الإجراء بشروط لازمة لصحته و ضمانات أساسية بهدف تحقيق موازنة بين مصلحة المجتمع في عقاب المجرم، و بين حقوق الأفراد وحرياتهم ، و من لشروط و الضمانات التي يجب توافرها منها ما هو موضوعي ومنها ما هو شكلي على النحو الآتي:

1 -**الشروط الشكلية للتفتيش في البيئة الرقمية**

إن القواعد الشكلية لا تهدف إلى تحقيق مصلحة العدالة في ضمان صحة الإجراءات التي تتخذ لجمع الأدلة فحسب، و إنما تقيم بالإضافة إلى مقتضيات الإجراء سياجا يحمي الحريات[627]الفردية و من أبرز هذه الشروط ما يأتي:

أ. إجراء التفتيش بحضور أشخاص معينين بالقانون: إن التفتيش فيه إطلاع على أسرار الغير التي تحرم أغلب التشريعات الإجرائية الإطلاع عليها، لذلك أوجبت التشريعات حضور أشخاص معينين في القانون في حالات معينة، و أجازت في أحوال أخرى إجراء التفتيش دون حضور أحد، و كان المشرع الجزائري من التشريعات الإجرائية التي أوجبت ضرورة حصول إجراء التفتيش المتعلق بالمساكن وملحقاتها بحضور المشتبه فيه عندما يتم تفتيش مسكنه من طرف الضبطية القضائية، وإن تعذر ذلك بإمتناعه عن حضور التفتيش أو كان هاربا يتم هذا الإجراء بحضور شاهدين من غير الموظفين الخاضعين لسلطة ضابط الشرطة القضائية القائم بالتفتيش[628] و ذلك لضمان الاطمئنان إلى سلامة الإجراء و صحة الضبط.

إلا أنه و بموجب التعديل الذي ألحقه على قانون الإجراءات الجزائية بالقانون 06/22 استثنى تطبيق هذا الشرط و بعدم حضور المشتبه فيه أو الشاهدين عندما يتعلق الأمر ببعض الجرائم و منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات [629]، و هو ما يعد إقرارا من المشرع بذاتية هذا النوع من الجرائم و ما يتطلبه التحقيق بشأنها من إحاطتها بنوع من السرية أثناء جمع الدليل الرقمي و القيام بالإجراءات الضرورية بالإضافة إلى الإسراع في استخلاصه قبل فقدانه.

ب. **الميعاد الزمني لإجراء التفتيش في البيئة الرقمية**:

---

[627]– **علي حسن الطوالبة**، مرجع سابق، ص 47.

[628]– المادة **45 من قانون الإجراءات الجزائية الجزائري** المشار إليه سابقا

[629]– نصت **المادة 45 في فقرتها الأخيرة من قانون الإجراءات الجزائية الجزائري** و المعدلة بالامر06–22 على أنه:" لا تطبق هذه الأحكام إذا تعلق الأمر بجرائم....و الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ....."

دائما في إطار المحافظة على حق الخصوصة و حرمة المساكن عمدت التشريعات على تحديد أوقات معينة ليتم فيها التفتيش قانونا، غير أن التشريعات الإجرائية قد اختلفت في وقت تنفيذ التفتيش، فمنها ما يحظر تفتيش المساكن ليلا إلا في أحوال معينة، ومنها لم يقيد القيام بهذا الإجراء بوقت معين وترك الأمر لتقدير القائم بالتفتيش لإختيار الوقت الملائم لتنفيذه ضمن المدة المحددة بالإذن[630].

و أن المشرع الجزائري عمد إلى حضر تفتيش المساكن و ما في حكمها في أوقات معينة وحدد ميقات تنفيذ هذا الإجراء من الساعة الخامسة صباحا إلى الساعة الثامنة مساءا[631].

إلا أن هناك حالات استثنائية يجوز فيها الخروج عن هذه المواعيد و يصح إجراء التفتيش في أي ساعة من ساعات الليل و النهار عندما يتعلق الأمر بالتحقيق في الجرائم المنصوص عليها بالمواد 342 إلى348 من قانون العقوبات المرتكبة في أماكن معينة أو في حالة رضا صاحب المسكن صراحة أو في حالة الاستغاثة بحسب ما جاء في المادة 47 من قانون الإجراءات الجزائية.

أما في نطاق التفتيش المتعلق بالجرائم الماسة بأنظمة المعالجة الآلية فإن الاستثناء الوارد بالفقرة الثالثة من المادة 47 من نفس القانون و المتعلقة بجواز إجراء ضابط الشرطة القضائية للتفتيش في كل ساعة من ساعات الليل أو النهار عندما يتعلق التحقيق بنوع معين من الجرائم، من بينها جرائم الأمن المعلوماتي حيث جاء في نصها".... عندما يتعلق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و ... فإنه يجوز إجراء التفتيش... في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناءا على إذن مسبق من وكيل الجمهورية المختص".

2-الشروط الموضوعية للتفتيش في البيئة الرقمية : إضافة إلى الشروط الشكلية المحددة سابقا يمكن تحديد القواعد الموضوعية لتفتيش النظم الرقمية والتي تعد الضوابط اللازمة لإجراء تفتيش صحيح و ذلك فيما يأتي:

أ. **سبب التفتيش:** إن سبب التفتيش في القواعد التقليدية العامة بوصفه إجراء من إجراءات التحقيق هو وقوع جريمة و إتهام شخص أو عدة أشخاص بارتكابها أو المساهمة فيها، و توافر أمارات و قرائن قوية

---

[630]- مشار إليه لدى : **رشيدة بوكر** ، مرجع سابق، ص 415/ و **نعيم سعيداني**، مرجع سابق، ص 153.

[631]- المادة **47 من قانون الإجراءات الجزائية الجزائري** و تقابلها المادة 59 من قانون الإجراءات الجزائية الفرنسي **Art 59 alinéa 1 de C.P.P.F** 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 ».

على وجود أشياء في كشف الحقيقة لدى المشتبه فيه أو غيره [632] و بناءا عليه وتطبيقا على الجرائم الماسة بأنظمة المعالجة الآلية فإن سبب التفتيش المتعلق بهذا النوع من الجرائم يعني:

- ضرورة وقوع جريمة من الجرائم الماسة بأنظمة المعالجة الآلية التي نص عليها المشرع في نصوص التجريم والعقاب طبقا لمبدأ شرعية الجرائم و العقوبات، كما فعل المشرع الجزائري الذي أدرج فصلا خاصا –الفصل السابع– في قانون العقوبات لجرائم الإعتداء على نظم المعالجة الآلية للمعطيات، ذلك أن التفتيش الذي يقع من أجل فعل لا يشكل جريمة يعتبر باطلا، بالإضافة إلى أن تكون هذه الجريمة قد وقعت فعلا فلا يجوز القيام بهذا الإجراء لضبط أدلة في جريمة مستقبلية ولو قامت التحريات والدلائل الجدية على أنها ستقع بالفعل[633].

إلا أنه و بالرجوع الى نص المادة 05 من القانون 09/04 نجد أن المشرع قد أجاز إمكانية اللجوء إلى إجراء تفتيش النظام المعلوماتي إما للوقاية من حدوث جرائم أو في حالة توفر معلومات عن احتمال وقوع جرائم معينة ذكرتها المادة الرابعة من نفس القانون، و هو الأمر الذي يفهم صراحة بقراءة نص المادتين معا .

- ضرورة الإشتباه في شخص معين أو اتهامه بارتكاب الجريمة أو المشاركة فيها، فلا يكف لقيام سبب التفتيش وقوع جريمة المساس بقواعد الأمن المعلوماتي بل لابد أن يكون هناك اتهام موجه ضد شخص معين أو أن تتوافر دلائل كافية تدعو للإعتقاد بإرتكابه للجريمة حتى يمكن إنتهاك حق الخصوصية لديه و تفتيش حاسوبه الشخصي و برامجه الخاصة[634].

و من الدلائل المستمدة من الواقع و القرائن التي تنبئ عن ارتكاب الشخص لجريمة معلوماتية وترجح إمكانية نسبتها له وفق السياق العقلي و المنطقي أن يتم تحديد هوية الحاسوب [635] (IP) الذي تم ارتكاب الجريمة به و كان ذلك الحاسوب يخص شخصا بعينه.

---

[632]- وهو ما أقرته محكمة النقض المصرية بإعتبارها أن الإذن بالتفتيش لا يصح إصداره إلا لضبط جريمة واقعة بالفعل وترجحت نسبتها إلى متهم معين وأن هناك من الدلائل ما يكفي للتصدي لحرمة مسكنه أو لحرمته الشخصية .طعن نقض جنائي جلسة 16/10/1967 مجموعة أحكام النقض س18 رقم 195، ص965. مشار إليه لدى، **نعيم سعيداني**، مرجع سابق، ص 154.

[633]– **عبد الله حسين علي محمود**، مرجع سابق، ص 370–372.

[634]– و يمكن الإستدلال على ذلك بما نصت عليه المادة 46 **إجراءات جزائية** " لا يجوز لضباط الشرطة القضائية الإنتقال إلى مساكن الأشخاص الذين يظهر أنهم ساهموا في الجناية ويحوزون أشياء لها علاقة بالأفعال الجنائية المرتكبة لإجراء التفتيش....".

[635]– **Internet Protocol** لكل حاسب رقم شخصي يمكن من خلاله تحديد هوية المتصل مع الانترنت من خلال هذا الرقم الذي يطلق عليه بروتوكول انترنت

ب.تحديد محل التفتيش: يقصد بمحل التفتيش المستودع الذي يحتفظ فيه الشخص بالأشياء التي تتضمن سره، و محل التفتيش في الجرائم الماسة بقواعد الأمن المعلوماتي هو نظام المعالجة الآلية بكل مكوناته المادية و المعنوية و شبكات الإتصال كما سبق شرحه وبيانه.

وحكم تفتيش هذه المكونات يتوقف على طبيعة المكان الموجود فيه، فيما إذا كان من الأماكن العامة أم من الأماكن الخاصة، وتكمن أهمية التفرقة هنا في أن هذه الكيانات في الأماكن الخاصة يكون لها حكم تفتيش المساكن بنفس الضمانات المقررة قانونا سيما إشتراط الإذن بالتفتيش من السلطات القضائية المختصة و هو ما نصت عليه المادة 44 من قانون الإجراءات الجزائية أنه لا يجوز لضباط الشرطة القضائية الدخول إلى المساكن و إجراء التفتيش إلا بإذن مكتوب من وكيل الجمهورية أو من قاضي التحقيق، وهذه الضمانة خاصة بجميع الجرائم بما فيها الجرائم المعلوماتية.

أما التفتيش الواقع على مكونات الحاسوب الموجودة في الأماكن العامة [636] فإن أغلب التشريعات تجيز لرجال الضبطية دخول المحال العامة المفتوحة للجمهور كمقاهي الانترنت من أجل مراقبتها والتأكد من احترامها للأخلاق و الآداب العامة بكل سهولة دون حاجة لإذن بالتفتيش[637].

ج.الإذن بالتفتيش : إن التفتيش التقليدي يهدف إلى جمع الأدلة المادية في حين أن النظم المعلوماتية جزء منها عبارة عن كيان معنوي و لا تتوافر له صفة المادة إلا إذا تحولت تلك المعلومات أو النبضات و الدبدبات لإلى مستخرجات، و إن محل التفتيش بصورته التقليدية عبارة عن مساكن و الأماكن الملحقة بها، فقد أضفى عليها القانون الإجرائي حماية خاصة لحرمتها و باعتبارها مكان سر الأفراد ومحلا لخصوصياتهم، و يعتبر الحصول على إذنمكتوب من السلطة القضائية المختصة بتفتيش هذه الأماكن من الضمانات المقررة في التشريعات الإجرائية الجزائية .

و بالتالي هل يمكن إعمال ذات الشرط عندما يتعلق الأمر بتفتيش منظومة معلوماتية أو جزء منها؟ أي هل أنه لا يجوز الولوج إلى البيئة الرقمية أو الانظمة المعلوماتية و القيام بتفتيشها من طرف الضبطية إلا بإذن مكتوب من السلطة القضائية المختصة؟

---

[636]– إذا كانت المكونات المادية للنظام متواجدة في أماكن عامة كمحلات بيع و صيانة الحاسبات الآلية و بحوزة شخص كما لو كان عامل صيانة فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص بنفس القيود و الضامنات المنصوص عليها في هذه الحالة: مشار إليه لدى؛ **رشيدة بوكر**، مرجع سابق، ص 396.

[637]– **علي حسن الطوالبة**، مرجع سابق، ص 81.

غالبا ما يصدر الإذن بتفتيش مسكن المتهم و ينصرف هذا الإذن إلى كل ما يتواجد في المسكن ومن ثم فهل يجوز بمتقضى هذا الإذن لضباط الشرطة القضائية الولوج إلى البيئة الرقمية والتغلغل في المنظومة المعلوماتية للبحث عن الأدلة الإثباتية التي يمكن أن تكون محل ضبط؟

خاصة و أن هذه الأنظمة المعلوماتية قد تحتوي العديد من الملفات الخاصة و السرية، وبالتالي هل يحتاج كل ملف إلى إذن قضائي؟

إن المشرع الجزائري لم يتطرق إلى هذه المسألة بصورة صريحة و مفصلة، ذلك أن القواعد الخاصة بإجراء التفتيش المذكورة في قانون الإجراءات الجزائية تتعلق بالتفتيش التقليدي الذي محله المساكن وملحقاتها، وكذا القواعد الخاصة بإجراء التفتيش في الأنظمة المعلوماتية الواردة بالقانون 09/04 لم يشر المشرع صراحة لهذا الشرط، كل ما في الأمر أنه تحدث عن إعلام جهات التحقيق لسلطة القضائية المختصة في حالة تمديد التفتيش و على وجه السرعة إلى منظومة معلوماتية أخرى.

فهل يعني هذا السكوت من طرف المشرع أنه يجوز تفتيش المنظومة المعلوماتية دون حاجة إلى إذن آخر بالتفتيش يخص المنظومة المعلوماتية و يكفي فقط الإذن المتعلق بالمسكن الذي يتواجد فيه الحاسوب؟

و حتى لو أجاز ذلك فما معيار ضبط هذا الإذن، خاصة و أن النظام المعلوماتي قد يحتوي على العديد من المعلومات و الملفات الشخصية، مما يحتاج من المشرع إعادة ضبط هاذ الأمر لما فيه من خطورة و مساسه بخصوصية الأشخاص و أسرارهم.

– **تحديد مجال الإذن بالتفتيش:** إن المشرع الجزائري بخصوص هذا الأمر لم يتطلب شرط التحديد الدقيق لاعتبار صحة الإذن بالتفتيش إذ نصت المادة 3/44 قانون إجراءات جزائية جزائري على أنه:"... يجب أن يتعين الإذن بالتفتيش بيان وصف الجرم و عنوان الأماكن التي يتم زيارتها و تفتيشها و ذلك تحت طائلة البطلان....".

و عليه في نطاق تفتيش الأنظمة المعلوماتية فمن المعلوم أن البيئة الرقمية تعد مجالا ضخما يمكنه تخزين كم هائل من المعلومات و الملفات، فكيف يكون التحديد الدقيق للإذن بالتفتيش؟

إن صياغة الإذن بالتفتيش الخاص بالأنظمة المعلوماتية و البيئة التي تتضمن الدليل الرقمي قد يشكل صعوبة و يواجه تعقيدات جمة، ذلك أن هذه البيئة قد تتضمن بيانات كثيرة و عناصر متداخلة قد لا تتناسب و سبب التفتيش، و قد يؤدي إصدار إذن مطلق بالتفتيش إلى المساس بالخصوصية مما يخلق

صعوبة في تفتيشها من قبل ضباط الشرطة القضائية [638]، و في نفس الوقت قد يحدث و أن يصادف المأذون له بالتفتيش جريمة أخرى عرضية[639] بمناسبة تفتيشه لكل المنظومة المعلوماتية، و بالتالي من الصعب جعل الإذن بالتفتيش شاملا مما ينبغي معه أن يكون أكثر تخصصا و مبررا.

و المشرع الجزائري مثل معظم التشريعات لم يعطي إجابة لهذه المسألة مما يتطلب معه إعادة النظر في النصوص الإجرائية الجزائية، و لعلى ما سبق بيانه يظهر مشكلة إثبات الجريمة التي تمس قواعد الأمن المعلوماتي لتعقد طرق و كيفية الحصول على الدليل الرقمي.

و من الدول التي نصت تشريعاتها على ضرورة تحديد مجال الإذن بالتفتيش الولايات المتحدة الأمريكية وكندا حيث نصتا على أن يكون إذن التفتيش متضمنا :

- البحث عن أدلة متحصلة من كيان الحاسب المنطقي و التي يدخل فيها برامج التطبيق و نظم التشغيل
- البيانات المستخدمة بواسطة برنامج الكومبيوتر
- السجلات التي تثبت إستخدام الأنظمة الآلية لمعالجة البيانات
- السجلات المستخدمة في عملية الولوج في النظام الآلي لمعالجة البيانات[640]

البند الثالث: ضبط الدليل الرقمي

إن القيام بإجراءات التفتيش لا شك أن هدفها هو ضبط الدليل [641] المراد الحصول عليه من أجل كشف الحقيقة و لكي تتجلى الوقائع إما ضد المشتبه فيه أو لصالحه.

جرى التحقيق في الجرائم التقليدية أن يقع الضبط على الأشياء المادية فقط بوصفها أدلة مادية للجريمة التي يجري التفتيش بشأنها، لكن في مجال الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات فإن الطبيعية العلمية و المعقدة لهذه البيئة تجعل السؤال يطرح حول كيفية ضبط الدليل في عالم إفتراضي ينتج نبضات رقمية تشكل قيمة و جوهر الدليل الرقمي؟ و هل يصلح هذا النوع من الدليل لأن يكون محلا للضبط و المحافظة عليه؟، و ما هي الإجراءات المتبعة في ذلك؟

أولا: صلاحية ضبط أدلة الجرائم الماسة بقواعد الأمن المعلوماتي

---

[638]- المواد **81،83،84،85 من قانون الإجراءات الجزائية الجزائري المشار اليه سابقا.**

[639]- المادة **5/44 من ق.إ.ج.ج:**" إذا اكتشفت أثناء هذه العمليات جرائم أخرى غير تلك التي ورد ذكرها في إذن القاضي فإن ذلك لا يكون سببا لبطلان الإجراءات العارضة" معدلة بموجب القانون رقم 06-22 المشار إليه سابقا.

[640]- **نعيم سعيداني**، مرجع سابق، ص 158.

[641]- المادة **84 من ق.إ.ج.ج**

إن الضبط هو وضع اليد على شيء يتصل بالجريمة و يفيد في كشف الحقيقة عنها وعن مرتكبها، و هو كما سبق القول يرد على الأشياء المادية، و إن كان كذلك فما حكم الضبط الذي يرد على الأشياء المعنوية التي تتكون منها الأنظمة المعلوماتية كالمعلومات و الإتصالات؟.

إن ضبط المكونات المادية للنظام المعلوماتي لا يثير مشاكل في الفقه المقارن [642] و لا يوجد خلاف بين فقهاء القانون في إمكانية ضبط هذه المكونات بل حتى إمكانية ضبط جهاز الحاسب الآلي بشكل كامل لتأكيد الاحتفاظ بالدليل إذا كان مشغل الجهاز غير متعاون مع جهات التحقيق[643].

أما فيما يخص مكوناته المعنوية فإنه ثار خلاف بشأنها ، حيث إختلفت التشريعات و الإتجاهات الفقهية[644] حول مسألة ضبط الأشياء المعنوية و الكيانات المنطقية و التي لا تصلح بطبيعتها محلا للضبط خاصة إذا كانت مجردة من دعامتها المادية المثبتة عليها.

نتيجة لذلك وجد المشرع الجزائري أمام حتمية استتباع إجراء التفتيش في المنظومة المعلوماتية و نص على طريقة ضبط الأدلة الرقمية من خلال القانون 04/09 السالف الذكر من خلال المادة 06 التي تنص على أنه" عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة يتم نسخ المعطيات محل البحث و كذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز و الوضع في أحراز وفق القواعد المقررة في قانون الإجراءات الجزائية....".

فلا شك أنها الطريقة المناسبة لضبط الأدلة الرقمية وفقا لطبيعتها في البيئة الرقمية.

642- **هاشم محمد فريد رستم**، مرجع سابق، ص 81.

643- **عفيفي كامل عفيفي**، مرجع سابق، ص 353.

644-إنقسم الفقه إلى إتجاهين: **الإتجاه الأول :** يرى أصحابه أنه لا يمكن تصور إجراء الضبط على الكيانات المنطقية للحاسوب لانتفاء الكيان المادي عنها، وبالتالي عدم صلاحية البيانات المخزنة آليا لأن تكون محلا للضبط بالكيفية المنصوص عليها بموجب النصوص التقليدية لإنتفاء الطابع المادي عن هذه البيانات في حال تجردها عن الدعامة المادية، و من التشريعات التي أخذت بهذا الإتجاه قانون الإجراءات الجنائية الألماني مشار إليه لدى: **عفيفي كامل عفيفي**، نفس المرجع، ص 358.

الإتجاه الثاني: يرى أنصار هذا الإتجاه أن المعطيات المخزنة آليا كونها مجردة عن الدعامة المادية التي تحويها لا يوجد ما يمنع من صلاحيتها بهذه الصورة لأن تكون محلا للضبط المنصوص عليه بمقتضى النصوص التقليدية مستندين إلى أن الغاية من التفتيش هو ضبط الأدلة التي تفيد في كشف الحقيقة، و بالتالي يمتد هذا المفهوم ليشمل البيانات الإلكترونية بمختلف أشكالها: مشار إليه لدى د. **عبد الفتاح بيومي حجازي** ، مبادئ الإجراءات الجزائية في جرائم الكمبيوتر و الانترنت، مرجع سابق، ص 93/كذلك: **نبيلة هبة مولاي على هروال**، مرجع سابق، ص 265.

و قبل المشرع الجزائري قام المشرع الفرنسي بإدخال تعديل على قانون الإجراءات الجزائية بموجب قانون الأمن الداخلي 239/2003 السابق الإشارة إليه، أين استحدث الفقرة الثالثة من المادة 57-1 التي تقضي بأن المعطيات التي يتم بلوغها في ظل الشروط المنصوص عليها في المادة السابقة يتعين نسخها على دعامات التخزين المعلوماتية" [645] .

و لا شك أن اتجاه المشرع الفرنسي قد نبع من ما جاء في الاتفاقية الأوروبية للإجرام المعلوماتي التي نصت على ذلك من خلال الفقرة الثالثة(03) من المادة 19 بقولها:" يجب على كل طرف أن يتبنى الإجراءات التشريعية التي يراها ضرورية من أجل تخويل سلطاته المختصة سلطة ضبط أو الحصول بطريقة مشابهة على البيانات المعلوماتية وفقا للفقرتين 1 و 2 و تشمل الإجراءات ما يلي:-

ضبط الوصول بطريقة مشابهة إلى نظام معلوماتي أو جزء منه أو إلى دعامة تخزين معلوماتية

- التحقق و التحفظ على نسخة من هذه البيانات المعلوماتية

- المحافظة على سلامة البيانات المخزنة...".

و بالتالي فإن كان يجوز ضبط الدليل الرقمي مهما كان شكله سواء كان في دعامة مادية كالأقراص الممغنطة أو الديسك أو على الحاسب الآلي، أو حتى على مستوى الشبكة المعلوماتية مخزنتا بها أو متناقلة عبرها، فإن السؤال الذي يطرح هنا هو كيف يتم ضبط هذا الدليل التقني و المحافظة عليه في سبيل إثبات الجرائم الماسة بقواعد الأمن المعلوماتي؟

ثانيا: إجراءات و قواعد ضبط الدليل التقني

تشمل الإجراءات المقررة ضبط العناصر المادية للنظام المعلوماتي و دعامات التخزين للبيانات أو المعلومات المعلوماتية و حتى البرامج المعلوماتية التي قد تستعمل في ارتكاب هذه الجرائم، و نظرا للطبيعة اللامادية لبعض عناصر المنظومة المعلوماتية فإن ضبطها فيه من الصعوبة أو الخطورة مما يستوجب إجراءات خاصة بهذا النوع من الأدلة، تختلف عما هي عليه عند ضبط العناصر المادية كالأقراص المرنة، المودم، و غير ذلك.

نص المشرع الجزائري من خلال القانون 09/04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها على بعض أشكال و طرق ضبط الأدلة الرقمية،

---

[645] **-Art 57-1 alinéa 4 de C.P.P.F** dispose que ; « Les données auxquelles il aura été permis d'accéder dans les conditions prévues par le présent article peuvent être copiées sur tout support. Les supports de stockage informatique peuvent être saisis et placés sous scellés dans les conditions prévues par le présent code » créé par **la loi n° 2003-239 du L.S.I.F**.

و تكون عن طريق نسخ المعطيات محل البحث و كذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون هذه الأخيرة قابلة لحجزها ووضعها في أحراز حسب ما هو مقرر في قواعد تحريز الدليل المنصوص عليه في قانون الإجراءات الجزائية [646]، و الإجراء الأخر يكون في حالة استحال إجراء الحجز وفقا لما هو منصوص عليه في المادة 6 من نفس القانون لأسباب تقنية، فإنه يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية و الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة أو إلى نسخها[647].

و عموما فإن كان الدليل الرقمي يخضع في ضبطه إلى قواعد تحريز الأدلة الجنائية إلا أنه ونظرا لخطورة الوضع، فإن عملية ضبطه و تحريزه تحتاج إلى بعض الإجراءات الخاصة لحمايته فنيا و الحفاظ عليه وصيانته من إمكانية العبث به أو إتلافه [648]، و هو ما أشار إليه المشرع في المادة

---

[646]- و ذلك وفقا **للمادة 06 من القانون رقم 09-04** السابق الإشارة إليه.

[647]- المادة **07 من القانون رقم 09-04** المشار إليه سابقا.

[648]- هناك عدة برامج مساعدة على البحث الرقمي حيث غالبا ما توجد الأدلة الرقمية في الأقراص المرنة والصلبة وأشرطة تخزين المعلومات، وأجهزة المودم وأجهزة التصوير ومواقع الويب والبريد الإلكتروني، لذا يوجد العديد من البرامج التي تساهم في مساعدة المختصين بالأمن الرقمي على مزاولة عملهم،في هذه الحالات ومنها:

برنامج إذن التفتيش Computer Scorch Warrant Program وهو برنامج قاعدة بيانات، يسمح بإدخال كل المعلومات الهامة المطلوبة لترقيم الأدلة وتسجيل البيانات منها. ويمكن لهذا البرنامج أن يصدر إيصالات بتَسَلُّم الأدلة والبحث في قوائم الأدلة المضبوطة لتحديد مكان دليل معين أوتحديد ظروف ضبط هذا الدليل.

قرص بدء تشغيل الحاسوب Bootable Diskette و هو قرص يُمكن المحقّق من تشغيل الحاسوب، إذا كان نظام التشغيل فيه محمياً بكلمة مرور ويجب أن يكون القرص مزوداً ببرنامج مضاعف المساحة Double space فربما كان المتهم قد استخدم هذا البرنامج لمضاعفة مساحة القرص الصلب.

برنامج معالجة الملفات مثل X tree Pro Gold : و هو برنامج يُمكن المحقّق من العثور على الملفات في أي مكان على الشبكة أو على القرص الصلب، ويستخدم لتقييم محتويات القرص الصلب الخاص بالمتهم، أو الأقراص المرنة المضبوطة، أو يستخدم لقراءة البرامج في صورتها الأصلية، كما يُمكّن من البحث عن كلمات معينة أو عن أسماء ملفات أو غيرها.

برامج كشف القرص مثل :AMA Disk, View disk :ويمكن باستعمال هذا البرنامج الحصول على محتويات القرص المرن، مهما كانت أساليب تهيئته، ولهذا البرنامج نسختان، نسخة عادية خاصة بالأفراد ونسخة خاصة بالشرطة.

برامج اتصالات مثل :LAN tastic : وهو يستطيع ربط حاسوب المحقق بحاسوب المتهم لنقل ما فيه من معلومات وحفظها في جهاز نسخ المعلومات ثم إلى القرص الصلب. هذه هي أهم الطرق العامة لجمع الأدلة الرقمية، والتي يجب أن يقوم بها خبراء في هذا المجال نظراً لعلمية ودقة هذه الأدلة: مشار إليه لدى **إياد علي الدرة**، الأدلة الجنائية الإلكترونية، **مجلة أمن المعلومات** تصدر عن الجمعية العلمية السورية للمعلوماتية، ع (72)، دمشق، فبراير 2012.

السادسة الفقرة الثالثة من القانون 09/04 حينما أوجب على السلطات التي تقوم بعملية التفتيش و الحجز أن تسهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية، غير أنه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات قصد جعلها قابلة للاستغلال لأغراض التحقيق و بشرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات.

و هو ما أكدت عليه كذلك الفقرة الثالثة من المادة 19 من الاتفاقية الأوروبية للإجرام المعلوماتي لسنة 2001.

البند الرابع: الأدلة الرقمية المتحصلة عن طريق الخبرة التقنية

الخبرة هي بحث لمسائل مادية أو فنية يصعب على المحقق أن يشق طريقه فيها أو يصعب و يعجز عن جمع الأدلة بالنسبة لها بالوسائل الأخرى للإثبات، كفحص بصمات عثر عليها بمكان الحادث، أو مدى نسبة توقيع معين إلى شخص بعينه.

و لأجل الوقوف على الحقيقة في مثل هذه المسائل العلمية و الفنية في البيئة الرقمية فإن القانون أجاز للمحقق أن يستعين بخبير متخصص في المسألة موضوع الخبرة.

و إذا نظرنا إلى ثورة الإتصالات و المعلومات عن بعد نجد أنها قد أتت بتقنيات علمية ذات طبيعة فنية متقدمة، و قد تولد عن هذه التقنيات جرائم ذات طبيعة فنية و علمية معقدة، يحتاج جمع الدليل بالنسبة لها إلى بحث مسائل علمية و فنية، فالأدلة قد تكون غير مرئية و يلزم تحويلها إلى أدلة مقروءة، وقد تكون نتيجة تلاعب في حسابات معينة أو في نظم إلكترونية معينة بحيث يحتاج الكشف عنها إلى متخصصين لإثبات هذا التلاعب.

و قد يحتاج الأمر إلى عمليات فنية دقيقة لإمكان الدخول إلى أنظمة الوسائل الإلكترونية نتيجة استخدام كود أو الأرقام السرية.

و إذا كان الهدف من الخبرة الوصول إلى الحقيقة في مسائل علمية و فنية و مادية فإنها لا تكون حكرا على سلطة التحقيق و إنما يحقق للمحكمة أن تأمر بها.

و بالنظر إلى الطبيعة الخاصة للجرائم الماسة بقواعد الأمن المعلوماتي فإن إماطة اللثام عنها قد يحتاج إلى خبرة فنية قد تظهر الحاجة إليها منذ بدء مرحلة التحري عن هذه الجرائم، ثم تستمر الحاجة إليها في مرحلتي التحقيق والمحاكمة نظرا للطابع الفني الخاص بأساليب إرتكابها والطبيعة المعنوية لمحل الإعتداء.

كما لا يمكن التصور رفض القاضي اللجوء إلى ندب خبير في قضايا الجرائم التقنية، إذ هي قضايا فنية تتطلب خبرة خاصة، و كذا إزاء نقص المعرفة لدى القانونيين بظاهرة تقنية المعلومات، لذلك فإن العلوم و التقنينات المتصلة بها تنتمي إلى تخصصات علمية و فنية دقيقة و متنوعة، و التطورات في مجالها سريعة و متلاحقة لدرجة قد يصعب معها على المتخصص تتبعها و استيعابها.

و يمكن القول أنه لا يوجد حتى الآن و بصفة عامة خبير لديه معرفة متعمقة في سائر أنواع الحاسبات و برامجها و شبكاتها كذلك لا يوجد خبير قادر على التعامل مع كافة أنماط الجرائم التي تقع عليها أو ترتكب بواسطتها [649]، فما بالك إذا كان الضابط أو القاضي من الدارسين في الدرسات و العلوم القانونية و ليسوا من أهل الخبرة في المجالات التقنية، مما يتطلب الإستعانة بخبير فني أو ذوي الإختصاص المعتمدين لدى الجهات القضائية.

أولا: أهمية الخبرة في البحث عن الدليل الرقمي

تظهر أهمية الخبرة في أن مشكلة الدليل الرقمي تكمن في القواعد المخزنة في صفحات الفضاء الالكتروني، إذ أن ما تحتويه من بيانات قد يكون الدليل بناءا علي الفعل المرتكب إن كان تحريفا أو دخولا غير مصرحا به، أو تلاعبا أو غير ذلك فكيف يقبلها

القضاء و هي ليست دليلا ماديا يضاف إلى محضر كالمستند الخطي ؟ أو أقوال الشاهد أو تقرير الخبرة ؟

و لتجاوز هذه المشكلة قد يلجا القضاء أو جهات التحقيق و كافة السلطات المختصة بالدعوى الجزائية إلى انتداب الخبراء لإجراء عمليات الكشف و التثبت من محتوى البيئة الرقمية و من ثم تقديم التقرير الذي يعد البينة و الدليل .

لذلك اهتم المشرع الجزائري بتنظيم أعمال الخبرة [650] و إعتبرها من إجراءات البحث عن الدليل حيث نصت المادة 143 أنه لجهات التحقيق أو الحكم عندما تعرض لها مسألة ذات طابع فني أن تأمر بندب خبير إما من تلقاء نفسها أو بناء على طلب من النيابة العامة و إما بطلب من الخصوم.

وإذا كانت الاستعانة بخبير فني في المسائل الفنية البحتة في الجرائم التقليدية أمر واجب على جهات التحقيق، فهي أوجب في مجال استخلاص الدليل الرقمي لإثبات الجرائم المعلوماتية حيث تتعلق

---

[649]- **عبد الله حسين علي محمود**، مرجع سابق، ص 374.

[650] – المواد 143 إلى 156 من **قانون الإجراءات الجزائية**

بمسائل فنية آية في التعقيد، يصعب على المحقق أن يشق طريقة فيها و يعجز عن جمع الأدلة بالنسبة لها بالوسائل الأخرى للإثبات[651].

و منذ ظهور الجرائم المعلوماتية فإن الضبطية القضائية وسلطات التحقيق عموما تستعين بأصحاب الخبرة الفنية المتميزة في مجال الحاسب الآلي والمنظومات المعلوماتية و ذلك بغرض كشف غموض الجريمة وتجميع أدلتها والتحفظ عليها، أو مساعدة المحقق في إجلاء جوانب الغموض في العمليات الإلكترونية الدقيقة ذات الصلة بالجريمة محل التحقيق و يلاحظ أن نجاح الإستدلالات و أعمال التحقيق في هذه الجرائم يكون مرتهنا بكفاءة و تخصص هؤلاء الخبراء.

فالمجرم المعلوماتي لا شك أنه متميز و متمكن من تقنيات الحاسوب و الشبكات المعلوماتية و له من الذكاء في هذا الجانب، ولا يكشفه إلا ذكاء وفن مماثلين.

كما تبرز أهمية الإستعانة بالخبير في مجال الجرائم المعلوماتية عند غيابه فقد تعجز الضبطية في كشف غموض الجريمة لنقص الكفاءة والتخصص اللازمين للتعامل مع الجوانب التقنية والتكنولوجية التي إرتكبت بواسطتها الجريمة، وهو ما قد يؤدي إلى تدمير الدليل ومحوه بسبب الجهل أو الإهمال عند التعامل معه[652].

ولعل هذه الأهمية للخبرة في مجال التحقيق في الجريمة المعلوماتية جعل بعض التشريعات لا تكتف بالنصوص التقليدية التي تنظم الخبرة وعمدت على إدراج نصوص قانونية خاصة تنظم الخبرة في هذا المجال، ومنها المشرع البلجيكي بموجب القانون الصادر في 23/11/2000 حيث نصت المادة 88 منه أنه يجوز للقاضي والشرطة القضائية أن يستعينا بخبير ليقدم وبطريقة مفهومة المعلومات اللازمة عن كيفية تشغيل النظام وكيفية الدخول فيه أو الدخول للبيانات المخزنة أو المعالجة أو المنقولة بواسطته، ويعطي القانون لسلطة التحقيق أن تطلب من الخبير تشغيل النظام أو البحث فيه أو عمل نسخة من البيانات المطلوبة للتحقيق أو سحب البيانات المخزنة أو المحمولة أو المنقولة على أن يتم ذلك بالطريقة التي تريدها جهة التحقيق[653] "

و المشرع الجزائري من جانبه كذلك لم يتخلف عن هذه التشريعات حينما أشار في المادة 05 الفقرة الأخيرة من القانون 09/04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات

---

[651]. **عائشة بن قارة**، مرجع سابق، 139.

[652]– **هشام محمد فريد رستم**، مرجع سابق، ص 29.

[653]– **عائشة بن قارة مصطفى**، مرجع سابق، ص 142.

الإعلام و الاتصال و مكافحتها أنه يمكن للسلطات المكلفة بتفتيش المنظومات المعلوماتية تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها.

ثانيا: القواعد القانونية و التقنية التي تحكم الخبرة القضائية في جرائم أمن المعلومات

الخبرة هي إجراء يستهدف إستخدام قدرات شخص الفنية و العلمية والتي لا تتوافر لدى رجل القضاء أو المحقق من أجل الكشف عن دليل يفيد في معرفة الحقيقة بشأن وقوع الجريمة.

و قد عرفها البعض بأنها الإستشارة الفنية التي يستعين بها القاضي أو المحقق لمساعدته في تكوين عقيدته على نحو المسائل التي يحتاج تقديرها إلى معرفة أو دراية علمية خاصة لا تتوافر لديه[654].

و الخبير هو كل شخص لديه دراية خاصة بمسألة من المسائل قد يستدعي التحقيق فحصها و يستلزم ذلك كفاءة خاصة فنية أو علمية لا يشعر المحقق بتوافرها في نفسه، فيمكنه أن يستعين بالخبير كما هو الحال مثلا في تقرير الصفة التشريحية في جرائم القتل أو فحص خطوط الكتابة في جريمة التزوير.

1 -**الضوابط القانونية لصحة الخبرة:**

لقد حرصت معظم التشريعات على تنظيم الخبرة و وضع شروط وضوابط لها، نظرا لما لها من دور فعال في عملية الإثبات في ا لمجال الجنائي، و من الشروط التي عملت التشريعات على تحديدها منها ما يتعلق بالخبير ومنها ما يتعلق بتقرير الخبرة.

فأما ما يتعلق بالخبير فأنه يشترط :

***اختياره من قائمة الخبراء** المحددة أسماؤهم ضمن الجدول المعد مسبقا من المجالس القضائية، و ذلك بعد استطلاع رأي النيابة العامة دون إلتزام بترتيب معين تبعا لثقة المحقق أو القاضي، وقد نصت المادة 144 من قانون الإجراءات الجزائية الجزائري على ذلك.

و إذا لم يتضمن الجدول من الخبراء المتخصصين في مجال الخبرة فإنه يجوز لجهات التحقيق بصفة استثنائية اختيار خبراء ليسوا مقيدين في الجدول و بقرار مسبب يتضمن أسباب ذلك[655].

و في الحقيقة فإن الاستعانة بالخبراء في إطار الجرائم الماسة بقواعد الأمن المعلوماتي أمر ضروري و إذا كان القانون يسمح بالاستعانة بخبراء ليسو مقيدين بالجداول المحددة سلفا فإن الوضع قد

---

[654]– مشار إليه لدى: **نعيم سعيداني**، مرجع سابق، ص 164.

[655]– المادة **144 من قانون الإجراءات الجزائية الجزائري**.

يتطلب حتى الاستعانة بخبراء أجانب في المجال التقني من أجل الكشف و تقرير الخبرة فيما يخص هذه الجرائم أو على الأقل العمل على تبادل الخبرات مع جهات أجنبية من أجل مكافحة الجريمة المعلوماتية[656].

كما أن القانون ترك للقاضي حرية نذب خبير أو خبراء متعددين و ذلك من خلال المادة 147 من قانون الإجراءات الجزائية الجزائري و لا شك أن هذا يساعد في تقوية الخبرة التقنية في العالم الافتراضي .

***حلف اليمين القانونية** : و هي أهم واجبات الخبير التقني إذ يلزم لصحة عمله أداء اليمين القانونية وذلك لحمله على الصدق والأمانة في عمله وبث الطمأنينة في آرائه التي يقدمها سواء بالنسبة لتقدير القاضي أو لثقة بقية أطراف الدعوى، حيث أوجب المشرع الجزائري أن يحلف الخبير اليمين القانونية قبل أداء مهمته [657] غير أنه إذا كان الخبير المعين مقيدا في الجدول، فإن ما استقر عليه الفقه و القضاء أن ذلك يغني عن أدائه اليمين في كل مهمة[658]، فلا يلزم أن يجدد حلفه لليمين مرة أخرى[659].

656– **خبراء إيرانيون يشرفون بالجزائر على دورة تكوينية في الجريمة الإلكترونية لنقل تجربتهم عن هذه الجرائم**
يستفيد إطارات متخصصة من الشرطة الجزائرية ابتداء من أول أمس بمعهد الشرطة الجنائية (بالسحاولة) الجزائر العاصمة من دورة تكوينية حول الوقاية ومكافحة الجريمة السيبرانية، حسب ما أفاد به بيان للمديرية العامة للأمن الوطني .
وأوضح ذات المصدر أن هذه الدورة التكوينية "تأتي في إطار تجسيد مساعي اللواء عبد الغني هامل المدير العام للأمن الوطني، لتوفير دورات تكوينية تقنية عالية المستوى في مجال مكافحة الجريمة بكل أشكالها لفائدة إطارات الأمن الوطني ".
وسيتم خلال الدورة التكوينية– التي تدوم خمسة (5) أيام و يشرف عليها وفد من خبراء الشرطة الايرانية–"تبادل الخبرات عن التشريعات الدولية وأفضل الممارسات والمساعدة التقنية والتعاون الدولي، بغية تعزيز سبل مكافحة هذا النوع من الجرائم الحديثة ".
وتأتي الدورة التكوينية العالية المستوى –حسب البيان– "لمواجهة ارتفاع مستويات الجرائم السيبرانية التي تعرفها دول العالم دون أي قيد جغرافي حيث يستغل الأفراد والجماعات الإجرامية المنظمة الفرص الجديدة المتاحة لارتكاب الجرائم بغية تحقيق الأرباح والمكاسب الشخصية ".
وأكد نفس المصدر أن من بين أهم المواضيع التي ستعنى بها الدورة التكوينية "أمن الشبكات وحماية البيانات الفردية والتطرق إلى كيفيات ضبط الأدلة الإلكترونية الضرورية كمادة إثباتية، وتأمين التعاملات الادارية والمالية عبر الشبكات ".
وتأتي أهمية هذه الدورة التكوينية في مسايرة فرق المحققين من الشرطة الجزائرية لأحدث التكنولوجيات والتحكم فيها، والاطلاع على الأساليب المعتمدة دوليا في الوقاية والمكافحة من الجريمة السيبرانية، "إذ يبذل الأمن الوطني جهودا معتبرة في الوقاية والتحسيس من هذه الجرائم الناجمة عن سوء استعمال الشبكة العنكبوتية خاصة من طرف الشباب والأطفال، باللجوء إلى العمل الاستباقي لإزالة الأخطار المحتملة وحماية الأفراد والمجتمع من هذا النوع من الجرائم الالكترونية، وهذا ما تسعى إليه المديرية العامة للأمن الوطني من تنظيم مثل هذه الدورات التكوينية المتخصصة." نشر **بجريدة الشروق** اليومي بواسطة دليلة.ب، 2015/08/09.

657– تقضي المادة **145 من قانون الإجراءات الجزائية الجزائري المعدل و المتمم** على أنه:" يحلف الخبير اليمين المقيد لأول مرة بالجدول الخاص بالمجلس القضائي يمينا أمام ذلك المجلس بالصيغة الآتي بيانها:
– أقسم بالله العظيم بأن أقوم بأداء مهمتي كخبير على خير وجه و بكل إخلاص و أن أبدي رأيي بكل نزاهة و استقلال
– ولا يجدد هذا القسم مادام الخبير مقيدا في الجدول...".

658– **عائشة بن قارة مصطفى**، مرجع سابق، ص 144/ د.عبد الناصر محمد محمود فرغلي، مرجع سابق، ص 24.

ولا شك أن الخبير في أدائه لمهمته هو خاضع للرقابة القضائية سواء من قبل قاضي التحقيق أو من قبل القاضي المعين من الجهة القضائية بحسب ما جاء في المادة 5/143 من قانون الإجراءات الجزائية الجزائري.

أما بخصوص تقرير الخبرة الذي هو عبارة عن خلاصة لما توصل إليه الخبير يعده و يقوم بتحريره[660] بعد انتهائه من أبحاثه و فحوصاته بعد تطبيق الأسس و القواعد العلمية الفنية على المسألة محل البحث.

وغالبا ما يرفق الخبير بالتقرير ملحقا إيضاحيا بالصور حتى يسهل على جهة التحقيق فهم الخبرة وعلى جهة الحكم تكوين عقيدتها و إقتناعها الذاتي بالدليل[661].

و إذا كان الحال كذلك بالنسبة لموضوعات الخبرة التقليدية فإن أهمية إعداد تقارير فنية مكتوبة و ملاحق توضيحية تفصيلية و مصورة إن أمكن تصبح حتمية في حالة الجرائم الماسة بأنظمة المعالجة الآلية، حيث يقتضي الأمر عرض وتوضيح وتحليل الدليل الجنائي الرقمي و كيفية اشتقاقه و استخلاصه من البيئة الإفتراضية، و على أن هذه التقارير هي مجرد استدلالات لإنارة القاضي و توجيهه إلى الحل أو الحكم الصحيح، و أن رأي الخبير يطرح على سبيل الاستشارة[662].

و يشترط أيضا فيما يتعلق بتقرير الخبرة أن يقوم الخبير بإيداع تقرير خبرته خلال المدة المحددة له في أمر أو حكم الندب، فإن لم يودع تقريره خلال هذه المدة جاز للقاضي إستبداله بغيره ما لم يقدم الخبير طلبا بتمديد هذه المهلة[663] و ذلك نظرا لما تتسم به الإجراءات الجزائية من طابع السرعة سيما إذا تعلق الأمر بجرائم المساس بأنظمة المعالجة الآلية للمعطيات.

2- القواعد الفنية لعمل الخبير في مجال الجرائم الماسة بالأمن المعلوماتي

إن الأنظمة المعلوماتية مترابطة و متشعبة لما تشمله من الوسائل الإلكترونية و الأجهزة التي تستخدم نظام المعالجة الآلية، و التي قد ترتبط بشبكات الإتصال التي قد تتنوع فيما بينها و تتمايز خصائصها الفنية مما يستوجب كذلك أن يتوافر لدى الخبير الإمكانيات والقدرات العلمية و

---

[659]- تقضي المادة 3/145 من **ق.إ.ج.ج** بأنه :" يؤدي الخبير الذي يختار من خارج الجدول اليمين قبل مباشرة مهمته اليمين السابق بيانها أما قاضي التحقيق أو القاضي المعين من الجهة القضائية".

[660]- المادة 153 من **ق.إ.ج.ج** السابق الإشارة إليه.

[661]- **رشيدة بوكر**، مرجع سابق، ص 432.

[662]- و ذلك طبقا للمادة 215 من ق.إ.ج.ج.

[663]- المادة 148 من **قانون الإجراءات الجزائية الجزائري**.

الدارية و الفهم الكبير بالأمور الفنية في مجال التخصص، وعلى جهات التحقيق أن تراعي في إختيارها للخبير المتخصص و الملم لكل تفاصيل هذا الأمر.

و نظرا للطبيعة الصعبة و المعقدة للدليل الرقمي و لأهميته في مجال الإثبات فإنه يلزم لعمل الخبير في هذا المجال اتباع خطوات و اساليب علمية تتناسب مع بيئة هذا الدليل:

أ. **متطلبات أعمال الخبرة في مجال الجريمة المعلوماتية** : إنه بالنظر إلى الطبيعة الفنية والعلمية [(2)] للخبرة في مجال الجريمة المعلوماتية فإنه ينبغي للخبير الإلمام بالموضوعات الآتية:

- الإلمام بتركيب الحاسب وصناعته وطرازه ونظم تشغيله الرئيسية والفرعية والأجهزة الطرفية الملحقة به وكلمات المرور أو السر ورموز التشفير .

– طبيعة البيئة التي يعمل في ظلها الحاسب من حيث تنظيم ومدى تركيز أو توزيع عمل المعالجة الآلية وتحديد أماكن التخزين والوسائل المستخدمة في ذلك

- .القدرة على أداء المهام دون أن يترتب على ذلك إعطاب أو تدمير الأدلة المتحصلة من الوسائل الإلكترونية.

- التمكن من نقل أدلة الإثبات غير المرئية وتحويلها إلى أدلة مقروءة أو المحافظة على دعامتها لحين القيام بأعمال الخبرة بغير أن يلحقها تدمير أو إتلاف، مع إثبات أن المخرجات الورقية لهذه الأدلة تطابق ما هو مسجل على دعائمها الممغنطة

- .بالإضافة إلى ضرورة إلمام الخبير أيضا بنظم الحاسب الآلي بمكوناته المادية والبرامجية

– معرفته لوسائل وطرق فحص نظام الحاسب الآلي كبرامج كشف وإزالة للفيروسات وبرامج إسترجاع البيانات والمعلومات وإصلاح التالف وإظهار المخفي منها

-معرفته لوسائل نسخ البرامج والملفات وعمل نسخ من القرص الصلب طبق الأصل.

- معرفته لكيفية الربط بين الدليل المادي والدليل الرقمي في الوقائع محل البحث .ولا ينجح الخبير المعلوماتي في أدائه لمهامه المنوطة به وإتمامه للمأمورية المكلف ا إن لم يكن لديه هذا القدر من المتطلبات الفنية[(664)].

فالخبرة في الجرائم المعلوماتية تساعد في النهاية على:

- الكشف عن الدليل الرقمي

---

[664]- **هشام محمد فريد رستم**، مرجع سابق، ص 142–143/ مشار اليه كذلك لدى: **رشيدة بوكر**، مرجع سابق، ص 431.

- .إجراء الإختبارات التكنولوجية على الدليل الرقمي للتحقق من أصالته ومصدره كدليل يمكن تقديمه لأجهزة إنفاذ القانون .

– تحديد الخصائص الفريدة للدليل الرقمي

- إصلاح الدليل الرقمي وإعادة تجميعه من المكونات المادية للكومبيوتر.

– عمل نسخة أصلية من الدليل الرقمي للتأكد من عدم وجود معلومات مفقودة أثناء عملية إستخلاص الدليل.

-جمع الآثار المعلوماتية الرقمية التي تكون قد تبدلت خلال الشبكة المعلوماتية

.ب. الأساليب الفنية في عمل الخبير المعلوماتي في إكتشاف الدليل الرقمي

للخبير المعلوماتي في سبيل تحري الحقيقة أن يقوم بكل ما يمكنه من التوصل إليها، وهو في إطار القيام بعمله له أن يستخدم الأساليب العلمية التي يقوم عليها تخصصه وليس للمحكمة أن ترفض تلك الأساليب ما لم يكن رفضها لها مسببا بشكل منطقي، و يعتمد عمل الخبير المعلوماتي في سبيل تحري الحقيقة في مجال الجرائم المعلوماتية على جمع مجموعة من الأدلة الرقمية وتحصيلها من خوادم المواقع (Les serveurs) ومن جهاز المعتدي بعد التوصل إلى تحديده، ثم يقوم بعملية تحليل رقمي لها لمعرفة كيفية إعدادها البرمجي ونسبتها إلى مسارها الذي أعدت فيه وتحديد عناصر حركتها، ومن ثم التوصل في النهاية إلى معرفة بروتكول الأنترنات (IP) للحاسوب الذي صدرت منه الرسائل والنبضات الإلكترونية.[665]

ويرى بعض[666] المتخصصين أن عمل الخبير المعلوماتي في إشتقاق وتجميع الأدلة الرقمية يتم عبر ثلاث مراحل :

المرحلة الأولى : تجميع المعلومات المخزنة لدى الطرف مقدم الخدمة من خلال تتبع الحاسبات الخادمة التي دخل منها المجرم المعلوماتي ومحاولة إيجاد أثر له.

المرحلة الثانية : مرحلة المراقبة ويتم ذلك بطرق مختلفة أهمها إستخدام برامج مراقبة يمكن تحميلها للبحث عن المعلومات المشتبه فيها وحصر وتسجيل بيانات كل دخول وخروج بالموقع .**المرحلة الثالثة:** فحص النظام المعلوماتي المشتبه فيه بعد ضبطه من طرف جهات التحقيق بمكوناته المادية والمعنوية

---

[665]- **نعيم سعيداني**، مرجع سابق، ص171.

[666]– **أحمد سعد محمد الحسيني** ، الجوانب الإجرائية للجرائم الناشئة عن استخدام الشبكات الالكترونية، رسالة دكتوراه، جامعة عين شمس، كلية الحقوق، الدراسات العليا، قسم القانون الجنائي، مصر، 2012، ص85-87.

لإشتقاق الدليل وتقديمه لجهات التحقيق وتقرير مدى وقوع الجريمة بإستخدام النظام المضبوط من عدمه .

وقد وضعت وزارة العدل الأمريكية إطارا عمليا يحدد خطوات أساسية لجمع الأدلة الرقمية ثم فحصها ومن ثم تحليلها وأخيرا كتابة النتائج المتوصل إليها في تقرير، ويمكن إيجاز هذه الخطوات في المراحل التالية :

- خطوات ما قبل التشغيل والفحص[667]

* التأكد من مطابقة محتويات أحراز المضبوطات لما هو مدون عليها.

*التأكد من صلاحية وحدات نظام التشغيل

* تسجيل معطيات وحدات المكونات المضبوطة.

خطوات التشغيل الفحص

* إستكمال تسجيل باقي معطيات الوحدات من خلال قراءات الجهاز .

*عمل نسخة من كل وسائط التخزين المضبوطة وعلى رأسها القرص الصلب لإجراء عملية الفحص المبدئي على هذه النسخة لحماية الأصل من أي فقد أو تلف أو تدمير سواء عن سوء الإستخدام أو لوجود فيروسات أو قنابل برمجية .

* تحديد أنواع وأسماء المجموعات البرامجية كبرامج النظام (برامج التشغيل)، برامج التطبيقات وبرامج الإتصالات، وما إذا كان هناك برامج أخرى ذات دلالة بموضوع الجريمة

* .إظهار الملفاة المخبأة والنصوص المخفية داخل الصور[668]

* .إسترجاع الملفات التي تم محوها من الأصل وذلك بإستخدام أحد برامج إستعادة المعلومات وكذلك بالنسبة للملفات المعطلة أو التالفة * .تخزين هذه الملفات أو المعطيات وعمل نسخ أخرى طبق الأصل من الأسطوانة أو القرص المحتوي لها ولفحصها عن طريق تطبيق الخطوات سالفة الذكر

* .إعداد قائمة يبجرد فيها الخبير كل الأدلة الرقمية التي تم الحصول عليها، مع إجراء مراجعة لكل صورة محتفظ بها في القرص الصلب لحاسوب آخر للتأكد من سلامة القائمة .

---

[667]- **عائشة بن قارة مصطفى**، مرجع سابق، ص 148-149.

[668]-**عبد الناصر محمد محمود فرغلي و عبيد سيف سعيد المسماري**، المرجع السابق، ص35،.

* تحويل الدليل الرقمي إلى هيأة مادية وذلك عن طريق طباعة الملفات أو تصوير محتواها أو وضعها في أي وعاء آخر حسب نوع المعطيات والمعلومات المكونة للدليل .وفضلا عما سبق فإن الخبير المعلوماتي و هو في إطار القيام بعمله له أن يستخدم العديد من الوسائل العلمية والبرمجيات التي تمكنه من إستخلاص الدليل الرقمي و تساعده في الوصول إلى المجرم المعلوماتي، و غالبا ما تكون هذه الوسائل أدوات فنية تستخدم في بنية نظام المعلومات .

ونذكر منها على سبيل المثال لا الحصر:

* **بروتوكول الانترنت** (IP) وهو المسئول عن تراسل حزم البيانات عبر شبكة الانترنت وتوجيهها إلى أهدافها، وهو يوجد بكل جهاز مرتبط بالانترنت ويتكون من أربعة أجزاء كل جزء يتكون من أربع خانات، حيث يشير الجزء الأول من اليسار إلى المنطقة الجغرافية، والجزء الثاني لمزود الخدمة، والثالث مجموعة الحاسبات المرتبطة، والرابع يحدد الكومبيوتر الذي تم الإتصال منه، مع ملاحظة أن عنوانIP قد يتغير في كل إتصال بشبكة الانترنت[669].

* **نظام البروكسي** :(PROXY)يعمل هذا النظام كوسيط بين الشبكة ومستخدميها بحيث يضمن مقدم الخدمة توفير خدمات الذاكرة الجاهزة، وتقوم فكره البروكسي على تلقي مزود البروكسي طلباً من المستخدم للبحث عن صفحة ما ضمن الذاكرة الجاهزة، فيتحقق البروكسي فيما إذا كانت هذه الصفحة قد تم تنزيلها من قبل فيقوم بإرسالها إلى المستخدم دون حاجة إلى إرسال الطلب إلى الشبكة العالمية، أما إذا لم يتم تنزيلها من قبل فيتم إرسال الطلب إلى الشبكة العالمية وهنا يستخدم البروكسي أحد عناوين IP.و من أهم مزايا هذا النظام أن الذاكرة المتوفرة لديه يمكن أن تتحفظ بتلك العمليات التي تمت عليها مما يجعل دوره قوي في الإثبات عن طريق فحص تلك العمليات المحفوظة[670] .

***برنامج الدمج وفك الدمج** (pkzip)ويستخدم هذا البرنامج لفك دمج البرامج، فقد يكون المجرم المعلوماتي قد قام بدمج برامجه فلا يمكن الإطلاع عليها إلا بعد فك الدمج.[671]

* **برنامج**a Visual route5.2 و هو عبارة عن برنامج يلتقط أي عملية فحص ضد الشبكة فيقوم بتقديم أجوبة تبين المعلومان التي حدث فيها المسح والمناطق التي تم فيها الهجوم، وبعد معرفة عنوان

---

[669]– **فهدعبد الله العبيد العازمي**، مرجع سابق، ص 372./ **نعيم سعيداني**، مرجع سابق، ص 173.

[670]– **نعيم سعيداني**، نفس المرجع، 173.

[671]– **رشيدة بوكر**، مرجع سابق، ص 433.

IPإسم الجهة يرسم البرنامج خطا يوضح من خلاله مسار الهجوم بين مصدره والجهة التي إستهدفها الهجوم

.* برنامج معالجة الملفات (Xtree Progold) : وهو برنامج يمكن من العثور على الملفات في أي مكان على الشبكة أو على القرص الصلب، ويستخدم لتقييم محتويات القرص الصلب الخاص بالمتهم والأقراض المرنة المضبوطة أو يستخدم لقراءة البرامج في صورتها الأصلية.[672]

الفرع الثاني: الإجراءات الحديثة لاستدلال و جمع الدليل التقني

إضافة إلى القواعد الإجرائية التقليدية السابق الإشارة إليها والتي قد لا تكفي لاستخلاص الدليل التقني كون له ذاتية خاصة تميزه عن الدليل التقليدي، و كون الاعتماد و الارتكاز على تلك الإجراءات فقط قد ينجم عنه إفلات العديد من المجرمين من العقاب، حيث لم تسلم طرق الإثبات من تأثيرات ثورة المعلومات وتكنولوجيا الإتصالات، فالتناغم المطلوب تحقيقه دائما بين طبيعة الدليل وطبيعة الجريمة التي يولد منها ويصلح لإثباتها، أفرز إلى حيز الوجود طرقا إجرائية تتناسب والطبيعة التقنية للجريمة المعلوماتية و للدليل الرقمي، لكي يمكن عن طريقها الوصول إليه و استخلاصه.

ونقصد بذلك تكريس تقنية المعلومات لجمع الدليل الرقمي، لذلك نجد أن التشريعات الحديثة و منها التشريع الجزائري قد ساير التطور و جاء بقواعد قانونية إجرائية حديثة، من خلال القانون 06-22 المعدل والمتمم لقانون الإجراءات الجزائية المشار إليه سابقا و من خلال إجرائي التسرب و اعتراض المراسلات، و كذا من خلال القانون 04/09 حيث استحدث إجراءين آخرين و هما المراقبة الإلكترونية و حفظ المعطيات المتعلقة بحركة السير ، و كذلك ما جاءت به التشريعات المقارنة و اتفاقية بودابست و الإتفاقية العربية لمكافحة جرائم تقنية المعلومات.

و تتمثل تلك الإجراءات فيما يلي:

البند الأول: التسرب و اعتراض المراسلات السلكية واللاسلكية

إن الجرائم الماسة بقواعد الأمن المعلوماتي تعتبر من بين الجرائم الماسة بالانظمة المعلوماتية للمعطيات و التي يمكن فيها اللجوء إلى إجراء التسرب أو اعتراض المراسلات إذا اقتضت ذلك ضرورات التحري أو التحقيق بشأنها.

---

[672]- **عائشة بن قارة مصطفى**، مرجع سابق، ص 151

أولا: :التسرب

تم تنظيم هذا الإجراء من خلال التعديل الجديد لقانون الإجراءات الجزائية الجزائري لسنة 2006 في ثمانية مواد من 65 مكرر 11 إلى 65 مكرر 18 ، كما أن المشرع الجزائري حدد نطاق هذا الإجراء بالجرائم المذكورة على سبيل الحصر في المادة 65 مكرر 5 من قانون الإجراءات الجزائية و التي من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، و عليه سوف أقوم بتحديد مفهوم التسرب و شروطه و كيفية تطبيقه في مجال الأمن المعلوماتي.

1 -**مفهوم التسرب:**

لغتا: فعل تسرب يتسرب تسربا أي دخل و إنتقل خفية، و تعني الولوج أو الدخول بطريقة تسللية إلى مكان ما، أو جماعة و جعلهم يعتقدون بأن المتسرب ليس غريبا و إشعاره بأنه واحدا منهم و هو ما يمكنه من معرفة توجهاتهم[673].

إصطلاحا: التسرب له عدة مصطلحات مشابهة كالتوغل أو الاختراق و هي تقنية يسمح بموجبها الدخول لوسط مغلق كجماعة إجرامية أو شبكة تتاجر في مواد ممنوعة مما يفيد إقحام عنصر أجنبي عن الجماعة المراد اختراقها[674].

و المشرع الجزائري عرفه بموجب المادة 65 مكرر 12 من قانون الإجراءات الجزائية على أنه:" قيام ضابط أو عون الشرطة القضائية تحت مسئولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك أو خاف".

يراد بالتسرب العملية المحضر لها و المنظمة، المراد من القيام بها التوغل داخل وسط لمعرفة حقيقته معرفة جيدة من خلال نشاطه البارز وكشف الخفي فيه، و يكون هذا الوسط محددا مسبقا بطبيعته و العمل من أجل الإستعلام عنه ومعرفة أدق تفاصيله و خصوصياته وأسراره حسب تطلعات الجهات الأمنية وفائدة المصلحة [675]، و لا شك أن التسرب عملية معقدة تتطلب دخول عون مكلف بالعملية في الاتصال بالأشخاص المشتبه فيهم في نشاط الخلية الإجرامية، و لا شك كذلك أنه إجراء خطير لأنه قد يتطلب المشاركة المباشرة للمتسرب و ضرورة قبوله في هذه الخلية.

673– **قادري أعمر**: أطر التحقيق،دار هومة للنشر، الجزائر، ط 2013، ص 72.

674– المرجع نفسه، ص 72.

675– **نعيم سعيداني**، مرجع سابق، ص175.

و يمكن تصور التسرب في جرائم تقنية المعلومات من خلال دخول ضابط أو عون الشرطة القضائية في العالم الافتراضي و اشتراكه في إتصال المباشر حول كيفية قيام الاشخاص باختراق الشبكات أو بث فيروسات مع ايهام الفاعلين على انه فاعل مثلهم.

و نص المشرع الفرنسي عن التسرب (Infiltration) في المواد 81-706 إلى 87-706 المضافة بالقانون رقم 2004-204[676] وكذا المادتين 694-7 و [677] 694 -9 من قانون الإجراءات الجزائية المعدل و المتمم .

2 -**شروط صحة التسرب** : باعتبار عملية التسرب إجراء غير عادي لجمع المعطيات و البيانات الخاصة التي تشير إلى كافة الأعمال الإجرامية و تمكين المصالح الأمنية من معرفة الامكانيات و الاساليب المستعملة لارتكاب الافعال المجرمة إلا أنه يعد من أخطر الإجراءات إنتهاكا لحرمة الحياة الخاصة للمشتبه فيه، فقد أحاطه المشرع بجملة من الشروط يتعين مراعاتها عندما تقتضي ضرورات التحري والتحقيق اللجوء إليه، و هي كالأتي:

أ. **الشروط الشكلية:** من الشروط الشكلية التي يجب أن تتوفر في عملية التسرب ما يلي:

أ.1 أن يكون التسرب بموجب إذن قضائي: لا تتم عملية التسرب دون أن يحصل ضابط الشرطة القضائية على إذن مسبق من قبل وكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية و هذا ما أكدت عليه المادة 65 مكرر 11 من قانون الاجراءات الجزائية الجزائري.

أ.2 – يجب أن يكون مكتوبا : يجب أن يكون هذا الإذن مكتوبا وإلا كان الإجراء باطلا، وهذا ما نصت عليه المادة 65 مكرر 15 إ.ج.ج بقولها " يجب أن يكون الإذن المسلم طبقا للمادة 65 مكرر 11 مكتوبا تحت طائلة البطلان " ذلك أن الأصل في العمل الإجرائي الكتابة، ومن جهة أخرى فإن الإذن يجب أن يتضمن مجموعة من الشروط يتوقف على تحديدها صحة الإجراء في حد ذاته كذكر هوية ضابط الشرطة القضائية الذي تتم عملية التسرب تحت مسؤوليته.

---

[676] - Art 706-81 au 706-87 du Code De Procédure Pénal Français Créé par art. 1 du la Loi n° 2004-204 du 9 mars **2004** ***portant adaptation de la justice aux évolutions de la criminalité***, JORF 10 mars 2004 en vigueur le 1er octobre 2004**.**

[677] -Art 694-7 et 694-9 du Code De Procédure Pénal Français Créé Par Art.17 Du La Loi n° 2004-204 du 9 mars 2004 ***portant adaptation de la justice aux évolutions de la criminalité,*** JORF 10 mars 2004 en vigueur le 1er octobre 2004.

أ.3 تحديد المدة لعملية التسرب : مدة سريان عملية التسرب حددها المشرع الجزائري بموجب نص المادة 65 مكرر 15 الفقرة الثالثة و التي يجب ألا تتجاوز أربعة أشهر و يمكن أن تجدد حسب مقتضيات التحري والتحقيق ضمن نفس الشروط الشكلية والزمنية، وفي نفس الوقت أجاز القانون للقاضي الذي أذن بهذا الإجراء أن يأمر في أي وقت بوقفه قبل انقضاء المدة المحددة إذا اقتضت الضرورة ذلك، كما أن المشرع استثنى الحالة التي يجد فيها المتسرب صعوبة الانسحاب من المجموعة أو الشبكة بأن يبقى لمدة قد تصل إلى ضعف المدة القانونية.

ب. الشروط الموضوعية:

يمكن إيجاز الشروط الموضوعية لعملية التسرب وفق الأحكام التي نظمها المشرع الجزائري في شرطين أساسين- :

الأول يتمثل في تحديد نوع الجريمة والتي يجب ألا تخرج عن الجرائم التي حددتها على سبيل الحصر المادة 65 مكرر 05 في سبعة أنواع وهي:" جرائم المخدرات، الجريمة المنظمة العابرة للوطنية، جرائم تبيض الأموال، الجرائم الإرهابية، جرائم الفساد، الجرائم المتعلقة بالتشريع الخاص بالصرف والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

و هذه الأخيرة يمكن إدراج الجرائم الماسة بالأمن المعلوماتي تحت مضلتها حتى يمكن القيام بإجراء عملية التسرب

أما الشرط الموضوعي **الثاني** فهو أن يكون الإذن بالتسرب مسبباً [678]، و ذلك بان يورد ضابط الشرطة القضائية المبرر من طلب الاذن لعملية التسرب و تبين العناصر التي تقنع الجهات القضائية المختصة لمنح الإذن و كذا تقدير العناصر التي دفعت ضابط الشرطة القضائية للجوء إلى هذا الإجراء.

فالتسبيب هو أساس العمل القضائي و من ثم كان لزاما عند إصدار الإذن بالتسرب سواء من طرف وكيل الجمهورية أو قاضي التحقيق اظهار جميع الأدلة[679] و إلا كان الإذن بالتسرب باطلا.

و ما يمكن الإشارة إليه أن الإذن المكتوب و المسبب يشترط إيداعه بملف الإجراءات المنجز عند نهاية عملية التسرب التي تتم في سرية.

3 - اثار التسرب

---

[678]– بحسب ماجاء في المادة 65 مكرر 15 من قانون الإجراءات الجزائية الجزائري و التي تقضي بأن: " يجب أن يكون الإذن المسلم طبقا للمادة 65 مكرر 11 مكتوبا و مسببا و ذلك تحت طائلة البطلان..."

[679]– رشيدة بوكر، مرجع سابق، ص 437.

يقوم العون بمباشرة عملية التسرب بعد حصوله على الإذن من الجهة المختصة وذلك بحسب ما تقتضيه هذه العملية و قد يترتب على ذلك مجموعة من الآثار من أهمها:

أ. تسخير الوسائل المادية و القانونية لتسهيل عمل المتسرب بحسب ما جاءت به المادة 65مكرر 14 إجراءات جزائية جزائري من إمكانية اقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتوجات أو وثائق أو معلومات متحصل عليها من إرتكاب الجرائم أو مستعملة في إرتكابها.

و كذا إستعمال أو وضع تحت التصرف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني مثل الرخص و البطاقات و الوثائق الرسمية التي تسهل العملية أو الوسائل المالية و وسائل النقل و الاتصال.

ب. إعفاء العون المتسرب من المسؤولية: يراد بذلك أن ضابط أو عون الشرطة القضائية القائم بالمهمة أو الذين يتم تسخيرهم في عملية التسرب غير مسئولين جزائيا عن اقتناء أو حيازة و نقل و تسليم و إعطاء مواد أو أموال أو منتوجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو المستعملة في ارتكابها و ذلك بحسب ما جاء في المادة 65 مكرر 14 ق.إ.ج.ج و كذلك فإن المتسرب يتمتع بالحماية القانونية حتى بعد انتهاء مهمته و كذلك عائلته[680].

ت. إضافة إلى ذلك فإنه لتمام عملية التسرب و نجاحها يجب أن تحاط بالسرية التامة، لذلك أقر المشرع الجزائري جزاء عقابي مشدد على من يظهر أو يكشف الهوية الحقيقية للضابط أو العون المتسرب الذي يقوم بها تحت هوية مستعارة(المواد 65مكرر 16 –65 مكرر 18).

ث. إذا تقرر وقف عملية التسرب سواء لانقضاء المهلة المحددة لها في إذن التسرب أو بسبب عدم تمديد المهلة، يجوز للعون المتسرب مواصلة نشاطه مع الجماعة الإجرامية للوقت الضروري الكافي لضمان انسحابه بشكل أمن دون أن يكون مسئولا جزائيا على أن لا يتجاوز ذلك مدة أربعة أشهر.

ثانيا: إعتراض المراسلات السلكية و اللاسلكية

في إطار الإجراءات الحديثة التي جاء بها المشرع الجزائري بموجب القانون رقم 06/22 المعدل و المتمم لقانون الإجراءات الجزائية استحدث هذه العملية من خلال الفصل الرابع من الباب الثاني من

---

[680]– المواد من **65 مكرر 16 إلى 65 مكرر 18** من **قانون الإجراءات الجزائية الجزائري.**

الكتاب الأول تحت عنوان إعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور، وقد ضمنه ستة مواد من المادة 65 مكرر5 إلى المادة 65 مكرر 10، وتناول من خلالها المقصود بهذا الإجراء و ضمانات استخدامه كما سيأتي بيانه :

1- مفهوم إجراء إعتراض المراسلات السلكية واللاسلكية و شروطه القانونية:

إستحدث المشرع الجزائري هذا الإجراء بموجب القانون رقم 06/22 المؤرخ في ديسمبر سنة 2006المعدل و المتمم لقانون الإجراءات الجزائية

أ. مفهوم إعتراض المراسلات السلكية و اللاسلكية:

من خلال نص المادة 65 مكرر 05 من قانون الإجراءات الجزائية نجد أن المشرع الجزائري يقصد بإعتراض المراسلات، إعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الإتصال السلكية واللاسلكية، و هذه المراسلات هي عبارة عن بيانات قابلة للإنتاج والتوزيع ،التخزين أو الاستقبال والعرض

أما المشرع الفرنسي فلقد كرس هذه التقنية في المادة 100 من قانون الإجراءات الجزائية التي تقضي بأنه" في الجنايات أو الجنح إذا كانت العقوبة تفوق سنتين يمكن لقاضي التحقيق إذا دعت مقتضيات البحث و التحري أن يأمر باعتراض و تسجيل و نقل المراسلات التي تتم عن طريق وسائل الاتصال"[681].

كذلك نجد في التشريع الجزائري المادة 9-6 من القانون 2000/03 المؤرخ في 05/08/2000 المحدد للقواعد العامة المتعلقة بالبريد والمواصلات،اعتبرت أن مادة المراسلات هي كل إتصال مجسد في شكل كتابي يتم عبر كافة الوسائل المادية التي يتم ترحيلها إلى العنوان المشار إليه من طرف المرسل نفسه أو بطلب منه، ولا تعتبر الكتب والجرائد والمجلات واليوميات كمادة مراسلات.

---

[681] - Art 100 de **CPPF** « 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 sont effectuées sous son autorité et son contrôle.

La décision d'interception est écrite. Elle n'a pas de caractère juridictionnel et n'est susceptible d'aucun recours » Modifie par ***Loi n°91-646 du 10 juillet 1991 - art. 2 JORF 13 juillet 1991 en vigueur le 1er octobre 1991***

و بالتالي فحسب مفهوم هذه المادة فإن المراسلات الخاصة تصبح محصورة في الرسائل المكتوبة بالمفهوم التقليدي .

إلا أنه وبالرجوع إلى نص المادة 39 من الدستور الجزائري التي تنص على أن سرية المراسلات و الإتصالات الخاصة بكل أشكالها مضمونة.

و كذلك نص المادة 303 من قانون العقوبات التي تعاقب كل من يفض أو يتلف رسائل أو مراسلات موجهة للغير، فإنه يمكن التوصل للقول أن المراسلات الخاصة تعني كل رسالة مكتوبة بأي شكل من الأشكال سواء ماديا أو إلكترونيا وسواء كانت على دعامة ورقية أو رقمية، مرسلة بأي وسيلة لعدد معين ومحدد من المرسل إليهم، بإستثناء الكتب والمجلات والجرائد والحوليات التي لا تعتبر مراسلات خاصة. وهذا ما يؤكده القانون 04/09 في المادة 02/الفقرة "و" في تعريفه للإتصالات الإلكترونية على أنها تراسل أو إرسال أو إستقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية .

تختلف و تتنوع المراسلات عبر وسائل الإتصالات الحديثة والتي من أهمها التراسل عبر البريد الإلكتروني، أو بواسطة مجموعة تطبيقات مخصصة للتراسل و الاتصال باستعمال شبكة الانترنت.

و للرسائل المرسلة من الأشخاص عبر الشبكة المعلوماتية أو أحد أجهزة الكمبيوتر أو الاتصال حرمة و سرية لا يجوز للغير انتهاكها أو إختراقها بدون رضا المرسل، و إذا كانت هذه المراسلات تتمتع بالخصوصية حمى المشرع سريتها بسن قوانين تعمل على توفير قدر كبير من الحماية الجزائية لها، إلا أن هذا الأمر ليس على إطلاقه فإذا إقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الإبتدائي في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، فإنه يجوز إعتراض هذه المراسلات وكشف السرية عنها في سبيل البحث عن الدليل [682]، وهو السند الشرعي المبرر لإباحة هذا الإجراء بسبب أنه يتضمن إعتداء جسيما على حرمة الحياة الخاصة وسرية الإتصالات، فيباح إستثناءا وفي حدود ضيقة وذلك للفائدة المنتظرة منه والتي تتعلق بإظهار الحقيقية وكشف الغموض عن الجريمة وضبط الجناة .

وتجدر الإشارة في هذا الصدد أن المراسلات التي تصلح لإجراء اعتراضها يجب أن تتسم بالخصوصية، ولكي تكون كذلك يلزم أن يتوافر لديها عنصران أساسيان هما:

---

[682]- **الموسوس عتو**، مرجع سابق، ص 370.

– عنصر موضوعي ويتعلق بموضوع ومضمون الرسالة في حد ذاتها بمعنى أن تكون الرسالة ذات طابع شخصي وسري أو خاص فيما تخبر به .

– وعنصر شخصي والمراد به إرادة المرسل في تحديد المرسل إليه ورغبته في عدم السماح للغير بالإطلاع على مضمون الرسالة[683].

ب.**الشروط والضمانات المقررة لإعتراض المراسلات السلكية و اللاسلكية** : لاشك أن أسلوب إعتراض المراسلات السلكية واللاسلكية دون علم أصحابها بقدر ما يفيد في كشف الحقيقة ويسهل إثبات كثير من الجرائم الغامضة كتلك المتعلقة بالجرائم المعلوماتية، فهو من جانب آخر يمثل إنتهاكا لحرمة الحياة الخاصة للأفراد و إعتداء على سرية مراسلاتهم و إتصلاتهم [684] التي كفلتها الدساتير والتشريعات العقابية كما سبق توضيحه

والمشرع الجزائري في هذا الصدد خرج عن الأصل العام و أعطى لسلطات التحقيق إمكانية إعتراض المراسلات كأسلوب مستحدث للبحث عن دليل يتماشى مع الأساليب المتطورة التي يلجأ إليها الجناة في تنفيذ جرائمهم وإخفاء أي أثر يدل عليهم، و من ناحية أخرى لم يجعل الأمر مطلق في اللجوء إلى هذه الوسيلة بل أحاط إستخدامها بشروط قانونية تعمل على منع التعسف وتصون الحرية الفردية وتتمثل هذه الشروط في:

*ترخيص السلطة القضائية ومراقبتها لعملية التنفيذ:

طبقا للمادة 65مكرر5 من قانون الإجراءات الجزائية فإنه لا يمكن لضابط الشرطة القضائية اللجوء إلى إجراء إعتراض المراسلات السلكية و اللاسلكية إلا بعد أن يحصل على إذن مكتوب ومسبب من طرف وكيل الجمهورية أو قاضي التحقيق في حالة فتح تحقيق قضائي.

فالسلطة القضائية هي وحدها المختصة بإصدار هذا الإذن و هو ما يعد ضمانة لازمة لمشروعية هذا الإجراء[685]، و على وكيل الجمهورية أو قاضي التحقيق قبل منح هذا الإذن تقدير فائدة إجراء

---

[683]- **نعيم سعيداني:** مرجع سابق، ص 178.

[684]- تماشيا مع ظهور الهاتف النقال كوسيلة إتصال و فتح المجال أما القطاع الخاص لتقديم خدمات الاتصال، تم إصدار مراسيم تنفيذية تتضمن الموافقة على منح رخص لاقامة و إستغلال شبكة عمومية للمواصلات اللاسلكية الخلوية من نوع GSM و هي المراسيم 219/01 و 186/02 و 09/04 حيث ألزم المشرع على مقدم الخدمة من خلالها ضمان عدم التعرض لحرمة الاتصالات الخاصة و للبيانات الشخصية للمشتركين إلا في حالة وجود طلب رسمي من قبل السلطات المختصة، **الموسوس عتو**، مرجع سابق، ص 370.

[685]– نصت المادة 65 مكرر 05 **اجراءات جزائية جزائري** على أنه :" إذا إقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الإبتدائي في جرائم.... أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات يجوز لوكيل الجمهورية أن يأذن بإعتراض

الإعتراض وجديته وملاءمته لسير إجراءات الدعوى من خلال معطيات التحريات التي قامت بها الضبطية القضائية مسبقا.

مع ملاحظة أنه في فرنسا ومنذ صدور القانون 2004/204 المؤرخ في 2004/03/09المعدل لقانون الإجراءات الجزائية أصبح حسب المادة 706/95 الإذن بإعتراض المراسلات من إختصاص قاضي الحريات والإحتباس بمنحه بناءا على طلب من وكيل الجمهورية إذا تعلق الأمر بالتحقيق في الجرائم المحددة حصرا بالمادة 73-706، وتخضع إجراءات الإعتراض لرقابته في أجل 15 يوم قابلة للتجديد بنفس الشروط في الشكل والأجل[686].

و قد نصت المادة 65 مكرر 09 على أن عملية تنفيذ إجراء إعتراض المراسلات تتم تحت رقابة السلطة القضائية التي أذنت به و ذلك من خلال قيام ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص بإعداد محضرا عن كل عملية إعتراض للمراسلات وكذا عن عمليات وضع الترتيبات التقنية لهذا الغرض، و يذكر في هذا المحضر تاريخ وساعة بداية هذه العمليات و الإنتهاء منها

* تحديد طبيعة المراسلة: وهذا ما يفهم صراحة من نص المادة 65 مكرر 7 التي نصت على أنه يجب أن يتضمن الإذن بإعتراض المراسلات كل العناصر التي تسمح بالتعرف على الإتصالات أو المراسلات المطلوب إعتراضها.

*تحديد الجرائم التي يجوز فيها الاعتراض: و هي إحدى الجرائم المحددة في المادة 65 مكرر 5 من ق.إ.ج.ج و التي يجوز فيها مباشرة إعتراض المراسلات و تسجيل الاتصالات و إلتقاط الصور نظرا لخصوصية هذه الجرائم و لعدم كفاية الإجراءات التقليدية لجمع الدليل التقني و استكمال مقتضيات التحقيق و من بين تلك الجرائم نجد جرائم المساس بأنظمة المعالجة الآلية للمعطيات.

المراسلات التي تتم عن طريق وسائل الإتصال السلكية واللاسلكية.... وفي حالة فتح تحقيق قضائي تتم العملية بناءا على إذن من قاضي التحقيق وتحت مراقبته المباشرة."

[686] –**Art** 706-95 du **C.P.P.F** dispose que ; « Si les nécessités de l'enquête de flagrance ou de l'enquête préliminaire relative à l'une des infractions entrant dans le champ d'application de l'article 706-73 l'exigent, le juge des libertés et de la détention du tribunal de grande instance peut, à la requête du procureur de la République, autoriser l'interception, l'enregistrement et la transcription de correspondances émises par la voie des télécommunications selon les modalités prévues par les articles 100, deuxième alinéa,100-1 et 100-3 à 100-7, pour une durée maximum d'un mois, renouvelable une fois dans les mêmes conditions de forme et de durée. Ces opérations sont faites sous le contrôle du juge des libertés et de la détention ».

* تحديد مدة الإعتراض: إستوجب المشرع أن لا تتجاوز مدة هذا الإجراء أربعة أشهر قابلة للتجديد حسب تقدير نفس السلطة مصدره الإذن وفقا لمقتضيات التحري والتحقيق طبقا للمادة 65 مكرر 7 الفقرة 02 و هي نفس المدة التي حددها المشرع الفرنسي في المادة 100 من قانون الإجراءات الجزائية الفرنسي.

و أمام هذه الإجراءات يتضح أن حقوق الأشخاص الأساسية بدأت تتضاءل أمام مكافحة الأشكال الحديثة للإجرام المعلوماتي التي قد تهدد أمن الأشخاص و ممتلكاتهم المادية و المعنوية.

البند الثاني: حفظ المعطيات المتعلقة بحركة السير

نظرا لطبيعة البيئة التي يوجد بها الدليل التقني الذي قد يتم إزالته بسرعة أو محاولة إتلافه، نجد أن المشرع قد تنبه لمسألة إجراء حفظ بعض المعطيات التي قد تفيد في كشف الجريمة الماسة بالمعالجة الآلية للمعطيات و للحفاظ على أدلة الإثبات و ألزم الجهات التي تقدم خدمات الاتصال [687] بواسطة منظومة معلوماتية بحفظ تلك المعطيات .

فما المقصود بحفظ المعطيات المتعلقة بحركة السير ؟ و كيف يتم حفظها و إلى متى؟

حفظ المعطيات أو التحفظ عليها هو إجراء قانوني و أداة جديدة للتنقيب في مجال مكافحة الإجرام المعلوماتي بمختلف أشكاله خاصة المرتكبة بواسطة شبكات الاتصال، و إحدى الوسائل للمحافظة على سلامة البيانات حيث يكون للسلطات المختصة بالتفتيش و التنقيب طريقة أخرى لضبط هذه البيانات و المعلومات و الحصول عليها من مزودي الخدمات.

و عليه يقصد بحفظ المعطيات قيام مزود الخدمة بتجميع المعطيات المعلوماتية و حفظها و حيازتها في أرشيف و ذلك بوضعها في ترتيب معين و الاحتفاظ بها في المستقبل في انتظار اتخاذ إجراءات قانونية أخرى كالتفتيش و غيره[688].

---

[687]- تعرف تلك الجهات **بمزودي الخدمات** و التي عرفها المشرع الجزائري في المادة (2) الفقرة (د) من القانون رقم ***09-04*** ***المتضمن الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها*** على أنها:" 1- أي كيان عام أو خاص يقدم لمستعملي خدماته، ضمانة القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام للاتصالات؛

2- و أي كيان أخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها".

كما عرفتها ***الاتفاقية العربية لمكافحة جرائم تقنية المعلومات*** في المادة (02) الفقرة الثانية على أنها:" أي شخص طبيعي أو معنوي عام أو خاص يزود المشتركين بالخدمات للتواصل بواسطة تقنية المعلومات، أو يقوم بمعالجة أو تخزين المعلومات نيابة عن خدمة الاتصالات أو مستخدميها".

[688]- **رشيدة بوبكر**، مرجع سابق، ص 448.

و في إطار تحديد المقصود بحفظ المعطيات المعلوماتية المخزنة أو التحفظ عليها المشار إليها في اتفاقية بودابست بموجب المادة السادسة عشر،أشارت المذكرة التفسيرية لاتفاقية إلى أهمية التفرقة بين مصطلحي " **التحفظ على البيانات** " و " **الاحتفاظ أو أرشفة البيانات**" فرغم أن للكلمتين معنيين متجاورتين في اللغة الشائعة لكن لهما معنى مختلف في لغة المعلوماتية؛ إذ أن عبارة "يحتفظ على البيانات" تعني حفظ بيانات سبق وجودها في شكل مخزن و حمايتها من كل شيء يمكن أن يؤدي إلى إتلافها أو تجريدها من صفتها أو حالتها الراهنة.

في حين أن عبارة: " الاحتفاظ بالبيانات" تعني حفظ البيانات لدى حائزها بالنسبة لمستقبل البيانات التي في طور الإنتاج و التوالد، فأرشفة البيانات يشير إلى تجميع البيانات في الوقت الحاضر و حفظها أو حيازتها في أرشيف،أي وضعها في ترتيب معين و الاحتفاظ بها في المستقبل[689].

و معنى ذلك أن " أرشفة البيانات" عبارة عن عملية تخزين للبيانات على عكس " التحفظ على البيانات" الذي يعني النشاط الذي يضمن للبيانات سلامتها و سريتها.

رجوعا للمشرع الجزائري بخصوص المعطيات المعلوماتية التي يراد الاحتفاظ بها من وراء هذا الإجراء هل يقصد بذلك كل المعطيات أم حددها بنوع معين من المعطيات؟

غن المشرع الجزائري حدد المعطيات المعلوماتية الواجب حفظها بما يسمى " **معطيات حركة السير** " أو بما يطلق عليها معطيات حركة المرور [690] و التي عرفها بموجب الماد الثانية فقرة " هـ" من القانون 09-04 على أنها: " أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة بإعتبارها جزءا في حلقة الاتصالات توضح مصدر الاتصال ، و الوجهة المرسل إليها، و الطريق الذي يسلكه و وقت و تاريخ و حجم و مدة الاتصال و نوع الخدمة".

ما يمكن ملاحظته في توضيح المشرع لهذا الإجراء انه تضمن بعض المصطلحات التقنية أكثر منها قانونية، و مما لا شك فيه أن مقصد المشرع من وراء هذا الإجراء هو التعرف على هوية الفاعل و كشف مصدر اتصالاته و مكان تواجده إلى غير ذلك من الإجراءات التي تساعد المحققين في كشف كل الأدلة التقنية.

689- **د. هلالي عبد اللاه أحمد**، الجوانب الموضوعية و الإجرائية لجرائم المعلوماتية، مرجع سابق، ص 186،187.

690- حددت **المادة (11) من القانون 09-04** المشار إليه سابقا بعض طوائف معطيات حركة المرور التي يلزم على مزود الخدمة الاحتفاظ بها.

إضافة إلى تحديد المعطيات محل هذا الإجراء فإن المشرع الجزائري كذلك ألزم مزود الخدمة بعدم الإحتفاظ بتلك المعطيات لفترة اكثر من سنة [691] من تاريخ التسجيل و هذا ما يستفاد من نص المادة الحادية عشر من القانون 09-04 بقولها:" ... تحدد مدة حفظ المعطيات المذكورة في هذه المادة بسنة واحدة ابتداء من تاريخ التسجيل..." و لعل مرجع تحديد تلك المدة يعود إلى رغبة المشرع في الاحتفاظ بحق الخصوصية.

كما أن المشرع الجزائري قد رتب عقوبات في حالة إخلال مزود الخدمة بهذا الالتزام و تقوم مسئوليته[692] إضافة إلى العقوبات الإدارية التي يحددها دفتر الشروط المحدد مع الهيئات التي يتعاملون معها، و حددت العقوبة الجزائية بموجب الفقرة الأخيرة من المادة 11 من القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحته.

المطلب الثالث: صعوبات تطبيق القواعد الإجرائية لاستخلاص الدليل التقني

يظهر التحري و البحث عن الدليل الرقمي في العالم الافتراضي و التحقيق في الجرائم المعلوماتية عامة و الماسة بقواعد الأمن المعلوماتي خاصة العديد من المعوقات و الصعوبات التي قد تعرقل سير هذه الإجراءات، و ما نتج عنها من تحديات تواجهها الجهات المختصة بالبحث و التحري في تطبيق القواعد الإجرائية التي نظمت لاستخلاص الدليل الرقمي، وقد تؤدي إلى التقليل من قيمتها في مكافحة هذا النوع من الجرائم و تؤثر على عملية التحقيق، و أن أي خطا فيها قد يؤدي إلى فوات فرصة كشف الجريمة أو فوات فرصة الإدانة حتى مع معرفة الجاني، ما ينعكس سلبا على المحقق بفقدانه الثقة في أجهزة التحقيق، بل و تنعكس على المجرم في حد ذاته حيث يشعر أن الجهات الأمنية غير قادرة على اكتشاف أمره و أن خبرة القائمين على مكافحة الجريمة و التحقيق فيها لا تجاري خبرته.

691- حددت **المادة 2/23 من** ***لاتفاقية العربية لمكافحة جرائم تقنية المعلومات*** مدة التحفظ العاجل على البيانات المخزنة في تقنية المعلومات بقولها:" 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 سلامة تلك المعلومات لمدة أقصاها 90 يوما قابلة للتجديد و من أجل تمكين السلطات المختصة من البحث والتقصي..".

692- تنص ***المادة 11 فقرة أخيرة من القانون رقم 09-04 المتضمن بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحته*** على أنه: ".....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. و يعاقب الشخص الطبيعي بالحبس من (06) أشهر إلى (05) سنوات و بغرامة من 50000 دج إلى 500000 دج ".

و من أهم الصعوبات التي قد تواجه الجهات المختصة بتطبيق إجراءات استخلاص الدليل التقني منها ما يلي:

الفرع الأول:المعوقات المتعلقة بجهات التحقيق وإجراءات الحصول على الدليل : من أهم المعوقات أو الصعوبات التي قد تواجه التحقيق في الجريمة المعلوماتية معوقات تتعلق بجهات التحقيق وإجراءات الحصول على الدليل، وسوف نحاول أن نتناول ذلك بشيئ من التفاصيل على النحو التالي:

البند الأول:المعوقات المتعلقة بجهات التحقيق

تتعلق هذه المعوقات بالعامل البشري القائم بالتحقيق في الجريمة المعلوماتية، فإذا كانت السلطات القائمة بالتحقيق من رجال الضبطية القضائية وقضاة بما لها من خلفية قانونية تلعب دورا كبيرا في التحري عن الجرائم والبحث عن مرتكبيها في إطار الجرائم التقليدية فإن وظيفتها في مكافحة الجرائم المعلوماتية لا ترق إلى نفس الدرجة، ذلك أن الطبيعة الخاصة للبيئة الإلكترونية التي تتعامل معها فضلا عن خصوصية الدليل الرقمي ينعكس على عمل الجهات المكلفة بالبحث والتحري.

حيث يتطلب الكشف عن هذه الجرائم إكتساب جهات التحقيق مهارات خاصة على نحو يساعدهم على مواجهة التقنيات المعلوماتية [693]، إذ يرى المتخصصون في مكافحة الجرائم المعلوماتية أن الأنظمة المعلوماتية وما يقع عليها من جرائم تعد تحديا هائلا لأجهزة العدالة الجنائية ذلك أن رجل الأمن غير المتخصص و الذي إنحصرت معلوماته في جرائم قانون العقوبات بصورته التقليدية من قتل وضرب وسرقة لن يكون قادرا على التعامل مع الجريمة المعلوماتية و التي تقع بطريقة تقنية عالية.

فنقص المهارة الفنية في إستخدام الكومبيوتر والانترنت وعدم توفر المعرفة بأساليب إرتكاب الجريمة المعلوماتية وقلة الخبرة في مجال التحقيق والتحري عن جرائم العالم الإفتراضي، عوامل من شأنها أن تضعف دور الأجهزة المختصة بالتحقيق في الجرائم وكشف النقاب عنها[694].

و ليس هذا فحسب فإن من المسائل التي تشكل عقبة أمام سلطات التحقيق مسألة كيفية التعامل والحفاظ على الأدلة الرقمية التي مكمنها الحواسيب والخوادم والمضيفات والشبكات .لأجل ذلك بدأت بعض الأجهزة الأمنية والقضائية في إستقطاب المتخصصين في الكومبيوتر ليكونوا ضمن كوادرها، كما يجري تدريب رجال الضبطية والقضاة على إستخدام الحواسيب وتكنولوجيا المعلومات، وعلى الرغم من

693- **رشيدة بوكر**، مرجع سابق، ص 461.

694– **نعيم سعيداني**، مرجع سابق، ص 186.

ذلك فقد تكون تلك الأجهزة غير قادرة على مواكبة التطور السريع في مجال تكنولوجيا المعلوماتية لعدة أسباب أهمها،

أن تكون أمام أجهزة الشرطة والقضاء مجالات متنوعة أخرى ينبغي تغطيتها فهي ليست متفرغة تماما للجرائم المعلوماتية وحدها .إزاء ذلك يرى البعض أنه من المستحسن أن توكل مهمة التحقيق في هذا النوع من الجرائم إلى جهات متخصصة في هذا المجال سيما مع وجود شركات عالمية متخصصة في تحقيق الجرائم المعلوماتية حققت النجاح في كثير من الحالات.

إلا أن هذا الرأي لم يلق القبول لدى الكثير من الأنظمة القانونية ذلك أن متطلبات العدالة الجنائية تقتضي تحمل الأجهزة الأمنية الحكومية كامل المسؤولية تجاه إكتشاف كافة الجرائم ومن بينها الجرائم المعلوماتية[695]، وفي هذا الصدد ألزمت الاتفاقية الأوروبية لجرائم تقنية المعلومات الدول الأطراف بضرورة تبني الإجراءات التشريعية أو أية إجراءات أخرى ترى أنها ضرورية وفقا لقانونها الداخلي من أجل إنشاء وتأسيس سلطات مختصة في مجال التنقيبات و الإجراءات الجنائية النوعية في مجال الجريمة المعلوماتية.

وقد بادرت مختلف الدول إلى إنشاء وحدات متخصصة في مجال البحث و التحري عن الجريمة المعلوماتية داخل الأجهزة الحكومية.

وفي الجزائر فإنه وبالاضافة إلى المصالح الضبطية القضائية التابعة للشرطة أو الدرك فإنه وبموجب المرسوم الرئاسي رقم 04/183 المؤرخ في 26/06/2004 تم إحداث المعهد الوطني للأدلة الجنائية وعلم الاجرام تحت وصاية القيادة العامة للدرك الوطني، حيث تنص المادة الثانية من هذا المرسوم أنه يكلف هذا المعهد بإجراء الخبرات و الفحوص العلمية في إطار التحريات الأولية و التحقيقات القضائية بغرض إقامة الأدلة التي تسمح بالتعرف على مرتكبي الجنايات و الجنح، وذلك بناء على طلب من القضاة أو المحققين أو السلطات المؤهلة، ويحتوي هذا المعهد على قسم الإعلام الآلي يختص بالتحقيق في كل ما يتصل بالجرائم المعلوماتية و إلى جانبه يوجد مركز الوقاية من جرائم الإعلام الآلي و الجرائم المعلوماتية تابع أيضا لقيادة الدرك الوطني وهو قيد الإنشاء، أما على مستوى المديرية العامة للأمن الوطني فتوجد مخابر الشرطة العلمية التابعة لمديرية الشرطة القضائية، ومن الفروع التقنية التي تضمها هذه المخابر، خلية الإعلام الآلي والتي تختص بالتحقيق في كل ما يتصل بالجرائم المعلوماتية بناء على تسخيرات أو إنابات قضائية.

---

[695]- نفس المرجع، ص 187.

وحتى تكتمل قدرات تلك الأجهزة في هذا المجال فقد تم إنشاء الهيأة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته و قد تم توقيع مرسوم رئاسي بشأنها[696]، تتولى هذه الهيأة خصوصا تنشيط وتنسيق عمليات الوقاية من هذا النوع من الجرائم وتعمل على تقديم المساعدة للسلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والإتصال، بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية كما يوكل لهذه الهيأة عملية تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكان تواجدهم[697] .

وفي إطار محاولة التغلب على المعوقات والصعوبات التي تواجه جهات التحقيق في مجال الجريمة المعلوماتية فإنه من غير الكافي أن يتم إنشاء أجهزة فنية متخصصة، بل لابد من إتباع ذلك بتوفير إستراتيجية تدريبية وتكوين متعمق في ميدان تكنولوجيات الإعلام والإتصال العاملين في مجال العدالة الجزائية بصفة عامة.

ثانيا: المعوقات المتعلقة بإجراءات الحصول على الدليل

إذا كان من السهل على جهات التحري والتحقيق أن تتحرى عن الجرائم التقليدية عن طريق المشاهدة أو التتبع أو سماع الشهود، فإنه قد يصعب عليها ذلك بهذه الطرق بالنسبة للجرائم المعلوماتية التي ترتكب بالوسائل الإلكترونية، وهذا راجع إلى الطبيعة الرقمية التي يتكون منها الدليل التقني سواء من حيث كونه غير مرئي في شكل نبضات مغناطيسية أو كهربائية لا يدركها الرجل العادي بالحواس الطبيعية، أو من حيث تواجده في العالم الإفتراضي على الكيفية المعنوية غير الملموسة ضمن مكون رقمي في شكل مختلط وذلك نتيجة لعدم إمكانية وجود فرز ذاتي في إطار التخزين الرقمي، وما يترتب على هذه الخاصية الأخيرة من صعوبة في جمع المعلومات الجنائية التي تفيد البحث والتحقيق الجنائي، ذلك لأنها عادة ما تكون مختلطة بغيرها من المعلومات العادية لمستخدمي الحواسيب غير المشتبه فيها وهو أمر قد يشكل تهديدا لخصوصية هؤلاء نظر لإمكانية إمتداد آثار تفتيش النظام المعلوماتي إليهم.

---

[696]- تم التصديق على إنشاء الهيئة الوطنية لمكافحة جرائم الاعلام و الاتصال بموجب **مرسوم رئاسي** رقم 15-261 بتاريخ 08 اكتوبر 2015 يحدد تشكيلة و تنظيم سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها، الملحق رقم 02 ص 321. و قد

[697]– حسب المادتين 14–13 من القانون 09/04 المتعلق **بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها**.

فضلا عن ذلك فإن المجرم المعلوماتي غالبا ما يضرب سياجا أمنيا على أفعاله غير المشروعة قبل إرتكابه لها، فيزيد بذلك من صعوبة تطبيق القواعد الإجرائية التي يتوقع حدوثها للبحث عن الأدلة التقنية التي تدينه وذلك بالعمل على ترميز أو تشفير المعلومات المخزنة إلكترونيا والمنقولة عبر شبكات الإتصال، بحيث يستحيل على غيره الإطلاع عليها ويصبح بذلك الدليل الرقمي مشفرا و بالتالي يكون عائقا أمام سلطات البحث والتحقيق أثناء تطبيقها للقواعد الإجرائية المقررة لإستخلاصه.

ومن الصعوبات التي تعيق التحقيق في مجال الجريمة المعلوماتية والمرتبطة بالدليل الرقمي هي سهولة محو هذا الدليل أو تدميره في زمن قصير جدا، فإرتباط الجريمة المعلوماتية بالبيئة التقنية إنعكس على طبيعة الدليل المترتب عنها من حيث أن أمر طمسه ومحو آثاره من قبل الفاعل أمرا في غاية السهولة، إذ بإمكان المستخدم الذي يتحكم في المعلومات أن يستعمل نظاما معلوماتيا من أجل محو تلك المعلومات التي تعد موضوعا للتنقيب الجنائي وبالتالي تدمير كل الأدلة.

فالجاني يمكنه أن يمحو الأدلة التي تكون قائمة ضده أو تدميرها بحيث لا تتمكن السلطات من كشف الجريمة، و إذا ما علمت بهذا لا تستطيع إقامة الدليل ضده لذلك فإن التحفظ على المعطيات يعتبر إجراء أوليا أو تمهيديا، الهدف منه هو الإحتفاظ على المعطيات قبل فقدانها.

وقد يكون ذلك بالتعاون مع الجهات التي تقدم الخدمة بإلزامهم بطريقة أو بأخرى على حفظ المعطيات المعلوماتية المخزنة بما في ذلك المعطيات المتعلقة بالمرور المخزنة بواسطة نظام معلوماتي.

وفي هذا الإطار نجد أن المشرع الجزائري قد ألزم في المادة 10 من القانون 09/04 مقدمي الخدمات بحفظ المعطيات المتعلقة بحركة السير و التي حددها في المادة 11 من نفس القانون ووضعها تحت تصرف السلطات المكلفة بالتحريات القضائية.

الفرع الثاني: المعوقات المتعلقة بالجهات المتضررة وصعوبة تحديد الجاني :بالإضافة إلى المعوقات المتعلقة بجهات التحقيق وإجراءات الحصول على الدليل، فهناك معوقات أخرى تتعلق بالجهات المتضررة والقدرة على تحديد الجاني.

البند الأول: معوقات التحقيق المتعلقة بالجهات المتضررة:

قد يكون للجهات المتضررة من الجريمة المعلوماتية يد في إعاقة التحقيق و الوصول إلى الدليل لإثبات الجريمة، فالتقنية المستخدمة في نظم المعلومات تعد مجال إستثمار و تسابق بين الشركات مما يدفعها في مقابل تحقيق الربح إلى تبسيط الإجراءات وتسهيل إستخدام البرامج وملحقاتها وزيادة المنتجات وإقتصار تركيزها على تقديم الخدمة في مقابل إهمال الجانب الأمني.

و قد وصل الحد ببعض مستخدمي شبكات الأنترنت عبر مزودي الخدمة في خضم التنافس التجاري إلى درجة عدم مطالبة المشتركين بتحديد هوياتهم عند الإشتراك في خدمة الانترنت مما يحول دون معرفة هوية المستخدم في حالة البحث والتحري عنها من طرف جهات التحقيق، ومن ناحية أخرى فإن كثيرا من الجهات التي تتعرض أنظمتها المعلوماتية للإعتداء تعمد إلى عدم الكشف و التبيلغ عن ذلك لدى السلطات المختصة [698] تجنبا للإضرار بسمعتها أو خوفا من أن الكشف عن أسلوب إرتكاب الجريمة قد يؤدي إلى تكرار وقوعها بتقليدها من طرف الآخرين .

فذاتية الجريمة المعلومية من حيث كونها مجهولة و مستترة تتم في بيئة تقنية لا تترك وراءها أي أثر خارجي تحول دون إكتشافها من طرف المجني عليه، وإذا ما تصادف وإكتشفها فإنه يعمد في أغلب الأحيان إلى التستر عليها والصمت بدل إبلاغ الشرطة للتحقيق بشأنها ومعرفة مرتكبها وهو ما ينجم عنه عدم التعاون مع السلطات المختصة لمكافحة هذا النمط الإجرامي.

لأجل ذلك فقد طرحت العديد من الإقتراحات لحمل المجني عليهم في الجريمة المعلوماتية على التبليغ والتعاون مع السلطات بأن تفرض النصوص القانونية المتعلقة بجرائم المعلوماتية إلتزاما على عاتق موظفي الجهات المجني عليها بالإبلاغ عما يصلهم من أخبار عن وقوع تلك الجرائم مع تقدير الجزاء عن الإخلال بهذا الإلتزام.

البند الثاني: صعوبة تحديد هوية الجاني

إن الوصول إلى الدليل الرقمي تعترضه عقبة أخرى تكمن في أن الجناة المتمرسين يجتهدون في إخفاء هوياتهم للحيلولة دون تعقبهم أو كشف أمرهم، بحيث تظل أنشطتهم مجهولة بمنأى عن علم السلطات المعنية بمكافحة الجريمة[699].

ومن الأمثلة التي تساق على ذلك إستخدام الجاني حاسبا آخر غير حاسبه الشخصي كإستخدام الحواسيب الموجودة في الأماكن العامة أو اللجوء إلى مقاهي الانترنت على إعتبار أن جل هذه المقاهي لا تقوم بتسجيل أسماء مرتاديها أو التحقق من هوياتهم لا سيما إذا علمنا أن شبكة الانترنت تتيح لمستخدميها إستعمال الخط الواحد من أكثر من شخص في آن واحد معا، ما يجعل مراقبة وتعقب المشتبه فيه أمرا ينطوي على الصعوبة وغير ميسور في كثير من الأحيان .

---

[698]- **رشيدة بوكر**، مرجع سابق، ص 470.

[699]- نفس المرجع، ص 475/ كذلك **موسى مسعود أرحومة** ، الإشكالات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية بحث مقدم المؤتمر المغاربي الأول حول المعلوماتية والقانون، تنظمة أكاديمية الدراسات العليا طرابلس الفترة من 29/10/2009-28.

وتعد مسألة صعوبة تحديد هوية مرتكب الجريمة المعلوماتية من إحدى المشاكل التي تطرح للكفاح ضد الإجرام المعلوماتي [700]، و إن كان يمكن معرفة النظام أي هوية الحاسوب والخادم والمضيف و الشبكات الذي إرتكبت من خلاله

وفي كل الأحوال فإن الأمر يتطلب تحسين أسلوب تتبع آثار الرسائل وتحديد هوية المستخدمين حتى يمكن تحديد هوية الشخص المسؤول جنائيا .

وفي هذا الإطار نجد أن المشرع الفرنسي قد أوجب على جميع مزودي خدمات الإتصال للجمهور أن يحددوا على مواقعهم هوية ناشر مضمون الرسالة وبياناته وذلك بموجب المادة 43 من قانون الصادر في 30/09/1986 وهذا الإجراء من شأنه أن يقدم الكثير من الشفافية بالنسبة للخدمات الموضوعة تحت تصرف الجمهور ويساعد على سهولة تحديد هوية الجاني، بالإضافة كذلك إلى ضرورة تحديد هوية المشتركين بشبكات المعلومات لتسهيل عمل الضبطية في حال وقوع أي مخالفة بحيث يجب على مؤدي الخدمة أن يكون قادرا على تقديم بيانات شخصية عن زبائنه في إطار التحقيقات عندما يطلب منه ذلك. [701]

المبحث الثاني

إقتناع القاضي الجنائي بالدليل الالكتروني

إن مسألة تقيم الدليل الجنائي في إثبات الواقعة الجرمية هي مسألة موضوعية محضة، للقاضي أن يمارس سلطته التقديرية فيها، لأجل هذا فالسائد في الفقه الجنائي أن القاضي الجزائي له الحرية في تقدير الأدلة الجنائية وتكوين قناعته، وأن يبني حكمه على أي دليل متى اطمأن إليه حتى ولو كان هذا الدليل مستمدا من محاضر جمع الاستدلالات[702].

ولا يشترط أن يكون الدليل الذي يستند إليه القاضي صريحا دالا على الواقعة المراد إثباتها بل يكفي أن يكون استخلاصها استنتاجا من الظروف و القرائن و ترتيب النتائج على المقدمات.

---

[700]– **نعيم سعيداني**، مرجع سابق، ص 191

[701]- مشار إليه لدى : **رشيدة بوكر**، مرجع سابق، ص 275،276.

[702]– **أميرة محمود بدوي الفقي**، مرجع سابق، ص159–168.

وأدلة الدعوى تخضع في كل الأحوال لتقدير القاضي ما دام هذا الدليل غير مقطوع بصحته، ويترتب على ذلك أن الأدلة الجزائية لا تحض أمام القاضي الجزائي بقوة حاسمة في الإثبات، و على هذا الأساس فكما يصح للقاضي أن يؤسس إقتناعه على أي دليل يصح له أيضا أن يهدره.

لكن في المقابل لا تعني حرية القاضي في الإقتناع التحكم المطلق بل إن القاضي يلتزم بأن يتحرى المنطق الدقيق في تفكيره الذي قاده إلى إقتناعه، ففي الوقت الذي منح فيه القانون للقاضي الجزائي حرية واسعة في مجال تقدير الأدلة وفقا لإقتناعه الشخصي وفتح أمامه باب الإثبات على مصراعيه كي يستلهم عقيدته من أي موطن يراه فإنه في المقابل لم يطلق له العنان ليقضي كيفما شاء أو أراد وفقا لمزاجه الشخصي وحسب أهوائه بل لقد أحاطه بسياج من القيود والضوابط التي تشكل في مجموعها شروطا لإعمال المبدأ و تطبيقه التطبيق الأمثل بما يضمن الوصول إلى الحقيقة الفعلية دون الافتئات على الحقوق والحريات

إلا أن تطبيق ذلك على الدليل الرقمي قد يثير بعض الصعوبات، فالقاضي بثقافته القانونية لا يمكنه إدراك الحقائق المتعلقة بأصالة الدليل الرقمي، فضلا عن تمتع هذا الدليل من حيث قوته بقيمة إثباتيه قد تصل إلى حد اليقين شأنه في ذلك شأن الأدلة العلمية عموما، ومن جهة أخرى فإن الطبيعة الفنية الخاصة بالدليل الرقمي تمكن من العبث بمضمونه على نحو يحرف الحقيقة دون أن يكون بمقدور غير المتخصص إدراك ذلك العبث، ومع نقص الثقافة المعلوماتية للقاضي الجزائي فهل عليه التوسع في سلطته عند تقدير الدليل لتمتد وتشمل الدليل الرقمي، وهل يمكن التسليم بخضوع الدليل الرقمي للمناقشة والبحث في مصداقيته لقبوله أو طرحه لعدم الإقتناع به .

وعلى حسبما سبق طرحه فإننا سوف نناقش ما هي الشروط التي يجب أن يتوافر عليها الدليل الرقمي حتى يعبر عن حقيقة علمية ثابتة (المطلب الأول) ومدى تأثير ذلك على مبدأ الإقتناع الشخصي للقاضي الجزائي (المطلب الثاني) على النحو الآتي:

المطلب الأول: سلطة القاضي في قبول الدليل التقني

نصت المادة 212 من قانون الإجراءات الجزائية على أنه يجوز إثبات الجرائم بأي طريق من طرق الإثبات و للقاضي أن يصدر حكمه تبعا لإقتناعه الخاص...."، كما نصت المادة 307 من قانون الإجراءات الجزائية أيضا أن القانون لا يطلب من القضاة أن يقدموا حسابا عن الوسائل التي بها قد وصلوا إلى تكوين إقتناعهم و أن يبحثوا بإخلاص ضمائرهم في أي تأثير قد أحدثته في إدراكهم الأدلة المسندة للمتهم "ومن خلال هذين النصين القانونيين يتضح جليا أن المشرع الجزائري قد تبنى كقاعدة

عامة نظام الإقتناع الشخصي للقاضي الجزائي، و استثناء نجده أخذ أيضا بنظام الأدلة القانونية في إثبات بعض الجرائم أين اشترط لإثباتها أدلة قانونية محددة مسبقا وعلى سبيل الحصر[703]

وبتحليل المادة 212 من قانون الإجراءات الجزائية نجدها تكرس قاعدتين تكمل إحداهما الأخرى، قاعدة الإقتناع الحر للقاضي الجزائي من جهة وقاعدة حرية إختيار وسائل الإثبات الجزائي من جهة أخرى .

وإذا كان الدليل الرقمي ذو الأصالة العلمية هو الأوفر والأنسب في إثبات الجريمة المعلوماتية فما مدى إمكانية إعمال القاضي الجزائي لمبدأ الإقتناع الشخصي حيال هذا الدليل طبقا لأحكام المادة 212 من قانون الإجراءات الجزائية .

الفرع الأول: مفهوم الإقتناع الشخصي للقاضي الجزائي

إن الاقتناع الشخصي للقاضي الجزائي هو عبارة عن نشاط عقلي لا يتدخل المشرع ليبين للقاضي كيفية ممارسته و ترجمته إلى واقع منتج ولا يرسم له كيف يشكل معادلاته الذهنية في مجال تقدير الأدلة ليصل من خلالها إلى الحقيقة

يعرف فقهاء القانون الجنائي الإقتناع بأنه حالة ذهنية ذاتية تستنتج من الوقائع المعروضة على بساط البحث، أو بمعنى آخر هو حالة ذهنية ذو خاصية ذاتية نتيجة تفاعل ضمير القاضي وأدلة الإثبات المطروحة والتي يثيرها الخصوم إما لإثبات أو إنكار إدعائهم

كما عرف الإقتناع الشخصي أيضا بأنه حالة ذهنية ذاتية تنجم عن إمعان الفكر في وقائع معروضة من أجل بحثها والوصول بعد ذلك إلى حالة تطرد الشك والإحتمال، ويجد هذا المبدأ مناخه الطبيعي الملائم في ظل مذهب الإثبات الحر الذي لا يضع تقديرا مسبقا لأدلة معينة لا يمكن (2) الوصول بغيرها إلى اليقين.

ومن خلال هذا التعريف فإن الإقتناع الشخصي للقاضي الجزائي يتميز بخاصيتين هما:

- أنه حالة ذهنية مبنية على الإحتمال وأن العبرة ليست بكثر الأدلة وإنما بما تتركه من أثر في نفسية القاضي، لأن هذا التأثير سيلعب دورا في تحديد مصير الدعوى الجزائية بالإدانة أو البراءة .

– و الخاصية الثانية تتمثل في أن القاضي حرفي أن يأخذ عقيدته أو إقتناعه من أي دليل لكن يجب التأكيد هنا أن حرية الإثبات في المسائل الجزائية ليست خاصية يتميز تها القاضي الجزائي لتتسع سلطته في الإدانة أو البراءة ولكنها، ترجع إلى أن الإثبات في المسائل الجزائية والوصول إلى

---

[703]- **أميرة محمود البدوي الفقي**، مرجع سابق، ص 160

الدليل مسألة جد صعبة وذلك لإختلاف أساليب إرتكاب الجريمة وأن المجرم عادة ما يسعى إلى إخفاء جريمته،

لذلك فالبحث عن الحقيقة من خلال الأدلة الجزائية لا يكون إلا عن طريق منح القاضي الجزائي هامشا عن الحرية لمناقشة الدليل الذي يراه مناسبا في إثبات الجريمة.

الفرع الثاني: و سائل تكوين الإقتناع الشخصي للقاضي الجزائي

إن الجهد الإستنباطي الذي يبذله القاضي من خلال نشاطه العقلي المكون لقناعته و الذي ينصرف إلى فرز الحقيقة من الدليل محل تقديره يرتكز فيه القاضي على :

– قبوله جميع الأدلة المطروحة أمامه في الجلسة و لا يحظر على القاضي أو يفرض عليه دليل محدد ولا يتقيد إلا بقيد مشروعية الدليل وأنه قد تم طرحه للمناقشة بالجلسة ..

– أن يقوم القاضي بوزن كل دليل على حدى عن باقي الأدلة المطروحة أمامه وله أن يهدر أي دليل مهما كانت قيمته طالما أنه لم يطمئن إليه.

- سلطة القاضي في تنسيق الأدلة المطروحة أمامه ومساندة الأدلة لبعضها أو ما يعرف بتساند الأدلة.

المطلب الثاني: القيود الواردة على حرية القاضي الجنائي بالاقتناع بالدليل الالكتروني (تقدير القاضي للدليل التقني)

إن الأصالة العلمية للدليل الرقمي في ضوء نظرية الإثبات الجنائي جعلت من سلطة القاضي في تقدير هذا الدليل محل خلاف فقهي، إذ أن هناك من يرى أن الدليل العلمي ومنه الدليل الرقمي له قوته الثبوتية الملزمة حتى للقاضي، مستندين في رأيهم إلى أن هذا الدليل يتسم بالدقة العلمية التي يبلغ معها إلى درجة اليقين ،[704] وهناك من يرى أن مبدأ حرية القاضي في الإقتناع يجب أن يبسط سلطانه على كل الأدلة دون إستثناء حتى على الدليل الرقمي، معتبرين أن إعطاء الدليل الرقمي قوة ثبوتية لا يستطيع القاضي مناقشتها أو تقديرها يعد بمثابة رجوع إلى مذهب الإثبات القانوني (المقيد).

والمشرع الجزائري كما سبق بيانه أجاز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا الجرائم التي قد يتطلب إثباتها دليلا معينا، ومنح القاضي الجزائي سلطة تقدير الدليل والحرية في تكوين إقتناعه من أي دليل يطمئن إليه، فهل تنصرف هذه السلطة التقديرية التي يتمتع بها القاضي الجزائي إلى الدليل الرقمي المستخرج من الوسائل الإلكترونية؟

---

[704]- **أميرة محمود بدوي الفقي**، مرجع سابق، ص 165،162.

لقد سبق الذكر أن الجريمة المعلوماتية في القانون الجزائري تشمل الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات وكذا كل جريمة أخرى ترتكب أو يسهل إرتكابها بواسطة منظومة معلوماتية أو نظام للإتصالات الإلكترونية، و هذه الأخيرة قد تنصرف إلى جرائم تقليدية منصوص عليها في قانون العقوبات يمكن حسب طبيعتها أن ترتكب بواسطة منظومة معلوماتية، وهذا يعني أن الإجرام المعلوماتي قد يأخذ وصف الجناية أو الجنحة أو المخالفة حسب وصف الجرم المرتكب بواسطة المنظومة المعلوماتية.

و إن كان مبدأ الإقتناع القضائي عام النطاق لدى كافة أنواع لمحاكم الجزائية سواء كانت محاكم الجنايات أم الجنح أم المخالفات فإن قواعد بيان عناصر تقدير الدليل تختلف حسب إختلاف وصف الفعل المجرم.

فإذا كان الفعل من طبيعة جنائية فإن محكمة الجنايات تتمتع بسلطة تقديرية مطلقة في مواجهة الأدلة المعروضة أمامها وتصدر أحكامها دون أن يكون قضايا مطالبين بتسبيب أحكامهم ولا رقابة لجهات الطعن عليهم.

أما إذا أخذ الفعل المجرم وصف الجنحة فإن قاضي الجنح مطالب بعرض و بيان تقديره للدليل المعروض عليه من خلال تسبيب حكمه، والذي يكون محل رقابة من جهات الطعن، لهذا فهو مطالب بإحترام القواعد العامة المنظمة للقوة الثبوتية لكل وسيلة من وسائل الإثبات والتي قد تأخذ شكل محاضر معدة بمناسبة تفتيش أو إعتراض مراسلات أو شكل تقرير خبرة محرر بمناسبة معاينة وفحص الأدلة المضبوطة من جهاز الإعلام الآلي أو دعامات إلكترونية.

فأما ما يتعلق بالمحاضر فإن المشرع إعتبر أنها كقاعدة عامة مجرد إستدلالات ما لم ينص القانون على خلاف ذلك، ولا يكون للمحضر أي قوة إثبات إلا إذا كان صحيحا من حيث الشكل، وأنه قد تم إعداده من طرف واضعه أثناء مباشرة أعمال وظيفته، ويكون مضمونه ما يدخل في إختصاصه.

إلا أن المحاضر التي يخول القانون لضباط الشرطة القضائية إعدادها بنص خاص لإثبات جنح معينة فإن هذه المحاضر تكون لها حجيتها ما لم يدحضها دليل عكسي.

أما بالنسبة لتقارير الخبرة فإن شأنها شأن باقي أدلة الإثبات تخضع للسلطة التقديرية لقاضي الموضوع[705]، لكن الطبيعة العلمية والتقنية للجريمة المعلوماتية غالبا ما تفرض على القاضي الإستناد

---

[705]- وهذا المعنى تؤكده المادة 215 من قانون الإجراءات الجزائية التي تنص على أنه:" لا تعتبر التقارير المثبتة للجنايات أو الجنح إلا مجرد استدلالات".

في تكوين إقتناعه على الخبرة الفنية والتقيد بالنتيجة المتوصل إليها من قبل الخبير في تقرير خبرته ولا يمكنه طرحها وإستبعادها إلا إذا قدر أن ما تحمله من أدلة لا يتوافق مع ظروف وملابسات الواقعة أو تتناقض مع الحقيقة العلمية.

فحسب الإجتهاد القضائي أنه أحيانا ما تكون الخبرة وحدها كافية بالنسبة للقاضي عندما يكون مطالبا للفصل في وقائع ذات طابع تقني دون أن يحتاج إلى مناقشتها[706] .

و عليه تنازعت الإتجاهات الفقهية قيمة الدليل الرقمي بين عدم كفايته كدليل للإدانة أمام القضاء بسبب طبيعته الفنية التي قد تمكن من العبث به و بالتالي هل من شأن ذلك إستبعاد الدليل الرقمي من دائرة الأدلة الجنائية لتعارضه و قرينة البراءة؟

غير أنه إستقر الفقه و القانون الوضعي على أن للقاضي سلطة واسعة في تقدير الدليل وإستنباط القرائن و ما تحمله الوقائع من دلالات، شريطة أن يكون الدليل ثابتا بيقين [707]، مرتبطا بالواقعية و منسجما مع التسلسل المنطقي للأحداث.

وفي الأخير يمكن القول أن إساءة استخدام التقنية المعلوماتية تعد من الموضوعات التي فرضت نفسها على المستوى الوطني و الدولي على حد سواء، وأجبرت التشريع الجزائي على التدخل من أجل مواجهتها بتشريعات حاسمة لمكافحتها ومعاقبة مرتكبيها، إلا أن ذلك يبدو غير كاف لتحقيق هذا الهدف فعلى المستوى الإجرائي تثير الجريمة المعلوماتية مشكلات عدة بدءا من مرحلة الإستدلال حتى صدور الحكم الجزائي لا سيما فيما يتعلق بإثبات الجريمة المعلوماتية و مدى صلاحية الدليل الرقمي للإثبات ومدى شرعية الأدلة المتحصل عليها عبر التقنية المعلوماتية وحجيتها أمام القاضي الجزائي، لذلك خصص هذا الفصل لتناول هذه المسائل من خلال تحديد الأجهزة المكلفة بالبحث و التحري عن الجريمة المعلوماتية، ثم التعريف بالخصائص التي يتميز بها هذا التحقيق و المحققون فيها، ثم بعد ذلك تم البحث في الدليل المناسب لإثبات هذا النوع من الجرائم وهو ما يعرف بالدليل الرقمي أين تم توضيح مفهومه وتحديد أشكاله ومصادر الحصول عليه، كما تم معالجة القواعد الإجرائية المستعملة في التحقيق من أجل استخلاصه وماهي الصعوبات و المعوقات التي تواجه القائمين على ذلك، وأخيرا تم بحث القيمة القانونية للدليل الرقمي في مجال الإثبات الجزائي وما هو موقف المشرع الجزائري من هذا الدليل.

---

[706]– قرار المحكمة العليا الغرفة الجنائية مؤرخ في 04/06/2002 نشرة القضاة رقم 58 لسنة 2006، ص255

[707]– **أحمد محمد سعد الحسيني**، مرجع سابق، ص 388.

الفصل الثالث:

التعاون الدولي في مجال الأمن المعلوماتي

إن من حق كل شخص يعيش في المجتمع الاتصال بغيره و تبادل المنافع المادية و المعنوية معه ليس فقط داخل دولته بل كذلك خارجها مع أشخاص من الدول الأخرى.

و إذا كانت الدول قد استطاعت الحد من ذلك الإتصال و التبادل في أوقات مضت تحت ستار حماية متطلبات أمنها القومي و الإقتصادي إذ أنها لم تعد كذلك في ظل عصر السماوات المفتوحة بفعل التقدم وسائل الاتصال عبر الأقمار الصناعية و وسائط نقل الأخبار المعلوماتية عبر الأثير و الموجات الكهرومغناطيسية لدرجة يمكن القول معها أن سيادة الدولة الأقليمية قد انحسرت عن الإقليم الفضائي أو الهوائي، و اقتصرت على إقليمها الأرضي و المائي فقط.

و كرست الاعمال القانونية الدولية حق الإتصال و الحصول على المعلومات و تداولها، و أكدت على أهمية ضمان ممارسته، و ضرورة وجود توافق دولي محكم في مجال الحق في المعلومات على وجه الخصوص من سهولة حركة المعلومات في أنظمة تقنية المعلومات حيث يرجع لهذه السهولة

في حركة المعلومات، أنه بالإمكان ارتكاب جريمة عن طريق الحاسب آلي موجود في دولة معينة بينما يتحقق نجاح النشاط الإجرامي لها في دولة أخرى.

لدى تستلزم مثل هذه الجرائم و الإعتداءات العابرة للحدود وجود تعاون دولي فعال، و الذي يعتبر ضروريا من أجل حماية حقيقية لأنظمة الاتصالات البعدية التي تمر بالعديد من الدول التي لا شك أن لها أوجه إختلاف بين قوانينها الوطنية و الخاصة بتقنية نظم المعلومات،التي سيكون لها نتيجة عكسية في صورة قيود وطنية على حرية حركة المعلومات(مبحث أول).

أما في مجال القواعد الإجرائية فإن التوافق بين مختلف سلطات التدخل الوطنية سيكون هاما من أجل التيسير دون عقبة لطلب المساعدة القانونية الوطنية، و أنه قد تلتمس إحدى الدول المساعدة القضائية من دولة أخرى بحيث يمكن لهذه الأخيرة أن تباشر التدابير التي تكون مقبولة طبقا لقوانينها الخاصة.

المبحث الأول: التدابير الواجب اتخاذها على المستوى الدولي

في العالم الإفتراضي الرحب يمكن أن يقوم شخص بارتكاب جرائم معلوماتية في أثناء وجوده في بلد معين ضد ضحايا قاطنين في بلد آخر مختلف، كما يمكن أن يتم ارتكاب هذه الجرائم في عدد من البلدان في نفس الوقت ومن ذات المنطلق، كما يمكن للأشخاص القائمين على توجيه الجرائم المعلوماتية أن يقوموا بتحريك موقع ارتكاب الجريمة من بلد إلى آخر حتى يستعصى الكشف عن الجريمة و يصعب تتبع الجناة، ومن ثمة فإن التقنية المعلوماتية أعطت نتيجة مؤداها أن أماكن متعددة في دول مختلفة قد تتأثر بجريمة معلوماتية واحدة و في آن واحد.

فالبعد الدولي [708] للجريمة المعلوماتية إذن يفرض على المجتمع الدولي البحث عن وسائل أكثر ملائمة لطبيعة هذه الجرائم لتضييق الثغرات القانونية التي برع مرتكبوها في استغلالها للتهرب من العقاب ولنشر نشاطهم الإجرامي في مناطق مختلفة من أنحاء العالم.

---

[708]– قد اعتبرت **إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية** المعتمدة من طرف الجمعية العامة للأمم المتحدة في 15/11/2000 في الباب الثالث منها أن أي جريمة تعد جريمة ذات طابع دولي إذا:

– تم ارتكابها في أكثر من دولة.

– تم ارتكابها في دولة ما ولكن جانب كبير من عمليات الاعتداء أو التخطيط أو التوجيه أو الإشراف عليها يتم في دولة أخرى.

– تم ارتكابها في دولة ما ولكن كان لها آثار شديدة على دولة أخرى

وإزاء ذلك كان لابد من تكاتف الدول من أجل مكافحة هذا النوع المستحدث من الجرائم التي لم تعد تتمركز في دولة معينة و لا توجه المجتمع بعينه، بل أصبحت تعبر الحدود لتلحق الضرر بعدة دول ومجتمعات مستغلة التطور الكبير للوسائل التقنية الحديثة في الاتصالات، و تعزيز التعاون بينها و اتخاذ التدابير الفعالة للحد منها والقضاء عليها ومعاقبة مرتكبيها[709] .

ورغم المناداة بضرورة التعاون الدولي، إلا أن هذا الأمر قد لاق من الصعوبات ما من شأنه الحد من فعاليته بإعاقة الأسس العلمية للتعاون الدولي اللازم والملائم لمكافحة الجريمة المعلوماتي، و مما تقدم سوف أوضح مظاهر التعاون الدولي ثم بيان الصعوبات التي تواجهه.

المطلب الأول: مظاهر التعاون الدولي في مكافحة جرائم الأمن المعلوماتي

أثبت الواقع العملي أن أي دولة لا تستطيع بجهودها المنفردة القضاء على الجريمة المعلوماتية، خاصة مع التطور الملموس والمذهل في الإتصالات وتكنولوجيات المعلومات، فإن كان من الضروري أن تمتلك الدول الإمكانات التشريعية و القضائية و الفنية لمكافحة الجريمة المعلوماتية، فان الأهم من ذلك أن تكون تلك القوانين متوائمة و متجانسة بين مختلف الدول، إذ هي تحمي مصلحة مشتركة و و تمنع الجريمة و الفعل الذي يتخطى الحدود.

والتعاون الدولي في مجال مكافحة جرائم المساس بالأمن المعلوماتي قد يأخذ مظهران، **الأول** يتعلق بضرورة التعاون في إنفاذ القانون لملاحقة و متابعة و معاقبة المجرمين بعد ارتكاب الجريمة والتي تعبر إختصاصات قضائية متعددة ذات نظم قانونية مختلفة، و يتمثل ذلك في التعاون القضائي، و **الثاني** يتعلق بالسعي إلى اتخاذ الإجراءات والآليات ذات الطبيعة التقنية الفنية التي تكفل منع ارتكاب الجريمة في مرحلة التنفيذ.

الفرع الأول: التعاون القضائي الدولي في مواجهة الجريمة المعلوماتية

إن التعاون القضائي الدولي يعد الآلية الرئيسية للكفاح ضد الجريمة العابرة للوطنية بأبعادها المختلفة[710]، و فيما يتعلق بالجريمة المعلوماتية فإن فعالية التحقيق والملاحقة القضائية غالبا ما

---

[709]– **حسين بن سعيد بن سيف الغافري** . الجهود الدولية في مواجهة جرائم الإنترانت ورقة مقدمة للاتحاد العربي للتحكيم الالكتروني 2007، ص02.

[710]- **فهد عبد الله العبيد العازمي**، مرجع سابق، ص 292./ **أبو المعالي محمد عيسى**، الحاجة إلى تحديث آليات التعاون الدولي في مجال مكافحة الجرائم، ورقة مقدمة في المؤتمر المغاربي الأول حول المعلوماتية و القانون المنعقد في 28-2009/10/29 بطرابلس-ليبيا، ص 02.

تقتضي الحاجة إلى مساعدة من السلطات في البلد الذي كان منشأً للجريمة، أو من السلطات في البلد الذي عبر من خلاله النشاط المجرم وهو في طريقه إلى الهدف، أو حيث قد توجد أدلة الجريمة، فقد يكون مرتكب الجريمة المعلوماتية من جنسية دولة ما مستعملا في جريمته حواسيب موجودة في دولة أخرى وتقع آثار جريمته في دولة ثالثة.

و من البديهي أن يقف مبدأ السيادة ومشاكل الحدود والولايات القضائية عقبة أمام اكتشاف هذه الجرائم ومعاقبة مرتكبيها، لذا فإن التحقيقات في الجرائم المعلوماتية ومتابعة مرتكبيها قضائيا تؤكد على أهمية المساعدة القضائية المتبادلة بين الدول و تبادل الانابة القضائية.

وتعرف المساعدة القضائية الدولية بأنها كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم[711].

ولقد نص المشرع الجزائري في القانون 09/04 على مبدأ المساعدة القضائية الدولية المتبادلة في المادة 16 منه، معتبرا أنه في إطار التحريات والتحقيقات القضائية الجارية لمعاينة الجرائم المعلوماتية يمكن للسلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني،وتتخذ المساعدة القضائية الدولية عدة صور أهمها:

البند الأول: تبادل المعلومات

يولي المجتمع الدولي لتبادل المعلومات أهمية قصوى بوصفه وسيلة لمكافحة الإجرام عموما والجريمة المعلوماتية خصوصا لما توفره المعلومات الصحيحة والموثوقة من مساندة لأجهزة تنفيذ القانون. ويشمل مبدأ تبادل المعلومات تقديم البيانات والوثائق والمواد الإستدلالية التي تطلبها سلطة أجنبية وهي بصدد النظر في جريمة معلوماتية ما.

فتميز الجريمة المعلوماتية بالعالمية وبكونها عابرة للحدود، فإن مكافحتها لا تتحقق إلا بوجود تعاون دولي على المستوى الإجرائي الجنائي، بحيث يسمح بالإتصال المباشر بين الأجهزة القضائية والأمنية في الدول المختلفة من أجل تبادل المعلومات المتعلقة بالجريمة والمجرمين.

ولهذه الصورة من صور المساعدة القضائية صدى كبير في كثير من الإتفاقيات، أهمها ما ورد في الفقرة الثانية من المادة الأولى لمعاهدة الأمم المتحدة النموذجية لتبادل المساعدة في المسائل

---

[711]- **سالم محمد سليمان الأوجلي**، أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوضعية .دكتوراه الحقوق. جامعة عين شمس، 1997، ص 425. / **فهد عبد الله العبيد العازمي**، مرجع سابق، ص293.

الجنائية[712] و كذا ما ورد في البند الثالث والرابع والخامس من المادة الثامنة لاتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة الوطنية، إذ أوجبت على الدول الأطراف تيسير تبادل المعلومات المتعلقة بكافة جوانب النشاط الإجرامي .

ويصدق الأمر أيضا على ما قضت به المادة الأولى من اتفاقية الرياض للتعاون القضائي العربي بشأن ضرورة تبادل المعلومات بين الدول الأطراف والتنسيق بين الأنظمة القضائية، و في هذا الإطار أيضا صاغ إتفاق شنجن للإتحاد الأوروبي نظاما متكاملا لتبادل المعلومات[713] .

وعلى المستوى التشريعي الوطني فقد نصت المادة 17 من القانون 09/04 على أن الدولة الجزائرية تستجيب لطلبات المساعدة القضائية الدولية الرامية لتبادل المعلومات وذلك في إطار الإتفاقيات الدولية ذات الصلة ومبدأ المعاملة بالمثل.

البند الثاني: نقل الإجراءات

و يقصد بهذه الصورة قيام دولة ما بمقتضى إتفاقية أو معاهدة باتخاذ إجراءات جنائية و هي بصدد التحقيق في جريمة معلوماتية ارتكبت في إقليم دولة أخرى و لمصلحة هذه الدولة متى توفرت مجموعة من الشروط، أهمها التجريم المزدوج والذي يقصد به أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والدولة المطلوب نقل الإجراءات إليها بالإضافة إلى شرعية الإجراءات المطلوب إتخاذها[714].

بمعنى أن تكون مقررة في قانون الدولة المطلوب إليها عن ذات الجريمة و أن تكون هذه الإجراءات ذات أهمية من شأنها أن تؤدي دورا مهما في الوصول إلى الحقيقة.

ولقد أقرت العديد من الإتفاقيات الدولية منها و الإقليمية هذه الصورة كإحدى صور المساعدة القضائية الدولية، منها معاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية [715]، و كذا اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للوطنية[716].

---

[712]– صدرت هذه المعاهدة في 14/12/1990 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 للدولة الطالبة المساعدة

[713] -**Michel QUELLIE** : stratégies en France par la police la criminalité organisée, 1996 p 199.

[714]- أحمد سعد محمد الحسيني، مرجع سابق، ص 297.

[715]– معاهدة نموذجية بشأن نقل الإجراءات في المسائل الجنائية اعتمدت بموجب قرار الجمعية العامة للأمم المتحدة رقم 45/118المؤرخ في 14 ديسمبر 1990.

البند الثالث: الإنابة القضائية الدولية

يقصد بهذه الصورة طلب إتخاذ إجراء قضائي من إجراءات الدعوى العمومية تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها، لضرورة ذلك عند الفصل في مسألة معروضة لدى السلطة القضائية في الدولة الطالبة لتعذر قيامها بهذا الإجراء بنفسها[717].

وهدف هذه الصورة تسهيل الإجراءات الجزائية 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 أقاليم الدول الأخرى لسماع شهود أو إجراء تفتيش أو غيرها .

ويحدث بدرجة متزايدة أن تشترط المعاهدات والاتفاقيات الخاصة بتبادل المساعدة القضائية الدولية على الدول الأطراف أن تعين سلطة مركزية عادة ما تكون وزارة العدل ترسل إليها الطلبات مباشرة بدلا من المرور عبر القنوات الدبلوماسية، و ذلك بغرض التسريع في الإجراءات.

البند الرابع: **تسليم المجرمين**

يعتبر تسليم المجرمين شكل من أشكال التعاون الدولي في مكافحة الجريمة، و هذا النوع من التعاون الدولي هو نتيجة طبيعية للتطورات التي حدثت في كافة المجالات ومنها مجال الإتصالات وتقنية المعلومات، حيث لم تعد الحدود القائمة بين الدول تشكل حاجزا أمام مرتكبي الجرائم، كما أن نشاطهم الإجرامي لم يعد قاصرا على إقليم معين بل امتد إلى أكثر من إقليم، حيث بات المجرم منهم يشرع في التحضير لارتكاب جريمته في دولة معينة ويقبل على تنفيذها في بلد آخر، وقد يفر إلى بلد ثالث للإبتعاد عن أيدي أجهزة العدالة، فالمجرم المعلوماتي أصبح بالتبعية مجرما دوليا.

---

[716]– اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية،اعتمدت وعرضت للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة رقم 25 الدورة الخامسة والخمسون المؤرخ في 15 نوفمبر2000، و لقد صادقت عليها الجزائر بتحفظ بموجب المرسوم الرئاسي رقم 02-55 المؤرخ في 05 فبراير 2002، ج.ر رقم 09 بتاريخ 10 فبراير 2002.

[717]– جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالانترنت، دار النهضة العربية، القاهرة- مصر، ص 83./ **فهد عبد الله العبيد العازمي**، مرجع سابق، ص299.

و لكون أنه لا يمكن لأي دولة أن تجاوز حدودها الإقليمية لممارسة أعمالها القضائية على المجرمين الفارين، كان لابد من إيجاد آلية معينة للتعاون مع الدولة التي ينبغي اتخاذ الإجراءات القضائية فوق إقليمها، تتمثل في تسليم المجرمين الفارين لها.

وهذا الإجراء يقوم أساسا على أن الدولة التي يتواجد على إقليمها المتهم بارتكاب جريمة معلوماتية عليها أن تقوم بمحاكمته إذا كان تشريعها يسمح بذلك، وإلا كان عليها أن تقوم بتسليمه لمحاكمته بمعرفة دولة أخرى مختصة، فهو يحقق بذلك مصلحة الدولتين الأطراف في عملية التسليم، إذ يحقق مصلحة الدولة الأولى في كونه يضمن معاقبة الفرد الذي أخل بقوانينها وفي ذات الوقت يحقق مصلحة الدولة الثانية المطلوب إليها التسليم كونه يساعدها على تطهير إقليمها من فرد خارج عن القانون.

ولذلك فقد حرصت معظم الدول على سن التشريعات الخاصة بتسليم المجرمين ومنها المشرع الجزائري الذي أخذ بهذا الإجراء كمظهر من مظاهر التعاون الدولي بين السلطات القضائية الأجنبية في قانون الإجراءات الجزائية في المواد 694 وما يليها.

الفرع الثاني: التعاون الفني الدولي في مواجهة الجريمة الماسة بالأمن المعلوماتي

لا يقتصر التعاون الدولي في مجال مواجهة الجريمة على المساعدة القضائية المتبادلة فحسب، وإنما يشمل كذلك المساعدة التقنية و تبادل الخبرات بين الدول، ذلك أن العنصر البشري سواء على مستوى الأجهزة القضائية أو الأجهزة الأمنية [718] ليس بذات الجاهزية و المستوى لمواجهة الجريمة المعلوماتية، وإنما يختلف من دولة إلى أخرى بحسب تقدم تلك الدولة ورقيها.

ونجد أن جميع الاتفاقيات الدولية أو الإقليمية ذات الصلة قد دعت صراحة إلى ضرورة وجود تعاون دولي في مجال التدريب ونقل الخبرات فيما بينها [719]، ذلك أن التقدم المتواصل في تكنولوجيات المعلومات يفرض على الجهات القضائية والأمنية أن تسير في خطوات متناسقة مع التطورات السريعة التي تشهدها هذه التقنيات والإلمام بها حتى يمكن التصدي للأفعال الإجرامية التي صاحبت هذه التكنولوجيا ومن ناحية أخرى فإن إعمال القانون في مواجهة الجرائم المعلوماتية يستلزم اتخاذ إجراءات قد تتجاوز المفاهيم والمبادئ المستقرة في المدونة العقابية التقليدية لما تتسم به هذه الجرائم من حداثة في الأسلوب وسرعة في التنفيذ وسهولة في إخفائها ومحو آثارها، وبالتالي فإن ظهور هذه الأنماط الجديدة من الجرائم أصبح يشكل عبئا ثقيلا على عاتق الأجهزة القضائية المختصة من قضاة تحقيق

---

[718]– يعتبر الانتربول من الأجهزة الامنية الدولية

[719]– المادة 29 من **اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية**، والمادة 09 من مشروع الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود.

وقضاة حكم. وكذا رجال الضبطية القضائية، لأجل ذلك كان لابد أن تكون تلك الأجهزة على مختلف أنواعها على درجة كبيرة من الكفاءة والمعرفة والقدرة في التعامل مع الجريمة المعلوماتية والمجرم المعلوماتي.

و من هذا المنطلق كانت الدعوى إلى ضرورة وجود تعاون دولي في مجال تدريب رجال القضاء والضبطية القضائية للاستفادة من مهارات وتجارب الآخرين من خلال أشخاص أكفاء ومؤهلين وقادرين على نقل هذه التجارب وتلك المهارات بوسائل سهلة ميسرة، و التدريب المقصود هنا ليس التدريب التقليدي فحسب، فلا يكف أن تتوافر لدى رجال القضاء الخلفية القانونية، بل لابد من إكسابهم خبرة فنية في مجال الجريمة المعلوماتية.

وهذه الأخيرة لا تتأت دون تدريب تخصصي[720] يراعى فيه العناصر الشخصية للمتدرب من حيث توافر الصلاحية العلمية والقدرات الذهنية والنفسية لتلقي التدريب، أما بالنسبة للمنهج التدريبي فيجب أن يشمل على بيان بالمخاطر والتهديدات ونقاط الضعف [721] و أماكن الإختراقات لشبكة المعلومات و أجهزة الحاسب الآلي وتحديد أنماط ونوعية الجرائم المعلوماتية، وبيانا لأهم الصفات التي يتميز المجرم المعلوماتي و الدوافع وراء ارتكابه للجريمة المعلوماتية.

أما فيما يتعلق بمنهج التدريب على التحقيق في الجريمة المعلوماتية فإنه لابد أن يشتمل على إجراءات التحقيق، التخطيط للتحقيق، تجميع المعلومات وتحليلها، أساليب المواجهة والاستجواب، طرق مراجعة النظم الفنية للمعلومات وأساليب المعمل الجنائي، بالإضافة إلى ما يتعلق بالتفتيش [722]والضبط وكيفية استخدام الحاسب الآلي كأداة للمراجعة والحصول على الأدلة .

وصفوة القول وخلاصته أنه ما من دولة يمكنها مجابهة هذا التحدي في مواجهة الجريمة المعلوماتية الغير محدودة و ألامنتهية بمفردها، فلا مفر إذن من مواصلة تطوير القدرة على التعاون الدولي في المجال التدريبي والتبادل التقني من خلال قيام الدول المتقدمة تقنيا و تكنولوجيا ولها صيت كبير في مواجهة الجرائم المعلوماتية بمساعدة الدول النامية لتعزيز مؤسساتها المتخصصة بالتحري والتحقيق والمحاكمة بتوفير سائر أنواع المعونة التقنية .

المطلب الثاني: الصعوبات التي تواجه التعاون الدولي في مكافحة الجرائم المعلوماتية

---

[720]- **فهد عبد الله العبيد العازمي**، مرجع سابق، ص 219-223./ **أميرة محمود بدوي الفقي**، مرجع سابق، ص 653-659.

[721]- **هشام محمد فريد رستم**. الجرائم المعلوماتية. أصول التحقيق الجنائي الفني. بحث مقدم لمؤتمر القانون والكومبيوتر والانترنات- كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة في الفترة 01/03/2005 الطبعة الثاني 2004 ص 496.

[722]- **أميرة محمود بدوي الفقي**، مرجع سابق، ص 653-659

رغم المناداة بضرورة التعاون الدولي في مجال مكافحة الجريمة المعلوماتية والذي بات مطلبا تسعى إلى تحقيقه أغلب الدول، إلا أنه ثمة صعوبات ومعوقات تجعل هذا التعاون ليس بالأمر اليسير وذلك كما يلي

الفرع الأول: عدم وجود نموذج موحد للنشاط الإجرامي

إذ لم تتفق الأنظمة القانونية في بلدان العالم على صورة محددة ونماذج معينة يتم الاتفاق المشترك بين الدول حولها تندرج في إطار الجريمة المعلوماتية، فما يكون مجرما في بعض الأنظمة قد لا يكون كذلك في أخرى .ولعل عدم الاتفاق بين الأنظمة القانونية المختلفة على صور موحدة للسلوك الإجرامي في الجريمة المعلوماتية يغري قراصنة الحاسب الآلي على ارتكاب جرائمهم دون تقيد بالحدود الجغرافية

الفرع الثاني: اختلاف النظم القانونية الإجرائية

إذ بسبب هذا الاختلاف قد تكون هناك طرق للتحري والتحقيق والمحاكمة التي تثبت فعاليتها في دولة ما، قد تكون عديمة الفائدة في دولة أخرى أو قد لا يسمح بإجرائها كما هو الحال مثلا بالنسبة للمراقبة الإلكترونية، فإذا ما اعتبرت أن طريقة ما من طرق جمع الإستدلالات أو التحقيق أنها قانونية في دولة معينة، قد تكون ذات الطريقة غير مشروعة في دولة أخرى.

بالإضافة إلى أنه قد لا تسمح دولة ما باستخدام دليل إثبات جرى جمعه بطرق ترى هذه الدول أنها طرق غير مشروعة .

المبحث الثاني: التدابير الواجب مباشرتها على المستوى الوطني

تقسم هذه التدابير إلى نوعين أحدها تدابير موضوعية(المطلب الأول) و الأخرى تدابير إجرائية (المطلب الثاني) نوضحها بشكل مختصر على النحو الآتي:

المطلب الأول: التدابير الموضوعية

ينبغي بخصوص هذا الأمر أن تتبع الدول سياسة جنائية موحدة لملاحقة الجناة ومحاصرتهم ، و تهدف إلى حماية المجتمع من مخاطر الجريمة المعلوماتية و ذلك من خلال وضع و تبني التشريعات الملائمة لمواجهة الخطورة المتمثلة في إمكان إستخدام شبكات الكمبيوتر و المعلومات الالكترونية في ارتكاب أفعال اجرامية مع إمكانية تخزين و نقل الدليل المتعلق بمثل هذه الأفعال عبر تلك الشبكات، لذا من الأهمية بما كان مباشرة التدابير الآتية:

أولا: يجب على كافة الدول أن تتبع و تتبنى التدابير التشريعية و غيرها من التدابير اللازمة لإدراك عملية الدخول غير المشروعة إلى سائر أو جزء من نظام كمبيوتر كجريمة جنائية وفقا لأحكام قوانينها إذا ما ارتكبت هذه الأفعال بصورة عمدية[723] .

ثانيا: ينبغي على الدول أن تتبنى مختلف الأفعال و السلوكات الإجرامية التي تشكل خطورة و مساسا بقواعد الأمن المعلوماتي و تجريمها في قوانينها الداخلية وفق نموذج موحد.

ثالثا: يجب على الدول أن تقوم بتكيف بعض النصوص التقليدية في العقاب على بعض الجرائم مثل جرائم السرقة و التزوير و الاحتيال و جعلها تستوعب الشكل الحديث لنفس السلوك الذي يتم باستعمال وسائل الاتصال الحديثة أو توسيع من مفهوم المال و الأشياء محل هذه السلوكات ليستوعب حتى الأموال و الأشياء المعنوية و ليس المادية فقط بهدف مكافحة مختلف جرائم المساس بقواعد الأمن المعلوماتي

رابعا: على الدول القيام بمساءلة الشخص المعنوي جزائيا و اتخاذ التدابير اللازمة لإمكانية ذلك، و ذلك عن الجرائم الناشئة عن استخدام النظم المعلوماتية خاصة في حالة قصور الرقابة و الإشراف أو في حالة تسهيل ارتكابها[724] من قبل الأشخاص الطبيعية الممثلة لها.

المطلب الثاني: التدابير الإجرائية

من التدابير الإجرائية الواجب على الدول إتحادها نحدد ما يلي:

أولا: تحديد قواعد الاختصاص القضائي في جرائم الأمن المعلوماتي

إن المقصود بالإختصاص القضائي هو السلطة السيادية للدولة التي تمكنها من تطبيق قوانينها الوطنية داخل إقليمها، و تعد الجرائم المعلوماتية بصفة عامة و جرائم المساس بالأمن المعلوماتي من

---

[723]- **عبد الله حسين علي محمود**، مرجع سابق، ص 397.

[724]– نفس المرجع، ص 398.

أكثر الجرائم التي تطرح مسألة الإختصاص القضائي، ذلك أن السلوك أو النشاط الإجرامي فيها لا يعترف بالحدود، فالعالم كله مرهون بمجرد نقرة بسيطة على لوحة مفاتيح جهاز الحاسوب،لذا يلزم على الدول أن تتخذ التدابير التشريعية اللازمة لمد اختصاصها القضائي على أساس أن أي من الجرائم الماسة بقواعد الأمن المعلوماتي قد أرتكبت:

– بصورة كلية أو جزئية على أراضيها أو على متن باخرة أو طائرة تحمل علمها أو مسجلة لديها.

– من قبل أحد مواطنيها إذا كانت الجريمة معاقب عليها طبقا لأحكام القانون الجنائي.

ثانيا: على الدول أن تتخذ التدابير و الإجراءات التشريعية اللازمة لتمكين سلطاتها المعنية في إصدار الأمر لأي شخص سواء كان متواجدا في إقليمها أو في أي مكان أخر تمارس عليه سلطاتها السيادية لكي يقدم أي بيانات محددة، و واقعة تحت سيطرته و مخزنة في أحد أنظمة الكمبيوتر أو أحد الوسائط المستخدمة في تخزين البيانات[725] و ذلك بالصورة التي تطلبها تلك السلطات لأغراض التحقيق.

ثالثا:يجب على الدول أن تتخذ التدابير اللازمة التي تمكنها من تسهيل عملية تفتيش أي منظومة معلوماتية .

رابعا: يلزم على الدول أن تتبنى الإجراءات التشريعية اللازمة لتمكين سلطاتها المعنية من الحصول على نسخة حفظ سريعة للبيانات المخزنة في أحد النظم المعلوماتية و ذلك لأغراض التحقيقات خاصة إذا ما 65تبين أنها عرضة للفقد و التلاعب بها.

---

[725]– د. **عبد الله حسين على محمود**، مرجع سابق، ص 399.

خاتمة

الخاتمة

ومرة أخرى يفتح التقدم العلمي للقانون آفاقا و أرضاً جديدة لم تدر يوما بخلد أحد ، فمن نقل الأعضاء إلى الهندسة الوراثية ، إلى الحاسب الآلي و تقنية الاتصال ، إلى الانترنت ، تتدخل أداة التشريع إما بتطويع القواعد التقليدية ، إن كان ذلك مفيداً ومجدياً ، و إما باستحداث قواعد جديدة تقنن الاستفادة من ثمار التقدم العلمي و تواجه في نفس الوقت مخاطره .

و بعد دراستنا لأحد أهم الموضوعات و معالجتها لإنعكاسات التقدم العلمي في مجال الاتصال و تكنولوجيا المعلومات و هو " الأمن المعلوماتي" الذي يعبر عن اتخاذ كافة الإجراءات الفنية و القانونية لحماية جميع أنواع المعلومات و مصادر الأدوات التي تتعامل معها و تعالجها من أجهزة و أنظمة معلومات ، و وسائط تخزين و الأشخاص من الاختراق و السرقة و النصب و التزوير و القرصنة و ذلك بإتباع إجراءات وقائية و ضوابط علاجية واضحة.

فهو يعبر عن آلية فنية هدفها بث ونشر الثقة والآمان لدى مستخدمي و جمهور المتعاملين بوسائل الاتصال الحديثة لا سيما شبكة الانترنت ، فمن نافلة القول التذكير بأن التقدم الحادث في هذا المجال قد طوى المسافات و اختصر الأوقات، و حول العالم باختصار إلى أصغر من قرية محدودة.

وهو ما إستتبع إدخال تعديلات جوهرية على التشريعات العقابية فيما يخص أساليب وأشكال ارتكاب الجرائم و التي تشكل مهددا لعناصر و قواعد الأمن المعلوماتي و المتضمنة في سرية المعلومات و وفرتها و ضمان عدم عبث بها.

طبيعي ، في ضوء هذا الواقع الجديد ، أن تنعدم الثقة أو تضعف و يقل تبعا لذلك ، عامل الأمن والاطمئنان ليس فقط فيما يتعلق موضوع أمن التعاملات و المخاطر التي تستهدفه من اختراق و إتلاف و التعدي على المعلومات و أنظمة معالجتها، و إنما كذلك في التشريع نفسه

إذا لم يردع و يحد من تلك الأفعال بمواجهتها و مكافحتها من خلال نصوصه التي يجب أن تواكب ذاك التطور، و معلوم أن بقاء الوضع على هذا الحال معناه الإحجام عن استعمال وسائل التقنية الحديثة في التعامل ، وهو ما يُعد الآن تخلفا وتراجعا، بكل ما تحمله الكلمة من معنى ، عن التطور و حديثا بغير اللغة التي يجيدها العالم المحيط .

و إزاء حتمية اللجوء إلى هذه الوسائل في تعاملات الحياة اليومية و المهنية ، ونظرا لضعف الأمان الذي توفره ، فالابد من الاحتكام إلى تنظيم قانوني شامل في هذا الخصوص، إضافة إلى التنظيم في الجانب الفني و التقني الذي يساعد في عمليات الأمن و السلامة المعلوماتية.

وقد أسفرت الدراسة عن النتائج و التوصيات الآتية:

أولا: أن الأمن المعلوماتي القانوني و الفني هو الوسيلة المتاحة حاليا لبعث الثقة و تأمين التعامل عبر وسائل الاتصال الحديثة لا سيما الانترنت و بتدعيم مبادئه تحقق السرية والسلامة و توفر المعلومات و أنظمة معالجتها، خاصة أن وسائل الاتصال في تطور مستمر و يتم الاعتماد عليها في الكثير من المعاملات لما توفره من تسهيلات، و لكنها في نفس الوقت تثير بعض المشكلات و المخاطر تهدد أمن و سلامة تلك المعاملات مما يجعل المتعاملين يفقدون ثقتهم فيها، خاصة إذا لم يكن هناك رادع أو عقاب للمتسببين في تلك المشكلات.

ثانيا: كشفت الدراسة كذلك عن أن المجال الأساسي للأمن المعلوماتي هو الإجرام الإلكتروني أو المعلوماتي ، وهذا هو المجال الذي يجب أن يحظى بتنظيم تشريعي واسع في مختلف الدول الغربية و العربية و بالاتحاد و التعاون بين الدول على مكافحته باعتباره إجرام عابر للحدود.

ثالثا: أن الجرائم المعلوماتية التي تعد مساسا بقواعد الأمن المعلوماتي، هي الجرائم التي تهدد أمن و سرية المعلومات، و عدم توفرها و تهدد أمن الأنظمة المعلوماتية التي تعالجها وثقة التعامل فيها.

رابعا: رغم أن معظم الدول العربية و منها الجزائر قد حاكت الدول الأوروبية في إصدار تشريعات لتنظيم الجرائم المعلوماتية باعتبارها أحد أخطار و مهددات قواعد الأمن المعلوماتي، إلا أن الواقع قد كشف عن عدم توافر إمكانات ممارسة هذا النشاط في الدول العربية على غرار ما هو متاح في الدول الأوروبية، سواء في ذلك الإمكانات المادية أو الفنية أو الكوادر البشرية.

خامسا: تشير الإحصائيات و تظهر أن الجريمة الإلكترونية في العالم في تزايد مستمر وذلك بسبب التوسع في استخدام الانترنت و ما يترتب عن استخدامها من سلوكيات مخالفة، و أن الازدياد في استخدام الانترنت يدعم التوقع بازدياد الجريمة الالكترونية ما لم يوافقها توعية وقوانين محرمة لهذه الجرائم و الأفعال، كما أن الجريمة المعلوماتية تخلف خسائر مادية وتسبب إساءة السمعة للمؤسسات و الشركات و فقدان ثقة المستخدمين.

سادسا: و بالنظر إلى التعقيدات المتزايدة التي تشهدها جرائم الانترنت بشكل مستمر، يظهر الأمر أن مستوى وعي مستخدمي وسائل الاتصال و مقدمي الخدمات ليس بمثل مستوى هذه التهديدات مما أصبح من الأهمية بما كان رفع هذا المستوى و بالوتيرة ذاتها.

سابعا: تتعرض المؤسسات و الشركات و الأشخاص و الحكومات لخطر سوء استخدام التكنولوجيا الرقمية أو لخطر مرتقب، مما يتطلب حماية فنية تقنية بالدرجة الأولى كإجراء وقائي و إتباع خطط و إستراتجيات فنية لدعم الأمن المعلوماتي بأهدافه و مبادئه، إضافة إلى حماية قانونية تأتي ردعا لتلك السلوكيات المخالفة و حتى لا يتهرب الجاني من العقاب.

كما الأمر يتطلب من رجال الشرطة أن تكون على أهبة الإستعداد للتعرف على هذه الجرائم وبأن تتسلح بالمعرفة اللازمة التي تمكنها من تتبعها قبل وقوعها، و يتطلب كذلك تجنيد عدد من الخبراء المختصين في امن الانترنت من شركات متخصصة في هذا المجال" مثل شركة كاسبرسكي لاب" العالمية لتدريب ضباط الشرطة من مختلف المستويات على هذه التهديدات المتفاقمة.

ثامنا: إن النصوص التشريعية سواء الموضوعية أو الإجرائية و التي جاء بها المشرع الجزائري من التعديلات الأخيرة للقوانين العقابية أظهرت عدم كفايتها لمواجهة أخطار و مهددات

قواعد الأمن المعلوماتي، و أن بعض الجرائم التقليدية التي قد تحدث بإستعمال وسائل الاتصال الحديثة، أو بواسطة أنظمة معلوماتية مثل السرقة المعلوماتية لا تنطبق عليها تلك التعديلات و لا يمكن معاقبة فاعلها بالنصوص التي نظمت الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات مما يستدعي استدراك المشرع لبعض أشكال الإجرام التقليدي التي تقع بواسطة أنظمة معلوماتية.

تاسعا: مواجهة رجال القضاء و المحققين لبعض الصعوبات أثناء القيام بإجراءات التحقيق والاستدلال للكشف عن الجرائم المعلوماتية عامة و الجرائم الماسة بقواعد الأمن المعلوماتي، وذلك قد يرجع لعدم توفر الخبرة الكافية لديهم من جهة و من جهة أخرى لحداثة هذه الإجراءات و لتعقد الظاهرة الإجرامية و للبيئة الواقعة فيها.

كما خلصت من خلال هذه الدراسة إلى مجموعة من التوصيات التي تسعى إلى مكافحة الجرائم الماسة بأنظمة المعالجة الآلية و التي تعد مساسا بقواعد الأمن و السلامة المعلوماتية ومن جميع النواحي و المجالات منها ما يلي:

*** بالنسبة للمجال الفني و التقني للأمن المعلوماتي:**

أولا: أنه يمكن دعم مسألة الأمن المعلوماتي من خلال التصدي لمهدداته مثل المحافظة على أمن الشبكة و خطوط الاتصال و كشف الثغرات الأمنية التي يتم إختراقها من طرف الهاكرز سواء على مستوى الحواسيب الشخصية أو بروتوكولات الاتصالات في شبكة الانترنت و كذا الموجودة في البريد الالكتروني حيث لازالت هذه المهددات في تطور دائم مما يستوجب أن تكون الحماية الفنية في تطور بمستوى تلك المهددات.

ثانيا: أخد الاحتياطات من الجانب الفني من قبل مستعمل الحاسب الآلي و الشبكة المعلوماتية باستعماله لبعض تقنيات الحماية الفنية الوقائية كتقنية التشفير و جدار الحماية والتوقيع الرقمي و البرامج المخصصة لكشف الفيروسات و الوقاية منها.

ثالثا: وضع سياسة أمنية فعالة للأنظمة المعلوماتية و تسخير كل الإمكانيات المادية والبشرية.

رابعا: الاحتفاظ بنسخ احتياطية لكل المعلومات و البيانات الحساسة و المهمة في أقراص أو حوامل إضافية بعيدة عن الحاسب الآلي و الشبكة المعلوماتية.

خامسا: وضع كود أو كلمة سر معقدة للحاسب و للبريد الإلكتروني حيث لا يمكن كشفها بسهولة.

*** بالنسبة للمجال القانوني الموضوعي و الإجرائي للأمن المعلوماتي:**

أولا: ينبغي لتحقيق الأمن المعلوماتي من الناحية القانونية أن يتم وضع الإطار التشريعي الملائم للظواهر الإجرامية الحديثة للتصدي لها، خاصة ما تعلق منها بالجرائم الماسة بقواعد الأمن المعلوماتي سواء من حيث تحديد الجرائم و العقاب عليها أو من حيث تحديد القواعد الإجرائية للتعامل مع هذه الظاهرة و مكافحتها على المستوى الوطني و الإقليمي و الدولي.

ثانيا: دعم الاستفادة من التطورات العلمية و التكنولوجية في مواجهة الإجرام المعلوماتي عامة و الجرائم الماسة بقواعد الأمن المعلوماتي خاصة.

ثالثا: ضرورة اعتماد ضمانات تشريعية لحماية سرية البيانات و المعلومات المتعلقة بمسألة الخصوصية و اختراقها أو عند الإطلاع على البيانات الشخصية المخزنة داخل نظام الحاسب الآلي خاصة عند القيام بإجراءات التفتيش و التحري.

رابعا: العمل على تحديد سياسة جنائية مشتركة بين الدول باعتبار أن الأمن المعلوماتي مسألة تهم الجميع، و أن مخاطره تمس كل الدول و لا يمكن التصدي لها ما لم يتم التعاون و الدعم من جميع الدول.

خامسا: العمل على إبرام اتفاقيات إقليمية، ثنائية، جماعية بين الدول المعنية لتفعيل مسألة التعاون الدولي القانوني و الفني لتسهيل الإجراءات بين الدول في حالة وقوع جرائم تمس قواعد الأمن المعلوماتي.

سادسا: أما فيما يخص إثبات الجرائم الماسة بقواعد الأمن المعلوماتي من الناحية الإجرائية فلابد أن يكون الدليل المستخلص من البيئة الافتراضية دليلا مشروعا وفقا للتشريع المعمول به.

سابعا: يجب أن توضح التشريعات الإجرائية قواعد و إجراءات تفتيش الأنظمة المعلوماتية و ضبط المعلومات المخزنة فيها أو المتناقلة عبرها، مع تمكين الجهات القائمة بالتفتيش بضبط الأجهزة محل التفتيش وفقا لنفس الشروط الخاصة بإجراءات التفتيش العادية و تحديد خصوصيات هذا التفتيش و الإجراءات الجديدة التي تناسب الاتصالات الإلكترونية.

ثامنا: ضمان حفظ الأسرار من قبل المحققين مع واجب أخذ الحيطة و الحذر أثناء التفتيش وعدم إطلاع الغير على محتويات النظام المعلوماتي.

تاسعا: العمل على تكوين ورشة عمل لمكافحة الجريمة المعلوماتية بمختلف أشكالها لفائدة ضباط الشرطة القضائية و القضاة و المحققين بهدف إطلاعهم على أخر التكنولوجيات لمحاربة الجريمة و كيفية استخدام الأدلة التقنية في التحقيق و المقاضاة، و تبادل الخبرات مع خبراء أجانب في الدول المختلفة.

عاشرا: دعوة المشرع الجزائري إلى المسارعة في إجراء التعديلات اللازمة في قانون الإجراءات الجزائية و تطوير الفعالية الفنية و التقنية للإدارة الخاصة بالتحقيق في الجرائم المعلوماتية، وضرورة تعزيز و تنشيط تبادل المعلومات بين الأجهزة المنوط بها تنفيذ القانون وبين خبراء نظم المعلومات من أجل معرفة أبعاد الجرائم المعلوماتية و مقدار الأضرار الناشئة عنها و سمات مجرميها و أساليب منع إرتكاب و ملاحقة مرتكبيها، ووضع سياسة أمنية محكمة من أجل المحافظة على أمن و سلامة و سرية المعلومات.

إحدى عشر : كما نوصي و يتطلب الأمر مواكبة التشريعات العقابية الإجرائية لمقتضيات التحقيق في الجرائم المعلوماتية و التعريف بالتفتيش كإجراء من إجراءات التحقيق في الجرائم المعلوماتية، و سعي الدولة القانونية إلى إقامة حالة التوازن بين حق المجتمع في إيقاع العقاب على من يقومون بجرائم المساس بأمن المعلومات و الحاسب الآلي و شبكات الاتصال و من يعملون على المحافظة على حقوق الإنسان في مجال الإجراءات الجزائية حيث ان هذه الإجراءات أشدها مساسا بالحرية الشخصية و هو التفتيش لأنه يتصل بحرية الأفراد و مستودع سرهم و حرية مساكنهم بالإضافة إلى انه يجمع بين استعمال السلطة و تقييد الحرية، حيث بدأت

الأجهزة الأمنية و مأموري الضبط القضائي تواجه هذه الظاهرة من جرائم تقنية المعلومات والحاسب الآلي.

اثنا عشر: لابد من التعاون القضائي الدولي الذي يشمل المساعدة القضائية في تبادل المعلومات و البيانات و الوثائق و المواد الاستدلالية التي قد تتطلبها سلطة قضائية أجنبية، و كذا أهمية التعاون الأمني بحيث أن الدول بجهودها لا تستطيع القضاء على الجريمة الالكترونية لأنها جريمة دولية عابرة للحدود لذا فإن التحقيق في هذا النوع من الجرائم يتطلب تحقيق أمني واسع و موسع.

ثلاثة عشر : إضافة إلى ذلك يتطلب الأمر تنظيم حلاقات نقاشية تستهدف نشر الوعي العام حول القانون و الجرائم المعلوماتية من قبل رجال القضاء و القانون و الاجتماع دعما للجهود السباقة التي تقودها الدولة على صعيد تطور التشريعات و القوانين التي من شانها مواكبة التطورات المتسارعة بالتزامن مع النهضة الحضارية الشاملة و مسيرة التحول إلى اقتصاد ذكي و مستدام قائم على الإبداع و الابتكار، و أن شيوع استخدام الكمبيوتر و شبكات الاتصال قد يكون في العمل المشروع و غير المشروع، و كخطوة لتأكيد إلتزامنا المطلوب بمسؤوليتنا الوطنية في إطار إرساء دعائم متينة لبناء نظام عدلي قوي و فعال من شأنه تجسيد أهداف رؤية الدولة الرقمية من أجل ضمان حماية أمن و سلامة الوطن و حرية الأشخاص و معاملاتهم.

أربعة عشر : نوصى كذلك بضرورة تهيئة البيئة العربية لاستقبال هذا الوافد الجديد والتعامل معه، مع ما يقتضيه ذلك من توفير الإمكانات المادية والفنية والكوادر البشرية بجانب التثقيف العام بأهمية هذه التقنيات و علاقتها بقواعد الأمن المعلوماتي.

قائمة المراجع

أولا: الكتب القانونية.

أ -المراجع العامة.

1 - **أشرف وفا محمد** ، تنازع القوانين في مجال الحقوق الذهنية للمؤلف، ط 1، دار النهضة العربية، القاهرة، 1999.

2 -**أيمن إبراهيم العشماوي** ، المسئولية المدنية عن المعلومات، دار النهضة العربية، القاهرة،2004.

3 - **أحسن بوسقيعة** ، الوجيز في القانون الجزائي الخاص، الجزء الأول، الطبعة الخامسة عشر، دار هومة، الجزائر، 2012-2013.

4 - **بن وارث.م**، مذكرات في القانون الجزائي الجزائري (القسم الخاص)، الطبعة الرابعة، دار هومة، الجزائر، 2009.

5 -**قادري أعمر**: أطر التحقيق،دار هومة للنشر، الجزائر، ط 2013.

6 - **عبد الله حسين علي محمود،** سرقة المعلومات المخزنة في الحاسب الآلي،" شرطة دبي"، الطبعة الرابعة، دار النهضة العربية، القاهرة.

7 - **عبد الرشيد مأمون و محمد سامي عبد الصادق** : حقوق المؤلف و الحقوق المجاورة في ضوء قانون حماية حقوق الملكية الفكرية الجديد رقم 82 لسنة 2002، الكتاب الأول، دار النهضة العربية، القاهرة.

8 - **عصام أحمد البهجي** ، حماية الحق في الحياة الخاصة في ضوء حقوق الإنسان والمسؤولية المدنية، دار الجامعة الجديدة، مصر، 2005.

9 - **محمد زكي أبو عامر وسليمان عبد المنعم** ، قانون العقوبات (القسم الخاص)، منشورات الحلبي الحقوقية، بيروت، لبنان، 2006.

10- **محمد حسام لطفي**، عقود خدمات المعلومات، دراسة في القانونين المصري الفرنسي ، القاهرة، 1994.

11- **محمود عبد المعطي خيال**: التأمين على المعلومات، ط 1999، القاهرة.

12- **محمد سامي الشوا** ، ثروة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، .1994

13- **محمد سامي عبد الصادق** ، خدمة المعلومات الصوتية والإلتزمات الناشئة عنها، 2005.

11- **نبيل صقر** ، الوسيط في شرح جرائم الاموال، دار الهدى، عين ميلة- الجزائر،2012.

ب-المراجع الخاصة.

1 **أحمد خليفة الملط**، الجرائم المعلوماتية-دراسة مقارنة-،ط2، دار الفكر الجامعي، الإسكندرية، مصر، 2006.

2 **أيمن عبد الله فكري** ، جرائم نظم المعلومات- دراسة مقارنة-دار الجامعة الجديدة للنشر، الإسكندرية، 2007.

3 **أيمن عبد الحفيظ** ، الاتجاهات الفنية و الأمنية لمواجهة الجرائم المعلوماتية، بدون ناشر،2005.

4 **بلال أمين زين الدين،** جرائم نظم المعالجة الآلية للبيانات في التشريع المقارن و الشريعة الإسلامية، دار الفكر الجامعي، الاسكندرية، 2008،

5 **جميل عبد الباقي الصغير** ، الجوانب الإجرائية للجرائم المتعلقة بالانترنت، دار النهضة العربية، القاهرة– مصر.

6 **حسن طاهر داود** ، جرائم نظم المعلومات،الطبعة الأولى، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2000،

7 **خالد بن سليمان الغثبر، ود. محمد بن عبد الله القحطاني** ، أمن المعلومات بلغة ميسرة، الطبعة الأولى، مكتبة الملك فهد للنشر، الرياض، 2009، كتاب لمركز التميز لأمن المعلومات، جامعة الملك سعود.

8 **خالد ممدوح إبراهيم** ، أمن المعلومات الإلكترونية، الدار الجامعية، الإسكندرية، 2008.

9 -**خثير مسعود** : الحماية الجنائية لبرامج الكمبيوتر، أساليب وثغرات، دار الهدى، عين مليلة، الجزائر طبعة 2010.

10 - **خيرت علي محرز** ، التحقيق في جرائم الحاسب الألي، دار الكتاب الحديث، القاهرة– مصر ، 2012

11 - **دلال صادق الجواد ود. حميد ناصر الفتال** ، أمن المعلومات، دار اليازوري، عمان الأردن، 2008.

12 - **زكي حسين الوردي** ، و د. مجبل لازم المالكي، المعلومات و المجتمع، ط1، الوراق للنشر و التوزيع، 2002.

13 - **زيبحة زيدان** ، الجريمة المعلوماتية في التشريع الجزائري و الدولي، دار الهدى، عين مليلة– الجزائر، 2011.

14 - **سليمان أحمد الفضل** ، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، القاهرة، 2007،

15 - **ضياء على أحمد نعمان** ، الغش المعلوماتي، الظاهرة و التطبيقات، سلسلة الدراسات القانونية في المجال المعلوماتي، الطبعة الأولى، الوراقة الوطنية، مراكش- المغرب- 2011.

16 - **طارق إبراهيم الدسوقي عطية** ، الأمن المعلوماتي- النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة للنشر، الإسكندرية، 2009.

17 - **عائشة بن قارة مصطفى** ، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري و القانون المقارن، دار الجامعة الجديدة، مصر، 2010

18 - **عبد الرحمان شعبان عطيات** ، امن الوثائق والمعلومات، ط 1، جامعة نايف العربية للعلوم الامنية، الرياض، 2004.

19 - **عبد الفتاح بيومي** ، النظام القانوني لحماية التجارة الإلكترونية، الكتاب الأول، ط1، دار الفكر الجامعي، الاسكندرية- مصر، 2002.

20 - **عبد الفتاح بيومي** ، النظام القانوني لحماية التجارة الإلكترونية، الكتاب الأول، ط1، دار الفكر الجامعي، الاسكندرية- مصر، 2002.

21 - **عبد الفتاح بيومي حجازي** : مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، الطبعة الأولى، الإسكندرية، 2006.

22 - **عبد الفتاح بيومي حجازي** ، الدليل الجنائي و التزوير في جرائم الانترنت والكمبيوتر، دار الكتب القانونية، مصر، 2005.

23 - **عفيفي كامل عفيفي** ، جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية و دور الشرطة و القانون- دراسة مقارنة- منشورات الحلبي الحقوقية، بيروت – لبنان- 2003.

24 - **علي كحلون** ، الجوانب القانونية لقنوات الاتصال الحديثة و التجارة الإلكترونية، دار إسهامات في أدبيات المؤسسة، تونس، 2002.

25 - **علي حسن محمد الطوالبة** ، التفتيش الجنائي على نظم الحاسوب والأنترنت، دراسة مقارنة، ط 1، عالم الكتب الحديثة، أربد- الأردن، 2004.

26 - **علي عبد القادر القهوجي** ، الحماية الجنائية لبرامج الحاسب الالي، الدار الجامعية للنشر و التوزيع، الإسكندرية، 1999.

27 - **علي عدنان الفيل** ، الإجرام الالكتروني، طبعة أولى، منشورات زين الحقوقية،صيدا، لبنان،2011.

28 - **عماد محمد سلامة،** الحماية القانونية لبرامج الحاسب الآلي و مشكلة قرصنة البرامج، الطبعة الأولى، دار وائل للنشر، عمان، الاردن، 2005.

29 - **عمر أبو الفتوح عبد العظيم الحمامي** ، الحماية الجنائية للمعلومات المسجلة إلكترونيا، دراسة مقارنة ، دار النهضة العربية، القاهرة، 2010.

30 - **عمر الفاروق الحسيني،** المشكلات العامة في الجرائم المتصلة بالحاسب الآلي وإبعادها الدولية، ط 2، 1995.

31 - **عمر حسن المومني** ، التوقيع الإلكتروني وقانون التجارة الإلكترونية، ط 1، دار وائل للنشر، عمان- الأردن، 2005.

32 - **عوض حاج علي أحمد و. عبد الأمير خلف حسين** ، أمنية المعلومات وتقنية التشفير، الطبعة الأولى، دار جامد للنشر والتوزيع، عمان (الأردن)، 2005،

33 - **فتحي محمد أنور عزت** ، الأدلة الالكترونية في المسائل الجنائية والمعلومات المدنية و التجارية، دار الفكر والقانون، المنصورة، مصر 2010،

34 - **كوثر مازوني** ، الشبكة الرقمية و علاقتها بالملكية الفكرية،دار هومة، الجزائر، 2008.

35 - **محمد الأمين البشري** ، التحقيق في جرائم الحاسب الآلي و الانترنت، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004.

36 - **محمد حماد مرهج الهيتي** ، التحقيق الجنائي والأدلة الجريمة، ط 1، دار المناهج للنشر والتوزيع، عمان الأردن، 2010.

37 - **محمد حماد مرهج الهيتي** ، جرائم الحاسوب،الطبعة الأولى، دار المناهج للنشر والتوزيع، عمان الأردن، 2006.

38 - **محمد طارق عبد الرؤوف الخن** ، جريمة الاحتيال عبر الانترنت (الأحكام الموضوعية والأحكام الإجرائية)، منشورات الحلبي الحقوقية، بيروت- لبنان، 2011.

39 - **محمد على العريان** : الجرائم المعلوماتية، دار الجامعة الجديدة الإسكندرية ،مصر، 2004 .

40 - **محمد محمود المكاوي** ، الجوانب الأخلاقية والاجتماعية والمهنية للحماية من الجرائم المعلوماتية،(جرائم الكمبيوتر و الانترنت)ط 1، المكتبة العصرية للنشر و التوزيع، مصر، 2010.

41 - **محمد مصطفى الشقيري** ، السرية المعلوماتية، ضوابطها وأحكامها الشرعية،ط1، دار البشائر الإسلامية، بيروت،2008

42 - **محمود أحمد عبابنة** ، جرائم الحاسوب و أبعادها الدولية، دار الثقافة، عمان – الأردن، 2009.

43 - **محمود الرشيدي** ، العنف في جرائم الانترنت- أهم القضايا: الحماية والتأمين، ط1، الدار المصرية اللبنانية، القاهرة، 2011

44 - **منصور عمر المعايطة** ، الأدلة الجنائية والتحقيق الجنائي، ط 1، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2009.

45 - **معوان مصطفى**، الإثبات في المعاملات الإلكترونية في التشريعات الدولية، التوقيعات و البصمات الالكترونية، دار الكتاب الحديث، الجزائر، 2010.

46 - **ناير نبيل عمر** ، الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية- مصر،2012.

47 - **نائلة عادل محمد فريد قورة** ، جرائم الحاسب الآلي الاقتصادية،الطبعة الأولى، منشورات حلبي الحقوقية، بيروت، لبنان، 2005.

48 - **نبيلة هبة هروال** ، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الإسكندرية، 2006.

49 - **نجوى أبو هبة** ، التوقيع الالكتروني تعريفه و مدى حجيته في الإثبات، دار النهضة العربية، سوريا، بدون تاريخ.

50 - **نعيم مغبغب** ، حماية برامج الكمبيوتر- دراسة في القانون المقارن- الطبعة الثانية،منشورات حلبي الحقوقية، بيروت- لبنان، 2009.

51 - **هشام محمد فريد رستم**، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الكاتبة، أسيوط- مصر، 1995.

52 - **هلالي عبد اللاه أحمد**، الجوانب الموضوعية و الإجرائية لجرائم المعلوماتية، على ضوء إتفاقية بودابست الموقعة في 23 نوفمبر 2001، الطبعة الأولى، دار النهضة العربية، القاهرة- مصر، 2003.

53 - **هلالي عبد اللاه أحمد**، تفتيش نظم الحاسوب الآلي وضمانات المتهم المعلوماتي.دراسة مقارنة. دار النهضة العربية.القاهرة 2006.

ثالثا: <u>الرسائل و الاطروحات الجامعية</u>

أ- <u>رسائل الدكتوراه</u>

1 -**أميرة محمود بدوي الفقي** ، الإثبات الجنائي للجرائم المرتكبة عبر الانترنت، رسالة مقدمة لنيل درجة الدكتوراه، جامعة عين شمس، كلية الحقوق، قسم القانون الجنائي، مصر، 2013.

2 -**الموسوس عتو** ، حماية الحق في الخصوصية في القانون الجزائري في ظل التطور العلمي و التكنولوجي- دراسة مقارنة- رسالة دكتوراه في العلوم تخصص

علوم قانونية فرع قانون تجاري، جامعة جيلالي ليابس، كلية الحقوق و العلوم السياسية، سيدي بلعباس، الجزائر، 2014-2015.

3 **أحمد سعد محمد الحسيني،** الجوانب الإجرائية للجرائم الناشئة عن استخدام الشبكات الالكترونية، رسالة دكتوراه، جامعة عين شمس، كلية الحقوق، الدراسات العليا، قسم القانون الجنائي، مصر، 2012.

4 - **خليفي مريم** ، الرهانات القانونية للتجارة الإلكترونية، رسالة دكتوراه في القانون الخاص، كلية الحقوق و العلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، 2012/2011.

5 -**عبد الرءوف طالب حسينات** ، الحماية المدنية لحق المؤلف، في التشريعين المصري و الأردني، رسالة دكتوراه، جامعة القاهرة، 2006.

6 -**عمر محمد أبو بكر بن يونس** ، الجرائم الناشئة عن استخدام الانترنت، رسالة دكتوراه في القانون الجنائي، جامعة عين شمس، كلية الحقوق،2004.

7 -**عبد الرحمن بن عبد الله السند** : أحكام تقنية المعلومات "الحاسب الآلي وشبكة المعلومات (الإنترنت)"رسالة مقدمة لنيل درجة الدكتوراه في الفقه المقارن، جامعة الإمام محمد بن سعود الإسلامية، المعهد العالي للقضاء، قسم الفقه المقارن، المملكة العربية السعودية، 1424-1425هـ .

8 -**سالم محمد سليمان الأوجلي** ، أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوضعية ،دكتوراه الحقوق، جامعة عين شمس، 1997.

9 -**راشد محمد المري** ، الجرائم الإلكترونية في ظل الفكر الجنائي المعاصر- دراسة تحليلية تأصيلية مقارنة- رسالة دكتوراه في القانون الجنائي، كلية الحقوق، جامعة القاهرة، مصر، 2013.

10 - **فهد عبد الله العبيد العازمي** ، الإجراءات الجنائية المعلوماتية، رسالة لنيل درجة الدكتوراه في الحقوق، جامعة عين شمس، كلية الحقوق، مصر، 2012.

ب - رسائل الماجستير.

1- **بن عمر ياسين** ، جرائم تقليد المصنفات الأدبية و الفنية و آليات مكافحتها في التشريع الجزائري، مذكرة ماجستير تخصص قانون جنائي، كلية الحقوق و العلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2010-2011.

2-**هناء جميل عبد الحافظ أبو حمدية** ، الإثبات الالكتروني في الدعوة الجزائية في الأردن، رسالة ماجستير، كلية الدراسات العليا،الجامعة الأردنية، 2006

3-**طعباش أمين** ، الحماية الجنائية للمعاملات الالكترونية، مذكرة ماجستيرفي العلوم القانونية تخصص علم الإجرام و العقاب، جامعة الحاج لخضر، كلية الحقوق و العلوم السياسية، باتنة، 2012-2013.

4-**نجاة عباوي** ، جرائم المعلوماتية في التشريع الجزائي الجزائري، رسالة ماجستير، كلية الحقوق و العلوم السياسية، جامعة بشار، 2008.

5-**منصور بن سعيد القحطاني** ، مهددات الامن المعلوماتي و سبل مواجهتها، رسالة ماجستير في العلوم الإدارية، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم العلوم الادارية، السعودية، 2008.

6-**نايت أعمر علي** ، الملكية الفكرية في إطار التجارة الالكترونية، مذكرة ماجستير فرع قانون دولي للأعمال، مدرسة دكتوراه للقانون و العلوم السياسية، كلية الحقوق و العلوم السياسية، جامعة مولود معمري، تيزي وزو تاريخ المناقشة 15 مارس 2014 .

7-**سعيداني نعيم**، آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجستير في العلوم القانونية تخصص قانون جنائي، جامعة الحاج لخضر، باتنة،2012-2013.

8-**سليمان غازي لعتيبي** ، درجة توافر كفايات البحث عن الدليل الرقمي في الجرائم المعلوماتية لدى ضباط شرطة العاصمة المقدسة، مذكرة ماجستير في علوم شرطية

تخصص قيادة أمنية، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، الرياض، 2010 .

9-**رصاع فتيحة** ، الحماية الجنائية للمعلومات عبر شبكة الانترنت، مذكرة ماجستير في القانون العام، جامعة أبي بكر بلقايد، كلية الحقوق و العلوم السياسية، تلمسان، 2011-2012.

10-**ياسين بن عمر** ، جرائم تقليد المصنفات الأدبية و الفنية و آليات مكافحتها في التشريع الجزائري، مذكرة ماجستير، كلية الحقوق و العلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2011/2010.

11 - **منصور بن سعيد القحطاني** ، مهددات الأمن المعلوماتي و سبل مواجهتها، رسالة ماجستير في العلوم الادارية، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم العلوم الإدارية، 2008

رابعا: المقالات و المؤتمرات العلمية

1- **أحمد حماد مرهج الهيتي** ، نطاق الحماية الجنائية للمصنفات الرقمية،دراسة مقارنة في القوانين العربية لحماية حق المؤلف، مجلة الشريعة و القانون، العدد الثامن والاربعون، جامعة المملكة، البحرين، أكتوبر .2011

2- **أبو المعالي محمد عيسى** ، الحاجة إلى تحديث آليات التعاون الدولي في مجال مكافحة الجرائم، ورقة مقدمة في المؤتمر المغاربي الأول حول المعلوماتية و القانون المنعقد في 28-2009/10/29 بطرابلس-ليبيا.

3- أسامة بن غانم العبيدي ، الإتلاف المعلوماتي، مجلة دراسات المعلومات، عدد الرابع، يناير 2009.

4- الظهران عوض المالكي : (12) اثنا عشر براءة اختراع في مجال الأمن المعلوماتي، حققها فريق بحث من جامعة الملك فهد بالظهران، جريدة الرياض، يومية تصدر عن مؤسسة اليمامة الصحفية، العدد 14914،بتاريخ 24 أبريل .2009

5- **إياد علي الدرة** ، الأدلة الجنائية الإلكترونية، مجلة أمن المعلومات تصدر عن الجمعية العلمية السورية للمعلوماتية، ع (72)، دمشق، فبراير 2012.

6- **موسى مسعود أرحومة** ، الإشكالات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، بحث مقدم إلى المؤتمر المعاربي الأول حول المعلوماتية و القانون، المنعقد بتاريخ 28-29 من شهر أكتوبر 2009، أكادمية الدرسات العليا، طرابلس، ليبيا.

7- **رقية عواشرية**، الحماية القانونية للمصنفات المنشورة إلكترونيا في ضل معاهدة الويبو لحقوق المؤلف 1996 ،دراسة تقيمية، مجلة جيل حقوق الإنسان، العدد الأول، لبنان، فيفري .2013

8- **راضية مشري** : الحماية الجزائية للمصنفات الرقمية في ظل قانون حق المؤلف، مجلة التواصل لكلية الحقوق، جامعة 08 ماي 45، قالمة، عدد 34، جوان 2013.

9- المركز القومي للبحوث الاجتماعية و الجنائية، " حق المؤلف و الحقوق المجاورة في إطار الملكية الفكرية"، المجلة الجنائية القومية، العدد 01 بتاريخ مارس- جويلية 1999.

10- **أمن المعلومات** ، الاجتماع الثاني لرؤساء الإدارات المختصة بتقنية المعلومات بالنيابات العامة العربية، المركز العربي للبحوث القانونية والقضائية، مجلس وزراء العدل العرب، جامعة الدول العربية، بيروت – لبنان، 5-7 مارس 2012.

11- **هالة كمال أحمد نوفل** : بحث حول "استطلاع رأي النخبة حول جرائم اختراق البيئة المعلوماتية الافتراضية واستشراف الاتجاهات الحديثة في مجال أمن المعلومات" مقدم للمؤتمر السادس لجمعيات المكتبات والمعلومات السعودية – البيئة المعلوماتية الآمنة، المفاهيم والتشريعات والتطبيقات- المنعقد بمدينة الرياض في 6-7 أبريل 2010.

12- **حسين بن سعيد بن سيف الغافري** . الجهود الدولية في مواجهة جرائم الإنترانت ورقة عمل مقدمة للاتحاد العربي للتحكيم الالكتروني .2007

13- **ضياء على أحمد نعمان** ، الغش المعلوماتي، الظاهرة و التطبيقات، سلسلة الدراسات القانونية في المجال المعلوماتي، الطبعة الأولى، الوراقة الوطنية، مراكش- المغرب- 2011.

<u>خامسا: الاتفاقيات الدولية و التشريعات</u>

أ - **المعاهدات و الاتفاقيات الدولية**

1-الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحرّرة بالقاهرة بتاريخ 21 ديسمبر سنة 2010.

2-معاهدة بودابست للإجرام الإلكتروني لسنة 2001.

3- إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية المعتمدة من طرف الجمعية العامة للأمم المتحدة في 15/11/2000.

4- معاهدة الويبو بشأن حق المؤلف كما اعتمدها المؤتمر الدبلوماسي في 20 ديسمبر 1996.

5-إتفاقية برن لحماية المصنفات الأدبية والفنية وثيقة باريس المؤرخة 24 يوليو 1971 والمعدلة في 28 سبتمبر 1979.

6-اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية (تربس).

7- الاتفاقية الأوروبية لحقوق الإنسان لسنة 1950.

ب:التشريعات الجزائرية

القوانين و الأوامر

- الدستور الجزائري لسنة 1996 المعدل و المتمم

1-القانون رقم 15-03 مؤرخ في أوّل فبراير سنة 2015 يتعلق بعصرنة العدالة، ج.ر عدد 06 بتاريخ 10 فبراير 2015.

2-القانون رقم 15-04 مؤرخ في أوّل فبراير سنة 2015 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكتروني، ج.ر عدد 06 بتاريخ 10 فبراير 2015.

3-القانون رقم 09-03 المؤرخ في 25 فبراير 2009 يتعلق بحماية المستهلك و قمع الغش، جريدة رسمية عدد 15 بتاريخ 08 مارس سنة 2009.

4-القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ،ج ر العدد 47 بتاريخ 16 أوت 2009.

5- الأمر رقم 06-09 المؤرخ في 15 يوليو 2006 المتعلق بمكافحة التهريب، الجريدة الرسمية عدد 47 بتاريخ 19 يوليو 2006

6- القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 156/66 المؤرخ في 08/06/1966 المتضمن قانون العقوبات،ج.ر العدد71لسنة2004 المعدل والمتمم .

7-الأمر رقم 03-05 المؤرخ في 19 يوليو 2003 المتعلق بحقوق المؤلف و الحقوق المجاورة، الصادر بالجريدة الرسمية عدد 44 بتاريخ 23 يوليو 2003.
8- الأمر رقم 03-08 المؤرخ في 19 يوليو 2003 يتعلق بحماية التصاميم الشكلية للدوائر المتكاملة ، الصادر بالجريدة الرسمية عدد 44 بتاريخ 23 يوليو 2003.
9-الأمر رقم 75-58 المؤرخ في 26 سبتمبر 1975 يتضمن القانون المدني المعدل والمتمم
10-الأمر رقم75-02 المؤرخ في 09 يناير 1975 المتعلق بالمصادقة عل الاتفاقية الدولية المتضمنة إنشاء المنظمة العالمية للملكية الفكرية الموقعة بستوكهولم في 14 يوليو 1967، ج.ر عدد 13 بتاريخ 14 فبراير 1975.
11-الأمر رقم 73-14 المؤرخ في 03 ابريل 1973 المتضمن حق المؤلف، الجريدة الرسمية عدد 29 بتاريخ 10 ابريل 1973.
12-الأمر 73- 26 المؤرخ في 05 يونيو 1973 يتعلق بإنظمام الجزائر للاتفاقية العالمية لسنة 1952 حول حق المؤلف المراجعة بباريس في 24 يوليو 1971، ج.ر عدد 53 بتاريخ 03 يوليو 1973.
13-الأمر رقم 66-155 المؤرخ في 8 يونيو 1966 يتضمن قانون الإجراءات الجزائية المعدل والمتمم.

المراسيم و القرارات

1-مرسوم رئاسيّ رقم 252-14 مؤرّخ في 8 سبتمبر يتضمّن التّصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحرّرة بالقاهرة بتاريخ 21 ديسمبر سنة 2010، ج.ر عدد 57 بتاريخ 28 سبتمبر 2014.
2- المرسوم الرئاسي رقم 02-55 المؤرخ في 05 فبراير 2002، يتضمن مصادقة الجزائر بتحفظ على إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، ج.ر رقم 09 بتاريخ 10 فبراير 2002.
3- المرسوم الرئاسي رقم 97-341 المؤرخ في 13/09/1997 المتضمن انضمام الجزائر بتحفظ إلى الاتفاقية برن لحماية المصنفات الأدبية والفنية المعدلة و المتممة ،ج ر عدد 61 بتاريخ 14 سبتمبر 1997 .

4-مرسوم تنفيذي رقم 10-116 مؤرخ في 18 أبريل 2010، و يحدد مضمون البطاقة الإلكترونية للمؤمن له إجتماعيا و المفاتيح الإلكترونية لهياكل العلاج و لمهنيي الصحة وشروط تسليمها و استعمالها و تجديدها، ج.ر عدد 26 بتاريخ 21 أبريل .2010

5-المرسوم التنفيذي رقم 7-162 المؤرخ في 30 ماي 2007 يعدل و يتمم المرسوم رقم 2001-123، يتعلق بنظام استغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية، و على مختلق خدمات المواصلات السلكية و اللاسلكية، ج.ر عدد 37 لسنة 2007.

6-المرسوم التنفيذي رقم 2-141 المؤرخ في 16 أبريل 2002 يحدد القواعد التي يطبقها متعاملوا الشبكات العمومية للمواصلات السلكية و اللاسلكية من أجل تحديد تعريفة الخدمات المقدمة للجمهور، الجريدة الرسمية عدد 28 لسنة 2002.

7-المرسوم التنفيذي رقم 2001-123 المؤرخ في 09 ماي 2001 يتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية و على مختلف المواصلات السلكية و اللاسلكية، ج.ر عدد 27 لسنة 2001.

8-المرسوم التنفيذي رقم 98-257 المؤرخ في 25 أوت 1998 يتعلق بضبط شروط وكيفيات إقامة خدمات الانترنت و استغلالها، المعدل بموجب المرسوم التنفيذي رقم 2000-307 المؤرخ في 14 اكتوبر 2000، ج.ر عدد 60 بتاريخ 15 أكتوبر 2000.

9-قرار مؤرّخ في 26 ديسمبر سنة 2011 يحدد المواصفات التقنية لجواز السفر الوطني البيومتري الإلكتروني، ج.ر العدد الأول بتاريخ 14 يناير 2012.

10-قرار وزاري مشترك مؤرخ في 30 أكتوبر سنة 2014 يحدد كيفيات تطبيق النظام المعلوماتي لمحاسبة التسيير في المؤسسات العمومية للصحة وكذا قائمة المؤسسات المعنية بتنفيذ هذا النظام، ج.ر العدد الأول، بتاريخ 07 يناير 2015.

ج- التشريعات العربية:

1-مرسوم سلطاني رقم 12/2011 بإصدار قانون مكافحة جرائم تقنية المعلومات، لسلطنة عمان، جريدة رسمية عدد .929

2-القانون الأردني لجرائم أنظمة المعلومات رقم 30 لسنة 2010، الجريدة الرسمية عدد 5056، بتاريخ 16 سبتمبر 2010

3-القانون رقم 05 لسنة 2004 المؤرخ في 03 فيفري 2004 يتعلق بالسلامة المعلوماتية، الرائد الرسمي للجمهورية التونسية عدد 10، بتاريخ 03 فيفري2004.

4-أمر عدد 1248 لسنة 2004 مؤرخ في 25 ماي 2004 يتعلق بضبط التنظيم الإداري و المالي و طرق سير الوكالة الوطنية للسلامة المعلوماتية، الرائد الرسمي للجمهورية التونسية عدد 45، بتاريخ 04 جوان 2004.

5-أمر عدد 1249 لسنة 2004 يتعلق بضبط شروط و إجراءات المصادقة على خبراء التدقيق في مجال السلامة المعلوماتية، الرائد الرسمي للجمهورية التونسية، عدد 45، بتاريخ 04 جوان 2004.

6-قانون العقوبات الأردني رقم 16/ 1960، ج.ر بتاريخ 1960/01/01 و المعدل بأخر قانون رقم 2011/8 في الجريدة الرسمية رقم 5090 بتاريخ 2011/05/02.

7-قانون المعاملات الالكترونية الأردني رقم 58 لسنة 2001.

8-قانون الاتصالات الأردني رقم 13 لسنة 1995 الجريدة الرسمية رقم 4072 ، بتاريخ / 1995 1/ 10، الصفحة2939 ، المعدل بموجب القانون رقم 21 لسنة 2011 والصادر بالجريدة الرسمية بتاريخ 2011/04/21.

9- القانون الاماراتي لمكافحة جرائم تقنية المعلومات رقم 02 لسنة 2006، الجريدة الرسمية عدد 442..

10- اللائحة التنفيذية لقانون التوقيع المصري الصادرة بقرار من وزارة الإتصالات وتكنولوجيا المعلومات، رقم 109 لسنة 2005، الوقائع المصرية، العدد 115 بتاريخ 25 ماي 2005 .

سادسا: مقالات و ابحاث على المواقع الإلكترونية.

1- **عبد الرحمن ألطاف** ، تحديات حماية الملكية الفكرية للمصنفات الرقمية، على الموقع http://www.f-law.net/law/threads/28525

2- **يونس عرب**، نظام الملكية الفكرية للمصنفات المعلوماتية، الدليل الالكتروني للقانون العربي، 2008، ، على الموقع: www.arablawinfo.com

3- **حسام الدين الأهواني**، حماية الملكية الفكرية في مجال الانترنت، الدليل الالكتروني للقانون العربي، على الموقع: www.arablawinfo.com

4- **أمجد حسان** ، الفيروسات إرهابا تهدد أنظمة المعلومات، مقال مقدم إلى ملتقى " الإرهاب في العصر الرقمي" المنعقد بجامعة الحسين بن طلال، البتراء، الأردن، ب 10-2008/07/12.

5-**ميلود العربي بن حجار** ، تشريعات الملكية الفكرية في حقل حماية البرمجيات بالجزائر - Cybrarians Journal ،ع26، سبتمبر 2011 متاح على

6-**خالد بن سليمان الغثبر** ، اختراق المواقع الالكترونية حال الأزمات تشخيص وحلول مركز التميز لأمن المعلومات، على الموقع :coeia.ksu.edu.sa/ اطلع عليه بتاريخ 2013./12/16

7- **رزيقة أدرغال** " الانترنت في الجزائر وسيلة للتشهير و انتهاك لخصوصية الغير"، جريدة الخبر، الجزائر ، 17 يناير .2015

8- **سلمى حراز**: مقال نشر بجريدة الخبر الجزائرية بعنوان : " الفيس بوك يشجع على ارتكاب الجريمة" ، بتاريخ 17 يناير 2015.

9 -مقال بعنوان " الإرهاب الالكتروني يهدد استقرار الجزائر" منشور بجريدة الخبر اليوم(يومية إخبارية جزائرية) بتاريخ 2013/02/02 .

10 - دويب حسن صابر ، مداخلة بعنوان: القوانين العربية وتشريعات تحريم الجرائم الالكترونية وحماية المجتمع، المؤتمر السادس لجمعية المكتبات والمعلومات، السعودية.

11 - ثانيا: المراجع باللغة الفرنسية.

A-Ouvrages généraux

1- **Béatrice CLEMENT, Gérard CLEMENT, Frédérique DUBOST, Jean-Philippe VICENTINI**, fiche de droit pénal spécial, éd Ellipses, Paris 2012

2- **Michel VERON**, Droit pénal spécial, 14e éd, Dalloz, Paris, 2012.

3- **Michel Veron**, droit pénal spécial,6 édition, Armand colin, paris,1998

4- **Valérie Malabat**, droit pénal spécial,6e édition, DALLOZ, Paris,2013.

B-Ouvrages spéciaux

1- **Elise Dragon**, Etude sur le statut juridique de l'information, D . 1998, chron ,

2- **frédéric duflot**, les informatiques bénéfiques chroniques d'un anathème, (DESS), Paris,2003 ,2004.

3- **Hubert Bitan** , Droit des créations immatérielles: logiciels, bases de données, autre œuvres sur la web, Ed Lamy, France, 2010

4- **Laure ZICRY**, Enjeux et maitrise des cyber risque, éd LARGUS de l'assurance, France, 2014

5- **Michel VIVANT**, Lamy droit de l'informatique ,éd Lamy,1989,N° 2479. **Raymons gassin** , Fraude informatique,Dalloz, 1995,

6- **Myriam QUEMENER, Yves CHARPENEL** ; Cybercriminalité droit pénal appliqué,Ed Economica , Paris,2012,

7- **Nicolas ARPAGIAN,** La Cyber Sécurité, éd ITCIS, Alger, 2014.

8- **Olivier ITEANU,** Tous Cyber Criminels, JACQUES-MARIE LAFFONT EDITEUR, Paris, 2004.

9- **XAVIER Linant de bellefond**s et **ALAIN hollande**, Pratique du droit de l'informatique, 4e éd, DELMAS, 1998.

10- **Xavier RAUFER**, Cyber-Criminologie, CNRS éditions, Paris, 2015.

***Les thèses ;**

1- Chamy (guillaume), fraude informatique, thèse tome 1 et 2, université Aix Marseille 1992

Les revues ;

1- Chamoux(F), La loi sur la fraude informatique, de nouvelles incrimination, J.C.P, 1998-1-3321,n°10.

2- Michel Vasseur ; ¨ Des responsabilités encours par le banquier a raison des informations avais et conseil dispenses a ses client » revu banque , 1983,

Les sites électroniques

1-Pierre-Hugues Vallée et **Ejan Mackaay**, La confiance Sa nature et son rôle dans le commerce électronique, Lex Electronica, vol. 11 n° 2 (Automne / Fall 2006) sur le site ;

2-Marc Robert :Remise du Rapport « Protéger les Internautes » le rapport du group de travail interministériel sur la lutte contre la cybercriminalité, communiqué de presse, N° 185, Paris, le 30 juin 2014,sur le site ; www.presse.justice.gouv.fr

3-Xavier LEMARTELEUR**,** Le scan de ports : une intrusion dans un STAD ,P 3 ; publier le 13 juin 2008,disponible à l'adresse suivante ; www.juriscom.net

4- Murielle Cahen, INTRUSION DANS UN SYSTEME INFORMATIQUE, disponible à l'adresse suivante ; www.murielle-cahen.com

5- **Thomas Adhumeau**, Le piratage d'un serveur de données par un Hacker: le délit de maintien frauduleux, sur le site http://gau mata.blogspot.com/2011/06/le-piratage-dun-serveur-de-donnees-par.html ' le 9 juin 2011.

6-**Valérie Sédallian** ; Légiférer sur la sécurité informatique : la quadrature du cercle? 5décembre 2003, P11 sur le site www.juriscom.net**.**

7-**MAITRE ANTHONY BEM**, L'INTRUSION ET LES ATTEINTES AUX SYSTEMES INFORMATIQUES SANCTIONNEES PAR LE DROIT PENAL,Article juridique publié le 10/09/2010 sur le site : http://www.legavox.fr/blog/maitre-anthony-bem/

http://www.lex-electronica.org/articles/v11-2/vallee_mackaay.htm

LES LOIS

1- La convention internationale pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel N°108 du 28 janvier 1981

2- Loi n°88-19 du 05 janvier 1988 relative à la fraude informatique, JORF du 06 janvier 1988.(LOI GODFRAIN)

3-Loi n° 2009-1311 du 28 octobre 2009 relative à la protetion pénale de la propriété littéraire et artistique sur internet, JORF Du 29 Octobre 2009, texte 1 sur 183.

4-Loi n° 2012-287 Du 1er mars 2012 relative à l'exploitation numérique des livres indisponibles du XXe siècle, JORF Du 2 mars 2012, texte 1 sur 133.

5-Loi n° 92-683 du 22 juillet 1992, portant réforme du code pénal, texte origine au 01 mars 1994.

5-Code pénal français version en vigueur sur le site ; www.legifrance.gouv.fr
6-Loi n° 2012-410 du 27 mars 2012 relative à la protection de l'identité, JOPF n°0075 du 28 mars 2012, texte n°2, P5604,(art 9 modifie les articles 323-1,323-2,323-3 de code pénal français).
7-Loi n° 2004-575 du juin 2004 pour la confiance dans l'économie numérique, JORF n°0143 du 22 juin 2004
8-Loi n°2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lute contre le terrorisme, art. 16, JOPF n° 0263 du 14 novembre 2014
9-loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, JORF n°0294 du 19 décembre 2013 page 20570 texte n° 1
10-Ordonnance n°2000-916 du 19 septembre 2000 - art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002.

11- Code de procédure pénale

12- Loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité, JORF 10 mars 2004 en vigueur le 1er octobre 2004

13-La Loi 2003-239 pour la sécurité intérieure du 2003-03-18 arts. 17 1° JORF du 19 mars 2003

14- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF du 7 janvier 1978 .

11- Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF n°182 du 7 août 2004 page 14063, texte n° 2.

Les jurisprudences;

-Tribunal de grande Instance, 3e section, 4echambre, 21 février 2013

-(Crim , 8 déc 1999, Bull n°296, Dr. penal 2000, comm.53)

-décision CA Paris, 11ème Chambre, 8 décembre 1997

-cour du 30 octobre 2002

-décision du 5 Avril 1994, la cour d'appel de Paris

-un arrêt du 3 octobre 2007, la Cour de Cassation

-T.G.I Pris, 13 éme ch, 18 septembre 2008

-C.A de paris,5 avril 1994, NCP, 104° édition, D, paris ;2009, P 916.

- un arrêt du 4 décembre 1992, la cour d'appel de paris

- C.A de paris, 15 décembre 1999,D ,2000,I.R

الفهـرس

فـهــرس

الباب الأول:
الجوانب الموضوعية لقواعد الأمن المعلوماتي