جامعة أحمد درايـة بـــأدرار

كليـة الـحقوق والعلوم السياسية

الآليات القانونية لمكافحة الجريمة الإلكترونية

(دراســـــة مقارنـــة)

أطـروحة مقدمة لنيل شهادة الدكتوراه الطور الثالث (ل م د)

تـخصص: القانون الجنائي

من إعداد الطالبـة:

شـنتير خـضـرة

إشـراف الأستاذ الدكتور:

بـاخـــويا دريـــس

تاريخ المناقشة: 2021/01/25

أعضاء لجنة المناقشة:

أ.د / بـومديـن محمـــــــد	أسـتاذ التعليم العالـي	جامعة أدرار	رئـيساً
أ.د / بـاخـويـا دريـــــس	أسـتاذ التعليم العالـي	جامعة أدرار	مشرفـاً ومقرراً
أ.د / مـــسعودي يـــــوسف	أسـتاذ التعليم العالـي	جامعة أدرار	مناقـشاً
أ.د / رحـمونـــي مـــحمـد	أسـتاذ التعليم العالـي	جامعة أدرار	مناقـشاً
أ.د / مـايـــنـو جـيـــلالـي	أسـتاذ التعليم العالـي	جامعة بشار	مناقـشاً

الـموسـم الـجامـعي:2021/2020

بسم الله الرحمن الرحيم

﴿ الْحَمْدُ لِلَّهِ رَبِّ الْعَالَمِينَ الرَّحْمَنِ الرَّحِيمِ مَالِكِ يَوْمِ الدِّينِ إِيَّاكَ نَعْبُدُ وَإِيَّاكَ نَسْتَعِينُ اهْدِنَا الصِّرَاطَ الْمُسْتَقِيمَ صِرَاطَ الَّذِينَ أَنْعَمْتَ عَلَيْهِمْ غَيْرِ الْمَغْضُوبِ عَلَيْهِمْ وَلَا الضَّالِّينَ ﴾

سورة الفاتحـــة

الإهـــــداء

إلى من ساندني وصبر عليَّ وتغاضى عن تقصيري زوجي العزيز.

إلى فلذة كبدي وقرة عيني أولادي الغوالي

إلى كل أفراد عائلتي الكريمة.

إلى كل الأصدقاء والأحباب وبالاخص عائلة أستاذي المشرف.

إلى كل من صلى وسلم على الحبيب المصطفى صلى الله عليه وسلم.

إلى أرواح من غيبهم الموت ولم ينسهم القلب، أمي وأبي وأجدادي

رحمهم الله جميعا وأسكنهم فسيح جناته

إن شاء الله.

الباحثة: شنتيـر خضرة

شـــكر وعـرفان

الشكر والحمد للمولى العلي القدير الذي منى عليَ باتمام هذه الرسالة.

أتقدم بجزيل شكري وبالغ امتناني وعرفاني لأستاذي الفاضل البروفيسور باخويا دريـس الذي تفضل بإشرافه على هذه الأطروحة، فلقد كان معطاءً بعلمه، مصوباً بإرشاده وتوجيهه وتعاليمه، كريماً بوقته، مساندا مساهماً بمراجعه وبحوثه، لم يدخر جهداً ولا نصيحة.

كما يشرفني أن أتقدم بجزيل الشكر والتقدير إلى السادة الأساتذة أعضاء اللجنة على قبولهم مناقشة هذا العمل المتواضع.

وأتقدم بالشكر والثناء إلى كل من؛ الدكتور مجيدي كمال أستاذ الأدب العربي بجامعة أدرار والأستاذ معزوزي الطاهر –أستاذ اللغة العربية في المستوى الثانوي- على كل التصحيحات اللغوية والكتابية التي قاما بها، والتي ساعدتني حتى أخرج هذه الرسالة في حُلتها هاته.

كما أتقدم بشكر خاص إلى كل أساتذتي من كلية الحقوق والعلوم السياسية على دعمهم لي ومساندتي في البحث وانشغالهم بأحوالي.

وإلى كل أولائك الذين كانت مراجعهم وبحوثهم ودراساتهم بمثابة النور الذي ينير الطريق ويسهل الدرب.

الطالبة: شنتير خضرة

قائمــة المختصرات

أولاً– باللغــة العربية:

الج.ر.ج ج	الجريدة الرسمية للجمهورية الجزائرية.
ص	الصفحة.
ق.إ.ج.ج	قانون الإجراءات الجزائية الجزائري.
ق.إ.ج.م	قانون الإجراءات الجنائية المصري.
ق.ع.ج	قانون العقوبات الجزائري.
ق.ع.ف	قانون العقوبات الفرنسي.
ق.ع.م	قانون العقوبات المصري.
ق.ع.مغ	قانون عقوبات مغربي.
ق.م.ج.م	قانون المسطرة الجنائية المغربي.

ثانياً– باللغة الاجنبية:

AFRIPOL	Une agence africaine de police criminelle.
ANSSI	Agence nationale de sécurité des systèmes d'information.
CNIL	Commission nationale de l'informatique et des libertés.
DGGN	La direction générale de la gendarmerie nationale.
DGPN	Direction générale de la police nationale.
EUROJUST	European Union Agency for Criminal Justice Cooperation.
Europol	L'agence européenne de police criminelle.
FBI	Le Federal Bureau of Investigation.
INTERPOL	L'Organisation internationale de police criminelle.
ibid.	C'est le terme utilisé dans les références d'un document stable, pour éviter la répétition lorsque la même source a été citée dans la référence précédente.
OCLCTIC	Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication.
OP. CIT	Ouvrage précité
p	Page.
PHAROS	Portail officiel de signalement des contenus illicites de l'internet.
TCP/IP	TCP/IP (Transmission control protocol Internet) : Suite de protocoles des noms des deux protocoles majeurs (TCP et IP).

مقدمـــــــة

مقدمـــــة:

جلب التطور التكنولوجي لحياة الإنسان العديد من المحاسن؛ فبه اختصرت المسافات، وحسن استغلال الوقت، ونقصت التكاليف والأعباء، وأصبح استعمال بعض الأشخاص للوسائل التكنولوجية الحديثة من الضروريات بعد أن كان من الكماليات، فأضحى الوصول إلى المعلومات ممكن في دقائق وثوانٍ معدودات، بفضل الأجهزة الإلكترونية التي لها درجة عالية من التخزين وذاكرة قوية يجافيها النسيان، وتواصلية إلكترونية يشارك فيها قرابة أربعة ملايير ونصف المليار (4.54) مستخدم للانترنت؛ هذا الفضاء الإفتراضي الذي قضى على كل الحدود الجغرافية والسياسية للبلدان، وساعد بأن يتحول المجتمع من خلاله إلى عالم شفاف أصبحت فيه بيوتنا وحياتنا عارية لأي متصفح؛ والذي يمكن أن يكون أي شخص من أفراد الفضاء الأزرق.

إن الاستخدامات الواسعة للوسائل التكنولوجية الحديثة أدت إلى استحداث أموراً جديدة كانت سبباً وبشكل مباشر في ظهور واستفحال نوع معين من الجرائم؛ هاته الجرائم التي انتشرت وتعددت صورها وازداد حجمها وتسارعت وتيرتها وسهل ارتكابها رغم اختلاف تسمياتها، فأصبحت تقاس مدة ارتكابها بالثواني، والأدهى أنها قد ترتكب في حضور المجني عليه دون علمه بحدوثها، فلم تعد الحدود الجغرافية ولا الحواجز الإدارية، ولا بُعد المسافات واختلاف اللغات عائقاً أمام مرتكبيها، وباتت مخاطرها تهدد أمن المجتمعات وقيمها، وشكل وجود جرائم إلكترونية بشكل مستمر ومتسارع تحديات كثيرة أمام النظم القانونية، الأمر الذي دفع الفقه والقضاء والباحثين القانونيين إلى البحث عن آليات مكافحة تكون قادرة على مجابهة هذه الظاهرة الإجرامية واحتوائها ومراعاة طبيعتها وخصوصيتها؛ لأنه ما لم نستطع تأمين بنيتنا التحتية الإلكترونية، وأمننا السيبراني[1]، فإن كل ما يحتاجه المجرم الإلكتروني لتهديد حياتنا الاجتماعية والاقتصادية والثقافية وحتى السياسية هي مجرد نقرات بسيطة على جهاز الحاسوب، أو أي جهاز إلكتروني آخر، والاتصال عن طريق الإنترنت لتنفيذ جريمته؛ لأنه من المرجح أن تصبح السيطرة على مصادر

1 الفقرة الثالثة من المادة (3/10) من القانون رقم 18-04، المؤرخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018، والذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، الصادر في الج.ر.ج العدد 27، بتاريخ 13 مايو 2018: "الأمن السيبراني: مجموع الأدوات والسياسات ومفاهيم الأمن والآليات الأمنية والمبادئ التوجيهية وطرق تسيير المخاطر والأعمال والتكوين والممارسات الجيدة والضمانات والتكنولوجيات التي يمكن استخدامها في حماية الاتصالات الإلكترونية ضد أي حدث من شأنه المساس بتوفير وسلامة البيانات المخزنة أو المعالجة أو المرسلة".

المعلومات ووسائل معالجتها أكثر أهمية من الموارد الأخرى، الطبيعية منها أو حتى العسكرية. ويعد هذا الأمر أحد الأسباب التي تدفع الباحثين إلى إيجاد آليات ناجعة في مكافحة الجريمة الإلكترونية.

إن عملية البحث عن آليات قانونية لمكافـحة الجـرائم الإلكترونية، يعد مسألة بالغـة الأهمية؛ العلمية منها والعملية خاصة مع تنامي دور التعاملات الإلكترونية في حياتنا اليومية، وبروز الحاجة إلى زرع الثقة والطمأنينة في قلوب المتعاملين بالأجهزة الإلكترونية على اختلاف أنواعها، وما هذه الدراسة المعنونة بـ: الآليات القانونية لمكافحة الجريمة الإلكترونية –دراسة مقارنة– إلا عينة من تلك البحـوث التي تهدف إلى المساهمة ولو بالقليل في إيجاد آليات قانونية فعالة في مكافحة الجرائم الإلكترونية باختلاف أنواعها.

وفي سبيل تحقيق ذلك سنحاول الإجابة عن إشكالية جوهرية، تتمثل فيما يلي: إلى أي مدى ساهمت النصوص الجنائية المقارنة في مكافحة الأنماط المستجدة للجرائم الإلكترونية ؟

وتندرج تحت هذه الإشكالية مجموعة من التساؤلات نجملها فيما يلي:

- بمَ تميّزت الجريمة الإلكترونية عن باقي الجرائم التقليدية؟
- كيف يمكن مراعاة مميزات هذه الجريمة عند القيام بالقواعد الإجرائية؛ خاصة تلك المتعلقة بالبحث والتحري عن الدليل الإلكتروني؟
- ما موقف المشرع الجزائري من الجريمة الإلكترونية، وما سبل التي أقرها لمكافحتها ؟
- أتعد الآليات الداخلية المخصصة في كل دولة كفيلة لوحدها بمكافحة الجريمة الإلكترونية ؟ أم أن ضرورة التعاون الدولي بات أمراً ملحاً توجب إقراره من قبل مختلف التشريعات المقارنة لمكافحة هذه الجريمة ؟
- فيما تتمثل صعوبات مكافحة هذا النوع من الاجرام ؟
- أيمكن إيجاد آليات مساعدة على مكافحة الجريمة الإلكترونية ؟

وللبحث عن إجابة لهذه الإشكالية وتلك التساؤلات تم اعتماد على مجموعة من المناهج؛ أولها المنهج التحليلي، والثاني هو المنهج الوصفي، واللذان لا يكتفِيان بوصف الظاهرة فقط، بل يساعدان على تحليلها للوقوف على الحقائق وتتبعها، خاصة حين التعرض لهذه الظاهرة الإجرامية وكذا مرتكبها المجرم الإلكتروني، والـدليل الناتج عنها، والمنهج الاستقرائي ليس استقراء كاملا، وإنما هو استقراء ناقص، حين الاطلاع على بعض التشريعات والمقارنة بينها للوصول إلى بعض الحقائق

الخاصة بالبحث في الجريمة الإلكترونية، حينما تم التطرق للنصوص القانونية الوطـنية منها والعربية والغربية، وكذا الاستعانة بالمنهج المقارن الذي يعد ضرورياً للمقارنة بين التشريعات، للوقوف على أوجه التشابه والاختلاف والتداخل حين وجودها بين التشـريع الوطني والتشريعات الأخرى المقارنة، خاصة التشـريع المصري والفرنســي، لنكون بذلك قد تطرقــنا لبعض المسائل المهمة التي وصل إليها الفكر القانوني المقــارن في عملية المكافحة، دون أن ننسى المنهج التاريخي والذي كان حاضراً في تتبع التشريعات تاريخياً حين تتبع التسلسل الزمني – أو التسلسل الكرونولوجي- لإصدار بعض الدول لقوانين تعنى بمكافحة الجريمة الإلكترونية، وكذا وقوع بعض الجرائم الإلكترونية عبر فترات زمنية متفرقة.

لقد عالجت العديد من رسـائل الدكتوراه موضوع الجريمة الإلكترونية، ومن أهم تلك الدراسات: رسالة دكـتوراه بعنوان: الجـريمة المعلوماتية في القانون الجزائري واليمني، للباحث فايز محمد راجع غلاب، الصادرة عن كلية الحقوق بجامعة الجزائر (01)، خلال السنة الجامعية 2009-2010، والتي تطرق من خلالها الباحث لبعض الجرائم الإلكترونية في القانون الجزائري والقانون اليمني؛ كالجرائم الماسة بالأمن القومي للدولة، مثل: التجسس وغسيل الأموال، والإرهاب الإلكتروني ضمن (الباب الأول)، إذ ركز على دراسة أركان الجريمة والعقوبات المقرر لها، أما الباب الثاني فقد خصصه لدراسة القواعد الإجرائية للجرائم المعلوماتية، وفيها درس مجموعة من القواعد الإجرائية المتبعة في عملية البحث عن الجريمة الإلكترونية والدليل الناجم عنها بصفة مغايرة عما تناولناه في دراستنا بحكم ميدان المقارنة المختلف.

وفي دراسة أخرى رسالة دكتوراه بعنوان: جـرائم الإنترنت دراسة مقارنة لصاحبتها هـروال هبة نبيلة، والصادرة عن كلية الحقوق والعلوم السياسية بجامعة أبو بكر بلقايد بتلمسان، خلال السنة الجامعية 2013-2014، والتي درست من خلالها الباحثة مجموعة من الجرائم الإلكترونية؛ كجرائم الاعتداء على الأشخاص عبر الإنترنت (الباب الأول)، وجرائم الاعتداء على الأموال عبر الإنترنت (الباب الثاني)، وجرائم العدوان على أمن الدولة عبر الإنترنت (الباب الثالث)، مما جعل دراستها ترتكز على الجانب الموضوعي والعقابي دون الجوانب الأخرى التي تطرقنا لها في دراستنا.

ومن بين الدراسات أيضاً؛ رسالة دكتوراه للـباحث ربيعي حسـين، بعنوان: آليات البحث والتحقيق في الجرائم المعلوماتية، والصادرة عن كلية الحقوق والعلوم السياسية بجامعة باتنة (01)،

بالموسم الجامعي 2015-2016، والذي قسم دراسته إلى ثلاثة فصول؛ الفصل الأول تطرق فيه للإطار المفاهيمي للجريمة المعلوماتية، والذي ذكر فيه مجموعة من أنواع الجرائم الإلكترونية، وخصص الفصل الثاني لمسألة شرعية إجراءات البحث والتحقيق في الجرائم المعلوماتية من وجهة نظر مجموعة من المذاهب الفقهية، كما تطرق إلى الجهات المختصة بتنفيذ إجراءات البحث والتحقيق، أما الفصل الثالث من دراسته فجاء بعنوان: الإجراءات الخاصة بالبحث والتحقيق في الجرائم المعلوماتية وآثارها، وبذلك يكون الاختلاف الموجود بين دراستنا ودراسة الباحث أن دراسته يغلب عليها الطابع الفقهي، بينما دراستنا يغلب عليها الطابع القانوني.

وعليه فإنه باتباعي لتلك المناهج وذلك الأسلوب في المعالجة أكون قد عالجت موضوع الآليات القانونية لمكافحة الجريمة الإلكترونية من زاوية مختلفة عما ورد في بعض الدراسات السابقة، خاصة وأنه أسعفني الحـــظ أن أتناول بـعضاً من الأحكام القانونية التي وردت في القانون المصري الجديد الخـاص بالجريمـــة الإلكترونية الصادر سنة 2018، وكذا بعضاً من الأحكام القضائية التي عالجت نقاط مهمة من نقاط البحث، والتي جعلت هذه الدراسة تختلف عما ورد في بعضٍ من رسائل الدكتوراه للباحثين الآخرين، على الرغم من أن موضوع الجريمة الإلكترونية قد شغـل بال الكثير من الباحثين الذين حاولوا البحث فيه.

ونظراً لِتَشَعُّبِ البحث وما يشتمل عليه من مسائل قانونية متعددة، انتهجت خِطة بحث متكونة من بابين؛ مسبوقين بفصل تمهيدي؛ جاء بعنوان المضامين الفكرية للجريمة الإلكترونية والمجرم الإلكتروني، تم التطرق فيه للإطار المفاهيمي للجريمة الإلكترونية والمجرم الإلكتروني. اما الباب الأول فقد خصص للآليات الإجرائية لمكافحة الجريمة الإلكترونية، اندرج تحته فصلان؛ الفصل الأول تم التطرق فيه لآليات التحقيق الجنائي التقليدية المعتمدة لمكافحة الجريمة الإلكترونية، أما الفصل الثاني فقد خصص للقواعد الإجرائية الحديثة المعتمدة للحصول على الدليل الإلكتروني. وخصص الباب الثاني للآليات المؤسساتية لمكافحة الجريمة الإلكترونية، وضم فصلين؛ تم التطرق في الأول منه للمكافحة المؤسساتية الوطنية للجريمة الإلكترونية، وفي الثاني للمكافحة المؤسساتية الدولية والإقليمية للجريمة الإلكترونية.

الفصل التمهيدي:
المضامين الفكرية للجريمة الإلكترونية والمجرم الإلكتروني

الفصل التمهيدي:

المضامين الفكرية للجريمة الإلكترونية والمجرم الإلكتروني.

مما لا شك فيه أن العالم يشهد تحولات جذرية، وبصفة مستمرة بفضل الثورة التكنولوجية خاصة في مجال المعلومات والاتصالات، التي ساهمت وبشكل كبير في إحداث تحولات كثيرة في حياة المجتمعات في مختلف المجالات، الاجتماعية، والثقافية، والعلمية، والاقتصادية، والسياسية، وبات من السهل اختراق مختلف الأنظمة المعلوماتية، بكل ما تحتويه من معلومات ومعطيات، سواء كانت عامة أو خاصة، وأصبح من الصعب؛ بل من المستحيل إحصاء عدد الجرائم الإلكترونية التي ترتكب انتهاكاً لتلك المعلومات، فسار من الضروري إيجاد آليات لمكافحة هذه الجريمة الخطيرة.

ولكن قبل البحث عن آليات مكافحة الجريمة الإلكترونية، لا بد أولاً من التطرق إلى الإطار المفهيمي للجريمة الإلكترونية، وكذا مرتكبها المجرم الإلكتروني، فمعرفة المجرم من المسائل الأساسية التي نالت اهتمام الكثيرين[1]، خاصة إذا كان المجرم الإلكتروني له من الصفات ما يجعله متميزاً عن غيره من المجرمين الآخرين، بحيث سهلت عليه هذه الصفات ارتكاب جريمته الإلكترونية بكل سلاسة وسرعة وحنكة في إخفاء آثارها في ثواني معدودة، مما يصعب عمليات البحث عنه والقبض عليه وتقفي آثاره، وعليه فإن معرفة هذه الظاهرة الإجرامية وكذا مرتكبها من الأمور المهمة التي ستمكننا من إيجاد السبل الصحيحة والمؤسسات المتخصصة في مكافحتها.

ولأجل كل ذلك فقد تم تقسيم هذا الفصل التمهيدي إلى مبحثين: خصص الأول للإطار المفاهيمي للجريمة الإلكترونية، والذي سنوضح من خلاله الأسباب والخصائص التي جعلت هذه الجريمة تختلف عن غيرها من الجرائم التقليدية، الأمر الذي يستدعي البحث عن آليات مكافحة خاصة تتلاءم مع طبيعتها المتسارعة العابرة للحدود، والتي جعلت منها جريمة تقف أمامها العديد من التشريعات عاجزة عن مجاراتها (المبحث الأول). بينما خصص الثاني للإطار المفاهيمي للمجرم الإلكتروني (المبحث الثاني).

1 نوار الطيب، إشكالية العوامل في جريمة القتل (الحلقة الأولى)، مجلة الشرطة، العدد 62، مارس 2001، ص 23.

المبحث الأول:
الإطار المفاهيمي للجريمة الإلكترونية.

تعتبر الجرائم الإلكترونية إحـدى أخطر الأوجه السلبية التي نتجت عن التقـدم السريع الذي مس جميع المجـالات العلمية والحياتية في عصرنا الحالي، هذه الجرائم التي عانت منها الدول المتقدمة قبل نظيرتها المتأخرة تكنولوجيًا وعلميًا، لذلك تنوعت أساليب ارتكاب الجريمة الإلكترونية تنوعاً كبيراً، وازداد عددها وشكلها، لاستغلالها التقنيات الحديثة المتواجدة في الحاسب الآلي وشبكات الإنترنت، حيث أدى التطور الملحوظ الذي شهدته هاته الجريمة في الآونة الأخيرة إلى صعوبة مواجهتها وتعقد أساليب مكافحتها، ولكي نستطيع إيجاد آليات مكافحة ناجعة لابد من التعرف جيداً على هذه الظاهرة الإجرامية، لذا فإنه لابد لنا من التطرق لبعض المفاهيم والمصطلحات التي تعد معرفتها بمثابة مدخل لموضوع الدراسة.

ولأجل ذلك، تم تقسيم هذا المبحث إلى مطلبين: خصص الأول لتعريف الجريمة الإلكترونية وبيان خصائصها (المطلب الأول)، بينما تم التطرق لمحل الجريمة الإلكترونية (المطلب الثاني).

المطلب الأول: تعريف الجريمة الإلكترونية وبيان خصائصها.

لم يتفق الفقه الجنائي على إيراد تسمية موحدة للجريمة الإلكترونية، فهناك من يطلق عليها تسمية الجريمة الإلكترونية[1] أو الجريمة المعلوماتية، الجريمة ذات التقنية العالية[2]، في حين يذهب آخـرون إلى تسميتها جريمة إساءة استخـدام تكنولوجيا المعلومـات والاتصال، جرائم الإنترنت[3]، الجرائم المستحدثة[4]، واستعمل آخرون[5] مصطلح جرائم الكمبيوتر. ومن جهة أخرى أطلق عليها بعضهم جرائم المساس بأنظمة المعالجة الآلية للمعطيات[6]، وهي التسمية التي أطلقها عليها المشرع الجزائري في تعديل قانون العقوبات لسنة 2004[7] حيث أضاف فصلاً ثالثاً في القسم السابع مكرر

1 دول كثيرة أفردت لها قوانين لمكافحتها، وكل منها أعطتها تسمية خاصة بها، كما هو الحال في القوانين التي سيأتي ذكرها: – قانون الجرائم الإلكترونية رقم 27 لسنة 2015 للمملكة الأردنية الهاشمية، قانون مكافحة الجرائم الإلكترونية الجديد بدولة قطر رقم 14 لسنة 2014، الصادر بتاريخ 15 سبتمبر 2014 المنشور بالجريدة الرسمية بتاريخ 02 أكتوبر 2014. **انظر**: راشد محمد الحسن السليطي، جرائم القذف والسب العلني عبر الانترنت (دراسة مقارنة)، المجلة القانونية والقضائية، مركز الدراسات القانونية والقضائية، وزارة العدل، قطر، العدد الأول، السنة التاسعة، يونيو 2015، ص 271.

2 ذياب موسى البدانية، الجرائم الإلكترونية: المفهوم والأسباب، ورقة مقدمة في الملتقى الخاص بالجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، كلية العلوم الإستراتيجية، جامعة عمان، الأيام من 02 إلى 04 سبتمبر2014، ص03؛ قصعة خديجة، جمال بن زروق، تفعيل آليات الحماية القانونية للحد من انتشار الجريمة الإلكترونية في العالم الجزائر، مجلة تاريخ العلوم والدراسات والأبحاث الايستمولوجية، جامعة زيان عاشور بالجلفة، العدد السادس، 2017، ص 247.

3 المادة العاشرة (5/10) من القانون رقم 18–04 الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، السالف الذكر.

4 عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية وأزمة الشرعية الجزائية، مجلةكلية القانون، مركز دراسات الكوفة، جامعة الكوفة، العراق، العدد السابع، 2008، ص 112؛ عبد الله جعفر كوفلي، مراقبة الاتصالات في التنظيم الدولي والداخلي، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، مصر،2017، ص.ص: 68–69.

5 القانون الدنمركي لسنة 1985 الخاص بمكافحة جرائم الحاسب الآلي والانترنت: عادل يوسف عبد النبي الشكري، نفس المرجع، ص 126؛ محمد الأمين البشري، تأهيل المحققين في جرائم الحاسب الآلي وشبكات الانترنت، الحلقة العلمية "الانترنت والإرهاب"، قسم البرامج التدريبية، كلية التدريب جامعة نايف العربية للعلوم الأمنية، بالتعاون مع جامعة عين شمس، جامعة القاهرة، أيام من 15 إلى 2008/11/19، ص.ص: 08–09.

6 منير محمد الجنبيهي، ممدوح محمد الجنبيهي، أمن المعلومات الإلكترونية، دار الفكر الجامعي، الازاريطة، الإسكندرية، مصر، 2005، ص 91.

7 الأمر رقم 66–156، المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966، ، المتضمن قانون العقوبات، المنشور بالج.ر.ج عدد 49 مؤرخة في 11 يونيو 1966، الصفحة 702، المعدل والمتمم بالقانون رقم 04–15، المتضمن تعديل قانون العقوبات لسنة 2004، المؤرخ في 10 نوفمبر 2004، الصادر في الج.ر.ج رقم: 71، ص.ص: 11 و12، والذي أضيفت بموجبه المواد من 394 مكرر إلى 394 مكرر 07.

03 والذي شمل المواد من 394 مكرر إلى 394 مكرر7، ثم في سنة 2009 سماها الجرائم المتصلة بتكنولوجيا الإعلام والاتصال[1].

ولبيان الخصائص التي تتميز بها الجريمة الإلكترونية عن غيرها من الجرائم، نتطرق بداية لتعريفها (الفرع الأول)، ثم بيان أحكام الجريمة الإلكترونية في التشريع الجـزائري والمقارن (الفرع الثاني)، وصولاً لخصائص الجريمة الإلكترونيـــة (الفرع الثالث).

الـــفرع الأول: تعريف الجريمة الإلكترونيـــة.

تعددت التعريفات التي أُطلقت على الجريمة الإلكترونية بسبب تعدد مصادرها، فكان بعضها لسياسيين، كما هو الحال بالنسبة لتعريف وزير الداخلية الفرنسي لها، والذي عرفها على أنها: "المصطلح المستخدم لوصف جميع الجرائم الجنائية التي تُرتكب عبر شبكات الكمبيوتر، ولا سيما على الإنترنت"[2].

وفي تعريف آخر لها قيل إنها: "كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازماً لارتكابه من ناحية، ولملاحقته وتحقيقه من ناحية أخـرى"[3]، اعتبر أصحاب هذا التعريف أن الفعل غير المشروع يعد جريمة الكترونية إذا توفر على قدر كبير من العلم بتكنولوجـيا الحاسبات الآلية حين ارتكابـها، وحين التحقيق فيها من جهة، وحين ملاحقة مرتكبيها من جهة أخرى، ولكن يؤخذ على هذا التعريف أنه ضيق مفهوم الجريمة الإلكترونية، إذ ربطها بتوفر العلم بتكنولوجيا الحاسبات الآلية لدى مرتكبيها، وثمة حالات يتحقق فيها النشاط الإجرامي الذي تقوم عليه الجريمة الإلكترونية، دون أن يتوفر ذلك القدر الكبير من المعرفة بتكنولوجيا الحاسبات الآلية لدى مرتكبيها، وكمثال بسيط على ذلك؛ إتلاف البيانات المخزنة داخل نظام الحاسب الآلي، هذا الفعل الذي يعتبر أحد صور الإجرام المعلوماتي المُـجَرَّم في عدة

1 القانون رقم 09 – 04، المؤرّخ في 14 شعبان عام 1430، الموافق 5 غشت سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المنشور بالج.ر.ج العدد 47 بتاريخ 16 غشت سنة 2009، ص 05.

2 Anmonka Jeanine-Armelle TANO-BIAN, *La répression de la cybercriminalite dans les etats de L'UNION européenne et de l'Afrique de l'ouest*, Thèse pour le Doctorat en Droit Public de l'Université de Paris Descartes, Jeudi 28 mai 2015, p 49 : « le terme employé pour désigner l'ensemble des infractions pénales qui sont commises via les réseaux informatiques, notamment, sur le réseau Internet . »

3 نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية دراسة نظرية وتطبيقية، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2005، ص.ص: 28-29.

تشريعات، يمكن أن يقوم به أي شخص ذي خبرة بسيطة بالحاسب الآلي، من خلال تحميل برامج تساعده في ذلك كالفيروسات التي تتلف البيانات الموجودة في الحاسب الآلي.

كما عرفها الأستاذان "روبرت ج.ليندكويست" (Robert J.Lindquist) و"جاك بولوقنا" (Jack Bologna) بأنها: "جريمة يستخدم فيها الحاسب كوسيلة أو أداة لارتكابها أو يمثل إغراء بذلك أو جريمة يكون الكمبيوتر نفسه ضحيتها"[1]، كما يرى جانب آخر من الفقه تعريف الجريمة الإلكترونية من زاوية فنية، وأخـرى قانونية، فالتعريف الفني يميل إلى القول بأن الجريمة الإلكترونية أو جريمة الحاسب الآلي هي "نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود"[2]. وإنها:"مجموعة من الجرائم ضد الممتلكات أو الأشخاص التي ارتكبت خلال استخدام التكنولوجيات الجديدة"[3]. ومن بين التعريفات التي لقيت استحساناً، تعريف خبراء منظمة التعاون الاقتصادي والتنمية OECD للجريمة الإلكترونية، والذين اعتبروا بأنها: "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها"[4].

إن المتمعن في التعريفات السابقة يرى بأنها قد وسعـت من مفهوم الجريمة الإلكترونية[5]، بحيث اعتبرت أن مجرد استعمال الكمبيوتر في الفعل المجرم يصبغ عليه تكييف الجريمة الإلكترونية، ولكن الواقع ليس كذلك، حيث أن هنالك جرائم رغم استعمال جهاز الكمبيوتر، إلا أنها تبقى جرائم عادية، وكمثال على ذلك تزوير النقود باستعمال الحاسب الآلي.

---

1 أيمن عبد الله فكري حسن، الجرائم المعلوماتية دراسة مقارنة في التشريعات العربية والأجنبية، الطبعة الأولى، مكتبة القانون والاقتصاد، الرياض، السعودية، 2014، ص 88؛ محمد على قطب، الجرائـم المعلوماتية وطـرق مواجهتها، مركز الإعـلام الأمني، الأكاديمية الملكية للشرطة، بدون بلد نشر، بدون سنة نشر، ص.ص: 9-10، المقال منشور على الموقع الإلكتروني الموالي: *http://www.policemc.gov.bh/mcms-store/pdf/* ، والذي تم تصفحه في: 2016/05/15.

2 عبد الفتاح حجازي، الإثبات الجـنائي في جـرائم الكمـبيوتر والانترنت، دار الكتب القانونية، القاهرة،2007، ص 13؛ محمد الأمين البشري، بحث بعنوان "التحقيق في جرائم الحاسب الآلي" مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، المنعقد الفترة من 01-03 مايو 2000 بكلية الشريعة والقانون، دولة الإمارات، ص 06.

3 Vincent Lemoine Chef du Groupe Cybercriminalité de la B.R Nanterre Expert non inscrit, *La CyberCriminalité (Les acteurs les infractions Cas concret et retour d'expérience)*, *http://www .andsi.fr/wp- content/uploads /2010/01/29 dapresention_andsi_091208.pdf: p 3.*

4 شرف الدين وردة، مشروعية أساليب التحري الخاصة المتبعة في مكافحة الجريمة المعلوماتية- في التشريع الجزائري-، مجلة المفكر، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، العدد الخـامس عشر (15)، جـوان 2017، ص 540.

5 عادل يحيي، السياسة الجنائية في مواجهة الجريمة المعلوماتية، الطبعـة الأولى، دار النهضة العربية، القاهرة، مصر، 2014، ص 45.

الفرع الثانـــي: الجريمة الإلكترونية في التشريع الجـزائري والمقارن.

المشرع الجزائري كغيره من التشريعات المقارنة لم يُعْطِ تعريفًا معينًا للجريمة الإلكترونية، بل لم يستعمل مصطلح الجريمة الإلكترونية أو المعلوماتية أو السيبرانية في القوانين التي تم سنها في هذا المجال، إذ كانت الجرائم الإلكترونية قبل تعديل قانون العقوبات الجزائري سنة 2004 تصنف ضمن جرائم النظام العام كالسرقة، وخيانة الأمانة، والاختلاس وغيرها من الجرائم، فالجرائم الإلكترونية رغم خصوصيتها واختلافها عن الجرائم التقليدية، إلا أنها كانت في غياب النص تلبس ثوب العقوبات المقررة لنظيرتها التقليدية[1].

وهو ذاته الأمر الذي حدث في المملكة المغربية قبل صدور القانون رقم: 03-07[2] القاضي بتتميم مجموعة القانون الجنائي فيما يتعلق بالجرائم المتعلقة بنظم المعالجة الآلية للمعطيات، فقبل صدور هذا القانون كان هناك تضارب قضائي على مستوى محاكم الدار البيضاء قبل توحيدها فيما يخص سرقة المعطيات المعلوماتية بين اتجاهين؛ الأول يُسندها لمقتضيات الفصل (505) من ق.ع.م المتعلق بالسرقة، والاتجاه الثاني يطبق عليها مقتضيات الفصل (521) من نفس القانون والمتعلق باختلاس قوى كهربائية[3]، وهو ما يبين الدور البارز الذي كان يلعبه القضاة في معالجة الجريمة الإلكترونية وفي تطوير القانون بصورة عامة قبل تدخل المشرع[4].

وفي سنة 2004 أطلق عليها المشرع الجزائري تسمية جرائم المساس بأنظمة المعالجة الآلية للمعطيات[5]، وذلك بمقتضى القانون رقم 04-15 المعدل والمتمم لقانون العقوبات[1]، وهي ذات

1 نشناش منية، الركن المفترض في الجريمة المعلوماتية، ورقة بحثية قدمت في الملتقى الوطني المتعلق بالجريمة المعلوماتية بين الوقاية والمكافحة، المنظم من قبل قسم الحقوق ومخبر الحقوق والحريات في الأنظمة المقارنة، بكلية الحقوق والعلوم السياسية، بجامعة بسكرة يومي 16-17 نوفمبر 2015، ص 12.

2 القـانون رقم: 03-07، القاضي بتتميم مجموعة القانون الجنائي في ما يتعلـق بالجرائم المتعلقة بنظم المعالجة الآلية للمعطيـات، الصادر بتنفيذ الظهير الشريف رقم 1.03.197 بتاريخ 16 رمضان 1424 الموافق 11 نوفمبر 2003، بالج.ر عدد 5171 بتاريخ 27 شوال 1424 الموافق 22 ديسمبر 2003، ص 4284.

3 هشام ملاطي، خصوصية القواعد الإجرائية للجريمة المعلوماتية – محاولة لمقاربة مدى ملائمة القانون الوطني مع المعايير الدولية-، مطبعة الأمنية بالرباط، المغرب، 2014، ص 76.

4 عبد الكريم غالي، الجريمة الإلكترونية في حقل الائتمان بين مواقف القضاء ومستجدات التشريع، تأثير الجريمة الإلكترونية على الائتمان المالي، سلسلة ندوات محكمة الاستئناف بالرباط، المغرب، العدد السابع، 2014، ص 104.

5 **لأكثر تفاصيل يمكن الاطلاع على:** أمحمدي بوزينة أمينة، الحماية الجنائية للمعطيات الإلكترونية في إطار القانون الجزائري (دراسة تحليلية لقانوني العقوبات وحقوق المؤلف)، مجلة القانون والمجتمع، دورية محكمة في الدراسات القانونية تصدر عن مخبر القانون والمجتمع،

التسمية كما رأينا في القانـون المغربي من خـــلال القانون 03-07، أما في سنة 2009 عاد المشرع الجزائري وسماها "الجرائم المتصلة بتكنولوجيات الإعلام والاتصال" بموجب القانون رقم: 09-04[2] المتضمن القواعد الخاصة للوقايـة من الجرائم المتصلة بتكنولوجيات الإعـلام والاتصال ومكافحتها، إذ جاء في نص المادة الثانية (02)، فقرة "أ" منه أن: "الجرائم المتصلة بتكنولوجيا الإعلام والاتصال: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية".

من خلال التعريف السابق يتبـين أن المشرع الجزائري قد وسع من تعريف الجريمة الإلكترونيـة، خاصة حين اعتبر بأنها أية جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية، ونحن نرى أنه قد أحسن ما فعل، لكي تدخل في دائرة التجريم أنواع جديدة أخرى من الجرائم الإلكترونية، والتي قد تُكتشف مستقبلاً.

أما عن التشريعات العربية الأخرى فنجد أن بعضها أعطى تعريفاً للجريمة الإلكترونية، كما فعل كلاً من المشرع الكويتي، والمشرع السعودي، فالأول عرفها في المادة الأولى (1) من قانون مكافحة جرائم تقنية المعلومات رقم: 63 لسنة 2015، كما يلي: "في تطبيق أحكام هذا القانون يقصد بالمصطلحات التالية، المعنى الموضح قرين لكل منها: ... الجريمة المعلوماتية: كل فعل يرتكب من خلال استخدام الحاسب الآلي أو الشبكة المعلوماتية أو غير ذلك من وسائل تقنية المعلومات بالمخالفة لأحكام هذا القانون"[3]. أما نظام مكافحة الجرائم المعلوماتية السعودي[4] فقد عرفها في

العدد السادس، جامعة أدرار، الجزائر، ديسمبر2015، ص.ص: 95- 132؛ نور الدين بن سولة، الجريمة الإلكترونية في ضوء التشريع الجزائري، مجلة الحوار المتوسطي، جامعة الجيلالي ليابس سيدي بلعباس، المجلد التاسع، العدد الأول، الجزائر، مارس 2018، ص 274.

1 الأمر رقم 66-156، المتضمن قانون العقوبات المعدل والمتمم، السالف الذكر.

2 القانون رقم 09 – 04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المشار إليه سابقاً.

3 قانون مكافحة جرائم تقنية المعلومات الكويتي رقم: 63 لسنة 2015، الصادر يوم الأحد 12 يوليو 2015، العدد 1244.

4 أقر نظام مكافحة الجرائم المعلوماتية السعودي مجلس الوزراء في جلسته الأسبوعية يوم الاثنين 1428/03/07هـ الموافق 2007/03/26، وصدر بموجب المرسوم الملكي رقم (م/17) بتاريخ 1428/3/8هـ، القانون موجود على الموقع الإلكتروني للجريدة الرسمية للمملكة العربية السعودية: *https://www.uqn.gov.sa/channels/royal_decrees*، تم الاطلاع: 2019/12/16.

الفقرة الثامنة من المادة الأولى (8/1) بأنها: "أي فعل يرتكب متضمناً استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام".

ويمكننا القول إن المشرعين الكويتي والسعودي تقدما على التشريعات العربية الأخرى عندما عرفا الجريمة الإلكترونية؛ ذلك أن تعريفها يعد نقطة ارتكاز مهمة للتشريع محل البحث لما للجريمة الإلكترونية من أهمية، كونها من الجرائم المستحدثة في العصر الحالي والتي تتطلب بيان مفهومها وتعريفها في صلب النصوص[1].

كما يتفق الكثير من الدارسين لهذه الظاهرة الإجرامية على أن تحديد مفهوم للجريمة الإلكترونية مسألة يكتنفها الغموض، إذ يعد تعدد المصطلحات والمفاهيم في اللغة العربية، وكذا في اللغات الأجنبية[2] من الأمور التي ساهمت في ذلك، لأن وضع تعريف لها مسألة بالغة الأهمية والصعوبة؛ لأنها ترسم حدود أي قانون أو معاهدة دولية، وينبغي عند صياغة تعريف لهذه الجريمة القيام بذلك بعناية كبيرة وإلا كانت النتيجة مجالاً واسعاً يحكم موضوعات غير واقعية، أو مجالاً ضيقاً لا يغطي جميع المسائل المطلوبة[3].

وبناءً على ما ذكر أعلاه يتضح لنا أن الجريمة الإلكترونية لم تحظ بتعريف شامل أو متفق عليه[4]، إذ أن وضع تعريف محدد لها أمر ليس باليسير، لذلك ذهب بعضهم إلى القول بضرورة مراعاة عدة اعتبارات مهمة عند وضع تعريف لها منها:

1 لورنس سعيد الحوامدة، الجريمة المعلوماتية أركانها وآلية مكافحتها"دراسة تحليلية مقارنة "، مجلة الميزان للدراسات الإسلامية والقانونية، جامعة العلوم الإسلامية العالمية، المملكة العربية السعودية، 2016-2017، ص 09.

2 سالم بن محمد السالم، السرقات العلمية في البيئة الإلكترونية: دراسة للتحديات والتشريعات المعنية بحماية حقوق التأليف، المؤتمر السادس لجمعية المكتبات والمعلومات السعودية، البيئة المعلوماتية الآمنة: المفاهيم والتشريعات والتطبيقات، المنعقد بالرياض، السعودية، خلال الفترة من 06 إلى 07 ابريل، 2010، ص 16.

3 السيد إيهاب ماهر السنباطي، الجرائم الإلكترونية (الجرائم السيبيرية): قضية جديدة أم فئة مختلفة؟ التناغم القانوني هو السبيل الوحيد!، مداخلة في أعمال الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر في إطار برنامج تعزيز حكم القانون في بعض الدول العربية "مشروع تحديث النيابات العامة"، المقام بالدار البيضاء، المملكة المغربية، يومي 19 و20 يونيو 2008، ص 19.

4 معاشي سميرة، الجريمة المعلوماتية (دراسة تحليلية لمفهوم الجريمة المعلوماتية)، مجلة المفكر، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر ببسكرة، الجزائر، العدد سبعة عشر (17)، جوان 2018، ص 414؛ أمين اعزان، مواجهة الجريمة الإلكترونية في ضوء القانون الجنائي المغربي، مجلة الحقوق المغربية، كلية العلوم القانونية والاقتصادية والاجتماعية، جامعة محمد الأول بوجدة، العدد الثاني عشر (12)، السنة السادسة (06)، المغرب، 2011.؛ بدرة عمارة، الحماية الجنائية للمعلومات الإلكترونية دراسة في القانون (04-15)، مجلة البحوث القانونية والسياسية،كلية الحقوق والعلوم السياسية، جامعة الدكتور الطاهر مولاي، سعيدة، الجزائر،

- أن يكون التعريف مقبولاً ومفهوماً على المستوى العالمي.
- أن يراعي التطور السريع والمتلاحق في تكنولوجيا المعلومات.
- أن يحدد ذلك التعريف الدور الذي يقوم به جهاز الحاسب الآلي في إتمام النشاط الإجرامي.
- أن يفرق التعريف بين الجريمة العادية والجريمة الإلكترونية، وذلك عن طريق إيضاح الخصائص المميزة للجريمة الإلكترونية[1].

الفرع الثالث: خصائص الجريمة الإلكترونيـــة.

لما كانت الجريمـة ظاهـرة اجتماعية؛ فإن مؤدى ذلك أن تكون أنمـاط ارتكابها وخصائصها في تغير مستمر، وتعتبر الجريمة الإلكترونية ثمرة هذا التغير والتطور في أنماط الجريمة، وهو ما أدى إلى تميزها بعدة خصائص عن غيرها من الجرائم[2]، ومن بين هذه الخصائص ما يلي:

أولاً– خفاء الجريمة وسرعة ارتكابها: من خصائصها أنها ممكنة الوقوع في أثناء المعالجة الآلية للبيانات والمعطيات الخاصة بالحاسوب[3]؛ ذلك أن الضحية لا تُلاحظها رغم أنها قد تقع في أثناء تواجده على الشبكة؛ كون الجاني يتمتع بقدرات فنية عالية في أغلب الأحيان تمكنه من تنفيذ جريمته بدقة، ومن أمثلة ذلك؛ إرسال الفيروسات[4] المدمرة وسرقة الأموال إلكترونياً، والأمثلة عليها

العدد الثاني، 2014، ص 454: "فإنه لا يـوجد لحد ألان إجـماع فقـهي على تعريف موحد لها مما أدى إلى القول بان الجريمة المعلوماتية تقاوم التعريف".

1 خالد ممدوح إبراهيم، الجرائم المعلوماتية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، 2009، ص 75.

2 جلال محمد الزغبي، أسامة احمد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية دراسة مقارنة، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2010، ص 91.

3 حازم محمد حنفي، الدليل الإلكتروني ودوره في المجال الجنائي، الطبع الأولى، دار النهضة العربية، القاهرة، مصر، 2017، ص 33؛ خالد حربي السعدي، جريمة إتلاف برامج ومعلومات الحاسب الآلي في التشريعيين الكويتي والمقارن، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 2012، ص 158؛ هروال هبة نبيلة، جرائم الانترنت دراسة مقارنة، أطروحة مقدمة لنيل شهادة الدكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، الجزائر، السنة الجامعية 2013-2014، ص 42.

4 استقي مصطلح الفيروس من العلوم البيولوجية، وهو يعني باللاتينية "سم"، وقد أصابت الفيروسات الحاسب الآلي قبل تسميتها بهذا الاسم. وأول من أطلق عليها هذا الاسم هو Fred cohem في عـام 1983 ويرجع الفضل إليه في إيضاح سهولة كتابة برامجها وسهولة إخفائها. وأشار إلى قدرتها الانتشارية السريعة في شبكات الاتصال. وبعد معرفة هذه الحقيقة أمكن وضع البرامج التي تكشف وجود الفيروس والقضاء عليه؛ ذلك لأن الفيروس المعلوماتي هو برنامج للحاسب الآلي مثل أي برنامج آخر، ولكنه يهدف إلى إحداث أكبر ضرر بنظام الحاسب وله قدرة على ربط نفسه بالبرامج الأخرى، وكذلك أعادة إنشاء نفسـه حتى يبـدو كأنه يتكاثـر، ويتـوالد ذاتياً، ويقـوم الفيرس بالانتـشار بين برامج الحاسب الآلي المختلفة، وبين مـواقع مختـلفة في الذاكرة. **ينظر في ذلك:** محمد على العـريان، الجـرائم المعلوماتيـة، دار الجامعة الجديدة للنشر، الازاريطة، الإسكندرية، 2004، ص 83؛ عبد الفتاح بيومي

كثيرة، ومنها؛ ما قام به "فلاديمير لوفين" –روسي الجنسية– في شهر أوت سنة 1994، حيث قام بتحويل مبالغ مالية من مصرف "سيتي بانك" في نيويورك، بعد أن اقتحم أنظمة المصرف الأمريكي المعلوماتية 18 مرة، إذ تمكن من فك شفرة حسابات كثير من عملاء البنك وسطا عليها[1]. كما أنه في كثير من الأحيان يكون الهدف من وراء الجريمة الإلكترونية الإطلاع على البيانات الخاصة أو إتلافها، والتجسس وسرقة المكالمات على سبيل المثال[2].

ثانياً– اعتبارها أقل عنفاً في التنفيذ: تتسم هذه الجريمة بأنها أقل عنفاً من الجرائم التقليدية الأخرى كالسرقة والقتل التي تحتاج إلى جهد عضلي، فركنها المادي قد لا يتجاوز مجرد لمسة بسيطة لمفاتيح التشغيل الخاصة بجهاز الحاسب الآلي أو ملحقاته[3].

ثالثاً– جريمة عابرة للحدود: أو كما يسميها بعضهم الجريمة العابرة للقارات أو الجريمة العالمية، ولا جدال أن الجرائم الإلكترونية أضحت من أخطر وأعقد الجرائم باعتبارها عابرة

حجازي، النظام القانوني للحكومة الإلكترونية، الكتاب الثاني الحماية الجنائية والمعلوماتية للحكومة الإلكترونية، دار الكتب القانونية، مصر، 2007، ص 67، **نقلاً عن:** عبادة أحمد عبادة، التدمير المتعمد لأنظمة المعلومات الإلكترونية، بحث منشور لدى مركز البحوث والدراسات، الإدارة العامة لشرطة دبي، مارس، 1999، ص 01؛ طه عيساني، القرصنة الإلكترونية؛ الضرر الاقتصادي والفكري، مركز جيل البحث العلمي، مجلة جيل الأبحاث القانونية المعمقة، العدد الخامس (05)، يوليو 2016، ص 109؛ عبد الحكيم زروق، تنظيم التبادل الإلكتروني للمعطيات القانونية عبر الانترنت، الطبعة الأولى، دار الامان، الرباط، المغرب، 2016، ص ص: 380-390.

1 مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، مطابع الشرطة، القاهرة، 2008، ص.ص: 154-156.

2 خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص84؛ صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجستير في القانون تخصص القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2013/03/06، ص.ص: 14-15، **نقلاً عن:** محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت، دار النهضة العربية، القاهرة، بدون سنة النشر، ص 32.

3 دليلة العوفي، إشكالية مواكبة الجزائر لمجتمع المعلومات من الفجوة الرقمية إلى الجريمة المعلوماتية، مجلة الحكمة للدراسات الإعلامية والاتصالية، تصدر عن مؤسسة كنوز الحكمة للنشر والتوزيع، المجلد 04، العدد 08، الجزائر، 2016، ص 160؛ محمد علي سالم، حسون عبيد هجيج، الجريمة المعلوماتية، مجلة جامعة بابل، كلية العلوم الإنسانية، جامعة بابل، العراق، المجلد 14، العدد 06، 2007، ص 92؛ ثنيان ناصر آل ثنيان، إثبات الجريمة الإلكترونية، دراسة تأصيلية، رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير، تخصص السياسة الجنائية، قسم العدالة الجنائية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، 2012، ص 22؛ محروس نصار غايب، الجريمة المعلوماتية، المعهد التقني، الانبار، العراق، 2011/03/05، ص من 5 -7.

للحدود[1]، حيث تستخدم فيها أحدث التقنيات وتتميز بانتشار مرتكبيها في أغلب الأحيان عبر دول مختلفة، بحيث فقدت معها الحدود الجغرافيـة كل أثر في الفضاء الشبكي المتشعب العلاقـات، وأصبحنا بالتالي أمام جرائم عابرة للحدود[2] تتم في فضاء إلكتروني معقد عبارة عن شبكة اتصال لا متناهية غير مجسدة وغير مرئية متاحة لأي شخص حول العالم، وغير تابعة لأي سلطة حكومية، يتجاوز فيها السلوك المرتكب معناه التقليدي، له وجود حقيقي وواقعي لكنه غير محدد المكان[3]. هذه الخاصية ستؤدي في وقت قصير إلى تصنيف الجريمة الإلكترونية من جريمة عالمية عابرة للحدود إلى جريمة دولية؛ لأنها تحمل في طياتها كل المواصفات التي قد تساعدها على ذلك، فليس مستبعد أن يقوم أحد الهاكرز بالدخول واختراق نظام الكتروني لقاعدة عسكرية نووية؛ ليقوم بعد ذلك بإطلاق رؤوس نووية يدمر بها دولة أو دول بأكملها، لذا وجب تصنيف هذه الجريمة الخطيرة في مصف الجرائم الدولية لتتكاثف الجهود من أجل محاربتها.

---

1 ولكن قبل التطرق إلى تفاصيل هذه الخاصية وجب التفرقة بين الجريمة الدولية والجريمة العالمية؛ فالجريمة الدولية هي تلك الجريمة التي ترتكبها الدولة أو الأفراد بصفاتهم الرسمية انتهاكا لقواعد القانون الدولي، إذ غالباً ما ترتكب ممزوجة بالدافع السياسي وبغية تحقيق أهداف سلطوية، حيث تشكل في ذاتها اعتداءً على حقوق الإنسان وحرياته الأساسية، وهي الحقوق والحريات التي ضمنها القانون الدولي واتفاقيات حقوق الإنسان، إذن فهي جريمة تقع ضد النظام العام العالمي، أما الجريمة العالمية فهي تلك الجريمة التي يمتد الضرر فيها لأكثر من دولة، وبذلك تظل الجريمة العالمية جريمة داخلية، وهي جرائم أفراد لا جرائم دول، فمصدرها القانون الجنائي الوطني، أو كما يسمى Droit pénal universel، لأنها لا تشكل مساسا بالنظام الدولي المشمول بالحماية الجنائية الدولية، فبالرغم من تعدد الجناة واختلاف جنسيتهم أو اختلاف جنسيات المعتدى عليهم فذلك لا يؤدي بالضـرورة إلى تصنيف الجرائـم العالمية ضمن الجرائم الـدولية، **لأكثر تفاصيل يمكن الاطلاع على:** عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي الجزائري والقانون المقارن، دار الجامعة الجديدة، الازاريطة، الإسكندرية، مصر، 2010، ص 44؛ محمد الصالح روان، الجريمة الدولية في القانون الدولي الجنائي، رسالة مقدمة لنيل شهادة الدكتوراه في العلوم، كلية الحقوق، جامعة منتوري، قسنطينة، الجزائر، السنة الجامعية 2008-2009، ص 82؛ فريجه محمد هاشم، دور القضاء الدولي الجنائي في مكافحة الجريمة الدولية، أطروحة مقدمة لنيل شهادة الدكتوراه علوم في الحقوق تخصص قانون دولي جنائي، قسم الحقوق،كلية الحقوق والعلوم السياسية، جامعة محمد خيضر ببسكرة، الجزائر، السنة الجامعية 2013-2014، ص ص: 33-34.

2 نعيم مغبغب، حماية برامج الكمبيوتر"الأساليب والثغرات دراسة في القانون المقارن"، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2006، ص 218؛ جلال محمد الزغبي، أسامة احمد المناعسة، المرجع السابق، ص 93؛ حكيم سياب، السمات المميزة للجرائم المعلوماتية عن الجرائم التقليدية، مجلة دراسات وأبحاث، جامعة زيان عاشور، الجلفة، الجزائر، العدد الأول، تاريخ النشر: 2009/09/15، ص 220؛ بردال سمير، الجريمة المعلوماتية في التشـريع الجزائري، مجلة القانون، معهد العلوم القانونية والإدارية بالمركز الجامعي أحمد زبانة، غليزان، الجزائر، العدد الثاني (02)، 2010، ص 182.

3 سومية عكور، الجرائم المعلوماتية وطرق مواجهتها: قراءة في المشهد القانوني والأمني، ورقة عـلمية مقدمة في الملتقى العـلمي حـول الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، كلية العلوم الإستراتيجية، عمان، الأردن، خلال الفترة من 02 إلى 04 سبتمبر 2014، ص 01.

رابعاً– امتناع المجني عليهم عن التبليغ: تتصف الجريمة الإلكترونية بالتكتم وعدم الإعلان أو الإبلاغ عنها ممن وقع ضحيتها، وعدم الكشف عنها يتأتى من خوف الضحية إما من الفضيحة كما هو الحال في الجرائم الإلكترونية التي تمس خصوصية الأفراد، أو إحجام الأشخاص عن التعامل مع الضحية إذا ما علموا بالهجوم الإلكتروني الواقع عليها، مثلما هو الحال في حالة المصارف، إذ قد يحجم الزبائن عن التعامل معها حينها خوفاً على مصالحهم[1].

كما أن خوف الشركات التجارية من أن تؤدي أعمال التحقيق التي تقوم بها الشرطة إلى احتجاز حواسيبها أو تعطيل شبكاتها لفترة طويلة، مما قد يتسبب في زيادة خسائرها المالية جراء التحقيق عطفاً على ما قد تسببت الجريمة في خسارته أصلاً، والواقع أن إجراءات التحقيق الخاطئة قد تتسبب في خسائر مادية تفوق تلك التي تسببت فيها الجريمة في المقام الأول"[2].

خامساً– سرعة محو الدليل وصعوبة الوصول إليه: إن المعلومات التي يحملها الإنترنت تكون في شكل رموز مخزنة على وسائط تخزين ممغنطة ولا تقرأ إلا بواسطة الحاسب الآلي، وهو ما يجعل الدليل الكتابي أو المقروء أمراً يصعب بقاؤه أو إثباته؛ لأن الجاني مرتكب هذه الجريمة لا يترك وراءه أي أثر مادي خارجي ملموس يمكن فحصه، الأمر الذي يؤدي إلى صعوبة اكتشاف الجريمة

1 نعيم مغبغب، حماية برامج الكمبيوتر "الأساليب والثغرات دراسة في القانون المقارن"، المرجع السابق، ص 218؛ عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون "دراسة مقارنة"، دار الكتب القانونية، الإسكندرية، مصر، 2002، ص 22؛ تركي بن حمد هلال النصر، التحقيق في جريمتي التحرش والابتزاز عبر الشبكات الإلكترونية دراسة تطبيقية على هيئة التحقيق والادعاء العام بالمنطقة الشرقية، رسالة مقدمة لاستكمال متطلبات نيل درجة الماجستير في الدراسات الأمنية، تخصص القيادة الأمنية، قسم الدراسات الأمنية، كلية العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2017، ص 41؛ صغير يوسف، الجريمة المرتكبة عبر الانترنت، المرجع السابق، ص 119؛ محمد على العريان، الجرائم المعلوماتية، المرجع السابق، ص 54؛ خالد ممدوح ابراهيم، أمن الجريمة الإلكترونية، الدار الجامعية، الإسكندرية، مصر، 2008، ص 51؛ عيسى سليم داود الزيدي، جرائم القرصنة الإلكترونية دراسة مقارنة، رسالة لنيل درجة الماجستير في الحقوق، قسم القانون الجنائي، كلية الحقوق، جامعة الإسكندرية، مصر، 2017/09/19، ص 109؛ فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية، دار الجامعة الجديدة، الإسكندرية، مصر، 2016، ص 135؛ شوقي يعيش تمام، فريد علواش، العوائق التي تواجه مكافحة الجريمة الإلكترونية (دراسة مقارنة)، مجلة العلوم السياسية والقانون، المجلد الثلث (03)، العدد الثالث عشر (13)، المركز الديمقراطي العربي، المانيا، يناير 2019، ص 130.

2 تركي بن عبد الرحمن المويشير، بناء أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته، الطبعة الأولى، جامعة نايف العربية للعلوم الأمنية فهرسة مكتبة الملك فهد الوطنية أثناء النشر، الرياض، السعودية، 2012، ص 152، **نقلاً عن:**

- Cowens, B & Miora ,M, *Computer Emergency quick team*, in bosworth S.& Kabay M.(ED), computer security handbook. 2002, pp 40.1 – 40.15.

ومعرفة مرتكبها، بخلاف الجريمة التقليدية[1]. ففي الفضاء الإلكتروني يعد من الأمور الصعبة إثبات نسبة الفعل الإجرامي لشخص طبيعي، وهو الأمر الذي جاء في عدة قرارات قضائية ومنها؛ ما ذهبت إليه محكمة الاستئناف بباريس في قرارها الصادر في السابع والعشرين (27) من شهر أبريل سنة 2007، مؤكدة على أن عنوان البرتوكول (IP)[2] لا يدل إلا على تسلسل أرقام مرتبطة بآلة وليس بالشخص[3].

1 عبد المومن بن صغير، الطبيعة الخاصة للجريمة المرتكبة عبر الانترنت في التشريع الجزائري والتشريع المقارن، ورقة بحثية قدمت في الملتقى الوطني المتعلق بالجريمة المعلوماتية بين الوقاية والمكافحة، المنظم من قبل قسم الحقوق ومخبر الحقوق والحريات في الأنظمة المقارنة، بجامعة بسكرة يومي 16-17 نوفمبر2015، ص 08؛ سميرة معاشي، ماهية الجريمة المعلوماتية، مجلة المنتدى القانوني، قسم الكفاءة المهنية للمحاماة، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر، العدد السابع، افريل 2010، ص 282؛ فريجة محمد هشام، النظام القانوني للجريمة المعلوماتية وصعوبات تحقيق الأمن الإلكتروني، حوليات جامعة قالمة للعلوم الاجتماعية والإنسانية، العدد الرابع والعشرون (24)، جوان 2018، ص 148؛ محمد بن أحمد بن على المقصودي، الجرائم المعلوماتية خصائصها وكيفية مواجهتها قانونيا التكامل الدولي المطلوب لمكافحتها، ورقة بحثية مقدمة في إطار أشغال المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية ICACC، كلية علوم الحاسب والمعلومات، جامعة الإمام محمد بن سعود الإسلامية، الرياض، المملكة العربية السعودية، نوفمبر 2015، ص 27؛ نبيل صقر، جرائم الكومبيوتر والانترنت في التشريع الجزائري، دار الهلال للخدمات الإعلامية، الجزائر، 2005، ص 158؛ أيمن عبد الحفيظ، إستراتيجية مكافحة جرائم استخدام الحاسب الآلي، دار النهضة العربية، القاهرة، مصر، 2003، ص 450؛ خليلي سهام، خصوصية المجرم الإلكتروني، مجلة المفكر، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، العدد الخامس عشر (15)، جوان 2017، ص 405، **نقلاً عن**: غازي عبد الرحمان هيان الرشيد، الحماية القانونية من جرائم الانترنت، أطروحة دكتوراه، كلية الحقوق، الجامعة الإسلامية في لبنان، 2004، ص.ص: 147- 148.

2 TCP/IP وهو البروتوكول الذي يتكون من بروتوكولين هما بروتوكول التحكم بالإرسال/ وبروتوكول الانترنت Transmission control protocol/Internet protocol، حيث يقدم هذا البروتوكول حلولا في مجال الاتصال ما بين الشبكات العالمية global internetworking، هذا يعني بان أي حاسب آلي أو نظام متصل بالانترنت فإنه يستخدم TCP/IP، وظيفة بروتوكول التحكم بالإرسال هو التأكد بان حاسبين آليين يستطيعان الاتصال ببعضهما البعض بطريقة يعول عليها كل اتصال لبروتوكول التحكم بالإرسال إذ يجب أن يقابله إشعار باستلام البيانات فإذا لم يتم الحصول على هذا الإشعار بعد فترة معينة فان على الجهاز المرسل إعادة إرسال البيانات ولكي تتم عملية الإرسال أو عملية إجابة الطلب فإن الطلب المرسل يجب تقسيمه إلى أقسام صغيرة تسمى بالرزم pachets كل رزمة تحوي على عنوان الجهاز المرسل والجهاز المستقبل وهنا يتدخل بروتوكول الانترنت لينسق الرزم ويوزع العناوين. انظر في ذلك: سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهادة الماجستير في العلوم القانونية، جامعة الحاج لخضر، باتنة، الجزائر، السنة الجامعية 2012-2013، ص 135؛ منير محمد الجنبيهي، ممدوح محمد الجنبيهي، بروتوكولات وقوانين الانترنت، دار الفكر الجامعي، الازاريطة، الإسكندرية، القاهرة، 2005، ص 26:

3 عبد الحكيم الحكماوي، الإثبات في الجريمة الإلكترونية، تأثير الجريمة الإلكترونية على الائتمان المالي، سلسلة ندوات محكمة الاستئناف بالرباط، العدد السابع، 2014، ص 160:

المطلب الثانـــي: محل الجريمة الإلكترونية.

تعتبر المعلومة من ناحية كميتها ونوعيتها وكذلك سرعة تدفقها، سمة هذا العصر الغالبة، إلى الحد الذي لا يمكن معه تصور نشاط اجتماعي ناجح لا يقوم على توظيف المعلومة. فالفرق اليوم بين مختلف المجتمعات هو في استثمارها؛ فهي شجون الحاضر وغموض المستقبل خاصة في ظل الرهانات والمتغيرات الحالية التي أفرزت لنا مجتمعا الكترونياً محضاً، انتقلت تجلياته إلى مختلف مجالات الحياة، تاركةً وراءها تغييراً جذرياً في نمط الحياة، إذ أجبرت مختلف الدول بالأخذ بهذا المبدأ سعياً للتطور ولتقليص الفجوة المعرفية[1]. صاحب التقدم الكبير في مجال العلوم التقنية تقدم آخر موازي في مجال الجريمة الإلكترونية التي اتخذت من المعلومات (الفرع الأول)، الأجهزة (الفرع الثاني)، والأشخاص الطبيعية والمعنوية، و/أو الجهات الحكومية منها والخاصة محلاً لها (الفرع الثالث).

الفرع الأول: المعلومات كمحل للجريمة الإلكترونية.

المعلومات هي إحدى المفردات المشتقة من المصدر (علم) ولهذه المشتقات العديد من المعاني منها ما يتصل بالعلم أي إدراك طبيعة الأمور والمعرفة؛ أي القـدرة على التمييز والتعليم والتعلم والدراسة والإحاطـة واليقـين والإتقـان والإرشاد والتوعيـة، والإعـلام والشهـرة والتمييـز والتيسيـر، ومصطلح Information أصله لاتيني يعني عملية الاتصال[2]، وتختلف المعلومات عن البيـانات فالأخيرة هي مجموعـة من الحقائـق أو القياسـات أو المعطيـات التي تتخـذ صورة أرقـام أو حروف أو رموز أو أشكال خاصة وتعبر عن فكرة أو موضوعاً أو حديثاً أو هدفاً معيناً؛ لذا توصف بأنها المـادة الخـام التي يتم تحويلها عن طريـق الحاسوب لغرض استخراج معلومات معينـة وتسمى العلاقة بين المعلومات والبيانات بالدورة الاسترجاعية؛ إذ يتم تجميع أو تشغيل البيانات للحصول على المعلومات، والتي تستخدم في إصدار قرارات تؤدي بدورها إلى مجموعة إضافية من

1 زغنوف عبد الغني، وعظيمي أحمد، المعلومة وأهميتها في المجتمع المعلوماتي، مجلة البحوث والدراسات الإنسانية، جامعة 20 أوت، سكيكدة، الجزائر، العدد 09، ديسمبر 2014، ص 169.

2 أحمد علي، مفهوم المعلومات وإدارة المعرفة، مجلة جامعة دمشق، سوريا، المجلد 28، العدد الأول، 2012، ص 04؛ محمد علي سالم، حسون عبيد هجيج، المرجع السابق، ص 02، **نقلاً عن:** انتصار نوري الغريب، أمـن الكمبيوتـر والقانـون، دار الراتـب الجامعيـة، بيروت، 1994، ص 81؛ فائزة يونس الباشا، السياسة الجنائيـة لجرائم الكمبيوتر التشريع الليبي (أنموذجاً ومقارناً)، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 2013، ص 13.

البيانات التي يحصل تجميعها ومعالجتها مرة أخرى للحصول على معلومات إضافية يعتمد عليها في إصدار قرارات جديدة[1].

في ما مضى كان تداول المعلومات بواسطة الأرشيف والطرق العادية يتضمن معلومات خاصة، قد لا تكون لعملية الكشف عنها بالغ الأثر، لكن كشفها جميعاً في آن واحد كما هو حال في المعلومات الموجودة في الحاسب الآلي فذاك يؤدي إلى أضرار أكيدة، فلم يعد للفرد أي إمكانية للتستر أو الاختباء، أو الانعزال والتراجع كما تقرر له الدساتير والقوانين، ولم يعد باستطاعته مقاومة الغير، فحق النكران المعترف به للفرد والمصان شرعاً لم يعد له وجود[2].

إن محل الجرائم الإلكترونية في هذه الحالة هو إما سرقة أو تغيير أو حذف أو إتلاف المعلومات والتي غالباً ما تكون لها قيمة مادية ومعنوية لدى صاحبها، لذا ضاعف المشرع الجزائري العقوبة المقررة لتغيير أو حذف هذه المعلومات، وذلك من خلال الفقرتين الثانية (2) والثالثة (3) من نص المادة (394 مكرر) من القانون 04-15[3] بقولها: "...تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر (06) إلى سنتين (02) والغرامة من 50.000 دج إلى 150.000 دج"، حيث إن العقوبة المقصودة هنا ذكرتها الفقرة الأولى من نفس المادة بقولها: "يعاقب بالحبس من ثلاثة (03) أشهر إلى سنة (01) وبغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك"، كذلك فعل المشرع الفرنسي في الفقرة الثالثة (3) من المادة 323 من القانون الفرنسي[4].

1 فائزة يونس الباشا، السياسة الجنائية لجرائم الكمبيوتر التشريع الليبي (أنموذجاً ومقارناً)، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 2013، ص 13.

2 نعيم مغبغب، مخاطر المعلوماتية والانترنت (المخاطر على الحياة الخاصة وحمايتها دراسة في القانون المقارن)، الطبعة الثانية، منشورات الحلبي الحقوقية، لبنان، 2008، ص ص: 162-163.

3 القانون 04-15 المتضمن تعديل قانون العقوبات لسنة 2004، السالف الذكر.

4 Article 323-3 de la Loi n° 88-19 du 5 janvier 1988. relative à la fraude informatique (LOI GODFRAIN) : « Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifie frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 euros d'amende ».

ومن أمثلة أن تكون المعلومات محل للجريمة الإلكترونية؛ النشاط الجرمي الذي يستهدف اختراق بريد إلكتروني[1] والعبث بمحتوياته أو سرقة المعلومات المخزنة في موقع ما؛ والاستفادة منها بما يحمل في طياته بعضاً من انتهاك الخصوصية[2]؛ هذه الخصوصية التي خصصت لها حماية على عدة أصعدة، كالتي جاء بها المشرع الأمريكي حين أصدر عام 1974 قانون الخصوصية (PA) Privacy ACT، وقانون خصوصية الاتصالات الإلكترونية عام 1986 (COPA) Electronic Communication Privacy Act1[3] ومن الأمثلة أيضاً؛ الاعتداءات الإلكترونية التي تقع على حقوق

1 عرف القانون الفرنسي البريد الإلكتروني في المادة 01 من القانون المتعلق بالثقة في الاقتصاد الرقمي الصادر في 22 يونيو 2004، وكذلك فعل التشريع الأمريكي في القانون المتعلق بخصوصية الاتصالات الإلكترونية الصادر في عام 1986، والمقنن في موسوعة القوانين الفدرالية الأمريكية، بأنه وسيلة اتصال نستطيع عن طريقها إرسال إلكترونيا كل المراسلات إلى المرسل إليه عبر شبكة خطوط تليفونية عامة أو خاصة، حيث يتم كتابة الرسائل على جهاز الحاسب الآلي في الغالب ثم يتم إرسالها إلكترونيا إلى الحاسب الآلي مزود الخدمة، والذي يخزنها لديه ثم ترسل إلى الحاسب الآلي التابع للمرسل إليه. **نقلاً عن**: عبد الهادي فوزي العوضي، الجوانب القانونية للبريد الإلكتروني، دار النهضة العربية، القاهرة، مصر، 2005، ص 13 و14؛ عبد الله جعفر كوفلي، المرجع السابق، ص.ص: 67-68؛ محمد أمين الشوابكة، جرائم الحاسوب والانترنت: الجريمة المعلوماتية، الطبعة الرابعة، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2011، ص 32؛ عبد الفتاح بيومي حجازي، الجريمة في عصر العولمة "دراسة في الظاهرة الإجرامية المعلوماتية مع التطبيق على القانون الإماراتي"، دار الفكر الجامعي، الازاريطة، الإسكندرية، مصر، 2008، ص 20.

2 تعد الجرائم الإلكترونية من أكثر الجرائم الماسة بحرمة حياة الإنسان الخاصة، هذه الحرمة التي عُنيت بحماية دولية ووطنية على غرار ما جاء في تعديل الدستور الجزائري لسنة 2020، في المادة 39 منه والتي جاء فيها:" تضمن الدولة عدم انتهاك حرمة الإنسان. يحظر أي عنف بدني أو معنوي، أو أي مساس بالكرامة. ..."؛ ولقد أدان القضاء الأمريكي أحد الأشخاص بتهمة الدخول غير المشروع إلى سجلات إحدى المحاكم الاتحادية، وهي تحوي سجلات إلكترونية خاصة تضم أحكام وقرارات ومستندات خاصة بدعاوى عرضت على المحكمة، أو صدر قرار فيها، بالإضافة إلى تقارير إحصائية تتعلق بعمل هذه المحاكم، حيث إن نظام حفظ هذه المعلومات مفتوح للجمهور، إلا أن حق النسخ أو الإنزال مقيد بسداد مقابل نقدي، لكن الجاني تمكن من نسخ الملايين من الصفحات باستخدام برنامج خاص لوضع ملفات إلكترونية خفية في النظام حتى لا يتم احتساب نفقات النسخ". **انظر**: براهمي حنان، جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية، أطروحة مقدمة لنيل شهادة دكتوراه علوم تخصص قانون جنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر، السنة الجامعية 2014-2015، ص48، **نقلاً عن**: أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني، دار النهضة العربية، الطبعة الاولى، القاهرة، 2006، ص 145؛ محمد أمين أحمد الشوابكة، جرائم الحاسوب والانترنت: الجريمة المعلوماتية، المرجع السابق، ص18؛ دنيا عبد العزيز فهمي، الحماية الجنائية من إساءة استخدام مواقع التواصل الاجتماعي "دراسة مقارنة"، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 2018، ص 115 وما بعدها.

3 محمد حماد مرهج الهيتي، التكنولوجيا الحديثة والقانون الجنائي، الطبعة الأولى، الإصدار الأول، دار الثقافة للنشر والتوزيع، الأردن، 2004، ص 184؛ عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنت (الجرائم الإلكترونية دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والانترنت مع الإشارة إلى جهود مكافحتها محليا وعربياً ودولياً)، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2007، ص 18.

الملكية الفكريـة[1]؛ لأن المصنف الرقمي هو أحد مفرزات التكنولوجيا الحديثة التي تحفظ وتسترجع بواسطة الحاسب الآلي من خلال تحويل كلماته المدخلة باللغة الطبيعية إلى لغة تفهمها الآلة وهي اللغة الثنائية (0.1).

ومن أهم النتائج التي ترتبت على كون برامج الحاسب الآلي ذات طبيعة ذهنية هي أن تلك البرامج ترتبط بشخصية صاحبها لأنها فكرته ونتاجه الذهني ولمسة من ابتكاره، لذلك قيل بأنها من الحقوق الذهنية والشخصية اللصيقة بالإنسان، فبمجرد أن تنتقل من كونها فكرة إلى كونها معلومة ضمن مكونـات برنامج معين تصبح بذلك قابلة للاستعمال، تصنف حينها من الحقـوق الذهنيـة؛ والتي تدخل هي الأخرى في إطار الحقوق المالية الشخصية[2].

فحقوق الملكية الفكرية كانت ولا زالت تحظى باهتمام عديد التشريعات، فالمبادرة الأولى للمشرع الجزائري في هذا الخصوص كانت سنة 1973 بموجب الأمر رقم 73-14 المتعلق بحق المؤلف[3] والذي أُلغي بموجب الأمر رقم 97-10 والمتعلق بحقوق المؤلف والحقوق المجاورة[4]، حيث أنه ولأول مرة يعتبر أن برامج الحاسب الآلي تعد من قبيل المصنفات المحمية قانوناً، إضافة إلى إدراج الحقوق المجاورة لحق المؤلف ومنحها الحماية القانونية، والذي أُلغي بدوره بالأمر رقم 03-05[5] الساري المفعول، حيث حاول المشرع الجزائري من خلال ما قام به من تعديلات مواكبة التطورات تماشياً والمعايير الدولية ولاسيما ما جاءت به اتفاقية برن، والتي انضمت إليها الجزائر سنة 1997[6].

---

1 هلالي عبد اللاه احمد، كيفية المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء اتفاقية بودابست، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 2011، ص 119؛ أحمد خليفة الملط، الجرائم المعلوماتية دراسة مقارنة، الطبعة الثانية، دار الفكر الجامعي، الازاريطة، الإسكندرية، مصر، 2006، ص 185؛ عبد الرحمان جميل حسين، الحماية القانونية لبرامج الحاسب الآلي"دراسة مقارنة"، قدمت هذه الأطروحة استكمالاً لمتطلبات درجة الماجستير في القانون الخاص بكلية الدراسات العليا، جامعة النجاح الوطنية في نابلس، فلسطين، 2008، ص 63.

2 خالد مصطفى فهمي، الحماية القانونية لبرامج الحاسب الآلي في ضوء قانون الملكية الفكرية المصري 82 لسنة 2002 (دراسة مقارنة)، دار الجامعة الجديدة، الازاريطة، الإسكندرية، مصر، 2005، ص ص 70-71.

3 الأمر رقم 73-14، المؤرخ في 03 أبريل 1973، المتعلق بحق المؤلف، الصادر في الج.ر عدد 29، مؤرخة في 10 أبريل 1973، ص 434.

4 الأمر رقم 97-10، المؤرخ في 06 مارس 1997، والمتعلق بحقوق المؤلف والحقوق المجاورة، الصـادر في الج.ر عدد 13، المؤرخة في 12 مارس 1997، ص 3.

5 الأمر رقم 03-05، المؤرخ في 19 يوليو 2003، والمتعلق بحقوق المـؤلف والحقـوق المجاورة، المنشور في الج.ر عدد 44، المؤرخة في 23 يوليو 2003، ص 3.

6 سلامي اسعيداني، التشريعات القانونية الدولية لحماية حقوق الملكية الفكرية الافتراضية رؤية نقدية من منظور إعلامي قانوني، الملتقى الدولي حول التعليم في عصر التكنولوجيا الرقمية، طرابلس، لبنان، من 22 إلى 24 أفريل 2015، ص 04؛ بن دريس حليمة، حماية

إلا أن المشرع الجزائري لم يوفر للمصنفات الإلكترونية؛ خاصة المصنفات الموجودة على الإنترنت الحماية الكافية من التعرض للجرائم الإلكترونية، وبالأخص التحميل غير الشرعي لها، بخلاف التشريع الفرنسي الذي شمل جميع المصنفات الإلكترونية والرقمية بالحماية الجزائية، إذ عاقب على مثل تلك السلوكات في قانون مستقل من خلال مواد وردت بقانون الملكية الفكرية الصادر سنة 1957، أين أدرجت فيه نصوص عقابية خاصة من خلال قانون *I-HADOPI*، *2- HADOPI*.[1]

أما المشرع المصري فقد خص هذه الحقوق بالحماية[2] من خلال القانون الخاص بالملكية الفكرية المصري رقم 82 لسنة 2002[3]، وبتطبيقات قضائية؛ والتي من بينها ما جاء في حكم محكمة النقض في جلسة يوم الثلاثاء الفاتح من سبتمبر سنة 2015: "لما كان ذلك، وكان قانون حماية حقوق الملكية الفكرية الصادر به القانون رقم 82 لسنة 2002 قد نص في المادة 181 منه على عقاب كل من ارتكب أحد الأفعال الآتية: "أولاً- بيع أو تأجير مصنف أو تسجيل صوتي أو برنامج إذاعي محمي طبقاً لإحكام هذا القانون أو طرحه للتداول بأية صورة من الصور بدون إذن كتابي مسبق من المؤلف أو من صاحب الحق المجاور،...، سابعاً- الاعتداء على أي حق أدبي أو مالي من حقوق المؤلف أو من الحقوق المجاورة المنصوص عليها في هذا القانون وكان البين من نص المادة 147 من القانون المذكور أن من بين حقوق المؤلف حقه الاستئثاري في الترخيص أو المنع لأي استغلال لمصنفه بأي وجه من الوجوه وبخاصة عن طريق النسخ أو الإتاحة للجمهور بما في ذلك إتاحته عبر أجهزة الحاسب الآلي.

وقد أوردت المادة 9/138 من القانون تعريفا للنسخ بأنه:"استحداث صورة أو أكثر مطابقة للأصل من مصنف أو تسجيل صوتي بأية طريقة أو في أي شكل بما في ذلك التخزين الإلكتروني الدائم أو الوقتي للمصنف أو التسجيل الصوتي". ومفاد النصوص آنفة البيان أن طرح المصنف

حقوق الملكية الفكرية في التشريع الجزائري، أطروحة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق، جامعة أبي بكر بلقايد، تلمسان، الجزائر، السنة الجامعية 2013-2014، ص 378.

1 بن دعاس فيصل، إشكالات الجريمة المعلوماتية في التشريع الجزائري، محاضرة في إطار التكوين المحلي المستمر للقضاة، مجلس قضاء قسنطينة، وزارة العدل، 2011/2010، ص 03 و04، المحاضرة متاحة على الموقع الإلكتروني الموالي:

- *https://courdeconstantine.mjustice.dz/benda3assfayssal.pdf*

والذي تم الاطلاع عليه يوم: 2018/04/25

2 محمد حماد مرهج الهيتي، المرجع السابق، ص 184؛ عبد الله عبد الكريم عبد الله، المرجع السابق، ص 18.

3 قانون حماية الملكية الفكرية المصري الصادر بالقانون رقم 82 لسنة 2002، المعدل والمتمم.

للتداول بأية صورة من الصور بدون إذن كتابي مسبق من المؤلف، أو إتاحته للجمهور بما في ذلك الإتاحة عبر أجهزة الحاسب الآلي هي أفعالاً معاقب عليها وتتوافر بها صورة الاعتداء على الحقوق الأدبية والمالية للمؤلف، وأن مجرد التخزين الإلكتروني الدائم أو الوقتي للمصنف هو نسخ له ويشكل بدوره اعتداء على حقوق المؤلف المذكورة. لما كان ذلك وكان الحكم الابتدائيقد أثبت في مدوناته- مما لا ينازع الطاعن في سلامة مأخذه من الأوراق- أن الطاعن قام بتحميل وتشغيل مصنف محمي ومسجل تحت رقم 1301 بمكتب حماية حقوق الملكية الفكرية هو برنامج سوف سمارت بيزنس بفرعي الدقي والمعادي بأرقام كودية 910-920 عن طريق الخادم الرئيسي المتصل بمقر الشركة، مما يعد نسخاً لهذا البرنامج وطرحاً له للتداول"[1].

ونظراً لما للمعلومة من أهمية، فقد أكد على ذلك الكثيرون، على غرار البروفيسور أحسن مبارك طالب، والذي يرى بأن المعلومة باتت الهدف الأول والأخير، ذلك أن سمات العالم الرقمي تعتمد أساساً على المعلومة كأداة للتعامل ومسرح الجريمة نفسه هو العالم الرقمي، بل وأدوات الجريمة هي أيضاً مستوحاة منه[2].

الفرع الثانـي: الأجهـزة كمحل للجريمة الإلكترونية.

الجهاز هو الأداة الأساسية للولوج إلى الشبكات، بدونه لا نستطيع إدراج أي معلومات، لذلك يجب حماية الأجهزة من أي تعطيل أو تخريب يطالها عبر إرسال معلومات مغلوطة أو مؤذية تؤدي إلى تعطيل البرمجة ومن ثم إلى تعطيل الجهاز[3].

لذا حين نقول الأجهزة كمحل للجريمة الإلكترونية فإننا لا نقصد بها فقط الأشياء المادية كجهاز الكمبيوتر أو المعدات الملحقة به من أسطوانات وشرائط ممغنطة وكابلات وخلافه فقط، لأن كل هذه المكونات قد تكون محلاً للسرقة أو الإتلاف العمدي كتكسيرها، أو حتى حرقها وما إلى ذلك من الجرائم التي تعد من قبيل الجـرائم العادية أو التقليديـة، إنما نعني الجــرائم التي تتسبب في تعطيل أجهزة الكمبيوتر وما في حكمها، أو تخريبها عبر إرسال الفيروسات أو البرامج التي تحوي

1 حكم محـكمة النقض المصرية، الدائـرة الجنائـية" غرفة المشـورة"، في الطعن المقيد بجدول المحكمة رقم 25992 لسنة 84 القضائية، في الجلسة العلنية المنعقدة بدار القضاء العالي بمدينة القاهرة، في يوم الثلاثاء 01 سبتمبر سنة 2015.

2 تاحي وحيد، المديرية العامــة لأمـن الوطني تنظم سلسلة محاضرات حول الجريمة المستحدثة، مجلة الشـرطة، باب الــواد، الجزائر، العدد 140، مارس 2018، ص 89.

3 نبيل صقر، الوسيط في جرائم الأموال، دار الهدى، عين مليلة، الجزائر، 2012، ص 200.

أنظمة هجومية قد تسبب تلفاً في هذه الأخيرة، مما يؤدي إلى شلل كل الأنشطة المرتبطة بهذه الأجهزة، وتزداد خطورة هذه الجرائم حينما تقع على البرامج وليس على المكونات المادية لها وذلك نظراً لقيمة ما تحتويه هذه البرامج من معلومات وبيانات، حيث يستلزم هذا النمط من الجرائم معرفة فنية عالية في مجال البرمجة[1].

لذا فقد عاقب كل من المشرع الفرنسي والمشرع الجزائري على تعمد إدخال الفيروسات المعلوماتيـة في برنامـج الغـير وكـذا الامتناع عن إخباره بذلك ولو حصـل ذلك بصفـة عرضيـة، ويدخـل في دائرة التجريم تعديل أو إزالة المعطيات التي يتضمنها نظام المعالجة الآلية للمعطيات، وذلك من خلال المادة 323 من قانون العقوبات الفرنسي، ونص المادة 394 مكرر 1 من قانون العقوبات الجزائري[2]، والحكمة من وراء تجريم هذه الأفعال هو توفير حماية للعتاد الضروري لتشغيل المنظومة المعلوماتية[3].

الفرع الثـالث: الأشخاص أو الجهات كمحل للجريمة الإلكترونية.

تعد الجريمة الإلكترونية من بين أبرز الجرائم الجديدة والمستحدثة التي يمكن أن تشكل خطراً جسيماً في ظل العولمة، ذلك أن التقدم التكنولوجي الذي تحقق خلال السنوات القليلة الماضية جعل العالم بمثابة قرية صغيرة، بحيث نجد أن هذا التقدم بقُدراته وإمكاناته قد تجاوز أجهزة الدولة الرقابية، وأضعف من قدراتها في تطبيق قوانينها، التي أصبحت لا تواكب هذا التطور، وبالتالي هذا الضعف والعجز أصبح يهدد أمن الدولة وأمن مواطنيها.

ولم تعد جرائم الاعتداء على الأشخاص كما في السابق، حيث كان يغلب عليها الطابع المادي[4]، وإنما أصبحت الاعتداءات تتم بواسطة شبكة الإنترنت؛ وفي الغالب هي جرائم السب

1 عمر الفاروق الحسيني، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية، الطبعة الثانية، دار النهضة العربية، القاهرة، 1995، ص 172.

2 تنص المادة 394 مكرر 1 من قانون العقوبات الجزائري على أن: "يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها".

3 شيخي عائشة، عياشي بوزيان، الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وأشكالها الاقتصادية وآليات مكافحتها، مجلة الدراسات الحقوقية، مخبر حماية حقوق الإنسان بين النصوص الدولية والنصوص الوطنية وواقعها في الجزائر، كلية الحقوق والعلوم السياسية، جامعة الدكتور الطاهر مولاي، سعيدة، العدد الرابع، ديسمبر 2015.

4 Marine vaLzer, *La cybercriminalité et les infractions liées à l'utilisation frauduleuse d'internet éléments de mesure et d'analyse pour l'année 2014*, Rapport de l'Observatoire national de la délinquance et des

والقذف[1]، والتشهير وبث الأفكار وأخبار من شأنها الإضرار الأدبي أو المعنوي بشخص أو جهة ما، ومن الأمثلة على ذلك القضية الجنائية رقم 3195 لسنة 2015، والتي اتهم فيها شخص بقذف شخصين –المجني عليهما– عبر شبكة التواصل الاجتماعي على حسابه الخاص، إذ ورد في حكم ما يلي: "بأن أسند إليهما أموراً لو كانت صادقة لأوجبت احتقارهما عند أهل وطنهما، كما وجه لهما سباً يتضمن خدشاً للشرف والاعتبار وطعناً في عرض الأفراد وخدشاً لسمعة العائلات، وتعدٍ على حرمة الحياة الخاصة للمجني عليها، بأن التقط لها صوراً شخصية ومقاطع مسموعة ومرئية في مكان خاص وهدد بإفشائها لحملهما على دفع مبالغ مالية دون وجه حق، وهدد المجني عليهما (....)، (....) بإفشاء أمور خادشة للحياء وكان التهديد مصحوباً بطلب وتكليف بأمر بالحصول على مبالغ مالية بدون وجه حق للحيلولة دون إتمام جريمته، كما شرع في الحصول على مبلغ مالي عن طريق التهديد، كما استخدم وسائل غير مشروعة لإجراء الاتصالات وتعمد إزعاج المجني عليهما سالفي الذكر بإساءة استعماله لتلك الأجهزة على النحو المبين في التحقيقات، فحكمت عليه المحكمة بالسجن لمدة ثلاث سنوات عما أسند إليه وألزمته المصاريف الجنائية ومصادرة الهاتف المحمول المضبوط"[2]. وفي سنة 2009 تم القبض على شاب فرنسي الجنسية يبلغ من العمر ثلاثة وعشرين (23) سنة، لأنه تمكن من الوصول إلى حسابات تويتر الخاصة بشخصيات أمريكية مثل باراك أوباما أو بريتني سبيرز، وعلى إثر ذلك حكمت عليه المحكمة بالسجن لمدة خمسة أشهر مع وقف التنفيذ[3].

---

réponses pénales (l'ONDRP), France, juillet 2015, p:06 " En 2014, 2 796 atteintes aux systèmes de traitement automatisé des données ont été recensées par la police et la gendarmerie, s'agissant essentiellement de l'accès ou du maintien frauduleux ..." .

1 حصة راشد محمد الحسن السليطي، جرائم القذف والسب العلني عبر الإنترنت (دراسة مقارنة)، المجلة القانونية والقضائية، مركز الدراسات القانونية والقضائية، وزارة العدل، قطر، العدد الأول، السنة التاسعة، يونيو 2015، ص331؛ خذيري عفاف، الجريمة الإلكترونية والأمن الوطني، المجلة الجزائرية للدراسات السياسية، المدرسة الوطنية العليا للعوم السياسية، بن عكنون، الجزائر، العدد الثامن (08)، ديسمبر 2017، ص 200؛ إبراهيم عبد الخالق، الشامل في جرائم الانترنت (جرائم الحاسوب والانترنت وفقاً لنصوص قانون العقوبات ومعلقاً عليها بالشرح والأيضاًح بأحدث أحكام النقض – التعويض عن الضرر الناتج عن جرائم الانترنت)، الطبعة الثانية، دار شادي للموسوعات القانونية، القلعة، القاهرة، 2018، ص 37؛ حنان ريحان مبارك المضحي، الجرائم المعلوماتية، دراسة مقارنة، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2014، ص 46.

2 حكم محكمة النقض المصرية، الدائرة الجنائية، في الطعن المقيد بجدول المحكمة رقم 26463، لسنة 86 القضائية، في الجلسة العلنية المنعقدة بدار القضاء العالي بمدينة القاهرة، في يوم الأحد 22 أكتوبر سنة 2017.

3 Emilie Bailly, Emmanuel Daoud, *Cybercriminalité et réseaux sociaux : la réponse pénale*, La base de données juridique des Éditions Dalloz, France, AJ Pénal 2012, p:252, p 02.

كما أنه من المتصور أن يقع ضحيتها-أو محلاً لها- جميع الأشخاص[1]، الطبيعية منها أو المعنوية، العامة أو الخاصة[2] طالما كانت تستخدم الحاسب الآلي في ممارسة أنشطتها سواء الاقتصادية منها أو الاجتماعية أو حتى السياسية والعسكرية.

فمن بين الجرائم التي باتت تهدد أمن المواطنين والدول على حد سواء، الإرهاب الإلكتروني والذي ساعدت التقنية الحديثة على استفحاله، وسرعة انتشاره وكذا تطبيقه، لما توفره من معلومات ووسائل وقلة تكاليف، فباستعمال شبكة الإنترنت تتمكن المنظمات الإرهابية المتفرقة من الاتصال مع بعضها البعض والتنسيق فيما بينها، فعدم وجود زعيم ظاهر للجماعة الإرهابية أصبحت سمة جوهرية للتنظيم الإرهابي الحديث، مختلفاً بذلك عن النمط الهرمي القديم للجماعات الإرهابية، لذا أصبح الإرهاب الإلكتروني أو ما يسمى بالإرهاب السيبراني Le Cyberterrorisme هو السائد حاليا[3]، معتمداً على اقتحام المواقع Storming Sites وتدميرها Distroying it وتغيير محتوياتها والدخول على الشبكات والعبث بمحتوياتها بإزالتها أو بالاستيلاء عليها أو الدخول على

1 عفيفي كامل عفيفي، المرجع السابق، ص 34.

2 نصت المادة (394 مكرر03) من القانون 04-15 السالف الذكر على: "تضاعف العقوبات المنصوص عليها في هذا القسم، إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات اشد."؛ أمر رقم 20-01، المؤرخ في 09 ذي الحجة عام 1441 الموافق 30 يوليو سنة 2020، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 08 يونيو سنة 1966 والمتضمن قانون العقوبات، الصادرة في الج.ر العدد 44 المؤرخة في 30 يوليو سنة 2020. يتمم هذا الأمر الفصل الخامس من الباب الأول من الكتاب الثالث من الجزء الثاني من قانون العقوبات بقسم أول مكرر، بعنوان: "الإهانة والتعدي على المؤسسات الصحية ومستخدميها" يشمل عدة مواد منها: المادة (149 مكرر 3)، والتي جاء فيها: "يعاقب بالحبس من سنتين (2) إلى خمس (5) سنوات، وبغرامة من 200.000 دج إلى 500.000 دج، كل من يقوم بتسجيل مكالمات أو أحاديث أو التقاط أو نشر صور أو فيديوهات أو أخبار أو معلومات على موقع أو شبكة إلكترونية أو في مواقع التواصل الاجتماعي أو بأي وسيلة أخرى، قصد الإضرار أو المساس بالمهنية أو بالسلامة المعنوية لأحد مهنيي الصحة أو أحد موظفي أو مستخدمي الهياكل والمؤسسات الصحية، أثناء تأدية مهامهم أو بمناسبتها. وتطبق نفس العقوبة إذا ارتكبت هذه الأفعال إضراراً بالمرضى وأسرهم أو الهياكل والمؤسسات الصحية أو مساساً بالحرمة الواجبة للموتى. وتضاعف العقوبات المنصوص عليها في هذه المادة، إذا تم تصوير الصور أو الفيديوهات أو الأخبار أو المعلومات بشكل مغرض أو تم التقاطها خلسة أو في الأماكن غير المفتوحة للجمهور بالهيكل أو المؤسسة الصحية أو إذا تم إخراجها عن سياقها". وقد تصل العقوبة إلى خمس عشرة (15) سنة، والغرامة إلى 1.500.000 دج، إذا ارتكبت تلك الأفعال خلال فترات الحجر الصحي أو خلال وقوع كارثة طبيعية أو بيولوجية أو تكنولوجية أو غيرها من الكوارث، أو ارتكبت تلك الأفعال قصد النيل من مصداقية الهياكل والمؤسسات الصحية ومهنيتها". كما قد تصل العقوبة على تلك الأفعال إلى السجن مدة عشرين (20) سنة، والغرامة إلى 2.000.000 دج، في إطار جماعة، إثر خطة مدبرة، بعد الدخول إلى الهياكل أو المؤسسة الصحية باستعمال العنف، باستعمال السلاح أو استعماله.

3 نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الأولى، الإصدار الأول، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2008، ص ص: 208-209؛ وانظر كذلك: Sujit Raman, Chair, John P. Cronan, and athers, *Report of the Attorney General Cyber-Digital Task Force*, United States Department of Justice, Washington, July 2, 2018, p :27.

شبكات الطاقة أو شبكات الاتصالات بهدف تعطيلها عن العمل أطول فترة ممكنة أو تدميرها نهائياً[1].

لذا خص المشرع الجزائري مرتكبي مثل هذه الأفعال بعقوبات تتراوح بين خمس (05) إلى عشر (10) سنوات سجن إضافة إلى غرامة مالية، وهو ما بينته مواد بالقانون رقم: 16-02 المعدل والمتمم لقانون العقوبات[2]، ومنها المادة (87 مكرر 12) المضافة بموجب المادة الثانية (02) منه، إذ نصت على أن: "يعاقب بالسجن المؤقت من خمس (5) سنوات إلى عشر (10) سنوات وبغرامة من 100.000 دج إلى 500.000 دج كل من يستخدم تكنولوجيا الإعلام والاتصال لتجنيد الأشخاص لصالح إرهابي أو جمعية أو تنظيم أو جماعة أو منظمة يكون غرضها أو تقع أنشطتها تحت طائلة أحكام هذا القسم أو ينظم شؤونها أو يدعم أعمالها أو أنشطتها أو ينشر أفكارها بصورة مباشرة أو غير مباشرة".

---

1 توفيق مجاهد، طاهر عباسة، جريمة الإرهاب الإلكتروني في ضوء أحكام الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر بالوادي، الجزائر، المجلد التاسع (09)، العدد الثالث (03)، ديسمبر 2018، ص.ص: 81-82؛ رابحي لخضر، بن بعلاش خاليدة، معالجة الجرائم المعلوماتية في ظل التعاون الدولي والاستجابة الوطنية، ورقة بحثية مقدمة الى الملتقى الوطني المتعلق بالجريمة المعلوماتية بين الوقاية والمكافحة، المنظم من قبل قسم الحقوق ومخبر الحقوق والحريات في الأنظمة المقارنة، بجامعة بسكرة يومي 16-17 نوفمبر 2015، ص03؛ أيسر محمد عطية، ورقة علمية بعنوان: دور الآليات الحديثة للحد من الجرائم المستحدثة الإرهاب الإلكتروني وطرق مواجهته، كلية العلوم الإستراتيجية، الملتقى العلمي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، عمان، الأردن، من 02 إلى 04 سبتمبر 2014، ص 13؛ منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الازاريطة، الإسكندرية، مصر، 2005، ص 111؛ حنان خرباشي، دور شبكات التواصل الاجتماعي في تشكيل الوعي بالظاهرة الإرهابية، مجلة اتجاهات سياسية، المركز الديمقراطي العربي، برلين، ألمانيا، العدد الثالث (03)، يناير 2018، ص 144؛ اسعيداني سلامي، طارق طراد، التجربة الجزائرية لمواجهة الجريمة الإلكترونية في ظل البيئة التفاعلية الجديدة (عرض تشريعي قانوني)، مجلة الحقوق والعلوم السياسية، جامعة عباس لغرور، خنشلة، الجزائر، العدد الثاني عشر (12)، جوان 2019، **نقلاً عن**: حسنين شفيق، الإعلام الجديد والجريمة الإلكترونية "التسريبات، التجسس، الإرهاب الإلكتروني"، دار فكر وفن للطباعة والنشر والتوزيع، مصر، 2015، ص 183؛ عادل جارش، الإرهاب الجديد: دراسة في المفهوم، الطبيعة، الأنواع وإجراءات المواجهة ، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر بالوادي، الجزائر، المجلد التاسع (09)، العدد الثالث (03)، ديسمبر 2018، ص 287، **نقلاً عن**:

- Mitko Bogdanoski, and Drage Petreski, *"Cyber Terrorism, Global Security Threat"*, International Scientific Defence and Peace Journal, p 61, look at the cite: *http://eprints.ugd.edu.mk/6849/1/CYBER%20TERRORISME2%80%93%20GLOBAL%20SECURITY%20THREAT%20-%20Mitko%20Bogdanoski.pdf*. The website has been viewed on: 20/11/2016.

2 القانون رقم 16-02، المؤرخ في 19 يونيو سنة 2016، يعدل ويتمم قانون العقوبات، المنشور بالج.ر العدد 37، المؤرخة في 22 يونيو سنة 2016، جاءت المادة الثانية (02) منه لتتم قانون العقوبات بثلاثة مواد منها المادة 87 مكرر 12.

لكن تبقى هذه العقوبات غير كافية إذا ما قورنت بالخسائر التي قد يتسبب فيها العمل الإرهابي الإلكتروني، خاصة إن وقع ضحيته شباب أو أطفال في مقتبل العمر.

ومن بين الأمثلة القضائية على استعمال الوسائل التقنية الحديثة في الأعمال الإرهابية في القانون المصري، قضية اتهمت فيها النيابة العامة الطاعنين وآخرين في القضية الجنائية رقم 2210 لسنة 2014 قسم العجوزة، بأنهم في الفترة من شهر جويلية سنة 2013 حتى 20 من يناير سنة 2014، كونوا: "جماعة أسست على خلاف أحكام القانون، وكان الغرض منها الدعوة إلى تعطيل أحكام الدستور والقوانين، ومنع مؤسسات الدولة والسلطات العامة من ممارسة أعمالها والاعتداء على الحرية الشخصية للمواطنين والحقوق العامة والإضرار بالوحدة الوطنية والسلام الاجتماعي بأن تولوا قيادة جماعة الإخوان المسلمين التي تهدف لتغيير نظام الحكم بالقوة والاعتداء على أفراد ومنشآت القوات المسلحة والشرطة، واستهداف المنشآت العامة ودور عبادة المسيحيين بهدف الإخلال بالنظام العام وتعريض سلامة المجتمع وأمنه للخطر، وكان الإرهاب من الوسائل التي تستخدمها هذه الجماعة في تنفيذ أغراضها على النحو المبين في التحقيقات، والمتهمون السادس، والعاشر حتى الثاني عشر، والثامن عشر حتى السابع والأربعين أيضاً: 1- بصفتهم مصريين أذاعوا عمداً في الخارج أخباراً وبيانات وإشاعات كاذبة حول الأوضاع الداخلية للبلاد بأن بثوا عبر شبكة المعلومات الدولية وبعض القنوات الفضائية مقاطع فيديو وصوراً وأخباراً كاذبة للإيحاء للرأي العام الخارجي بعدم قدرة النظام القائم على إدارة شؤون البلاد وكان من شأن ذلك إضعاف هيبة الدولة واعتبارها والإضرار بالمصلحة القومية للبلاد على النحو المبين بالتحقيقات. 2- أذاعوا عمداً أخباراً وبيانات وإشاعات كاذبة بأن بَثوها على شبكة المعلومات الدولية وبعض القنوات الفضائية- على النحو المبين بالاتهام الوارد بالبند سادساً، وكان من شأن ذلك تكدير الأمن العام وإلقاء الرعب بين الناس وإلحاق الضرر بالمصلحة العامة على النحو المبين بالتحقيقات. سابعاً:- المتهمون الثامن والحادي والأربعون حتى التاسع والأربعون أيضاً:- حازوا أجهزة اتصالات لاسلكية (هاتف ثريا وأجهزة بث إرسال واستقبال) دون الحصول على تصريح بذلك من الجهات المختصة بغرض المساس بالأمن القومي على النحو المبين بالتحقيقات..."[1].

1 حكم محكمة النقض المصرية، في الطعن المقيد بجدول المحكمة برقم 21819 لسنة 85 القضائية، في الجلسة العلنية المنعقدة بدار القضاء العالي بمدينة القاهرة، جلسة 03 ديسمبر سنة 2015.

ومن بين أنواع الجرائم الإلكترونية الأخرى التي باتت تهدد المؤسسات الاقتصادية والدول ما يسمى بالتجسس الإلكتروني، أو كما يسميه بعضهم التجسس المعلوماتي، والذي أصبح يشمل الجوانب الصناعية والتقنية والتجارية للمؤسسات الاقتصادية، كما قد يشمل أيضاً الجانب العسكري والأمني للدولة. ولا شك أن التقدم الكبير الذي لحق الاتصالات وصناعة الحواسيب أسفر عن إيجاد وسائل أكثر فاعلية في التجسس، ومن الأمثلة على ذلك ما قام به هاكرز حين الإغارة على شبكات معلوماتية تابعة لوكالة الفضاء ناسا ومواقع أسلحة ذرية تابعة لحكومة الولايات المتحدة الأمريكية[1].

كل هاته الجرائم وغيرها أصبح من السهل إرتكابها بفعل مجرم ارتبط اسمه بها؛ ألا وهو: المجرم الإلكتروني، فمن هو ؟ وما هي أهم سماته ؟ وما هي دوافعه وراء ارتكابه للجرائم الإلكترونية ؟

1 نهلا عبد القادر المومني، المرجع السابق، ص 92؛ هروال هبة نبيلة، المرجع السابق، ص 361.

المبحث الثانـــي:
الإطار المفاهيمي للمجرم الإلكتروني.

المجرم الإلكتروني هو ذلك المجرم الذي لديه قدرة على تحويل نواياه إلى لغة رقمية باستخدام التقنية الرقمية المعلوماتية، وذلك بأداء فعل أو الامتناع عنه، مما يحدث اضطرابات في المجتمع المحلي أو الدولي نتيجة مخالفته قواعد الضبط الاجتماعي محلياً أو دولياً، هذا الصنف من المجرمين لديهم تأثير خطير جداً على الأشخاص الطبيعيين صغاراً كانوا أو كباراً، أو على الأشخاص المعنويين كالمؤسسات والدول.

ولذلك، كان لا بد من معرفة أهم السمات التي تميزه عن باقي المجرمين، وكذا الدوافع التي تقف وراء ارتكابه الجريمة الإلكترونية، وهو ما سيأتي بيانه من خلال دراسة سمات المجرم الإلكتروني (المطلب الأول)، ومعرفة الدوافع التي تقف وراء ارتكاب المجرم الإلكتروني لجريمته الإلكترونية (المطلب الثاني).

المطلب الأول: مفهوم المجرم الإلكتروني وسماته.

المجرمون الإلكترونيون–مرتكبوا الجريمة الإلكترونية– أو من يُطلق عليهم البعض تسمية المخترقون، ويسميهم آخرون بالقراصنة؛ والمقصود بالقرصنة هنا هي عملية التوصل إلى كافة المعلومات في الكمبيوتر بصورة غير مشروعة ونسخ البرامج دون وجه حق؛ أي الحصول على المعلومات بطرق ملتوية وغير مشروعة. وهناك نوعين من القراصنة؛ الصنف الأول يطلق عليه اسم الهواة وهم الشباب الفضوليين الذين يسعون للتسلية ولا يشكلون خطورة على الصناعات وأنظمة المعلومات، والصنف الثاني وهم المحترفون (Crackers) وهم أكثر خطورة من الصنف الأول وقد يحدثون أضراراً كبيرة، كما يمكن أن يؤلفوا أندية لتبادل المعلومات فيما بينهم.[1]

إن لهذا النوع من المجرمين صفات كثيرة تختلف عن صفات مرتكبي الجرائم التقليدية الأخرى، والتي سنقتصر على ذكر أهمها:

أولاً– الذكاء: يعتبر الذكاء من أهم صفات مرتكبي الجرائم الإلكترونية؛ لأن ذلك يتطلب منهم المعرفة التقنية الكافية والاحترافية لكيفية الدخول إلى أنظمة الحاسب الآلي، والقدرة على التعديل والتغيير في البرامج بطريقة تمكنهم من ارتكاب جرائم السرقة والنصب وغيرها من الجرائم بطريقة أسهل وأكثر أماناً[2].

ثانياً– المعرفة والمهارة والـخبرة: في كثير من الأحيان تجد المجرم الإلكتروني يمتلك قدراً كبيراً من المعرفة والمهارة في استخدام التقنية المعلوماتية، ويعود ذلك لامتلاكه الخبرة في البرمجة ومعالجة الشبكات والقدرة على اتخاذ الإجراءات التقنية المناسبة لتخطي الحواجز الموضوعة لحماية

1 نعيم مغبغب، مخاطر المعلوماتية والانترنت "المخاطر على الحياة الخاصة وحمايتها: دراسة في القانون المقارن"، المرجع السابق، ص 221؛ القاضي وليد العاكوم، مفهوم وظاهرة الإجرام المعلوماتي، بحوث مؤتمر القانون والكمبيوتر والانترنت بالتعاون مع مركز الإمارات للدراسات والبحوث الإستراتيجية ومركز تقنية المعلومات بالجامعة، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، المجلد الأول، من 01 إلى 03 مايو 2004، ص 12.

2 خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص 134؛ محمود مدين عبد الرحمان، الجريمة الإلكترونية وتحديات الأمن القومي، دار المصرية للنشر والتوزيع، القاهرة، 2017، ص 34؛ هلالي عبد اللاه أحمد، جرائم الحاسب والانترنت بين التجريم الجنائي وآليات المواجهة (مجموعة محاضرات أُلقيت على طلاب كلية الحاسبات والمعلومات)، دار النهضة العربية، القاهرة، مصر، 2015، ص 177؛ مصطفى محمد موسى، أساليب إجرامية بالتقنية الرقمية ماهيتها، مكافحتها دراسة مقارنة، دار الكتب القانونية، مصر، 2005، ص 19؛ عبد الصبور عبد القوى على مصري، المحكمة الرقمية والجريمة المعلوماتية (دراسة مقارنة)، الطبعة الأولى، مكتبة القانون والاقتصاد، الرياض، المملكة العربية السعودية، 2012، ص 52.

الشبكات، كما يقوم بتنمية تلك القدرة الفنية بالممارسة الطويلة في فهم لغات البرمجة وأنظمة التشغيل[1]، أما الخبرة فيكتسبها من خلال الدراسة أو التكوين في هذا المجال، أو من خلال الإحتكاك بالآخرين، وما أصبحت توفره مختلف البرامج المتواجدة على الوسائط الإلكترونية الكثيرة أو حتى عبر شبكة الإنترنت مباشرة.

ثالثاً– المجرم الإلكتروني إنسان اجتماعي: يقال عن المجرم الإلكتروني أنه شخص اجتماعي؛ لأنه لا يضع نفسه في حالة عداء سافر مع المجتمع الذي يحيط به، بل إنه إنسان متوافق معه، فمعدل الذكاء المرتفع لديه يساعده على عملية التكيف مع المجتمع؛ فالذكاء في نظر الكثيرين ليس سوى القدرة على التكيف، ولا يعني ذلك التقليل من شأن المجرم الإلكتروني، بل إن خطورته الإجرامية قد تزداد إذا ما زاد تكيفه الاجتماعي مع توفر الشخصية الإجرامية لديه[2].

رابعاً– المجرم الإلكتروني مجرم عائد للإجرام: يعود كثير من مجرمي المعلومات إلى ارتكاب جرائم أخرى في مجال الكمبيوتر انطلاقاً من الرغبة في سد الثغرات التي أدت إلى التعرف عليهم وتقديمهم للمحاكمة في المرة السابقة، ويؤدي ذلك إلى العودة إلى الإجرام، وقد ينتهي بهم الأمر كذلك في المرة التالية إلى تقديمهم للمحاكمة،[3] ومن الأمثلة على ذلك ما قام به الهاكرز

---

1 عائشة بن قارة مصطفى، المرجع السابق، ص 41؛ ليندة بوسيف، آليات وسبل مكافحة الجريمة الإلكترونية، مجلة الاتصال والصحافة، تصدر عن المدرسة الوطنية العليا للصحافة وعلوم الإعلام، المجلد الرابع، العدد الثاني، الجزائر، 2017/06/15، ص235.

2 عبد الله حسين على محمود، سرقة المعلومات المخزنة في الحاسب الآلي، الطبعة الأول، دار النهضة العربية، القاهرة، مصر، 2001، ص 50؛ محمد أمين الرومي، جرائم الكمبيوتر والانترنت، دار المطبوعات الجامعية، الإسكندرية، 2004، ص 22؛ محمد على العريان، المرجع السابق، ص 62؛ رحموني محمد، خصائص الجريمة الإلكترونية ومجالات استخدامها، مجلة الحقيقة، جامعة أحمد دراية أدرار، العدد 41، جوان 2017، ص 444؛ براهيم رمضان ابراهيم عطايا، الجريمة الإلكترونية وسبل مواجهتها في الشريعة الإسلامية والأنظمة الدولية– دراسة تحليلية تطبيقية، مجلة كلية الشريعة والقانون بطنطا، العدد الثلاثون، الجزء الثاني، مصر، أبريل 2015، ص 373؛ خليل يوسف جندي، المواجهة التشريعية للجريمة المعلوماتية على المستويين الدولي والوطني (دراسة مقارنة)، مجلة كلية القانون للعلوم القانونية والسياسية، جامعة كرموك، العراق، المجلد السابع (07)، العدد السادس والعشرون (26)، 2018، ص 95، **نقلاً عن:** شمسان ناجي صالح الخيلي، الجرائم المستخدمة بطرق غير مشروعة لشبكة الانترنت، دار النهضة العربية، القاهرة، 2009، ص 42.

3 عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والانترنت، المرجع السابق، ص 80؛ عبد الله حسين على محمود، المرجع السابق، ص 56؛ عطوي مليكة، الجريمة المعلوماتية، مجلة حوليات جامعة الجزائر، العدد 21، الجزء الأول، جامعة الجزائر 01 بن يوسف بن خدة، جوان 2012، ص 12؛ غانم محمد غانم، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والانترنت وجرائم

البريطاني "جاري ميكنون Gary Mckinnon" الذي اخترق حسابات وكالة الفضاء الأمريكية "ناسا NSAS " بين سنتي 2001 و2002، وتم القبض عليه للمرة الأولى سنة 2002، ولكن السلطات أفرجت عنه لعدم كفاية الأدلة، ثم تم القبض عليه مرة أخرى في سنة 2005، وحـكم عليه بالوضع تحت المراقبة، وبالحرمان من استخدام شبكة الإنترنت[1].

المطلب الثاني: دوافع ارتكاب المجرم الإلكتروني لجريــمته الإلكترونية.

تتباين الدوافع المؤدية لارتكاب الجريمة الإلكترونية تبعاً لطبيعة المجرم ومدى ثقافته ومعرفته بمجال الحاسب الآلي، لذلك نجد أن هذه الدوافع تتنوع، فمنها الشخصية بنوعيها المالية، مثل البحث عن الربح، أو الذهنية كالسعي إلى إظهار التفوق، وأخرى خارجية كالانتقام مثلاً.

الفرع الأولاً: ارتكاب الجريمة الإلكترونية من أجل كسب المال.

يعد هذا الدافع من بين أكثر الدوافع تحريكاً للجناة لاقتراف الجرائم الإلكترونية[2]، فعادة ما يكون الدافع لارتكاب الجرائم التقليدية هو تحقيق النفع المادي كما يحدث في السرقة، غير أن النفع المادي الذي يمكن أن يتحقق عن طريق الجرائم الإلكترونية أكثر من ذلك بكثير، والأمثلة متعددة عن الجرائم الإلكترونية التي حصد مرتكبوها مبالغ مالية كبيرة، كجريمة انتحال الشخصية بطريقة إلكترونية، والتي تعد وسيلة من وسائل الاحتيال للحصول على الأموال، فهذه الجريمة الإلكترونية تقوم على مبدأ انتحال شخصية الغير، والقيام بممارسات وأعمال غير مشروعة واستخدام هوية الشخص الضحية؛ لتحقيق استفادة مادية بطريقة تجعل من الصعب اكتشاف الفاعل الحقيقي[3]. ومن الأمثل ما حدث في الولايات المتحدة الأمريكية، حين وقع عدد كبير من الشعب الأمريكي

الاحتيال المنظم باستعمال شبكة الانترنت، الطبعة الأولى، دار الفكر والقانون، المنصورة، مصر، 2017، ص 14؛ هروال هبة نبيلة، المرجع السابق، ص 47.

1 هلالي عبد اللاه أحمد، مرجع سابق، ص ص 179-180.

2 ماجدة غريب، حسن الأمير، مدى الوعي لدى الفئة العمرية الشابة بنظام عقوبات الجرائم المعلوماتية السعودي، المجلة العربية الدولية للمعلوماتية، المملكة العربية السعودية، المجلد الخامس (05)، العدد التاسع (09)، 2017، ص 27؛ عبيد صالح حسن، سياسة المشرع الإماراتي لمواجهة الجرائم الإلكترونية، مجلة الفكر الشرطي، مركز بحوث الشارقة، الإمارات العربية المتحدة، المجلد الرابع والعشرون (24)، العدد الرابع (04)، اكتوبر 2015، ص 38؛ سعيدي سليمة، حجاز بلال، جرائم المعلومات والشبكات في العصر الرقمي، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، 2016، ص 37.

3 عبد الحليم موسى يعقوب، الإعلام الجديد والجريمة الإلكترونية، الطبعة الأولى، الدار العالمية للنشر والتوزيع، مصر، 2014، ص 215؛ احمد خليفة الملط، المرجع السابق، ص.ص 187-188.

ضحية لجرائم نصب عبر الإنترنت، من قبل أشخاص قاموا بإنشاء مواقع على شبكة الإنترنت بغرض جمع تبرعات لضحايا أحداث 11 سبتمبر 2001[1] مستغلين تعاطف الشعب مع الضحايا. ولأجل تحقيق مكاسب مالية أكبر تتم تلك الجرائم عن طريق جماعات منظمة[2].

الفرع الثاني: ارتكاب الجريمة الإلكترونية رغبة في التعلم وإثبات الذات وقهر النظام المعلوماتي.

هناك طائفة عريضة من الناس يُخالجهم الشعور بالفخر إذا ما تمكنوا من اختراق مواقع على شبكة الإنترنت، أو وصلوا إلى قاعدة بيانات محمية، إذ يعد ذلك من الأمور التي يتباهون بها أمام أقرانهم، ويشبعون بها فضولهم، ويثبتون بها قدراتهم على اختراق البرامج[3]، ويسعون من خلالها إلى تحقيق شهرة ما، مع العلم أنهم قد لا يملكون المعرفة الحقيقية لشن الهجمات الإلكترونية، ولكنهم يستعينون ببرامج موجودة على مواقع على شبكة الإنترنت، والتي لا يتطلب استعمالها معرفة كبيرة بالحاسوب أو الشبكات تساعدهم في هجماتهم الإلكترونية على أنظمة المعلومات، لذلك كثيراً ما نسمع أشخاصاً يتظاهرون بأنهم من قراصنة الإنترنت، أو ما يطلق عليهم اسم (Hackers)، وهم في الحقيقة مجرد مبتدئين، يسميهم المتخصصون في مجال أمن المعلومات، أطفال البرامج الجاهزة scipt kiddies[4]، ذلك لأنهم استفادوا من برامج تعينهم على شن هجمات إلكترونية؛ ما كان لهم أن يشنوها لولا توفر هذه البرامج، لذا نجد المشرع الفرنسي يعاقب على تَوفير تلك الوسائل والبرامج

---

1 أيمن عبد الحفيظ، المرجع السابق، ص 273.

2 محمد حماد مرهج الهيتي، التكنولوجيا الحديثة والقانون الجنائي، المرجع السابق، ص 165؛ نعيم مغبغب، حماية برامج الكمبيوتر"الأساليب والثغرات دراسة في القانون المقارن"، المرجع السابق، ص 220.

3 نعيم مغبغب، حماية برامج الكمبيوتر، المرجع السابق، ص 219؛ مزيود سليم، الجريمة المعلوماتية واقعها في الجزائر وآليات مكافحتها، المجلة الجزائرية للاقتصاد والمالية، مخبر الاقتصاد الكلي والمالية الدولية، جامعة الدكتور يحي فارس، العدد الأول، المدية، افريل 2014، ص 98؛ طاق عفيفي صادق احمد، الجرائم الإلكترونية جرائم الهاتف المحمول دراسة مقارنة بين القانون المصري والإماراتي والنظام السعودي، الطبعة الأولى، المركز القومي للاصدرات القانونية، مصر، 2015، ص 65.

4 خالد سليمان عبد الله الغثبر، مهندس محمد عبد الله على القحطاني، أمن المعلومات بلغة ميسرة، مكتبة الملك فهد الوطنية، الطبعة الأولى، الرياض، السعودية، 2009، ص 27؛ **وانظر أيضاً:**

- Mira Carignan, L'origine géographique en tant que facteur explicatif de la cyberdélinquance, mémoire présenté à la faculté des études supérieures en vue de l'obtention de M.SC.en criminologie, Université de Montréal Faculté des études supérieures, Septembre 2015, P : 30 : « Plus simplement, Goodell (1996) a défini les cyberdélinquants comme les «hackers», les «crackers»et les «phreakers». Les «hackers» constituent ceux motivés par la curiosité intellectuelle et le désir d'acquérirde nouveaux apprentissages. Les «crackers» ont un objectif malsain de destruction, de vandalisme de sites Internet et de pages web. Quant aux «phreakers», leurs délits sont dirigés vers la manipulation de systèmes téléphoniques ou vers des attaques de ces derniers » .

المصممة خصيصًا لارتكاب هجوم أو تسلل إلى نظام معالجة البيانات الآلي[1]، واعتبرها انتهاك للمادة (323-3-1) من قانون العقوبات الفرنسي، وهو ما أكده القضاء الفرنسي كذلك[2].

الفرع الثالث: ارتكاب الجريمة الإلكترونية رغبة فـــي الانتقام.

نزعة الانتقام من أخطر الدوافع التي يمكن أن تدفع الشخص إلى ارتكاب الجريمة، ومنها التي يقوم بها موظف تم فصله من العمل أو تخطيه في الحوافز أو الترقية[3]. ومن أمثلتها أيضاً ما قام به شاب هندي يبلغ من العمر ست عشرة (16) سنة، بإنشائه لموقع إباحي على شبكة الإنترنت للانتقام من زملائه في الدراسة الذين كانوا يسخرون منه، فتضمن الموقع نصوصاً بأسماء بعضاً من زملائه وزميلاته ومعلميه بها تعليقات غير أخلاقية بجانب اسم كل منهم، وبتاريخ السابع والعشرين (27) من شهر أبريل سنة 2001 ألقت عليه الشرطة الهندية القبض وقدم للمحاكمة، فحكمت عليه محكمة الجنح الهندية بالحبس[4]، كما قام أحد الطلبة بدافع الانتقام من صديقته التي هجرته، بتخزين صورها ذات الطابع الإباحي مصحوبة بتعليقات مسيئة عن أخلاقها وسلوكها على موقعها الشخصي بشبكة الإنترنت دون علمها، وبدافع تشويه صورة الإسلام قامت المخابرات الإسرائيلية باختراق موقع حركة حماس على شبكة الإنترنت ونشرت صوراً إباحية عليه[5].

---

1 **Code pénal - Article 323-3-1,** Créé par LOI n°2010-1594 du 20 décembre 2010 - art. 84, « 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. »

2 Cour de cassation, chambre criminelle, Audience publique du 27 octobre 2009, N° de pourvoi: 09-82346 (Publié au bulletin).

3 ربيعي حسين، المجرم المعلوماتي – شخصيته وأصنافه، مجلة العلوم الإنسانية، جامعة محمد خيضر ببسكرة، الجزائر، العدد الأربعون (40)، جوان 2015، ص 292؛ جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات– رؤية جديدة للجريمة الحديثة–، الطبعة الأولى، دار البداية، عمان، الأردن، 2007، ص 168؛ عمر الفاروق الحسيني، المرجع السابق، ص 61؛ محمد على العريان، المرجع السابق، ص 66؛ محمد أمين الرومي، المرجع السابق، ص 25 ؛ محمد دباس الحميد، ماركو ابـراهيم نينو، حماية أنظمة المعلومات، الطبعة الأولى، دار الحامد للنشر والتوزيع، عمان، الأردن، 2007، ص 71؛ رابحي عزيزة، المرجع السابق، ص 101؛ نبيل دريس، الجريمة السيبرانية بين المفاهيم والنصوص التشريعية الجزائر أنموذجاً، مجلة القانون والمجتمع، مخبر القانون والمجتمع، جامعة أحمد دراية أدرار، الجزائر، العدد العاشر، ديسمبر 2017، ص 32؛ **وانظر أيضاً**:

- Emilie Bailly, Emmanuel Daoud, Cybercriminalité et réseaux sociaux : la réponse pénale, La base de données juridique des Éditions Dalloz, France, AJ Pénal 2012, p:252, P 04.

4 مصطفى محمد موسى، المرجع السابق، ص 179.

5 علي عبود جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، الطبعة الأولى، منشورات زين الحقوقية، لبنان، 2013، ص 117.

الفرع الرابع: دوافــع أخرى وراء ارتكاب المجرم الإلكتروني للجريمة الإلكترونية.

هناك دوافع أخرى قد تكون وراء ارتكاب الجريمة الإلكترونية[1]، نذكر منها على سبيل المثال لا الحصر:

1- التنافس السياسي والاقتصادي[2]، ومثالها ما قام به بعض القراصنة المتواجدين على الأراضي الروسية باختراق حاسبات حكومية في الولايات المتحدة الأمريكية مدة عام كامل، حيث قاموا بسرقة معلومات غير سرية ولكنها حساسة من أجهزة الحواسيب العسكرية الأمريكية[3].

2- التسابق الفضائي والعسكري بين الدول[4].

---

1 حاولت دراسة "Vladimir Golubev"، بعــنوانها المجرمين في الجرائم المتصلة بالكمبيوتر سنة 2009، الوقوف علي دوافع مجرمي الكمبيوتر، وقد أوضحت الدراسة أن 33 % منهم لا يتجاوز 20 عاما، و45 % منهم يتراوح عمرهم من 20- 40 عاما، و13 % منهم أكبر من 40 عاما، وهذا يشير إلي أن النسبة الغالبة تتراوح ما بين 13- 20 عاما. كما أوضحت الدراسة أن عدد المجرمين يتضاعف خمس مرات سنويا، وأن 7.5 % لديهم قدرات تقنية عالية، وخاصة أولئك الذين يعملون في وظائف تتصل بالمحاسبة والسكرتارية والإدارة وغيرها.": مديحة فخري محمود محمد، دراسة مستقبلية لدور الجامعات المصرية في مواجهة الجرائم الإلكترونية لدي الطلاب، ورقة بحثية مقدمة في إطار أشغال أبحاث مؤتمر التربية في عالم متغير، محور الإدارة التربوية، المقام في الجامعة الهاشمية، الأردن، يومي 07 و08 افريل 2010، ص 175.

2 من مخاطر التجارة الإلكترونية عن طريق الانترنت إمكانية سرقة الأموال والبيانات المتداولة فيها بطريق الانترنت، لذا تجرم التشريعات تلك الأفعال، **انظر في ذلك:** على عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب، دار الجامعة الجديدة للنشر، الازاريطة، الإسكندرية، مصر، 1997، ص.ص: 63-64؛ تركي بن عبد الرحمن المويشير، المرجع السابق، ص.ص: 105–106؛ عبد الفتاح بيومي حجازي، الجريمة في عصر العولمة "دراسة في الظاهرة الإجرامية المعلوماتية مع التطبيق على القانون الإماراتي"، المرجــع السابق، ص 29.

ومن نتائج الجرائم الإلكترونية أنها تمثل عائقًا أمام تطور التجارة الإلكترونية، وعدد آخر من الخدمات المهمة للمواطن والاقتصاد الوطني، هذه المعاملات والجرائم يمكن أن تعمق الشرخَ الرقمي الذي يَفصل بين الجزائر والبلدان المتقدمة إذا لم تتخذ إجراءات صارمة، حيث إنه وبسرقة الأرقام السرية لبطاقات القروض مثلاً أو بطاقات الائتمان يمكن الدخول إلى موقع يعرض سلعًا وبضائع عن طريق التجارة الإلكترونية ليشتريها على حساب صاحب البطاقة، هذه الحالة تثبط من عزيمة الأنترنوت في العالم وفي الجزائر، قبل حتى أن يعيشوا الجانب الإيجابي من الدفع (On line)"، **انظر في ذلك:** آمنة بن عبدربه، الجزائر في مجتمع المعلومات سنة 2003: حصيلة وآفاق، مذكرة لنيل شهادة الماجستير في علوم الإعلام والاتصال، قسم علوم الإعلام والاتصال، كلية العلوم السياسية والإعلام، جامعة الجزائر، السنة الجامعية: 2005-2006، ص 85.

3 نهلا عبد القادر المومني، المرجع السابق، ص 93.

4 لطرش فيروز، بن عزوز حاتم، الجريمة الإلكترونية في الجزائر من جريمة فردية إلى جريمة منظمة، مجلة آفاق للعلوم، جامعة زيان عاشور بالجلفة، العدد 01، 2016، ص 328.

3- ومن الدوافع أيضاً الدعوة للإلحاد، حيث أن هناك مواقع الإلحاد التي تطالب بإلغاء الدين والدولة والأسرة[1]. كما أن هنالك مواقع وحسابات إلكترونية يهدف أصحابها إلى إثارة التمييز والكراهية في المجتمع[2].

4- ومن بين أبرز دوافـــع ارتكاب الجرائم الإلكترونية، عمليات غســيل الأموال والتي ساعدت في ارتكابها وبشكل كبير السرية المصرفية، والتقنية الحديثة[3].

ومن الدوافع أيضاً: الإرهاب الإلكتروني[4]وحروب المعلومات، والتي ساعـد الحاسب الآلي وشبكـة الإنترنت على انتشارهـا وسهولة التخطيط لها، وسرعة ارتكابها، فمن الأمثلة على استعمال الإنترنت في الأعمال الإرهابية ما قام به أحد الأشخاص في مصر، عند إنشائه صفحة على الإنترنت تسمى شبكة الثورة، والتي قام باستغلالها من أجـل الترويـج لأفكار تلك الجماعـة ونشر بيانات وأسمـاء ضبـاط الشرطة ورجالها والتحريض على العنف قبلهم ونشر منشورات تحريضية ضد مؤسسات الدولة"[5]، لذا حكمت عليه محكمة الجنايات، حكماً حضورياً بتاريخ الخامس (05) من شهر جوان سنة 2016 بعقوبة السجن المشدد لمدة ثلاث سنوات، ومصادرة

1 ياسمينة بونعارة، الجريمة الإلكترونية، مجلة جامعة الأمير عبد القادر للعلوم الإسلامية، قسنطينة، العدد تسعة وثلاثون (39)، 21 جوان 2016، ص 18؛ يوسف أبو الحجاج، أشهر جرائم الكمبيوتر والانترنت، الطبعة الأولى، دار الكتاب العربي، القاهرة، مصر، 2010، ص 157.

2 تنص المادة (34) من القانون رقم 20-05، المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما، السالف الذكر، أنه: "دون الإخلال بالعقوبات الأشد، يعاقب بالحبس من خمس (5) سنوات إلى عشر (10) سنوات وبغرامة من 5.000.000 دج إلى 10.000.000 دج كل من ينشئ أو يدير أو يشرف على موقع إلكتروني أو حساب إلكتروني يخصص لنشر معلومات للترويج لأي برنامج أو أفكار أو أخبار أو رسوم أو صور من شأنها إثارة التمييز والكراهية في المجتمع."

3 تقرير لخلية الاستعلام المالي (CTRF) على مستوى وزارة المالية لسنة 2015 أسفر على وجود 1250 شبهة تبييض الأموال على مستوى البنوك، **انظر كذلك**: قارة ملاك، الجريمة المعلوماتية في القطاع البنكي وأساليب مكافحتها إشارة لحالة الجزائر، مجلة الحكمة للدراسات الإعلامية والاتصالية، تصدر عن مؤسسة كنوز الحكمة للنشر والتوزيع، العدد السابع، الجزائر، 2016، ص 422؛ عبد الفتاح بيومي حجازي، دراسة متعمقة عن جريمة غسيل الأموال عبر الوسائط الإلكترونية في التشريعات المقارنة، الطبعة الأولى، المركز القـومي للإصدارات القـانونية، مصر 2009، ص 40 وما بعدها؛ عبـد الفتاح بيومي حجازي، الجريمة في عصر العولمة "دراسة في الظاهرة الإجرامية المعلوماتية مع التطبيق على القـانون الإماراتي"، المرجع السابق، ص 31؛ باخويا دريس، وشنتير خضرة، أثر تطبيق مبدأ السرية المصرفية في محـاربة جريمة غسيل الأموال، مجلة القـانون والمجتمع، مخبر القانون والمجتمع، جامعة أحمد دراية أدرار، الجزائر، العـدد العـاشر، ديسمبر 2017، ص 164.

4 حكيم غريب، الجريمة الإلكترونية والجهود الدولية لمكافحتها، المجلة الجزائرية للدراسات السياسية، المدرسة الوطنية العليا للعلوم السياسية، المجلد الثاني، العدد الأول، الجزائر، 2015/09/03، ص 75.

5 حكم محكمة النقض، الدائرة الجنائية، في الطعن المقيد بجدول المحكمة برقم 29953 لسنة 86 القضائية، السالف الذكر.

المضبوطات وتحميله المصاريف. ومن الدوافع أيضاً الدوافع السياسية[1] والإيديولوجية، كما ترتكب الجرائم الإلكترونية بدافع المنافسة للاستيلاء على الأسرار التجارية. كما وأن الفعل الواحد قد يعكس دوافع متعددة خاصة إذا ما اشترك فيه أكثر من شخص انطلق كل منهم من دوافعه الخاصة والتي تختلف عن دوافع غيره[2].

ومن أمثلة الجرائم الإلكترونية التي تهدد الأمن القومي، ما وقع سنة 2000 من قبل أربعة تلاميذ بريطانيين والذين أرسلوا بريدا الكترونيا بعنوان تهنئة بمناسبة الأعياد إلى الرئيس الأمريكي حينها –بيل كلينتون– وطالبوا فيها بدفع مليون دولار وإلا سيفجرون البيت الأبيض، وبعد التحقيقات والعمليات التي قام بها مكتب التحقيقات الفيدرالية (FBI)، وبالتعاون مع شرطة اسكوتلانديارد، تم التوصل إلى أولائك التلاميذ؛ الذين تم حرمانهم من استخدام البريد الإلكتروني لمدرستهم خاصة بعد التأكد أن ما قاموا به كان مجرد مزحة[3]. وفي دراسة لـ"Vladimir Golubev" أجراها حول المجرمين في الجرائم المتصلة بالحاسب الآلي استنتج فيها بأن دوافع مجرمي الحاسب الآلي تختلف، إذ توصل إلى أن 66 % لديهم دوافع تجسسية[4]، و17 % لديهم دوافع سياسية، و7 % منهم لديهم فضول بحثي، و5 % منهم لديهم دوافع تتعلق بمشاهدة المواقع الجنسية[5].

1 يحياوي محمد، مخاطر القرصنة على الحكومة الإلكترونية، مجلة البحوث والدراسات العلمية، المركز الجامعي الدكتور يحي فارس، المدية، الجزائر، العدد الخامس (05)، جويلية 2011، ص 271.

2 سمير شعبان، الجريمة الإلكترونية، مقاربة تحليلية لتحديد مفهوم الجريمة والمجرم، مجلة دراسات وأبحاث، جامعة زيان عاشور، الجلفة، الجزائر، العدد الأول، تاريخ النشر: 2009/09/15، ص 126.

3 سامر سليمان الجبوري، جريمة الاحتيال الإلكتروني دراسة مقارنة، الطبعة الأولى، مكتبة زين الحقوقية والادبية، لبنان، 2018، ص 141.

4 أصبح المحمول من أحدث وأدق الوسائل الاستخباراتية في العالم وذلك عن طريق أنظمته الحديثة خاصة ERP,GPS التي يمكن اختراقها بسهولة، بسبب عدم تشفير معظم شبكات المحمول. **انظر:** هلالي عبد اللاه أحمد، التزام الشاهد بالإعلام في الجرائم المعلوماتية دراسة مقارنة، الطبعة الثانية، دار النهضة العربية، القاهرة، مصر، 2008، ص 21؛ شريفي الشريف، مدى احترام الحق في الخصوصية في الحسابات الإلكترونية على الانترنت، مجلة القانون والمجتمع، مخبر القانون والمجتمع، جامعة أحمد دراية، أدرار، الجزائر، العدد السابع، جوان 2016، ص 123؛ عبد الوهاب عمر البطراوي، مخاطر الهاتف المحمول (مجالها وأسبابها وعلاجها)، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 2003، ص.ص: 24-25.

5 مديحة فخري محمود محمد، المرجع السابق، ص 175؛ **نقلاً عن:**

- Vladimir Golubev, Criminal in Computer Related Crimes, Computer Crime, Research center, Availablhttp://www .polcyb .org,12/10/2009.

الباب الأول:
الآليات القانونية الإجرائية
لمكافحة الجريمة الإلكترونية

الباب الأول:
الآليات الإجرائية القانونية لمكافحة الجريمة الإلكترونية.

يعد التشريع اللبنة الأولى والأساسية التي يمكن من خلالها مكافحة الجريمة مهما كانت، فلا جريمة ولا عقوبة إلا بنص[1]، لذا نجد أن دولاً كثيرة حاولت وضع قوانين خاصة للتصدي لهذه الظاهرة الإجرامية، إذ تعد دولة السويد من بين أوائل الدول التي اتجهت إلى سن تشريعات قانونية جديدة خاصة بالجرائم الإلكترونية، إذ أصدرت سنة 1973 قانون سمي بقانون البيانات[2]، تليها الولايات المتحدة الأمريكية بقانون خاص بحماية أنظمة الحاسب الآلي سنة 1976، وأتبعته بقوانين أخرى[3]، كما قام المشرع الفرنسي بإصدار قانون خاص بالمعلوماتية والحقوق الشخصـية سـنة 1978، وأعقب ذلك بإصدار مرسوم في أواخر سنة 1981 يتعلق بتحديد بعض المخالفات المرتبطة بجرائم المعلومات، ثم أصـدر في سنة 1988 قانـوناً لحماية نظـم المعالجـة الآلية للمعطيات والمعلومات، واتبع ذلك بتعديلات لقانون العقوبـات[4] وقوانين أخرى في هذا المجال، كما قامـت بريطانيا عام 1981 بإصدار قانون لمكافحة التزوير والتزييف، عرفت من خلاله أداة التزوير ووسائط التخـزين الحاسوبيـة المتنوعـة أو أي أداة أخرى يتم التسجيل عليها سواء بالطـرق الإلكترونيـة أو التقليدية أو أي طرق أخرى[5].

ولأن الجرائم الإلكترونية تمـس كافة الدول دون استثناء؛ حرص المجلس الأوربي على التصدي لها من خلال اتفاقية بودابست الموقعة في الثالث والعشرين (23) من شهر نوفمبر سنة 2001

1 المادة الأولى من الأمر رقم 66-156، المتضمن قانون العقوبات، المعدل والمتمم، السالف الذكر.

2 عطوي مليكة، المرجع السابق، ص 18؛ منير محمد الجنبيهى، ممدوح محمد الجنبيهى، أمـن المعلومات الإلكترونية، دار الفكر الجامعي، الاسكندرية، 2005، ص 186.

3 الطيب بلواضح، الجهود الدولية لحماية البريد الإلكتروني جـنائيا، مجلة الحقوق والعلـوم الإنسانية، جامعة زيان عاشور، الجلفة، الجزائر، العدد تسعة عشر(19)، 2014/06/01، ص 226.

4 محمد أمين الرومي، المرجع السابق، ص 101؛ محمد أمين أحمد الشوابكة، جرائم الحاسوب والانترنت (الجريمة المعلوماتية)، المرجع السابق، ص18.

5 أما المشرع الانجليزي، فقد بادر إلى مواجهة المشكلات القانونية الناجمة عن تطور تقنيات المعلوماتية، بإفراده حماية خاصة للأطفال من الاستغلال الجنسي بقانون حماية الطفل لعام 1978، (Child protection ACT)، وأصدر قانوناً خاصاً يتعلق بإساءة استعمال الحاسوب سنة 1990، (computer abuse ACT)، كما كفل حماية الأفراد من مخاطر ثورة المعلومات في قانون العدالة الجنائية والنظام العام لعام 1994: محمد أمين احمد الشوابكة، جرائم الحاسوب والانترنت (الجريمة المعلوماتية)، المرجع السابق، ص 18.

والمتعلقة بالجرام الكوني (Convention sur la cyber criminalité, Budapest 23,X1.2001)، وذلك إيماناً من الدول الأعضاء في المجلس والدول الأخرى الموقعة على هذه الاتفاقية بالتغيرات العميقة التي حدثت بسبب الرقمية La numérisation، والتقارب La convergence والـعولمة المسـتمرة La mondialisation permanente للشـبكات المعلوماتية Des réseaux informatiques[1].

ولنفس السبب حرصت الأمانة العامة لمجلس وزراء الداخلية العرب على مكافحة هذه الجرائم بوضع إستراتيجية عربية تنبثق من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، التي اعتمدها مجلس وزراء الـداخلية الـعرب في القـاهرة في دورتـه الحـاديـة والثلاثين بتاريخ: 21 ديسمبر 2010[2]، والتي كانت الجزائر من بين الموقعين عليها سنة 2014؛ لأن بداية المشرع الجزائري مع الجرائم الإلكترونية كانت سنة 2004 من خلال تعديله وتتميمه لقانون العقوبات[3].

إلا أن النصوص القانونية مهما كثرت تبقى غير كافية في ظل غياب القواعد الإجرائية والمؤسساتية، فهذه القواعد مجتمعةً هي التي يمكن من خلالها تجسيد القانون على أرض الواقع؛ وإعطائه الديناميكية التي يحتاجها لمكافحة الجريمة والقبض على مرتكبها.

فهذا الباب هو الجزء الأول من الدراسة؛ والذي سندرس من خلاله الآليات القانونية الإجرائية لمكافحة الجريمة الإلكترونية، بحيث قسم هذا الباب إلى فصلين؛ تم التطرق فيهما لآليات التحقيق الجنائي التقليدية المعتمدة لمكافحة الجريمة الإلكترونية (الفصل الأول)، ثم القواعد الإجرائية الحديثة المتبعة من أجل جمع الأدلة الإلكترونية الناتجة عن الجريمة الإلكترونية حتى نتوصل إلى آليات المكافحة الأكثر فاعلية (الفصل الثاني).

1 هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها، الطبعة الأولى، دار النهضة العربية، القاهرة، 2007، ص 05.

2 محمد أحمد السويحلي، تكاثف الجهود العربية لمكافحة الجريمة الإلكترونية، مجلة الدراسات المالية والمصرفية، السنة الثالثة والعشرون، العدد الأول، الأردن، مارس 2015، ص 06.

3 الأمر رقم 66-156، المتضمن قانون العقوبات، السالف الذكر، المعدل والمتمم بالقانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 (الج.ر.ج رقم 71 ص.ص: 11 و12).

الفصل الأول:
آليات التحقيق الجنائي التقليدية المعتمدة لمكافحة الجريمة الإلكترونية

الفصل الأول:
آليات التحقيق الجنائي التقليدية المعتمدة لمكافحة الجريمة الإلكترونية.

الجرائم الإلكترونيـة نـوع من الإجرام المعاصر الذي يثير إشكالات عديدة من نواحي مختلفة، فالخصائـص التي تميزهـا عن غيرها من الجرائـم –كما أوضحناه سابقاً– ساهمت وبشكـل كبير في ذلك، مما صعب عملية اكتشافها وإثباتها، إضافة إلى أن هذا النوع من الإجرام يتسم مرتكبوه بالمكر والحيلة والدهاء، مستخدمين تقنيات معلوماتية عالية الكفاءة لتنفيذ جرائم الغش والاحتيال، ومختلف الجرائم الإلكترونية الخطيرة[1].

لذا فقد خُصصت لهذه الجرائـم قواعـد قانونيـة وإجرائيـة للتصدي لها تتناسب مع خصائصها؛ ويعد التحقيق الجنائي في الجرائم الإلكترونية مثال على تلك القواعد والإجراءات؛ فهو علم كسائر العلوم الأخرى له قواعد قانونية وفنية، بل هو فن ودراسة، خبرة وفراسة، صراع بين الحقيقـة والخيال، بين الصدق والضلال، وكم ضاعت الحقيقة في الصحف فقضي ببراءة مجرم آثم أو إدانة برئ نتيجة لتحقيق خاطئ أو لقصور فيه[2]. فالتحقيق الجنائي هو ذلك التعبير المجازي الذي يقصد من ورائه التحقيق في جميع الجرائم بمختلف تصنيفاتها؛ الجنايات والجنح والمخالفات وليـس فقط الجنايـات، فاقتران اسم التحقيق بمصطلح الجنائي يعود لأهمية التحقيق في الجنايات باعتبارها أعلى مراتب الجريمة من حيث التصنيف[3]، وأشدها من حيث الخطورة. وتعد آليات

1 عبد الفتاح حجازي، الإثبات الجنائي في جـرائم الكمبيـوتر والانتـرنت، المرجع السابق، ص 46، **نقلاً عن**: محمد محي الدين عوض، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات– الكمبيوتر–، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، 25–28 اكتوبر1993. **وكذلك**: هدى حامد قشقوش، جـرائم الكمبـيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، بحث مقدم لنفس المؤتمر السالف الذكر.

2 خالد ممدوح إبراهيم، فـن التحقيـق الجنائي في الجريمة الإلكترونيـة (دراسة مقارنة)، الطبعة الأولى، دار الفكـر الجـامعي، الإسكندرية، مصر، 2018، ص 18، **نقلاً عن**: محمد أنور عاشور، التحقيـق الجنائي، عالم الكتب للطباعة والنشر والتـوزيع، القاهرة، 1987، ص 02.

3 عبد الكريم خالد الردايدة، المعوقات التي تؤثر على سير التحقيق في مسرح الجريمـة، قسم البرامج التدريبية، كليـة لتدريب، الدورة التدريبية حول إجراءات التحري والمراقبة والبحث الجنائي، الرياض، السعودية، خلال الفترة من 05 إلى 16 جويلية 2012، ص 04.

التحقيق الجنائي إحدى السبل المهمة التي يمكن من خلالها الكشف عن الجريمة الإلكترونية والحصول على الدليل الإلكتروني خاصة إذا تمت بشكل صحيح ووفقاً للقانون.

ولأجل التطرق لمختلف النقاط المدروسة في هذا الفصل فقد تم تقسيمه إلى شقين؛ خصص الأول للدليل الإلكتروني وسلطة القاضي في تقديره (المبحث الأول)، والشق الثاني خصص لدراسة المعاينة والتفتيش ودورهمافي جمع الأدلة الإلكترونية (المبحث الثاني).

المبحث الأول:
الدليل الإلكتروني وسلطة القاضي في تقديره.

إن الأدلة هي سبيل من سُبل تحديد الوقائع ذات الصلة بذنب أو براءة الشخص المتهم والمبحوث عنه، "والأدلة الإلكترونيـة هي كل المـواد الإثباتيـة التي توجـد بشكـل إلكتـروني أو رقمـي، والتي تكون مخزنة أو عابرة، وقد تتخـذ شكل ملفـات حاسوبـية أو مـواد منقولـة أو سجلات أو بيانات فوقية أو بيانات شبكية"[1]، ولأن الأدلة الإلكترونية لها طابعها الخاص، أدى ذلك إلى تعدد التعاريف التي أُطلقت عليها، وإن كانت تصب كلها في اتجاه واحد، كما تنوعت أقسامهـا، واستلزم أمر قبولها والاعتداد بها أمام القضاء عدة شروط تتشارك في بعضها مع صفات أدلة الإثبات الأخرى، كالمشروعية واليقين، والبعد عن الشك والظن والتخمين، وإجبارية مناقشتها من طرف القاضي بشكل حضوري. خاصة ونحن أمام أدلة تتميز بصعوبة الوصول إليها وسهولة إخفائها وطمس آثارها.

ولأكثر تفصيل حول الموضوع قسمنا هذا المبحث إلى مطلبين؛ المطلب الأول يحمل عنوان: مفهوم الدليل الإلكتروني، والمطلب الثاني تحت عنوان: شروط صحـة الدليل الإلكتـروني وسلطـة القاضي في تقديره.

المطلب الأول: مفهوم الدليل الإلكتروني.

بالرغم من تعدد أنواع الأدلة الجنائية، إلا أن التقسيم الشائع لها يصنفها ضمن أربع مجموعات هي: الأدلة المادية، القولية، الفنية، والقانونية؛ وهي التي يحددها المشرع ويعين قوتها، كما أنها أدلة غير محصورة في المسائل الجنائية، والقاضي حر في تكوين قناعته من أي دليل في الدعوى كأصل عام، أما الأدلة الفنية فهي التي يقوم بها الفنيون والمختصون بشأن وقائع معينة، والمجموعة الثالثة وهي الأدلة القولية التي يصدرها أشخاص أدركوها بإحدى حواسهم، ومنها الاعتراف وأقوال الشهود، والمجموعة الرابعة وهي الأدلة المادية التي تجسدها الحالة القانونية التي تنشأ عن ضبط الأثر

1 فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، دراسة شاملة عن مشكلة الجريمة السيبرانية والتدابير التي تتَّخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدِّي لها، مقر الدراسة: فيينا، بتاريخ: 25-27 فبراير 2013. (UNODC/CCPCJ/EG.4/2013/2)، ص 12.

المادي لجريمة ما[1]، وهناك نوع جديـد من الأدلة أصبحنا نسمع عنها كثيراً، وهي الأدلة الإلكترونيـة، والتي تجـد أساسـها في العالم الافتراضي، وتقود إلى الجريمة الإلكترونية[2]؛ وهذه الأدلة خصصت لها عدة تعاريف فقهية وقانونية، وقسمت إلى مجموعات كما سيتم بيانه من خلال الفرعين المواليين.

الفرع الأول: تعريف الدليل الإلكترونـــي.

قبل التطرق إلى تعريف الدليل الإلكتروني، لابد أن نشير إلى أن المشرع الجزائري قرن بين مصطلحي الإلكتروني والإثبات في المادة 323 مكرر 1 من القانون المدني، وذلك في خضم تعديله للقانون السالف الذكر سنة 2005، حيث اعتبر أن الإثبات بالكتابة في شكلها الإلكتروني كالإثبات بالكتابة على الورق، بشرط أن يتم التأكد من هوية الشخص الذي أصدرها، وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها[3]، وهو نفـس الحكم الذي نجـده في القانون الفرنسي في المادة 1366 من القانون المدني الفرنسي[4].

تتنوع الأشكال التي يمكن أن يتخذها الدليل الإلكتروني، لذا تعددت التعاريف التي أطلقت عليه، إذ يرى بعضهم بأن الدليل الإلكتروني هو: "الدليل الصادر عن أجهزة الحاسب الآلي،

---

1 إلهام شهرزاد روابح، الدليل الرقمي بين مشـروعية الإثبات وانتهاك الخصوصية المعلوماتية، مجلة البحوث والدراسات القانونية والسياسية،كلية الحقوق والعلوم السياسية، جامعة لونيسي علي، البليدة 02، الجزائر، العـــدد العاشر (10)، جانفي 2017، ص.ص: 187-188.

2 طاق عفيفي صادق احمد، المرجع السابق، ص 275، **نقلاً عـــــن**:

- Amanda Hoey, Analysis of the police and criminale evidence act see.69/computer generated evidence-WEB, journal of carrent legal issues UK, 1996 Issue1, p1.

3 قانون رقم 05-10، المؤرخ في 13 جمادى الأولى عام 1426 الموافق 20 يونيو سنة 2005، يعدل ويتمم الأمر رقم 75-58 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975 والمتضمن القانون المدني، المعدل والمتمم، الصادر بالج.ر العدد 44. بتاريخ 26 يونيو سنة 2005، : المادة الرابعة والأربعون (44): "يتمم الأمر رقم 75-58 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975 والمذكور أعلاه، بالمادتين 323 مكرر و323 مكرر 1، وتحرران كما يأتي: المادة 323 مكرر: "ينتج الإثبات بالكتابة من تسلسل حروف أو أوصاف أو أرقام أو أية علامات أو رموز ذات معنى مفهوم، مهما كانت الوسيلة التي تتضمنها، وكذا طرق إرسالها". المادة 323 مكرر 1: "يعتبر الإثبات بالكـتابة في الشـــكل الإلكتروني كالإثبات بالكـتابة على الورق، بشرط إمكانية التأكد من هـــوية الشخص الذي أصـــدرها وأن تكون معدة ومحفوظة في ظروف تضـــمن سلامتها.".

4 Article 1366 du **Code civil**, Modifié par Ordonnance n°2016-131 du 10 février 2016 - art. 4 : « L'écrit électronique a la même force probante que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité. »

ويـكون في شـكل مجـال أو نبضات كهرومغناطيسية يمكن جمعها وتحليلها باستخـدام برامج وتطبيقات وتكنولوجيا خـاصة، وهو أيضاً مكون رقمي لتقديم معلومات في أشـكال متنوعـة مثل النصـوص المكتوبـة أو الصور أو الأصوات أو الأشكال أو الرسوم"[1]، كما يرى آخرون[2] بأنه: "برامج الحاسوب وبياناته التي تستخدم للإجابة عن الأسئلة الهامة حول الحادثة الأمنية"، كما أن الأدلة الإلكترونية تتواجد في شكل بيانات ومعلومات ذات هيئة الكترونية غير ملموسة، لا تدرك بالحواس العادية، بل يتطلب إدراكها الاستعانة بأجهزة ومعدات وأدوات الحاسبات الآلية (Hardware)، واستخدام نظم برامجية حاسوبية (Software).[3]

وفي إطار التعريف القانوني للدليل الإلكتروني، قام المشرع المصري بتعريفه في الفقرة العشرين (20) من المادة الأولى (01) من قانون تقنية المعلومات بقوله: "الدليل الرقمي: أي معلومات إلكترونية لها قـوة أو قيمـة ثبوتية مخزنة أو منقولة أو مستخرجة أو مأخوذة من أجهزة الحاسب أو الشبكات المعلوماتية وما في حكمـها، ويمكن تجميـعها وتحليـلها باستخدام أجهزة أو برامج أو تطبيقات تكنولوجية خاصة"[4]، ونظراً لأهمية الأدلة الإلكترونية في عملية الإثبات، فقد حثت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في المادة الثانية والعشرين (22) منها على أن كل

1 سلامة محمد المنصور، تطبيق مبدأ الاقتناع القضائي على الدليل الإلكتروني، أطروحة مقدمة لاستكمال متطلبات الحصول على درجة الماجستير في القانون، قسم القانون العام، كلية القانون، جامعة الإمارات العربية المتحدة، نوفمبر 2018، ص 06، **نقلاً عن**: محمد أحمد المنشاوي، سلطة القاضي الجنائي في تقـدير الدليل الإلكتروني، مجلة الحقوق، المجلد 36، العدد الثاني، الكويت، 2012، ص 515، **وعن**: أحمد فتحي سرور، الوسيـط في قانون الإجراءات الجنائية، دار النهـضة العربية، الطبعة الـسابعة، 1996، ص 747.

2 وردة شرف الدين، مجالات للمساعدة القضائية المتبادلة فيما يخص جمع الأدلة الرقمية – وفقا للاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 –، مجلة العلوم السياسية والقانون، المجلد الثلث (03)، العدد الخامس عشر (15)، المركز الديمقراطي العربي، المانيا، ماي 2019، ص 142، عن :

- MICHEAL.G. Solomon and others, *Computer Forensics jump start*, published by Wiley- Default, 2005, p :4.

3 فؤاد أمين السيد محمد، جرائم مراقبة المراسلات الإلكترونية "دراسة مقارنة"، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 2016، ص 111.

4 قانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات المصري، الصادر بالجر.ر.م، العدد 32 مكرر (ج) – السنة الحادية والستون، بتاريخ 3 ذى الحجة سنة 1439هـ، الموافق 14 أغسطس سنة 2018 م.

دولة ملزمة بتبني جميع التشريعات الداخلية والإجراءات الضرورية من أجل جمع الأدلة عن الجرائم بشكل إلكتروني[1].

الفرع الثاني: أقسام الدليل الإلكتروني.

لأن الدليل الإلكتروني، أو الدليل الرقمي (Digital evidence) قد يكون صورة رقمية (image) أو مطبوعة من أصل رقمي أو يكون متناً (text) لموضوع أو رسالة أو غيرها"[2]، فإنه من حيث المبدأ يجب أن يكون الدليل الإلكتروني مثل كل الأدلة الأخرى، تعامل بعناية وبطريقة تحافظ على قيمتها الاستدلالية، ولا يتعلق ذلك فقط بالسلامة البدنية لعنصر أو جهاز ما، ولكن أيضاً بالبيانات الإلكترونية التي يحتوي عليها، فقد تتطلب أنواعاً معينة من الأدلة الإلكترونية معاملة خاصة، كالجمع أو التغليف أو التحريز أو النقل بطريقة معينة حماية لتلك البيانات التي قد تكون عرضة للضرر أو التغيير إذا ما تعرضت لمجالات كهرومغناطيسية؛ مثل تلك التي تولدها الكهرباء الساكنة والمغناطيسات وأجهزة الإرسال الراديوية وغيرها من أنواع التشويش الإلكتروني[3].

فالمصادر المحتملة والممكنة للحصول على أدلة إلكترونية تتنوع وتختلف؛ وتختلف معها الأساليب الواجب إتباعها من أجل الحصول على تلك الأدلة الإلكترونية، فهذه الأخيرة قد تتواجد في القرص الصلب سواء الداخلي أو الخارجي، القرص المرن، الأقراص المضغوطة (CD) وأقراص الفيديو الرقمية (DVD)، (pen drives, flash drives,routers)، المودام، الهـواتف النقـالة، أشرطـــة التسجيـــل، الكاميرات، مشغلات (MP3)، (jaz/zip cartridges)، أجهزة الشبكات، الأجهزة المتصلة بخاصية البلوتوت، أجهزة الأشعة تحت الحمراء، أجهزة (Wifi)" وغيرها[4].

1 الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر سنة 2010، المصادق عليها بالمرسوم الرئاسي رقم 14-252، السالف الذكر: جاء في المادة الثانية والعشرين منه: "...، ج) جمع الأدلة عن الجرائم بشكل إلكتروني..."

2 محمد رضوان هلال، المحكمة الرقمية مفهومها- مقوماتها، دار العلوم للنشر والتوزيع، القاهرة، مصر، 2006، 91.

3 John Ashcroft, Electronic Crime Scene Investigation:, *A Guide for First Responders*, Written and Approved by the Technical Working Group for Electronic Crime Scene Investigation, Washington, July2001, p : 29.

4 أحمد محمد عبد الباقي، التحقيق الجنائي الرقمي، دار النهضة العربية، القاهرة، مصر، 2015، ص 257.

ولقد قسم بعضهم[1] الأدلة الإلكترونية إلى ثلاث مجموعات: أولها؛ السجلات المحفوظة والمكتوبة في جهاز الحاسب الآلي كملفات برامج معالجة الكلمات، ورسائل البريد الإلكتروني وغرف الدردشة. والمجموعة الثانية وهي السجلات التي تم إنشاؤها بواسطة الحاسب الآلي، والتي يعتبرها بعضهم من مخرجات الحاسب الآلي التي لم يلمسها الإنسان، مثل (log files)، وسجلات الهاتف وفواتير أجهزة السحب الآلي (ATM). أما المجموعة الثالثة فهي السجلات التي جزء منها تم حفظه بالإدخال، وجزء آخر تم إنشاؤه بواسطة الحاسب الآلي، ومن أمثلتها أوراق العمل التي يستعمل فيها برنامج (Excel)، والتي تمت معالجتها ببرنامج إجراء العمليات الحسابية، وهناك تقسيم آخر يتطابق مع التقسيم الذي قررته وزارة العدل الأمريكية لسنة 2002، والذي يقسم الأدلة الإلكترونية إلى: 1- أدلة رقمية خاصة بأجهزة الحاسب الآلي وشبكاتها، 2- أدلة رقمية خاصة بالشبكة العالمية للمعلومات الإنترنت، 3- أدلة رقمية خاصة ببروتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات، 4- أدلة خاصة بالشبكة العالمية للمعلومات"[2].

المطلب الثاني: شروط صحة الدليل الإلكتروني وسلطة القاضي في تقديره.

تتجمع بيانات ومعلومات في هيئة رقمية غير ملموسة لا تدرك بالحواس العادية لتكون أدلة إلكترونية، يتطلب إدراكها الاستعانة بأجهزة ومعدات وأدوات الحاسبات الآلية بحيث يكون بينها وبين الجريمة رابطة من نوع ما، وتتصل بالضحية على النحو الذي يحقق هذه الرابطة بينها وبين

1 خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص.ص: 178-179.

2 أحمد عبد الحكيم عبد الرحمن شهاب، نور عزم الميل بن ماربي، شـروط قبول الأدلة الإلكترونية أمام القاضي الجنائي الفلسطيني، مجلة العلوم السياسية والقانون، المركز العربي الديمقراطي للدراسات الإستراتيجية والسياسية والاقتصادية، ألمانيا، برلين، المجلد الثاني (02)، العدد السابع (07)، فبراير 2018، ص 126؛ **انظر أيضاً:**

- Comite européen de coopération juridique (CDCJ), *L'UTILISATION DES PREUVES ELECTRONIQUESDANS LES PROCEDURES CIVILES ET ADMINISTRATIVESET SON IMPACT SUR LES REGLES ET MODES DE PREUVE*, Etude comparative et analyse Rapport préparé par Stephen MASON avec le concours de Uwe RASMUSSEN, Strasbourg le 27 juillet 2016, sur le site : *https://rm.coe.int/16807007ca*, p: 10 : « Il existe trois types d'éléments de preuve qui pourraient être obtenus lors d'une procédure judiciaire: (i) les preuves en provenance de sites internet accessibles au public, tels que (cette listen'est qu'indicative) les blogs et les images publiées sur les réseaux sociaux; (ii) les preuves substantielles (ou probantes), comme l'e-mail ou des documents en format numérique qui ne sont pas rendus publics et détenus sur un serveur; (iii) l'identité présuméed'un utilisateur etdes données de trafic(«métadonnées») qui sont utiliséespour aider à identifierune personneen découvrantla sourcede la communication, mais pas le contenu. »

الجاني[1]، فعلى الرغم من صعوبة إثبات تلك الرابطة إلا أنها ليست مستحيلة، فعملية البحث عن الدليـل الإلكتروني تقف أمامها عدة عقبات يعود بعضها إلى طبيعة الجريمة الإلكترونية في حد ذاتها، وبعضها الآخر إلى مرتكبها وما له من ذكاء ومعرفة بالعالم الرقمي، الأمر الذي سهل عليه إخفاء الأدلة الإلكترونية بكل سهولة وبسرعة فائقة وبدون مساعدة من أحد.

وبالرغم من ذلك إلا أن الدول بتشريعاتها المختلفة لم تقف مكتوفة الأيدي حيال ذلك، بل خصصت آليات موضوعية وإجرائية ومؤسساتية من أجل مكافحة الجريمة الإلكترونية والوصول إلى الجاني واثبات جرمه بأدلة إلكترونية تتوفر فيها شروط معينة تضمن قبولها من قبل المحكمة وتساعد في تكوين عقيدة القاضي بشكل يسهل عليه إصدار حكمه في القضية المطروحة أمامه، لأن صعوبة الإثبات الجنائي لا يمكن أن تكون عقبة في سبيل التجريم، فالتجريم مسألة موضوعية والإثبات يتعلق بمسائل إجرائية ولا يمكن أن نجعل صعوبة الإثبات في بعض المسائل الجنائية سبباً في عدم التجريم[2]، وإفلات الجناة من العقاب.

لذلك، نتطرق في هذا المطلب إلى شروط صحة الدليل الإلكتروني (الفرع الأول)، ثم إلى سلطة القاضي في تقدير الدليل الإلكتروني (الفرع الثاني).

الفرع الأول: شروط صحة الدليل الإلكتروني

للدليل الإلكتروني أهمية بالغة في إثبات الجريمة الإلكترونية، وليس هي فحسب، بل تتعد تلك الأهمية إلى الجرائم التقليدية الأخرى كالاتجار بالمخدرات، غسيل الأموال، جرام القتل، الاختطاف وغيرها من الجرائم الأخرى التي تُستَخدم التكنولوجيا الحديثة في ارتكابها[3]، وحتى يحظى الدليل الإلكتروني بتلك الأهمية السابقة لابد من أن تتوفر فيه بعض الشـروط لكي يعتـد به في

1 تومي يحي، جرائم الاعتداء ضد الأفراد باستخدام تكنولوجيا الإعلام والاتصال، أطروحة من أجل نيل شهادة الدكتوراه علوم تخصص قانون، كلية الحقوق، جامعة الجزائر 01، الجزائر، السنة الجامعية 2017-2018، ص ص: 249-250، **نقلاً عن**:

- Eoghan Casey , *Digital évidence and Forensit science ,Computer and the internet ,Computer Crime* , 1st ed , acadimic Press, USA, 2000 p 9.

2 هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، مصر، إصدار 1992، ص 67.

3 بن طالب ليندا، الدليل الإلكتروني ودوره في الإثبات الجنائي (دراسة مقارنة)، أطروحة لنيل شهادة دكتوراه علوم تخصص قانون، قسـم الحقوق،كلـية الحقـوق والعلوم السـياسية، جامعة مولود معمري بتيزي وزو، الجزائر، تاريخ المناقشة 2019/01/23، ص 35.

الإثبات، وهو ما أكده المشرع المصري من خلال المادة (11) من قانون مكافحة جرائم تقنية المعلومات[1] حيث جاء فيها: "يكون للأدلة المستمدة أو المستخرجة من أجهزة أو المعدات أو الوسائط أو الدعامات الإلكترونية أو من النظام المعلوماتي أو من برامج الحاسب، أو من أي وسيلة لتقنية المعلومات ذات قيمة وحجية الأدلة الجنائية المادية في الإثبات الجنائي متى توافرت بها الشروط الفنية الواردة باللائحة التنفيذية لهذا القانون".

ونظراً لطبيعة الأدلة الإلكترونية الخاصة، والتي تفرض معاملة خاصـة ومتخصصة لهـذه الأخيرة، أوضحت مختلف التشريعات التي تطرقت لموضوع الأدلة الإلكترونية ضرورة إحاطتها بمجموع من الشروط التي قد تضفي عليها المصداقية وتقربها من الحقيقة وتجعلها مقبولة كأدلة إثبات في المواد الجنائية، ومن هذه الشروط:

1- أن يكون الدليل الإلكتروني المتحصل عليه له علاقة بموضوع الجريمة الإلكترونية؛ وهو شرط تمت الإشارة إليه في المادة (401) من قانون الإثبات الفيدرالي الأمريكي، والمعروف بمبدأ العلاقة الكاشفة (The Principal of Relevance)، حيث يتطلب هذا القانون أن يكون هناك علاقة من نوع ما بين الدليل وبين الواقعة محل الدعوى، ولإثبات تلك العلاقة الكاشفة يتطلب الأمر شرطاً آخر، وهو مطابقة الدليل الإلكتروني المستخرج من الكمبيوتر للأصل الموجود بداخله، وليكون ذلك لابد من ألا يكون هناك ادعاء أو دفع بأن البيانات غير صحيحة بسبب عدم دقة عمل الكمبيوتر[2].
2- ثاني شرط يلزم وجوده في كل الأدلة بشتى أنواعها وخاصة الجنائية منها، ألا وهو شرط المشروعية، وبدايته أن تكون الجهة المختصة بجمعه قد التزمت بالشروط المحددة قانونا، انطلاقاً من الحصول على إذن النيابة العامة للقيام بالإجراءات اللازمة للحصول عليه كالتفتيش والضبط؛ فإذن النيابة العامة هي مسألة جوهرية في المواقع التي فرضتها القوانين للتأكد من سلامة الإجراءات وحفاظاً على الحقوق والحريات، وضماناً لصدق مضمون الدليل الإلكتروني، ففي حالة التلبس قد لا يتوفر الإذن حين التفتيش، ويكون بذلك الإجراء

1 قانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات المصري، السالف الذكر.

2 خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص 188، **نقلاً عن**: عمر محمد ابو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، رسالة دكتوراه حقوق، عين شمس، القاهرة، 2004، ص 992؛ سلامة محمد المنصور، المرجع السابق، ص 51.

صحيحاً، وهو ما استقر عليه الفقه والقضاء في مصر حيث أُعطي الحق لمأمور الضبط القضائي في تفتيش الأجهزة التقنية الموجودة بحوزة المتهم بناءً على قبض صحيح وتطبيقاً لذلك: "قضت المحكمة الاستئنافية بصحة الدليل المستمد من تفتيش جهاز حاسوب ضبط بحوزة المتهم نتيجة لواقعة تلبس، وذلك في قضية تتلخص وقائعها أن أحد البنوك تقدم ببلاغ ضد مجهول لقيامه بسرقة أرقام بطاقات الائتمان الخاصة ببعض العملاء واستخدامها في شراء البضائع عبر مواقع التسوق الإلكترونية، حيث تم ضبط المتهم حال استلامه لتلك البضائع وضبط بحوزته حاسوب محمول وبفحصه عثر على الرسائل المتبادلة بين المتهم ومواقع التسوق وكذا الآلاف من بيانات البطاقات الائتمانية المختلفة"[1]، وجاء في حكم آخر عن محكمة النقد المصرية: "أن الحكم قد أفصح عن اطمئنان المحكمة إلى أن ما تم ضبطه بمعرفة رجال الشرطة بحوزة المتهمين، هو ما تم عرضه على النيابة العامة، وما تم عرضه بجلسات المحاكمة، هو ما أرسـل إلى المعامل الفنية، وكان قضاء المحكمة قد استقر على أنه متى كانت محكمة الموضوع قـد اطمأنت إلى أن ما تم ضبطه هو الذي أرسل للمعامل الفنية، واطمأنت كذلك إلى النتيجة التي انتهت إليها المعامل الفنية، فلا تثريب عـليها إن هي قـضت في الدعوى بناءً على ذلك" [2].

ويتبين من خلال ذلك أن الحصول على الدليل الإلكتروني يجب أن يتم بطرق مشـروعة تدل على الأمانة والنزاهة، إذ لا يصح التعويل على الدليل المستمد من إجراءات المراقبة والتفتيش، التي قام بها الضابط دون أن يُندب من النيابة العامة، أو أن يكون الإذن بالتفتيش صادراً من جهة غير مختصة أصلاً[3]، فعدم احترام الشروط القانونية يجعل من الدليل الإلكتروني دليلاً باطلاً بطلاناً مطلقاً؛ لأن طريقة الحصول عليه تمت مخالفة لمبدأ المشروعية

1 حكم في قضية رقم 10123 لسنة 2014 جنح قسم اول اكتوبر والمستأنفة برقم 21093 لسنة 2014 جنوب الجيزة، **نقلاً عن**: مصطفى على خلف، الضوابط الإجرائية لجرائم التقنية الحديثة (دراسة مقارنة)، نادي القضاة، مصر، 2017، ص 149.

2 حكم محكمة النقـض المصرية، الدائرة الجنائية، الأربعاء (أ)، في الطعـن المقيد بجدول المحكمة رقم 29658 لسنـة 86 القضائيـة، في الجلسة العلنية المنعقدة بدار القضاء العالي، القاهرة، في 12 رمضان سنة 1438هـ الموافق 07 جوان 2017، ص 22.

3 هشام زوين، التجسس والتنصت (مراقبة التيلفون والموبايل وتسجيل المكالمات والتصوير وتتبع الرسائل الإلكترونية عبر شبكة الانترنت ونشر الأفلام المخلة بالآداب وتداولها بالموبايل)، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، مصر، 2014، ص 152؛ سوزان نوري فقي محمد، الإثبات في جرائم الانترنت في القانون العراقي والقانون المقارن، رسالة مقدمة لنيل درجة الماجستير في الحقوق، قسم الدراسات العليا، كلية الحقوق، جامعة المنصورة، مصر، 2015، ص 64.

الذي يفرضه القانون[1]، ففي هولندا يتم استبعاد حتى الملفات المسجلة لدى الشرطة إذا تم الحصول عليها بطريقة غير مشروعة[2]، في حين قبلت محكمة في مقاطعة (KOFV) باليابـان دليـلاً نتـج عن عمليـة تنـصت، مبينة أنها تَعُده مشروعاً إذا ما دعت إليه ضرورة التحريات، وكان بالإمكان الأخذ بعين الاعتبار الإجراءات المستخدمة في تلك التحريات[3]، أما في القانون الفرنسي فإن الأدلة الإلكترونية المقبولة هي الأدلة التي أخذ بها المشرع، ويقبل بها القضاء في إطار مجموعة من الشروط؛ من أهمها أن يتم الحصول عليها بطريقة شرعية ونزيهة، لذا حكمت محكمة النقض الفرنسية بأن أشرطة التسجيل الممغنطة التي يكون لها قيمة دلائل الإثبات يمكن أن تكون صالحة للتقديم أمام القضاء الجنائي"[4]، إذن فالدليل الإلكتروني حتى يكون مشروعاً يجب أن يستوفي شروط صحته وعناصره الجوهرية التي نص عليها القانون، وأن لا يكون وليد إجراءات غير مشروعة وباطلة[5].

1 علاء محمود يسن حراز، الحماية الجنائية للمعلومات المعالجة آليا "دراسة مقارنة بين القانون الوضعي والشـريعة الإسـلامية"، رسالة مقدمة لنيل درجة الدكتوراه في الحقوق، قسم القانون الجنائي، كلية الحقوق، جامعة عين شمس، مصر، 2015، ص 446، **نقلاً عـن**: رمزي رياض عوض، مشروعية الدليل الجنائي في مرحلة المحاكمة وما قبلها "دراسة تحليلية تاصيلية مقارنة"، دار النهضة العربية، القاهرة، 1997، ص 85 وما بعدها؛ **ونقلا عن**: أحمد عوض بلال، قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائية المقارنة، دار النهضة العربية، القاهرة، 1994، ص 16 وما بعدها؛ هلال أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دار النهضة العربية، القاهرة، 2008، ص 118؛ لعوارم وهيبة، مشروعية الدليل الإلكتروني الناشئ عن التفتيش الجنائي، مجلة الفقه والقانون، العدد العشرون (20)، المغرب، يونيو 2014، ص 104.

2 لؤي عبد الله نوح، مدى مشروعية المراقبة الإلكترونية في الإثبات الجنائي وحجية مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي وعوامل حجية الصورة والصوت في الإثبات الجنائي "دراسة مقارنة"، الطبعة الأولى، مركز الدراسات العربية للنشر والتوزيع، الجيزة، مصر، 2018، ص 49؛ أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات –دراسة مقارنة–، الطبعة الثانية، دار النهضة العربية، القاهرة، 1989، ص ص 93-94.

3 محمد الأمين البشري، العدالة الجنائية ومنع الجريمة "دراسة مقارنة"، الطبعة الأولى، أكاديمية نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، 1997، ص 79.

4 فؤاد احمد حسين السايس، الجريمة المعلوماتية، بحث مقدم للحصول على درجة الماجستير في القانون، قسم البحوث والدراسات القانونية، معهد البحوث والدراسات العربية، القاهرة، مصر، 2015، ص 338، **أشار إليه كذلك**: هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دار النهضة العربية، القاهرة، مصر، 2006، ص 42-43.

5 ياسر حسين بهنس، الإثبات بالوسائل العلمية الحديثة وسلطة القاضي الجنائي في تقديرها، دار النهضة العربية، القاهرة، مصر، 2017، ص 81؛ يوسف بن سعيد بن محمد الكلباني، الحماية الجزائية للبيانات الإلكترونية في التشريعين العماني والمصري (دراسة مقارنة)، الطبعة الأولى، دار النهضة العربية، القاهرة، 2017، ص 426.

3- أما الشرط الثالث فهو أن تكون الأدلة الإلكترونية يقينية؛ أي بعيدة عن الظن والتخمينات، ومفاد ذلك أن لا يكون الدليل قابلا للشك، وإذا كان كذلك فإن الشك يفسر لصالح المتهم[1]، فهذا الشرط يوجب على القاضي الجنائي تحري الحقيقة، إما بمعرفته الحسية التي يدركها بحواسه، أو بالمعرفة العقلية مستعملاً المنطق للوصول إلى التحليل والاستنتاج الصحيحين مبتعداً عن الذاتية محكماً عقله وضميره من أجل الوصول إلى الحقيقة[2]، وهو ما أكدته الأحكام القضائية المختلفة،كحكم المحكمة العليا لسلطنة عُمان، والذي جاء فيه: "لمحكمـة الموضوع سلطة واسعة في سبـيل تقصي ثبوت الجرائم أو عدم ثبوتها وتكوين عقيدتها من جميع الأدلة المطروحة عليها بطريق الاستقراء والاستنتاج ما دام استخلاصها سليما لا يخرج من الاقتضاء العقلي والمنطقي"[3].

4- والشـرط الرابع الذي يجب توفره في الدليل الإلكتروني هو أن تتم مناقشته في جلسة الحكم، وهـو ما يعبر عنه بشرط "وضعية الدليل"، أي أن يكـون للـدليل أصـل ثـابت في أوراق الدعوى، ثم يطرح للمناقشة أثناء المحاكمة، وليس معنى ذلك أن تتم مناقشة ذلك الدليل علناً، بل يكفي أن يوضع في ملف الدعوى الموضوعة تحت نظر القاضي، وأن يُتاح للخصوم الاطلاع عليه ومناقشته إن شاؤوا[4]، عملاً بالفقرة الأخيرة من المادة (212) من قانون

1 ممدوح حسن مانع العدوان، ونادر عبد الحليم السلامات، مشـروعية وحجية الدليل المستخلص من التفتيش الإلكتـروني في التشريع الجزائي الأردني، مجلة دراسات، حقل علوم الشريعة والقانون، عمادة البحث العلمي، الجامعة الأردنية، المجلد الخامس والأربعون (45)، العدد الرابع (4)، الملحق الثاني (2)، الأردن، 2018، ص 64، **نقلاً عن**: الصغير جميل عبد الباقي، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، 2001، ص 17؛ أبـو عامر محمد زكى، الإثبات في المـواد الجنائية، الفنية للطباعة والنشر، الإسكندرية، مصر، 1985، ص 156 وما بعدها؛ نور الهـدى محمودي، حجيـة الدليل الرقمي في إثبات الجريمة المعلوماتية، مجلة الباحث للدراسات الأكاديمية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر (جامعة باتنة 1)، الجزائر، العدد الحادي عشر (11)، جوان 2017، ص 919.

2 أحمد عبد الحكيم عبد الرحمن شهاب، نور عزم الميل بن ماريني، المرجع السابق، ص 131؛ خالد حمد، القناعة القـضائية في مجال تقدير الأدلة، مجلة البحثية، العدد الثالث، الرباط، المغرب، ربيع 2015، ص 136.

3 حكم جلسة المحكمة العليا المؤرخ في: 2002/06/10 الطعون رقم: 74 و86 و84 لعام 2002، **أشار إليه**: يوسف بن سعيد بن محمد الكلباني، المرجع السابق، ص 459.

4 مستاري عادل، المنطق القضائي ودوره في ضمان سلامة الحكم الجزائي، رسالة مقدمة لنيل شهادة دكتوراه العلوم في الحقوق، فرع القانون الجنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر، السنة الجامعية 2010-2011، ص 63، **نقلاً عن**: ماروك نصر الدين، محاضرات في الإثبات، الجزء الأول، دار هومة، الجزائر، 2003، ص 638.

الإجراءات الجزائية الجزائري، والتي جاء فيها: "ولا يسوغ للقاضي أن يبني قراره إلا على الأدلـة المقدمة له في معرض المرافعات والتي حصلت المناقشـة فيها حضورياً أمـامه"[1]، وهو نفس الحكم أقرته المادة (302) من قانون الإجراءات الجنائية المصري[2]، والمادة (287) من قانون المسطرة الجنائية المغربي[3]، وكذا المادة (427) من قانون الإجراءات الجنائية الفرنسي[4]، مع العلم أن الأطراف لهم كامل الحرية في أن يقدموا للمحكمة ما توفر لديهم من وسائل إثبات، شرط أن تناقش أمام المحكمة حتى يحصل القاضي الناظر في القضية إلى اقتناع في الدعوى المعروضة عليه[5].

وهذا ما يستخلص أيضاً من الأحكام القضائية مثل حكم محكمة النقض المصرية لسنة 2017 بقولها: "...وكان من المقرر أن المحكمة ليست ملزمة بالتحدث في حكمها إلا عن الأدلة ذات الأثر في تكوين عقيدتها، وكان من المقرر –أيضاً– أن الأدلة في المواد الجنائية إقناعية، وللمحكمة أن تلتفت عن دليل النفي ولو حملته أوراق رسمية –وفق المبدأ السالف سرده– ولا عليها أن تتعقبه في كل جزئية من جزئيات دفاعه؛ لأن مفاد التفاتها عنها أنها أطرحته"[6].

1 الأمر رقم 66-155، المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966، المتضمن قانون الإجراءات الجزائية الجزائري المعدل والمتمم، المنشور في الج ر عدد 48 المؤرخة في 10 يونيو 1966، الصفحة 622.

2 قانـون الإجراءات الجنائية المصري (طبقا لأحدث التعـديلات بالقانون 95 لسنة 2003)، الصادر بالقانون رقم 150 لسنة 1950، المادة 302 (معدلة بالقانون رقم 37 لسنة 1972، الج.ر.م رقم 39 الصادر في 1972/9/28): "يحكم القاضي في الدعوى حسب العقيدة التي تكونت لديه بكامل حريته، ومع ذلك لا يجوز له أن يبنى حكمه على أي دليل لم يطرح أمامه في الجلسة. وكل قول يثبت أنه صدر من أحد المتهمين أو الشهود تحت وطأة الإكراه أو التهديد به يهدر ولا يعول عليه".

3 قانون المسطرة الجنائية المغربي،كما تم تعديله وتتميمه بمقتضى القانون رقم 23.05 والقانون رقم 24.05، الج.ر عدد 5374 بتاريخ 28 من شوال 1426 (فاتح ديسمبر2005)، المادة 287: "لا يمكن للمحكمة أن تبني مقررها إلا على حجج عرضت أثناء الجلسة ونوقشت شفهياً وحضورياً أمامها".

4 Article 427 du Code de procédure pénale : « ... Le juge ne peut fonder sa décision que sur des preuves qui lui sont apportées au cours des débats et contradictoirement discutées devant lui. »

5 عبد الحكيم الحكماوي، المرجع السابق، ص 148.

6 حكـم محكمة النقض المصريـة، الدائرة الجنائية، الأربعاء (أ)، في الطعن المقيد بجدول المحكمـــة رقم 29658 لســنة 86 القضائية، السالف الذكر، ص 21.

الفرع الثانـي: سلطة القاضي في تقدير الدليل الإلكترونـي.

يعرف الإثبات الجنائي على أنه: "إقامة الدليل على وقوع الجريمة لدى السلطات المختصة بالإجراءات الجنائية على حقيقة واقعة ذات أهمية قانونية وذلك بالطرق التي حددها القانون"[1]، لذا يعد من أهم مواضيع الإجراءات الجنائية؛ والتي بها ترسم طرق وضوابط كشف الجريمة وإقامة الأدلة على وقوعها، ونسبتها إلى فاعلها، دون أن ننسى الدور المهم الذي يلعبه القاضي في كشف الحقيقة والوصول إلى حل للدعوى المعروضة عليه، وقد تختلف سلطته التقديرية في الأخذ بالأدلة المعروضة عليه على حسب نظام الإثبات المتبع، ففي الساحة القانونية هنالك ثلاثة أنظمة رئيسية للإثبات، تحاول كل منها أن تفرض سيادتها على التشريعات الإجرائية المختلفة: وهذه الأنظمة هي: 1- نظام الأدلة القانونية أو النظام المقيد، 2- نظام حرية الإثبات أو نظام الاقتناع الذاتي للقاضي، 3- نظام الإثبات المختلط[2]، فرغم اختلاف تلك الأنظمة إلا أن هدفها واحد وهو إثبات الجرائم بشتى أنواعها[3].

إن قبول الدليل الإلكتروني كوسيلة من وسائل الإثبات مسألة حسمتها مختلف التشريعات التي أعطته قيمة وحجية الأدلة الجنائية المادية في الإثبات الجنائي متى توافرت فيه الشروط المحددة قانوناً ومذكورة سالفاً، ومن تلك التشريعات كما تمت الإشارة إليه التشريع المصري من خلال مواد قانون مكافحة جرائم تقنية المعلومات المصري لسنة 2018، وخاصة المادة (11) منه، فهذا الأمر يعد إضافة في مجال الإثبات الجنائي، لأنه ولأول مرة في التشريع الجنائي المصري وفي أدلة الإثبات يكون للدليل الإلكتروني حجية الإثبات[4].

1 لؤي عبد الله نوح، المرجع السابق، ص 26، **نقلاً عن:** محمود نجيب حسني، الاختصـاص والإثبات في قانون الإجراءات الجنائية، دار النهضة العربية، مصر، 1992، ص 53.

2 لأكثر تفاصيل يمكن الاطلاع على: فتوح الشاذلي، عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون (دراسة مقارنة)، منشورات الحلبي الحقوقية، بيروت، لبنان، 2003، ص 385.

3 حكم محكمة النقض المصرية، الدائرة الجنائية" غرفة المشورة"، في الطعن المقيد بجدول المحكمة رقم 25992 لسنة 84 القضائية، السالف الذكر: "... لما هو مقرر إن الجرائم على اختلاف أنواعها إلا ما استثني قانوناً بنص خاص جائز إثباتها بكافة طرق الإثبات ومنها البينة وقرائن الأحوال ...."

4 القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات، السالف الذكر.

ومن التشريعات أيضاً التي اهتمت بهذا الموضوع الولايات المتحدة الأمريكية التي أصدرت عدة قوانين تنظم الإثبات الجنائي، منها تشريع صدر في ولاية كاليفورنيا عام 1983، والذي اعتبر أن النسخ المستخرجة من البيانات التي يحتويها الحاسب الآلي تعد أفضل الأدلة لإثبات هذه البيانات، وسنة بعدها صدر في ولاية "أيوا (IOWA)" قانون الحاسب الآلي، والذي يقبل بمخرجات الحاسب الآلي كأدلة إثبات بالنسبة للبرامج والبيانات المخزنة فيه، وهذا ما أكده القضاء الأمريكي في أحكامه المختلفة على أن الأدلة الإلكترونية المتحصل عليها من أجهزة الحاسب الآلي يجب أن تكون مقبولة كأدلة إثبات، ما دام هذا الأخير يؤدي وظائفه بصورة سليمة وكان القائم عليه تتوفر فيه الثقة والطمأنينة[1].

تطبيقاً لمبدأ حرية الإثبات الجنائي، أصبح بالإمكان إثبات الجرائم بكل طرق الإثبات الجائزة قانونا، والمنصوص عليه في المواد القانونية؛ كالفقرة الأولى من المادة (212) من ق.إ.ج.ج: "يجوز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعاً لاقتناعه الخاص. ... "[2]، وكذا الفقرة الأولى من المادة (302) من ق.إ.ج.م[3]، والمادة (286) من ق.م.ج.م[4]، وكذا الفقرة الأولى من المادة (427) من ق.إ.ج.ف[5].

1 إحسان طبال، النظام القانوني للتحقيق الدولي في جرائم الكمبيوتر، أطروحة دكتوراه في الحقوق، كلية الحقوق، جامعة الجزائر 01، الجزائر، السنة الجامعية 2013-2014، ص 130؛ خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص ص: 199-200، **وكذلك**: هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دار النهضة العربية، القاهرة، 1997، ص 55، **نقلاً عن**:

- Rostoker Michaek D, and Rines Robert H, *Computer Jurisprudence Legal Responses to Information Revolution*, Ocean Publication, INC, 1986, p 320.

2 الأمر رقم 66-155، المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966، المتضمن قانون الإجراءات الجزائية الجزائري المعدل والمتمم، المنشور في الج ر عدد 48 المؤرخة في 10 يونيو 1966، الصفحة 622.

3 المادة 302 من قانون الإجراءات الجنائية المصري السالف الذكر، والتي تنص: "يحكم القاضي في الدعوى حسب العقيدة التي تكونت لديه بكامل حريته، ...".

4 المادة 286 من قانون المسطرة الجنائية المغربي، السالف الذكر، والتي تنص على أن: "يمكن إثبات الجرائم بأية وسيلة من وسائل الإثبات، ما عدا في الأحوال التي يقضي القانون فيها بخلاف ذلك، ويحكم القاضي حسب اقتناعه الصميم ويجب أن يتضمن المقرر ما يبرر اقتناع القاضي وفقاً للبند 8 من المادة (365) الآتية بعده. إذا ارتأت المحكمة أن الإثبات غير قائم صرحت بعدم إدانة المتهم وحكمت ببراءته."، وجاء في الفقرة الثامنة (08) من المادة (365) من نفس القانون ما يلي: "...8- الأسباب الواقعية والقانونية التي ينبني عليها الحكم أو القرار أو الأمر ولو في حالة البراءة؛ ...".

5 Article 427 du Code de procédure pénale: « Hors les cas où la loi en dispose autrement, les infractions peuvent être établies par tout mode de preuve et le juge décide d'après son intime conviction.... ».

كما نصت أحكام قضائية عديدة على هذا المبدأ، مثلما هو الحال في حكم محكمة التمييز الأردنية التي أكدت على أن الأدلة في المسائل الجزائية اقتناعية بما فيها اعتراف المتهم الصادر بطوعه ورضاه[1]، وبناءً عليه فإنه يمكن للمحكمة أن تلتفت عن دليل النفي ولو حملته أوراق رسمية مادام يصح في العقل والمنطق أن يكون غير ملتئم مع الحقيقة التي اطمأنت إليها من باقي الأدلة القائمة في الدعوى[2]. فكل تلك المواد والأحكام بينت أنه يمكن للقاضي أن يُكون اقتناعه الشخصي من أي دليل يطرح أمامه في الدعوى، ويصدر حكمه تبعاً لاقتناعه الخاص، إذا لم يكن مفروضاً عليه دليل معين بموجب القانون[3]، فاقتناع القاضي هو اقتناع عقلي (de une convicition raison) ومنطقي يجد مصدره في العقل لا في العاطفة باعتباره عملاً ذهنياً (un travail intellectuel) يُحصله القاضي في صمت وفي مناخ من الصدق وسلامة السوية[4].

لذا فإنه في نظر الفقه الفرنسي فإن حجية الدليل الإلكتروني لا تثير مشكلة، فالأساس هو حرية القاضي في تقدير تلك الأدلة الناشئة عن الآلة مثل أجهزة التصوير وأشرطة التسجيل، وأجهزة التنصت، فله وحده أن يقبلها أو يطرحها رغم قطعيتها من الناحية العلمية[5]، فقبول المخرجات لا يعني الإلزام بصحة البيانات الواردة فيها، إذ يميز النظام الانجلـيزي بدقة بين مسألة قبول الدليل؛ وهي مسالة ينظمها القانون، ومسألة قوة الدليل (The weight of evidence) وهي

1 تمييز جزء رقم 64/52، مجلة نقابة المحامين، سنة 1965، **نقلاً عن**: فؤاد أحمد حسين السايس، الجريمة المعلوماتية، بحث مقدم للحصول على درجة الماجستير في القانون، قسم البحوث والدراسات القانونية، معهد البحوث والدراسات العربية، القاهرة، مصر، 2015، ص 335.

2 حكم محكمة النقض المصرية، الدائرة الجنائية، في الطعن المقيد بجدول المحكمة رقم 8426 لسنة 87 القضائية، في الجلسة العلنية المنعقدة بدار القضاء العالي بمدينة القاهرة، في يوم السبت 04 نوفمبر سنة 2017.

3 تومي يحي، المرجع السابق، ص 247؛ رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة مقدمة لنيل شهادة الدكتوراه علوم في القانون الخاص، قسم القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، الجزائر، السنة الجامعية 2017-2018، ص 267.

4 خالد حمد، القناعة القضائية في مجال تقدير الأدلة، مجلة البحثية، العدد الثالث، الرباط، المغرب، ربيع 2015، **نقلاً عن**: محمد زكي أبو عامر، الإثبات في المواد الجنائية –محاولة فقهية وعملية لإرساء نظرية عامة–، دار الجامعة الجديدة، الإسكندرية، 2011، ص 187.

5 حازم محمد حنفي، المرجع السابق، ص 155؛ هلالي عبد اللاه أحمد، التزام الشاهد بالإعلام في الجرائم المعلوماتية دراسة مقارنة، المرجع السابق، ص 44.

الاقتنـاع بصحتـه في ثبوت الواقعـة، وهذه مسألة متروكة تماماً للاقتناع الحر للقاضي أو المحلفين[1]، وذلك على الرغم من صـعوبة الإثبات في الجريمة الإلكترونية لسهولة إخفاء الدليل الإلكتروني والعبث والتلاعب بمخرجات الطابعة وبيانات الحاسوب التي قد تشكل أدلة إلكترونية[2].

فمن المقرر أن الأحكام يجب أن تبنى على الأدلة التي يقتنع منها القاضي بإدانة المتهم أو ببراءته، صادراً في ذلك عن عقيدة يحصلها هو مما يجريـه مـن تحقيق، مستقلاً في تحصيل هذه العقيدة بنفسه، لا يشاركه فيها غيره، ولا يصح في القانون أن يدخل في تكوين عقيدته بصحة الواقعة التي أقام عليها قضاءه، أو بعدم صحـتها حكماً لسـواه، وكان من المقـرر كذلك أنه وإن كان يجوز للمحكمـة أن تعـول في تكوين عقيدتها على التحريات بحسبانها قرينة تعزز ما ساقته من أدلة، إلا أنها لا تصلح بمفردها أن تكون دليلاً كافياً بذاته، أو قرينـة مستقلة على ثبوت الإتهام، وهي من بعد لا تعدو أن تكون مجرد رأي لصاحبها، يخضع لاحتمالات الصحة والبطلان والصدق والكذب، إلى أن يُعرفَ مصدرها ويتحدد، حتى يتحقق القاضي بنفسه من هذا المصـدر، ويستطيع أن يبسط رقـابته على الدليـل، ويقدر قيمته القانونية في الإثبات[3]، فالمحكمة تتحرى بنفسها "...ذلك بأن الأحكام الجنائية يجب أن تنبني على الأدلة التي يقتنع منها القاضي بإدانة المتهم أو ببراءته صادراً في ذلك عن عقيدة يحصلها هو مما يجريه من التحقيق مستقلاً في تحصيل هذه العقيدة بنفسه لا يشاركه فيها غيره ولا يصح في القانون كما فعل الحكم أن يدخل في تكوين عقيدته بصحة الواقعة التي أقام قضاءه عليها أو بعد صحتها حكماً لسواه فإن الحكم يكون معيباً بالقصور الموجب لنقضه..."[4]، ولكن الطابع التقني الذي تتميز به الجريمة الإلكترونية قد يدفع القاضي في بعض الأحيان إلى الاستعانة بالخبرة لتوضيح الصورة حول مسالة ما.

1 سيد أحمد محمود، إلكترونية القضاء والقضاء الإلكتروني وإلكترونية التحكيم والتحكيم الإلكتروني " دراسة مقارنة"، دار الفكر والقانون للنشر والتوزيع، المنصورة، مصر، 2015، ص 44.

2 عمر محمد بن يونس، التحكيم في جرائم الحاسوب وردعها (المراقبة الدولية للسياسة الجنائية)، دار النهضة العربية، مصر، 2008، ص 96.

3 حكـم محكمـة النقـض المصرية، الدائرة الجنائية، الأربعاء (أ)، في الطعـن المقيد بجدول المحكمة رقم 29658 لسنة 86 القضائية، في الجلسة العلنية المنعقدة بدار القضاء العالي بمدينة القاهرة، في يوم الأربعاء 12 رمضان سنة 1438هـ الموافق 07 جوان 2017، ص 28.

4 حكم محكمة النقض المصرية، في الطعن المقيد بجدول المحكمة رقم 3860 لسنة 57 القضائية، في الجلسة العلنية المنعقدة بدار القضاء العالي بمدينة القاهرة، في يوم الثلاثاء 14 يناير سنة 1988.

كما "يمكن تسليم البيانات التي تم جمعها لجهة أخرى أو شركة متخصصة للقيام بعملية الفحص والتحليل بالنيابة عن المؤسسة التي قامت بالحصول على الدليل في حال لم تكن لديها الإمكانيات للقيام بكامل عملية التحقيق بعد هذه الخطوة[1]، فالاستعانة بالخبير في الجرائم الإلكترونية هو أمر سمح به القانون وأيدته الأحكام القضائية بقولها: "إذا كانت المسألة المعروضة على المحكمة من المسائل الفنية البحتة التي لا تستطيع المحكمة أن تشق طريقها إليها لإبداء الرأي فيها، فالمحكمة ملزمة بندب خبير، بل إنها ملزمة بالأخذ برأي هذا الخبير، إذا كان العلم قد انتهى برأي قاطع إلى صحة النتائج التي تم التوصل إليها"[2]، بينما هي ليست ملزمة بالاستجابة إلى طلب قدم في الدعوى من أجل ندب خبير، وكانت الأمور قد وضـحت لديها دون اللجوء إلى رأي الخـبير، كما في قضية الحال التالية: "... أنه من المعلوم بالضرورة أن المضبوطات من الهاتف المحمول والحاسب الآلي تعد من الأشياء الخاصة اللصيقة بالشخص ولا يستخدمها أو يستعملها غيره إلا استثناءً وللحظات قصيرة بالنسبة للهاتف لإجراء مكالمة عند الضرورة لا تؤثر على محتواه من ملفات تنم عن شخصية وديانة وثقافة حامله وكذلك الحاسب الآلي، ولما كان الثابت من التحقيقات أن المضبوطات ضبطت بحجرة نوم المتهم وأنه أقر بملكيته لها ومن ثم فهي تخضع للسيطرة الفعلية والمادية له، ولا ينال من ذلك ما قرره المتهم بالتحقيقات من أن وحدة تشغيل الحاسب الآلي الخاص به والمضبوطات كانت لدى شركة صيانة لإصلاحها ولا يعلم شيء عن مقاطع الفيديو المحملة عليها إذ أن ذلك القول جاء منه مرسلاً لم يقصده بدليل، كما أنه لم يفصح عن اسم هذه الشركة وعنوانها حتى تتمكن النيابة العامة أو المحكمة من تحقيق دفاعه الذي جاء مرسلاً تلتفت عنه المحكمة. لما كان ذلك وكان الحكم قد أقام قضاءه على ما استقر في عقيدة ووجدان المحكمة من انبساط سلطان الطاعن على الهاتف المحمول ووحدة الحاسب الآلي المضبوطين، كما رد على ما أثير من دفع بشيوع التهمة رداً سائغاً على النحو المتقدم بيانه- فإن ما يعيبه الطاعن على هذا الرد لا يكون له من وجه"[3].

1 أحمد محمد عبد الباقي، المرجع السابق، ص 262.

2 نقض 13 ماي 1968 مجموعة الأحكام رقم 107 حكم رقم 303 لسنة 1968، ص 38.

3 حكم محكمة النقض المصرية، الدائرة الجنائية، في الطعن المقيد بجدول المحكمة رقم 24908 لسنة 84 القضائية، في الجلسة العلنية المنعقدة بدار القضاء العالي بمدينة القاهرة، في يوم السبت 10 اكتوبر سنة 2015..

وجاء التأكيد على نفس الأمر في حكم محكمة النقض لسنة 2015 على أن المحكمة ليست ملزمة بالاستجابة لطلب ندب خبير إذا لم ترتئي ذلك:"...إن محكمة الموضوع لا تلتزم بإجابة طلب ندب خبير مادامت الواقعة قد وضحت لديها، وما دام في مقدورها أن تشق طريقها في المسألة المطروحة عليها، ولما كانت المحكمة قد اطمأنت إلى الدليل المستمد من تقرير النيابة العامة الناتج عن تفريغ مقاطع الفيديوهات المسجلة بما يفصح عن أنها لم تكن بحاجة إلى ندب خبير، فإنه لا تثريب عليها إن هي أغفلت دفاع الطاعنين ويَضحى ما أثير في هذا الصدد غير قويم..."[1].

إن الأدلة الإلكترونية التي يتم ضبطها بطريقة مشروعة مستوفية لجميع الشروط التي فرضها القانون، والمتحصل عليها وفق إجراءات قانونية سليمة واستقرت عقيدة المحكمة عليها، أكيد أنها تعد عاملاً مهماً في الكشف عن الجرائم الإلكترونية والقبض على مرتكبيها والمساهمة بذلك في مكافحتها. ولكن هناك نقطة مهمة يجب التطرق إليها، وهي مسألة مصير أدلة الإثبات المتحصل عليها بعد انقضاء الدعوى بصفة نهائية، كمصير السند المادي للتسجيل[2]، خاصة إذا كان هذا التسجيل يخص فئة الأطفال؛ وبالتحديد أولئك الذي وقعوا ضحية اعتداءات جنسية وتم تصويرهم، فبقاء هذه التسجيلات والفيديوهات سليمة قد يعرض حياتهم المستقبلية، وخاصة المهنية للخطر، لذا عمدت بعض القوانين إلى إبادتها وتحطيمها بعد اكتساب الحكم الصادر في الدعوى قوة الشيء المقضي به، أو بعد التقادم، ومن تلك القوانين ما جاء في المادة (113) من ق.م.ج.م[3]، والمادة (100-6) من ق.إ.ج.ف، إذ لا يجوز حفظ المعلومات بصورة لا متناهية، وإنما يحق للمرء المطالبة بتطبيق مبدأ الحق بالنسيان (le droit de l'oubli) بعدما تم استعمال المعلومات في الغرض المشروع الذي وجدت من أجله[4].

1 حكم محكمة النقض المصرية، الدائرة الجنائية (دائرة الثلاثاء (ج)، غرفة المشورة)، في الطعن المقيد بجدول المحكمة رقم 18572 لسنة 84 القضائية، في الجلسة العلنية المنعقدة بدار القضاء العالي بمدينة القاهرة، في يوم الثلاثاء 27 يناير سنة 2015.

2 نجيمي جمال، قانون الإجراءات الجزائية الجزائري على ضوء الاجتهاد القضائي، الجزء الأول، الطبعة الثالثة، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2017، ص 141؛ عبد الكافي الورياشي، نظام تسليم المجرمين، قراءات في المادة الجنائية، الجزء الأول، الطبعة الأولى، مجلة الحقوق (R.D) سلسلة المعارف القانونية والقضائية، دار نشر المعرفة، الرباط، المغرب، 2013، ص 113.

3 جاء في المادة 113 من قانون المسطرة الجنائية المغربي السالف الذكر أن: "يتم بمبادرة من قاضي التحقيق أو من النيابة العامة المختصة إبادة التسجيلات والمراسلات عند انصرام أجل تقادم الدعوى العمومية أو بعد اكتساب الحكم الصادر في الدعوى قوة الشيء المقضي به. ويحرر محضر عن عملية الإبادة يحفظ بملف القضية."

4 Article 100-6 du Code de procédure pénale, Créé par Loi n°91-646 du 10 juillet 1991 - art. 2 JORF 13 juillet 1991 en vigueur le 1er octobre 1991.

المبحث الثاني:
المعاينة والتفتيش ودورهما في جمع الأدلة الإلكترونية.

كشفاً للجرائم وتعقباً لمرتكبيها وبحثاً عن الأدلة الناتجة عنها، تقوم الجهات المختصة بإتباع أساليب البحث والتحري المختلفة من أجل الوصول إلى كل ما سبق ذكره، فالتحقيق في مجال القانون هو مجموعة الإجراءات التي تباشرها سلطة التحقيق عند وقوع جريمة أو حدث بهدف البحث والتنقيب عن الأدلة التي تفيد في كشف الحقيقة[1]، فالإجراءات المتبعة هي في الغالب التي ينص عليها قانون الإجراءات الجزائية، ومنها التي سيتم التطرق لها في هذا المبحث؛ كالمعاينة والتفتيـش عن الأدلـة وضبطها وتحريزها وفقاً لما ينص عليه القانـون، وبالرغم من أن كل تلك الإجراءات تقليدية في غالبها، إلا أن طبيعة الجريمة الإلكترونية وخصائصها استوجبت القيام بكل ذلك وفقاً لإتباع أساليب معينة، يغلب عليها الطابع التقني في كثير من الأحيان.

لذلك، وبناء على ما تم ذكره، تم تقسيم هذا المبحث إلى مطلبين؛ يتم التطرق فيهما للمعاينة في الجريمة الإلكترونية (المطلب الأول)، ولدراسة التفتيش والضبط في مجال الجريمة الإلكترونية (المطلب الثاني).

1 خالد ممدوح إبراهيم، فـن التحقيـق الجنائي في الجريمة الإلكترونيـة (دراسة مقارنة)، المرجع السابق، ص 18.

المطلب الأول: المعاينة فـــي الجريـمة الإلكترونيـــة.

المعاينة هي إجراء ينتقل بمقتضاه المحقق أو القاضي لمكان وقوع الجريمة؛ ليشاهد بنفسه ويجمع الآثار المتعلقة بها، ويعرف كيف وقعت، ويقوم بجمع الأشياء التي تفيد في كشف الحقيقة[1]. ويعد مسرح الجريمة بمثابة الشاهد الصامت، الذي إذا أحسن المحقق استنطاقه حصل على معلومات مؤكدة، في حين يؤثر كل عنصر من العناصر السابقة للجريمة ويتأثر بالعناصر الأخرى، وبالتالي يأخذ وينقل آثاره إلى بقية العناصر، وهي أساس نظرية العالم الفرنسي "ادموند لوكارد" سنة 1918 التي تسمى بـ "نظرية تبادل المواد" والتي تعني: "عند تلامس أي جسمين لبعضهما البعض فإنه يوجد دائماً انتقال للمادة من كليهما إلى الآخر، وأن كل مادة تترك أثراً على الأخرى"[2].

وسنتطرق في هذا المطلب لإجراء معاينة مسرح الجريمة الإلكترونية (الفرع الأول)، ثم للضوابط الواجب مراعاتها عند معاينة مسرح الجريمة الإلكترونية (الفرع الثاني).

الفرع الأول: معاينة مسرح الجريمة الإلكترونية.

يقع مسرح الجريمة الإلكترونية داخل بيئة الحاسوب[3]، والبيانات الرقمية[4] التي تتواجد وتنتقل داخل بيئته وشبكاته، وفي ذاكرته وفي الأقراص الصلبة الموجودة بداخله[5]، والمقصود بمعاينة

---

1 مونة جنيح، وأحمد الزعري، تدبير مسرح الجريمة وتحويل الآثار إلى أدلة جنائية، الطبعة الأولى، مطبعة الأمنية، الرباط، المغرب، 2015، ص 55، **نقلاً عن**: مأمون محمد سلامة، الإجراءات الجنائية الحديثة والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، 2002، ص 15.

2 ادموند لوكارد هو أستاذ فرنسي، من مواليد عام 1877، وتوفي سنة 1966، تخصص في الطب الشرعي والقانون وصاغ نظرية تبادل المواد المعروفة في قضايا الطب الشرعي بعبارة "كل اتصال يترك اثرا" Every contact leaves a trace، اشتغل بالمباحث الجنائية وساهم في إنشاء مخابر الشرطة. **نقلاً عـــن**:

- Levy, A, *La police scientifique : La technologie de pointe au service des enquêteurs*, Paris, Hachette, 2008, p : 25.

3 يعرف القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات المصري، السالف الذكر الحاسب الآلي بأنه:"كل جهاز أو معدة تقنية تكون قادرة على التخزين وأداء عمليات منطقية أو حسابية، وتستخدم لتسجيل بيانات أو معلومات أو تخزينها أو تحويلها أو تخليقها أو استرجاعها أو ترتيبها أو معالجتها أو تطويرها أو تبادلها أو تحليلها أو للاتصالات".

4 يعرف نفس القانون، في الفقرة الثالثة (3) من نفس المادة البيانات والمعلومات الإلكترونية بأنها:"كل ما يمكن إنشاؤه أو تخزينه أو معالجته أو تخليقه أو نقله أو مشاركته أو نسخه، بواسطة تقنية المعلومات، كالأرقام والاكواد والشفرات والحروف والرموز والإشارات والصور والأصوات، وما في حكمها".

5 تركي بن عبد الرحمن المويشير، المرجع السابق، ص 166.

مسرح الجريمة الإلكترونية هو معاينة الآثار والبصمات الإلكترونية التي يتركها مستخدم الشبكة المعلوماتية أو الإنترنت[1]، والتي تشمل الرسائل المرسلة منه أو الواردة إليه، وكافة الاتصالات الإلكترونية[2] التي تمت من خلال الحاسب والشبكة العالمية[3]، فالمعاينة تتم داخل تلك الأجهزة، كما تتم داخل شبكة الإنترنت نفسها عن طريق بيانات المتهم، كالولوج إلى بريده الإلكتروني[4]،

1 يعرف القانون رقم 175 لسنة 2018، السالف الذكر، في الفقرة 12 من المادة الأولى الشبكة المعلوماتية بـ:"مجموعة من الأجهزة أو نظم المعلومات تكون مرتبطة معا، ويمكنها تبادل المعلومات والاتصالات فيما بينها، ومنها الشبكات الخاصة والعامة وشبكات المعلومات الدولية، والتطبيقات المستخدمة عليها."؛ وعرفت الفقرة الخامسة من المادة العاشرة (5/10) من القانون رقم 18-04، الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، السالف الذكر، الانترنت بأنه:"شبكة معلوماتية عالمية تتشكل من مجموعة شبكات وطنية وإقليمية وخاصة، موصولة فيما بينها عن طريق بروتوكول الاتصال IP وتعمل معا بهدف تقديم واجهة موحدة لمستعمليها".

وIP (Internet Protocol Adresse) هو الهوية الإلكترونية للمستخدم على شبكة الانترنت، أي أنه المعرف التقني أو الدال الرقمي على مكان الحاسوب أثناء تصفح شبكة الانترنت. وتقنيا يتشكل" بروتوكول الانترنت "من أربعة 04 أرقام أولها يرمز للبلد والثاني للشركة موزعة الخدمة والثالث للمؤسسة المستخدمة والرابع مخصص للمستخدم. ومن ميزات هذا الرقم أنه يتغير مع أي دخول جديد إلى الشبكة. **انظر في ذلك:** بومامي العباس، الجريمة الإلكترونية بين التحصين التقني والتحصين الجنائي، مذكرة مكملة لنيل شهادة الماجستير في علوم الإعلام والاتصال، قسم علوم الإعلام والاتصال، كلية علوم الإعلام والاتصال، جامعة الجزائر 3، العام الجامعي 2014-2015، ص 23؛ **وانظر كذلك:** سعيداني نعيم، المرجع السابق، ص 135؛ ج. اسماعيل، مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها، مجلة الجيش، مجلة شهرية تصدر عن مؤسسة المنشورات العسكرية، العدد 599، الجزائر، جوان 2013، ص 17. كما يمكن الرجوع إلى:

- Eric LAURENT-RICARD, *Rétablir la confiance dans les messages électroniques, Le traitement des causes du "spam"*, Thèse de doctorat, école doctorale d'informatique, Université Panthéon-Assas, France, soutenue le 9 décembre 2011, p 76.

2 عرفت الفقرة الأولى من المادة العاشرة (1/10) من القانون رقم 18-04، السالف الذكر، والفقرة 11 من المادة 03 من القانون رقم 18-07، المؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الصادر في الج.ر العدد 34، بتاريخ 10 يونيو 2018، ص 11، الاتصالات الإلكترونية هي: "كل إرسال أو تراسل أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو بيانات أو معلومات مهما كانت طبيعتها، عبر الأسلاك أو الألياف البصرية أو بطريقة كهرومغناطيسية".

3 محمد كمال عبد السميع شاهين، الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي (دراسة مقارنة)، أطروحة من أجل الحصول على شهادة الدكتوراه في الحقوق، كلية الحقوق، جامعة حلوان، مصر، سنة 2015، ص 171.

4 محمد أمين الشوابكة، جرائم الحاسوب والانترنت: الجريمة المعلوماتية، المرجع السابق، ص 32؛ عبد الفتاح بيومي حجازي، الجريمة في عصر العولمة "دراسة في الظاهرة الإجرامية المعلوماتية مع التطبيق على القانون الإماراتي"، المرجع السابق، ص 20.

أما عن مفهوم البريد الإلكتروني فيمكن الرجوع إلى الفقرة 16 من المادة الأولى من قانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات المصري السالف الذكر، والتي ترى بأن: "البريد الإلكتروني وسيلة لتبادل رسائل إلكترونية على عنوان محدد، بين أكثر من شخص طبيعي أو اعتباري، عبر شبكة معلوماتية، أو غيرها من وسائل الربط الإلكترونية من خلال أجهزة الحاسب الآلي وما في حكمها".

أو معاينة حسابه على مواقع التواصل الاجتماعي[1]، كما يمكننا من خلال معاينة الحاسب الآلي للمتهم معرفة المواقع الإلكترونية التي زارها، أو الملفات التي حملها، والحسابات التي اخترقها[2].

فالمعاينة في الجريمة الإلكترونية ليست مسألة مرتبطة بالضرورة بالانتقال عبر العالم المادي، بل قد تتم عبر العالم الافتراضي، وهناك عدة طرق يستطيع بها عضو سلطة التحقيق أو مأمور الضبط القضائي أن ينتقل من خلالها إلى العالم الافتراضي للمعاينة، ومن ذلك:

1- من مكتبه بالمحكمة من خلال الحاسب الآلي الخاص به.
2- كما يمكنه اللجوء إلى مقهى الإنترنت Internet Café.
3- وأيضاً يجوز له اللجوء إلى مقر عمل مزود خدمة الإنترنت Internet Server Provider، الذي يعتبر أفضل مكان يمكن إجراء المعاينة فيه.
4- كما يستطيع المحقق الإنتقال إلى العالم الافتراضي للمعاينة من خلال مقر مكتب الخبير التقني المختص إذا توفر له في القانون ما يبيح ذلك، ولعل هذا متوفر في مصر من خلال إدارة مكافحة الجريمة الإلكترونية التابعة لوزارة الداخلية[3].

---

1 حازم محمد حنفي، المرجع السابق، ص 56.

2 جاء في الفقرة السابعة (7) من المـادة الثانيـة (2/7) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر سنة 2010، المصادق عليها بالمرسـوم الرئاسي رقم 14-252، السالفة الذكر، على أن تعريف الموقع هو: "إمكان إتاحة المعلومات على الشبكة المعلوماتية من خلال عنوان محدد."؛ كما جاء في الفقرة (13) من المادة الأولى من القانون المصري رقم 175 لسنة 2018، السالف الذكر، تعريف الموقع على أنه: "مجال أو مكان افتراضي له عنوان محدد على شبكة معلوماتية، يهدف إلى إتاحة البيانات والمعلومات للعامة أو الخاصة"؛ وجاء في الفقرة (15) من المادة الأولى من نفس القانون رقم 175 لسنة 2018، تعريف الحساب الخاص على أنـه: "مجموعة من المعلومـات الخاصة بشخص طبيعي أو اعتبـاري، تخول له دون غيره الحـق في الدخـول على الخدمات المتاحـة أو استخدامها من خلال موقع أو نظام معلوماتي". وعرفت الفقرة (11) من نفس المـادة النظـام المعلومـاتي بأنه:"مجموعة برامج وأدوات معدة لغرض إدارة ومعالجة البيانات والمعلومات، أو خدمة معلوماتية."؛ جـاء في الفقرة (18) من نفس المـادة ونفس القانون، تعريف الاختراق على أنه:"الـدخول غـير المرخص به أو المخـالف لأحـكام الترخيص، أو الدخول بأي طريقة غير مشروعة إلى نظام معلوماتي أو حاسب آلي أو شبكة معلوماتية وما في حكمها.".

وللمزيد بخصوص هاته المفاهيم والمصطلحات، يمكن الرجوع إلى: أحمد يوسف أحمد حسين الطحطاوي، الأدلة الإلكترونية ودورها في الإثـبات الجـنائي"دراسة مقارنة"، رسـالة مقدمـة لنيل درجـة الدكـتوراه في القانـــون الجنائي، قسم القانون الجنائي، كلية الحقوق، جامعة حلوان، مصـر، سنة 2015، ص 248؛ سلامة عماد محمد، الحماية القانونية لبرامج الحاسب الآلي ومشكلة قرصنة البرامج، الطبعة الأولى، دار وائل للنشر، الإسكندرية، 2005، ص 26.

3 خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجريمة الإلكترونية (دراسة مقارنة)، المرجع السابق، ص.ص: 156-157.

فالمعاينة قد تكون إجراء تحقيق أو إجراء استدلال، إذ لا تتوقف طبيعتها على صفة من يجريها، بل على مدى ما يقتضيه إجراؤها من مساس بحقوق الأفراد؛ فإذا أُجريت المعاينة في مكان عام كانت إجراء استدلال، وإذا اقتضى إجرائها دخول مسكن أو مكان له حرمته الخاصة كانت إجراء تحقيق[1]، حينها يجب مراعاة مبدأ الشرعية والخصوصية المعلوماتية للأفراد دون البحث في المحتوى[2] إلا في حدود السلطات الحصرية الممنوحة لسلطة التحقيق أو للسلطات المختصة[3]. وهو الأمر الذي نصت عليه مختلف المواد القانونية كالمادة (79) من ق.إ.ج.ج[4] والمادة (91) من ق.إ.ج.م [5]، وما أكده أيضاً الحكم القضائي لمحكمة النقض المصرية لسنة 2016[6].

1 عبد الله حسين على محمود، المرجع السابق، ص 386؛ علاء محمود يسن حراز، المرجع السابق، ص 357؛ نديم محمد حسن الترزي، سلطات النيابة العامة في الجرائم المعلوماتية (المعاينة– التفتيش)، مجلة الأندلس للعلوم الإنسانية والاجتماعية، صنعاء، اليمن، العدد الثالث عشر (13)، المجلد الخامس عشر (15)، ابريل 2017، ص 311.

2 يـعرف القانون المصري رقم 175 لسنة 2018 السالف الذكر، في الفقـــرة (19) من المادة الأولى المحتوى بأنه:"أي بيانـات تـؤدي بـذاتها أو مجتمعة مع بيانات أخرى إلى تكوين معلومة أو تحديد توجه أو تصور أو معنى أو إشارة إلى بيانات أخرى".

3 إن مصطلح السلطة المختصة Autorité Compétente يعني سلطة قضائية، أو إدارية، أو بوليسية مؤهلة قانونا Policière Habilitée في القانون الداخلي يناط بها الأمر أو التصريح أو مباشرة تنفيذ إجراءات جمع أو إنتاج عناصر الإثبات المرتبطة بالتنقيبات والإجراءات الجنائية. **ينظر في ذلك:** محمد كمال شاهين، الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، مصر، 2018، ص 171.

4 تنص المادة (79) من الأمر رقم 66-155، المتضمن قانون الإجراءات الجزائية الجزائري المعدل والمتمم، المرجع السابق: "يجـــوز لقاضي التحقيق الانـتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو القيام بتفتيشها...".

5 تنص المادة (91) من قانون الإجراءات الجنائية المصري (طبقاً لأحدث التعديلات بالقانون 95 لسنة 2003)، الصادر بالقانون رقم 150 لسنة 1950، على أن: "تفتيش المنازل عمل من أعمال التحقيق ولا يجوز الالتجاء إليه إلا بمقتضي أمر من قاضي التحقيق بناءً على اتهام موجه إلي شخص يقيم في المـنزل المراد تفتيشه بارتـكاب جنـاية أو جـنحة أو بإشراكه في ارتكابها أو إذا وجدت قرائن تدل على أنه حائز لأشياء ما تتعلق بالجريمة. ولقاضي التحقيق أن يفتش أي مكان ويضبط فيه الأوراق والأســلحة وكل ما يحتمل أنه استعمل في ارتكاب الجريمة أن نتج عنها أو وقعت عليه وكل ما يفيد في كشـف الحقيقة. وفي جميع الأحوال يجب أن يكون التفتيش مسبباً".

6 حكم محكمة النقض المصرية، الدائرة الجنائية، في الطعن المقيد بجدول المحكمة رقم 37025 لسنة 85 القضائية، في الجلسة العلنية المنعقدة بدار القضاء العالي بمدينة القاهرة، في يوم الأربعاء 16 نوفمبر سنة 2016، والذي جاء فيه: "... ولما كان ذلك، وكان من المقرر أن تقدير جدية التحريات وكفايتها لإصدار إذن التفتيش هو من المسائل الموضوعية التي يوكل الأمر فيها إلى سلطات التحقيق تحت إشراف محكمة الموضوع، وكانت المادة (58) من الدستور والمادة (91) من قانون الإجراءات الجنائية بعد تعديلها بالقانون رقم 37 لسنة 1972 لم يشترط أيهما قدراً معيناً من التسبيب أو صورة بعينها يجب أن يكون عليها الأمر الصادر بالتفتيش إنما يكفي لصحته أن يكون رجل الضبط القضائي قد علم من تحرياته واستدلالاته أن جريمة وقعت وأن هناك دلائل وأمارات قوية ضد من يطلب الإذن بضبطه وتفتيشه وتفتيش مسكنه وأن يصدر الإذن بناء على ذلك، ...".

الفرع الثاني: الضوابط الواجب مراعاتها عند معاينة مسرح الجريمة الإلكترونية.

المعاينـة هي مناظـرة ووصـف وفحـص للمكـان الذي ارتكبـت فيه الجريمـة، أو لشيء أو لشخص له علاقة بالجريمة، كونها إجراءً جائزاً في كافة الجرائم، إلا أن غالبية التشريعات تقتصرها على الجنايات والجنح الهامة دون المخالفات، وتعتبر وجوبية في الجنايات وجوازية في الجنح والمخالفات[1]، وهو ما يستشف من المادتين 21 و31 من ق.إ.ج.م[2]. ولكن بمقتضى المادة 06 من قانون تقنية المعلومات الجديد أصبح بإمكان جهات التحقيق المختصة أن تصدر أمراً مسبباً لمأموري الضبط القضائي المختصين[3]، لمدة لا تزيد على ثلاثين (30) يوماً قابلة لتجديد مرة واحدة من أجل:

1- ضبـط أو سحـب أو جمـع أو التحفـظ على البيانـات والمعلومـات أو أنظمـة المعلـومـات، أو تتبعها في أي مكان أو نظام أو برنامج أو دعامة إليكترونية أو حاسب تكون موجودة فيه، ويتم تسليم أدلتها الرقمية للجهة مصدرة الأمر على ألا يؤثر ذلك على استمرارية النظم وتقديم الخدمة إن كان لذلك مقتضى.

1 شيرين محمد إحسان عبد الحافظ، العلاقة بين جهود منظمات مكافحة الجريمة الإلكترونية وتحـقيق الأمـن الاجتماعي، أطروحـة ضمن مـقتضيات الحصول على درجة دكتوراه الفلسفة في الخدمة الاجتماعية، قسم تنظيم المجتمع، كلية الخدمة الاجتماعية، جامعة حلوان، مصر، سنة 2016، ص 110؛ الشحات إبراهيم محمد منصور، الجرائم الإلكترونيـة، الطبعة الأولى، دار الفكر الجـامعي، الإسكندرية، مصر، 2011، ص 195؛ فتوح الشاذلي، عفيفي كامل عفيفي، المرجع السابق، ص 367.

2 تنص المادة 21 من قانون الإجراءات الجنائية المصري، السالف الذكر، على أنه: "يقوم مأمورو الضبط القضائي بالبحث عن الجرائم ومرتكبيها وجمع الاستدلالات التى تلزم للتحقيق فى الدعوى"، وتنص المادة 31 من نفس القانون على أنه: "يجب على مأمور الضبط القضائي في حالة التلبس بجناية أو جنحة أن ينتقل فوراً إلى محل الواقعة، ويعاين الآثار المادية للجريمة، ويحافظ عليها، ويثبت حالة الأماكن والأشخاص، وكل ما يفيد في كشف الحقيقة، ويسمع أقوال من كان حاضراً، أو من يمكن الحصول منه على أيضاحات في شأن الواقعة ومرتكبها. ويجب عليه أن يُخطر النيابة العامة فوراً بانتقاله ويجب على النيابة العامة بمجرد إخطارها بجناية متلبس بها الانتقال فوراً إلى محل الواقعة".

3 حسب المادة 05 من القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات، السالف الذكر، يجوز بقرار من وزير العدل بالاتفاق مع الوزير المختص وهو الوزير المعني بشؤون الاتصالات وتكنولوجيا المعلومات منح صفة الضبطية القضائية للعاملين بالجهاز القومي لتنظيم الاتصالات أو غيرهم ممن تحددهم جهات الأمن القومي؛ والتي تشمل كل من: رئاسة الجمهورية، ووزارة الدفاع، ووزارة الداخلية، والمخابرات العامة، وهيئة الرقابة الإدارية – حسب الفقرة 26 من المادة الأولى من ذات القانون-.

2- البحث والتفتيش والدخول والنفاذ إلى برامج الحاسب وقواعد البيانات وغيرها من الأجهزة والنظم المعلوماتية تحقيقاً لغرض الضبط[1]، متى كان ذلك مفيداً في إظهار الحقيقة على ارتكاب جريمة من الجرائم التي نص عليها قانون تقنية المعلومات المصري.

فالمشرع المصري بذلك يكون قد وسع من النطاق المكاني للمعاينة، وكذا المجال الزمني الذي حدده بثلاثين (30) يوماً قابلة للتجديد مرة واحدة، دونما تحديد لساعات القيام بذلك؛ نظراً لأن المعاينة في الجرائم الإلكترونية لها خصوصيتها؛ سرعة وسهولة إخفاء دليل ارتكابها، لذا فقد أجاز المشرع الجزائري هو الآخر عملية المعاينة والتفتيش في غير الساعات المحددة[2] لعملية المعاينة في الجرائم العادية، تفادياً لضياع الدليل الإلكتروني من مسرح الجريمة.

ولأجل القيام بعملية المعاينة بشكل صحيح لابد من مراعاة عدة إجراءات وضوابط، نذكر منها على سبيل المثال:

1- الإعداد الجيد قبل المعاينة، بحيث يكون هناك فرق متخصصة في هذا النوع من الجرائم متكونة من خبراء وفنيين ومحققين لهم تكوين عالٍ في ميدان مكافحة الجريمة الإلكترونية، وقبل البدء في المعاينة يجب إخطار الفريق الذي سيتولى المعاينة بوقت كافٍ حتى يستعد هذا الأخير، وتكون له خطة وإمكانات مناسبة لضبط الأدلة الإلكترونية بعد معاينتها حتى لا تضيع هذه الأخيرة ويذهب مجهودهم سُدى.

2- تصويـر جهاز الحاسوب والأجهزة الطرفية[3] المتصلة به والمحتويات والملحقات، والتحفظ على المستندات الخاصة بالإدخال وكذلك ملحقات الحاسب الآلي المادية والورقية، والتي قد تحمل آثاراً لارتكاب الجريمة، ويراعى تسجيل وقت وتاريخ ومكان التقاط كل صورة.

---

1 المادة 06 من نفس القانون.

2 تنص المادة 47 من الأمر رقم 66-155، السالف الذكر، على:"لا يجوز البدء في تفتيش المساكن ومعاينتها قبل الساعة الخامسة (5) صباحا، ولا بعد الساعة الثامنة (8) مساءً إلا إذا طلب صاحب المنزل ذلك أو وجدت نداءات من الداخل أو في الأحوال الاستثنائية المقررة قانوناً... وعندما يتعلق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجـرائم تبييض الأموال والإرهاب وكذا الجرائم المتعلقة بالتشريع الخاص بالصرف فإنه يجوز إجراء التفتيش والمـعاينة والحجز في كل محل سكني أو غير سـكني في كل سـاعة من ساعات النـهار أو الليل وذلك بناءً على إذن مسبق من وكيل الجمهورية المختص".

3 عرفت الفقرة 43 من المادة العاشرة (10) من القانون رقم 18-04، الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية السالف الذكر: "نقاط طرفية: نقاط وصل مادية تستجيب لمواصفات تقنية ضرورية للنفاذ إلى شبكة الاتصالات

3- الملاحظة الجيدة للطريقة التي تم بها إعداد النظام والآثار الإلكترونية، وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام، وبوجه خاص السجلات الإلكترونية التي تتزود بها شبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز الذي تم عن طريقه الولوج إلى النظام أو الموقع الإلكتروني، حتى تكون عملية المقارنة والتحليل ممكنة عند عرض الأمر أمام المحكمة.

4- التحفظ على المعلومات الموجودة بالقرب من الأجهزة وفي سلة المهملات، من أوراق أو ملفات، أو أوراق كربون، أو شرائـط وأقراص ممغنطة السليمـة منها، وغـير سليمـة، والهواتف النقالة، وفحصها، ورفع ومضاهاة ما قد يوجد عليها من بصمات.

5- عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل إجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الحاسوب الآلي من أي مجالات لقوى مغناطيسية يمكن أن تتسبب في محو البيانات المسجلة.

6- الحرص على عدم إتلاف أي بيانات يتم استخراجها من الجهاز، والتأكد من وجود نسخة منها داخل الجهاز نفسه، مع الفحص الدقيق لكل الملفات للتعرف على جميع العمليات التي قـام بها مستخـدم الجهاز والمـواقع التي ارتـادها على شبكـة الإنترنت، وكذلك أسماء حساباته في مواقع التواصل الاجتماعي وكلمات المرور الخاصة به[1].

ولأن مسرح الجريمة هو مستودع سرها، الذي يحتوي على الآثار المختلفة عن ارتكابها؛ فهو أفضل طريق للوصول إلى إثبات أو نفي وقوعها، وفيه توجد الإجابة عن كيفية وقوعها والظروف التي تمت فيهـا وعلاقة المتهم بها[2].

فبالمعاينـة يمكن فـك غمـوض الجريمـة وحـل شفراتهـا المبهمـة، خاصة في الجرائم الإلكترونية، فهي –المعاينة– ذات أهمية في مجال التحقيق الجنائي، من ناحيتين؛ القانونية والعلمية، لأنها تُترجم

الإلكترونية والاتصال بفعالية عن طريقها، وهي جزء لا يتجزأ من الشبكة. عندما يتم توصيل شبكة اتصالات الكترونية بشبكة أجنبية، تعد نقاط الربط لهذه الشبكة نقطة طرفية".

1 أحمد يوسف الطحطاوي، الأدلة الإلكتروني ودورها في الإثبات الجنائي (دراسة مقارنة)، دار النهضة العربية، القاهرة، مصر، 2015، ص ص: 134-135؛ علاء محمود يسن حراز، المرجع السابق، ص 385، **نقلاً عن**:

- Robert Taylor, *Cpmouter Crime in criminal investigation*, edited by charles swanson,N.chamelin and L.territt o,hill inc.5th edition, 1992, p 450.

2 عبد الكريم خالد الردايدة، المرجع السابق، ص 11.

ما قام به الجاني من أفعال والتي تشكل جرماً بدون تجنٍ عليه، فبها يتأكد وقوع الجريمة ونفيها، وصدق أقوال أطراف الواقعة، وبيان ركن الخطأ أو العـمد في الواقعة. كما أنها ذات أهمية في تحديد الوصف القانوني للواقعة، وتساعد القاضي على تكوين عقيدة واقتناع معين[1]، وحتى تعطي عمليـة المعايـنة نتائجها لابـد أن تتم وفق مبدأ المشـروعية وفي إطار ما تنص عليه القوانين الجنائية[2].

المطلب الثانـــي: التفتيش والضبط في مجال الجريمة الإلكترونية.

يعرف التفتيش بأنه البحث عن الشيء في مستودع السر، غايته البحث عن أشياء تتعلق بجريمة معينة تفيد في كشف الحقيقة. ولقد ورد اختلاف بين رجال الفقه والقانون حول مسالة التفتيش في الجريمة الإلكترونية؛ هل يخضع لتطبيق القواعد الإجرائية التقليدية، أما يجب إيجاد قواعد جديدة للتفتيش عن الدليل الإلكتروني ؟

فـي جميع الأحوال يعتبر التفتيش، أو الولوج كما يُفضل تسميته بعض الدارسين والمحققين الجنائيين في الجريمة الإلكترونية، أهم إجراءات التحقيق؛ لأنه ينتهي في أغلب الأحيان بضبط الأدوات التي استعملت في ارتكاب الجريمة، أو ضبط أي شيء آخر يفيد في كشف الحقيقة كالأدلة المادية مثلا[3]، ويعتبر الضبط هو غاية التفتيش القريبة، وهو الوسيلة القانونية التي تضع

1 نبيل محمد عثمان عرعارة، الحماية الجنائية للحق في حرمة المراسلات عبر البريد الإلكتروني، الطبعة الأولى، المصرية للنشر والتوزيع، القاهرة، مصر، 2018، ص 159، **نقلاً عن:** هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، اسيوط، 1992، ص ص 59 إلى 60.

2 أحمد يوسف الطحطاوي، الأدلة الإلكتروني ودورها في الإثبات الجنائي (دراسة مقارنة)، دار النهضة العربية، القاهرة، مصر، 2015، ص ص 134-135.

3 محمد أبو العلا عقيدة، مراقبة المحادثات التليفونية دراسة مقارنة في تشريعات الولايات المتحدة الأمريكية وانجلترا وايطاليا وفرنسا ومصر، دار الفكر العربي، مصر، 1994، ص 63، **نقلاً عن:** محمود محمود مصطفى، شرح قانون الإجراءات الجنائية، الطبعة 12، 1988 رقم 178، ص 221، **وأيضاً لدى:** رؤف عبيد، مبادئ الإجراءات الجنـائية في القـانون المـصري، الطبعة 17 لسنة 1989، ص 417؛ يوسف قجاج، خصوصية القواعد الإجرائية في مجال البحث عن الجريمة الإلكترونية –دراسة مقارنة–، دار السلام للطباعة والنشر والتوزيع، الرباط، المغرب، 2016، ص 54؛ علي شملال، المستجدات في قانون الإجراءات الجزائية الجزائري (الكتاب الثاني: التحقيق والمحاكمة– نسخة معدلة ومنقحة 2017–)، الطبعـة الثانيـة، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2017، ص 63؛ محمود نجيب حسني، شرح قانون الإجـراءات الجنائية وفقاً لأحـدث التعـديلات التشريعية، ترجمة، تحقيق فوزية عبد الستار، دار النهضة العربية، مصر، 2018، ص 592، **وكذلك نقلاً عن:**

- Merie Roger et Vitu Andre, *Traité de droit criminel tome II*, 2éme édition, (VIAS, Paris, 1973 , N° 1115,p.334)

بواسطتها السلطة المختصة يدها على جميع الأشياء التي وقعت عليها الجريمة أو نتجت عنها أو استعملت لاقترافها[1]، ولذلك يتعين عند إجرائه توافر القواعد نفسها التي تنطبق بشأن التفتيش[2].

الفرع الأول: التفتيش في الجريمة الإلكترونية.

يعد التفتيش إجراء من إجراءات التحقيق التي تهدف للبحث عن أدلة من جناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة المسكن أو تفتيش شخص[3]، أو أشخاص معينين إما بصفتهم فاعلين أصليين أو شركاء في ارتكابها[4]، فالتفتيش بهذا المعنى يعتبر إجراء من إجراءات التحقيق الابتدائي وليس إجراء من إجراءات الاستدلال، وهو ما نصت عليه مختلف المواد القانونية؛ كالمادة 91 من ق.إ.ج.م، والمادة 138 من ق.إ.ج.ي[5]، وكذلك المادة 80 من نظام الإجراءات الجزائية السعودي[6]، إذ لا يمكن لضابط الشرطة القضائية الدخول إلى المنازل وإجراء تفتيش فيها إلا بتفويض أو رخصة من السلطة القضائية، وذلك لما ينطوي عليه مثل هذا الإجراء من المساس بحرمة المسكن وأسرار الأشخاص وحرماتهم[7].

1 وردة شرف الدين، المرجع السابق، ص 152.

2 توفيق مجاهد، طاهر عباسة، المرجع السابق، ص 91.

3 تنص المادة 133 من قرار جمهوري بالقانون رقم 13 لسنة 1994م، بشأن الإجراءات الجزائية اليمنية معدل ومتمم، الصادر في الج.ر رقم 19 ج 4 لسنة 1994، على أن: "تفتيش الشخص يكون بالبحث عما يكون في جسمه أو ملابسه أو أمتعته الموجودة معه".

4 مرنيز فاطمة، الاعتداء على الحق في الحياة الخاصة عبر شبكة الانترنت، أطروحة مقدمة لنيل شهادة الدكتوراه في القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، الجزائر، السنة الجامعية 2012-2013، ص240؛ خالد عياد الجلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن، 2011، ص 149.

5 المادة 91 من ق.إ.ج.م السالف الذكر تنص: "تفتيش المنازل عمل من أعمال التحقيق..."، وتنص المادة (138) من ق.إ.ج.ي، السابق الذكر، على أن: "تفتيش المساكن عمل من أعمال التحقيق ولا يجوز الالتجاء إليه إلا بمقتضى أمر من النيابة العامة بناءً على اتهام موجه إلى شخص يقيم في المنزل المراد تفتيشه بارتكاب جريمة معاقب عليها وفقاً لقانون العقوبات النافذ".

6 المادة 80 من نظام الإجراءات الجزائية السعودي، الصادر بموجب المرسوم الملكي رقم (م/2)، بتاريخ: 2013/11/25، تنص: "تفتيش المساكن عمل من أعمال التحقيق، ولا يجوز الالتجاء إليه إلا بناءً على اتهام بارتكاب جريمة موجه إلى شخص يقيم في المسكن المراد تفتيشه، أو باشتراكه في ارتكابها، أو إذا وجدت قرائن تدل على أنه يحوز أشياء تتعلق بالجريمة. وللمحقق أن يفتش أي مكان ويضبط كل ما يحتمل أنه استعمل في ارتكاب الجريمة أو نتج منها، وكل ما يفيد في كشف الحقيقة بما في ذلك الأوراق والأسلحة. وفي جميع الأحوال يجب أن يُعِد محضرًا عن واقعة التفتيش يتضمن الأسباب التي بُنِيَ عليها ونتائجه، مع مراعاة أنه لا يجوز دخول المساكن أو تفتيشها إلا في الأحوال المنصوص عليها نظامًا وبأمر مسبب من هيئة التحقيق والادعاء العام".

7 علي شملال، المرجع السايق، ص 63.

وبعيداً عن الجدال الفقهي الدائر حول إمكانية تفتيش المنظومة المعلوماتية من عدمه، كان موقف المشرع الجزائري واضحاً من خلال المادة الخامسة (05) من القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما[1]، وكذا من خلال المادة 26 من المرسوم الرئاسي رقم 14-252 المتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر سنة 2010[2]، والتي أجاز من خلالهما صراحة تفتيش المنظومة المعلوماتية[3]، فالتشريع الجزائري حذا حذو مشرعين آخرين، كالتشريع اليوناني وكذلك التشريع الكندي وفقاً للمادة 487 من القانون الجنائي الكندي، وقانون المنافسة الكندي The Competition Act الذي بين ضوابط تفتيش مكونات الحاسب الآلي، وخول لمأمور الضبط القضائي كلما حصل على أمر قضائي تفتيش أنظمة الحاسب الآلي والتعامل معها وضبطها[4].

1 جاء في المادة الخامسة (05) من القانون رقم 09–04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، السالف الذكر: "يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية، في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4 أعلاه، الدخول، بغرض التفتيش، ولو عن بعد، إلى: أ- منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها. ب- منظومة تخزين معلوماتية... "، والحالات التي نصـت عليها المـادة (04) من نفس القانون هي: "يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 03 أعلاه في الحالات الآتية: أ- للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، ب- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام والدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، ت- لمقتضيات التحريات والتحقيقات القضائيـة، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية، ث- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة. لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية المختصة...".

2 تنص الفقرة الأولى من المادة (1/26) الخاصة بتفتيش المعلومات المخزنة، من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر سنة 2010، المصادق عليها بالمرسوم الرئاسي رقم 14-252، السالفة الذكر، ص 04، على أن: تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين سلطاتها المختصة من التفتيش أو الوصول إلى:

أ- تقنية معلومات أو جزء منها والمعلومات المخزنة فيها أو المخزنة عليها،

ب- بيئة أو وسيط تخزين معلومات تقنية معلومات والذي قد تكون معلومات التقنية مخزنة فيه أو عليه...".

3 ليندا بن طالب، التفتيش في الجريمة المعلوماتية، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر بالوادي، الجزائر، العدد ستة عشر(16)، جوان 2016، ص 490؛ توفيق مجاهد، طاهر عباسة، المرجع السـابق، ص 91.

4 منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، المرجع السابق، ص188؛ عبد الصبور عبد القوي علي مصري، المحكمة الرقمية والجريمة المعلوماتية دراسة مقارنـة، مرجع سابق، ص 109؛ الطويل خالد بن محمد، التعامل مع الاعتداءات الإلكترونية من الناحية الأمنية مركز المعلومات الوطني، وزارة الداخلية، ورقة عمل مقدمة لورشة العمل الثالـثة (أحكام في المعلوماتية)، الذي نظمه مشروع الخطة الوطنية لتقنية المعلومات، الرياض، 1423/10/19هـ؛ يوسف بن سعيد بن محمـد الكلباني، المرجع السابق، ص 341، **وقد أشار إلى ذلك أيضاً كلاً من:**

كما نص قانون إساءة استخدام الحاسب الآلي بانجلترا الصادر عام 1990، على أن إجراءات التفتيش تشمل أنظمة الحاسب الآلي، بينما أجازت تشريعات أخرى اتخاذ أي إجراء يكون لازماً لجمع أدلة الجريمة، ومن أمثلة تلك التشريعات قانون الإجراءات الجنائية اليونـاني في مادته 251 التي تجيز لسلطة التحقيق أن تتخذ أي إجراء أو أي شيء يكون لازماً لجمع الدليل، وفسر الفقه الجنائي اليوناني عبارة " أي شيء" بأنها تشمـل جميع بيانات الحاسوب المادية والمعنوية، سواء كانت هذه البيانـات مخزنة في حاملتها أم كانت معالجة آليا في الذاكرة الداخلية للحاسوب[1].

وفي عام 1994 أصدرت إدارة العدل الأمريكية المرشد الفيدرالي لتفتيش وضبط الحواسيب The Federal Guidelines for Searching & Seizing Computers لكي يكون معاوناً للجهات القضائية في تقصي الجرائم الإلكترونية، كما صدرت له عدة ملاحق ليتم في سنة 2001 إصـدار نسخـة منقحة بعنوان: نظـم تفتيش وضبـط الحـواسيب والحصول على الأدلـة في التحقيقات الجنائية[2]، أما المشرع الفرنسي فقد تطرق لهذا الموضوع من خلال عدة مواد نذكر منها الفقرة الأولى من المادة 56-1 من ق.إ.ج.ف، والمادة 97 من ذات القانون التي سمحت بالبحث عن المستندات أو البيانات الخاصة بالحاسب الآلي والتي تفيد في كشف الحقيقة، بينما نصت الفقرة الأولى من المادة 60-1 من ذات القانون، أنه بإمكان النائب العام أو ضباط الشرطة القضائية الذين تحت إمرته أن يطلبوا من أي شخص أو أي مؤسسة أو هيئة خاصة أو عامة أو أي إدارة تزويدهم بمعلومات ذات الصلة بالتحقيق، بما في ذلك البيانات الخاصة بنظام حاسب آلي أو معالج

- Vassilaki lrini, *Computer Crimes and other Crimes against Information Technology in Greece*, R.I.D.P, 1993, p:371.

- Piragoff Donnaldk, *Computer Crimes and other Crimes against Information Technology in Canada*, R.I.D.P, 1993, p:241.

1 الحاسوب هو اسم اطلقه J.Perret في سنة 1955 على آلة معالجة البيانات والمعلومات L'information ويحتوي على معالج وذاكرة وميكانيك، ويتكون من شاشة ووحدة مركزية، ولوحة مفاتيح، وفارة، ويمكن أن نضيف إليه أشياء أخرى كالطابعة والسكانير...ألخ، **نقلاً عـــن:**

- Bouchelit Rym , *Les perspectives d'E-banking dans la stratégie E- Algérie 2013*, thèse de doctorat en sciences économiques, faculté des sciences économiques, Commerciales et de gestion , université Abou Bekr Belkaid, Tlemcen, 2014-2015, page 14.

2 عمر محمد ابوبكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، رسالة دكتوراه في القانون الجنائي، كلية الحقوق، جامعة عين شمس، مصر، 2004، ص 789.

بيانات أو بيانات شخصية، خاصة في شكلها الرقمي، مع عدم قدرة هذه الجهات على المعارضة دون سبب مشروع، وكذا التزامها بالسر المهني المفروض قانوناً[1].

في حين لم يَستجب قانون المسطرة الجنائية في بداية الأمر لمتطلبات البحث والتفتيش في قواعد المعطيات الآلية[2]، رغم أن المشرع المغربي أصدر في عام 2014 قانوناً يقضي بموجبه الموافقة على اتفاقية مكافحة الجريمة الإلكترونية المسماة "بودابست"[3]، ويعتبر أيضاً أن الاتفاقيات الدولية في حالة المصادقة عليها تسمو على القوانين[4]، كان لزاما عليه وضع قوانين تتماشى مع التطورات

1 **Code de procédure pénale - Article 56,** Article 56-1 (Modifié par LOI n°2019-222 du 23 mars 2019 - art. 49 (V): « Si la nature du crime est telle que la preuve en puisse être acquise par la saisie des papiers, documents, données informatiques ou autres objets en la possession des personnes qui paraissent avoir participé au crime ou détenir des pièces, informations ou objets relatifs aux faits incriminés, . » ; **Article 97** (Modifié par LOI n°2019-222 du 23 mars 2019 - art. 54 (V)) : « Lorsqu'il y a lieu, en cours d'information, de rechercher des documents ou des données informatiques et sous réserve des nécessités de l'information et du respect, le cas échéant, de l'obligation stipulée par l'alinéa 3 de l'article précédent, le juge d'instruction ou l'officier de police judiciaire par lui commis a seul le droit d'en prendre connaissance avant de procéder à la saisie.. » ; **Article 60-1** (Modifié par LOI n°2019-222 du 23 mars 2019 - art. 47 (V): « Le procureur de la République ou l'officier de police judiciaire ou, sous le contrôle de ce dernier, l'agent de police judiciaire peut, par tout moyen, requérir de toute personne, de tout établissement ou organisme privé ou public ou de toute administration publique qui sont susceptibles de détenir des informations intéressant l'enquête, y compris celles issues d'un système informatique ou d'un traitement de données nominatives, de lui remettre ces informations, notamment sous forme numérique, le cas échéant selon des normes fixées par voie réglementaire, sans que puisse lui être opposée, sans motif légitime, l'obligation au secret professionnel. Lorsque les réquisitions concernent des personnes mentionnées aux articles 56-1 à 56-5, la remise des informations ne peut intervenir qu'avec leur accord. A l'exception des personnes mentionnées aux articles 56-1 à 56-5, le fait de s'abstenir de répondre à cette réquisition dans les meilleurs délais et s'il y a lieu selon les normes exigées est puni d'une amende de 3 750 euros. A peine de nullité, ne peuvent être versés au dossier les éléments obtenus par une réquisition prise en violation de l'article 2 de la loi du 29 juillet 1881 sur la liberté de la presse».

2 أحمد آيت الطالب، تقنيات البحث وإجراءات المسطرة المتبعة في جرائم الانترنت والمعلوميات، مجلة الملف، العدد التاسع (09)، المغرب، نوفمبر 2006، ص.ص: 30-35.

3 موافقة المشرع المغربي على اتفاقية بودابست والبروتوكول الإضافي الخاص بها: بالظهير شريف رقم 1.14.85 صادر في 12 من رجب 1435 الموافق 12 ماي 2014، بتنفيذ القانون رقم 136.12 الموافق بموجبه على اتفاقية الجرائم المعلوماتية، الموقعة ببودابست في 23 نوفمبر 2001.

4 جاء في آخر ديباجة –تصدير– الدستور المغربي الصادر بموجب: ظهير شريف رقم 1.11.91 الصادر في 27 من شعبان 1432، الموافق 29 يوليو 2011، الخاص بتنفيذ الدستور، المنشور بالج.ر، العدد 5964 مكرر، السنة المائة، الصادرة في 30 يوليو 2011، ص 3600، بأن: "...جعل الاتفاقيات الدولية، كما صادق عليها المغرب، وفي نطاق أحكام الدستور، وقوانين المملكة، وهويتها الوطنية الراسخة، **تسمو**، فور نشرها، على التشريعات الوطنية، والعمل على ملائمة هذه التشريعات، مع ما تتطلبه تلك المصادقة".

الحاصلة في منظومتـه القانونية، لذا نص في خضم مشروع قانون المسطرة الجنائية[1] على بعض التعديلات في هـذا الشأن، نذكر منها ما جاء في المادة 59 منه والتي جاء فيها:"... يجري التفتيش في جميع الأماكن التي يمكن أن يعثر بها على مستندات أو وثائق أو معطيات أو أدوات أو برامج معلوماتية أو أشياء مفيدة في إظهار الحقيقة...".

أما المشرع المصـري وكما رأينا فيما سبق، فقد أجاز عملية البحث والتفتيش في الجريمة الإلكترونية من أجل ضبط الأدلة الإلكترونيـة التي تفيد في كشف الحقيقة من خلال الفقرة الثانية من المادة السادسة (06) من القانون رقم 175 لسنة 2018 المتضـمن مكافحـة جـرائم تقنية المعلومات[2]، ولأن عملية التفتيش لها ما لها مـن الأهميـة في التحقيق الجنائي والمساس بحرمة الإنسان وكرامته، وحتى تتم عملية التفتيش بشكل صحيح فرضت لها التشريعات مجموعة من الشروط الموضوعية والشكلية القانونية، والتي نذكر منها:

البند الأول: شروط إجراء عملية التفتيش في الجريمة الإلكترونية.

لأجل مكافحة الجريمـــة الإلكترونية سمحت العديـد من القوانين بالتفـتيش عن هذه الجـــريمـة، والحصول على دليل الكتروني يمكـن من خلاله إثبـات أو نفي هذه الأخيرة عن المتهم أو المتهمين بها، ففي التشريع الجزائري كانت بعض مواد القانون رقم 09–04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها مصدر مشروعية لهذا الإجراء، فقد جاء في المادتين الثالثة (03) والخامسة (05) منه أنه: "في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام والدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، أو لمقتضيات التحريات والتحقيقات، وفي إطار قانون الإجراءات الجزائية يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية، الدخول بغرض التفتيـش إلى منظومـة معلومـاتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها، و/أو

1 المادة 59 من مسودة مشروع قانون يقضي بتغيير وتتميم قانون المسطرة الجنائية، على موقع وزارة العـدل للمـملكة المغـــربية: https://www.*justice.gov.ma/lg-1/documents/doccat-4.aspx*، تاريخ الإطلاع: 15-09-2019.

2 الفقرة الثالثة من المادة السادسة (3/6) من القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات، السالف الذكر: "... البحث والتفتيش والدخول والنفاذ إلى برامج الحاسب وقواعد البيانات وغيرها من الأجهزة والنظم المعلوماتية تحقيقاً لغرض الضبط ..".

الدخول وتفتيش منظومة تخزين معلوماتية، ولأن التفتيش يمس بخصوصية الأفراد ومستودع أسرارهم، خص هذا الإجراء بمجموعة من الضمانات التي تسمح بإيجاد توازن بين المصلحة العامة والخاصة".

والمادة 44 من ق.إ.ج.ج تضمنت مجموعة من هذه الضمانات؛ إذ لا يمكن القيام بعملية تفتيش مساكن الأشخاص الذين يظهر أنهم ساهموا في جناية أو جنحة متلبس بها أو التحقيق في الجرائم الإلكترونية، أو تفتيش مساكن أشخاص يتبين أنهم يحوزون أوراق أو أشياء لها علاقة بالأفعال الجرمية المرتكبة إلا بإذن مكتوب صادر من وكيل الجمهورية أو من قاضي التحقيق، مع التأكيد على ضرورة إظهار ذلك الإذن قبل الدخول والشروع في التفتيش[1]، كما أكدت فقرات تلك المادة على أن يتضمن الإذن وصفاً للجرم المرتكب وكذا عنوان الأماكن التي سيتم زيارتها والتفتيش فيها، وكل ذلك تحت طائلة البطلان. وهو ذات الأمر نجده في المادة 91 من قانون الإجراءات الجنائية المصري، والتي قضت بأنه: "لا يجوز القيام بالتفتيش إلا بمقتضي أمر من قاضي التحقيق بناءً على اتهام موجه إلى شخص بارتكاب جناية أو جنحة أو باشتراكه في ارتكابها أو إذا وجدت قرائن تدل على أنه حائز لأشياء ما تتعلق بالجريمة المرتكبة".

فمن خلال المواد السابقة يتبين أنه لا يكفي مجرد وقوع الجريمة لإجراء التفتيش، بل لا بد أن تكون مما يعتبره القانون جناية أو جنحة، بحيث تستبعد المخالفات في كثير من الأحيان، إلا إذا

1 تنص المادة 48 من التعديل الدستوري، المصادق عليه في استفتاء أول نوفمبر سنة 2020، المؤرخ في 15 جمادى الأولى عام 1442 الموافق 30 ديسمبر سنة 2020، الصادر بالمرسوم الرئاسي رقم 20-442، المنشور بالج.ر.ج، العدد 82، بتاريخ 30 ديسمبر سنة 2020، والمعدل للدستور الجزائري الصادر بموجب استفتاء شعبي في 28 نوفمبر 1996، الصادر بموجب المرسوم الرئاسي رقم 96-438 الممضي في 07 ديسمبر1996، المنشور بالج.ر.ج، عدد 76 مؤرخة في 08 ديسمبر 1996، الصفحة 6، ومعدل:- بالقانون رقم 02-03 المؤرخ في 10 أبريل 2002، الج.ر.ج، عدد 25 المؤرخة في 14 أبريل 2002، الصفحة 13، - والقانون رقم 08-19 المؤرخ في 15 نوفمبر 2008، الج.ر.ج، عدد 63 المؤرخة في 16 نوفمبر2008، الصفحة 8، - والمعدل بالقانون رقم 16-01 المؤرخ في 26 جمادى الأول عام 1437 الموافق 06 مارس 2016، المنشور بالج.ر.ج، عدد 14 المؤرخة في 07 مارس 2016 ص 02، على: تضمن الدولة عدم انتهاك حُرمة المسكن. لا تفتيش إلا بمقتضى القانون، وفي إطار احترامه. ولا تفتيش إلا بأمر مكتوب صادر عن السّلطة القضائية المختصة".

طلب ذلك وكيل الجمهورية[1]، كونها ليست بتلك الخطورة التي تبرر إهدار الحرية الفردية وحرمة المسكن بإجراء تفتيش من أجلها[2].

إن شرط وقوع جريمة جنائية هو شرط أساسي في القانون المقارن، حيث يتعين وفقاً للقانون الانجليزي حتى يتم إصدار أمر التفتيش، أن يوضح طَالبُ إصدار الإذن أن لديه سبباً معقولاً Resonable Cause، أو سبباً راجحاً Probale Cause للاعتقاد بأن الجريمة قد تم ارتكابها، أما في القانون الأمريكي فإنه لا يشترط وقوع الجريمة بالفعل لكي يصدر إذن التفتيش والضبط، ويكون بذلك الإذن صحيحاً رغم أن الجريمة لم تقع بعد، وهو التفتيش الذي يطلق عليه اسم Prospective Search Warrant[3].

في هذا الإطار ومن خلال استقراء المواد القانونية، خاصة قانون الإجراءات الجزائية يتبين أن المشرع الجزائري قصد مراعاة القواعد الإجرائية المنصوص عليها قانوناً والمتعلقة بدخول المنازل وفقاً للمواد 44، و45، و47 من ق.إ.ج.ج، وذلك حينما يتعلق الأمر بتفتيش منظومـة معلوماتية لحاسب آلي موجود في منزل أو محل لـه خصوصيتـه، ولأن المادة 81 من ق.إ.ج.ج، نصت على أن عملية التفتيش تبـاشر في جميع الأماكن التي يمكن العثور فيها على أشياء يكون كشفهـا مفيـداً لإظهـار الحقيقـة، فعليه يمكن أن يشمل البحث في مجال الجريمة الإلكترونية مختلف الأماكن والأشخاص الطبيعية والمعنوية، وأجهزة الحواسيب وملحقاتها، وكذا الأنظمـة والشبـكات

1 المادة (66) من ق.إج.ج: "التحقيق الابتدائي وجوبي في مواد الجنايات. أما في مواد الجنح فيكون اختيارياً ما لم يكن ثمة نصوص خاصة. كما يجوز إجراءه في مواد المخالفات إذا طلبه وكيل الجمهورية".

2 سوزان نوري فقي محمد، الإثبات في جرائم الانترنت في القانون العراقي والقانون المقارن، رسالة مقدمـة لنيل درجة المـاجستير في الحقـــوق، قـــسم الدراســات العليا، كـلية الحـقوق، جامعة المنصورة، مـــصر، السنة الجامعية 2014- 2015، ص 77، عن: حسن صادق المرصفاوي، أصول الإجراءات الجـنائية، الجـــزء الأول، منشاة المعـــارف، الإسكـندرية، مصر، 1996، ص 465؛ رضا هميسي، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسيّة، جامعة الشهيد حمه لخضر بالـــوادي، العـــدد الخامس(05)، جوان 2012، ص 164.

3 ابراهيم محمد ابراهيم محمد، النظرية العامة لتفتيش المساكن في قانون الإجراءات الجنائية "دراسة مقارنة"، رسالة للحصول على درجة الدكتوراه في الحقوق، قسم القانون الجنائي، كلية الحقوق، جامعة القاهرة، مصر، 2005، ص 151، **نقلاً عـــن:**

- Fellman David, The law relating to entry, Search, Seizure, No.4-15, p :76

المعلوماتية؛ أي كل ما يمكن أن يكون ذا طبيعة مادية أو معنوية[1]، كل ذلك من أجل الحصول على دليل الكتروني يكون مفيداً في كشف هذه الجريمة.

كما يمكن أن يمتد التفتيش إلى نظم معلوماتية أخرى قد تكون داخل[2] أو خارج الدولة، فبموجب تلك المواد أعفى المشرع الجزائري جهات التحقيق من الالتزام بمواعيد التفتيش المعتادة في الجرائم التقليدية[3]، وكذا الشرط الخاص بحضور المتهم أو من ينوب عنه، أو غير المتهم ممن اتضح

1 يتكون الحاسب الآلي من مكونات مادية Haed ware ومكونات معنوية (منطقية) Soft ware وشبكات الاتصال Network، والمكونات المادية الملموسة قادرة على إدخال وإخراج البيانات وتجميعها واستخراج النتائج منها، أما الكيان المنطقي للحاسب الآلي فيتمثل في برامج (logiciels) عبارة عن مجموعة من التعليمات والأوامر المستخدمة لإدارة ومراقبة وتشغيل جهاز الحاسب يتم إعدادها من طرف مبرمجين. **انظر فـــي ذلك:** زروق يوسف، حجية وسائل الإثبات الحديثة، رسالة مقدمة لنيل شهادة دكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، السنة الجامعية 2012-2013، ص.ص: 121-113، **نقلاً عن:** عـلاء حسين مطـلق التميمـي، الأرشـيف الإلكتروني –دراسة مقارنـة–، دار النهضة العربية للنشر والتـوزيع، الطبعة الثانية، القاهـرة، 2010، ص 09؛ أمـــال قـارة، الحماية الجزائية للمعلوماتـــية في التشـــريع الجـزائري، الطبعة الأولى، دار هومة، الجزائر، 2006، ص 33؛ خالد مصطفى فهمي، المرجع السابق، **نقلاً عن:** محمد فؤاد غنيم وآخرون، أساسيات الحاســب الآلي ونظـم التشغيل، كلية العلوم، جامعة طنطا، مصر، 2004، ص 116؛ نزيهة مكاري، إثبات الاعتداء على حـق المؤلف عبر الانترنت في التشريع الجزائري (دراسة مقارنة)، مجلة العلوم الاقتصادية وعلوم التسيير، كلية العلوم الاقتصاديـة والتجارية وعلوم التسيير بجامعة سطيـف1، العدد التاسع (09)، 2009، ص 132.

2 تم تمديد الاختصاص المحلي فيما يخص البحث والتحري والتحقيق في الجرائم الإلكترونية في نصوص قانونية متعددة، نذكر من بينها الفقرة السابعة من المادة 16 من ق.إ.ج.ج التي تم بموجبها تمديد اختصاص ضباط الشرطة القضائية إلى كامل التراب الوطني، والمادة 37 تم بموجبها تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى، وكذلك المادة 40 من نفس القانون التي تم بموجبها تمديد الاختصاص المحلي لقاضي التحقيق إلى دائرة اختصاص محـاكم أخرى، حيث كان اختصاصه يتحدد بمكان وقوع الجريمة أو بمحل اقامة احد الأشخاص المشتبه في مساهمتهم في اقترافها أو بمحل القبض على احد هؤلاء الأشخاص حتى ولو كان القبض قد حصل لسبب آخر.

3 حسب نص المادة (62) من ق.م.ج.م فإن عملية تفتيش المنازل، لا يمكن أن تتم قبل الساعة السادسة صباحاً وبعد التاسعة ليلاً، ولكن إذا تعلق الأمر بجريمة إرهابية واقتضت ذلك ضرورة البحث، أو في حالة الخشية على اندثار الأدلة فإنه يمكن التفتيش قبل تلك الساعتين شرط وجود إذن كتابي من النيابة العامة.

ولمزيد من التفاصيل بخصوص ذلك ينظر: عبير بعقيقي، وفيصل نسيغة، الإثبـات في الجـرائم المعلوماتية على ضـوء القـــانون 09-04، مجلـــة العلـــوم القانونيـــة والسياسيـة،كلية الحقوق والعلوم السياسيّة، جامعة الشهيد حمّه لخضر بالوادي، المجلد التاسع (09)، العدد الثاني (02)، جوان 2018، ص 46؛ خضراوي الهادي، بوقرين عبد الحليم، تجربة الجزائر في مكافحة الجريمة الإلكترونيـة، ورقة بحثية مقدمة في إطار أشغال المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية ICACC، كلية علوم الحاسب والمعلومات، جامعة الإمام محمد بن سعود الإسلامية، الرياض، المملكة العربية السعودية، نوفمبر 2015، ص 168؛ منيرة عبيزة، أبوبكر مصطفى، الدليل الإلكتروني والسلطة التقديرية للقاضي، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر بالوادي، الجزائر، المجلد التاسع (09)، العدد الثالث (03)، ديسمبر 2018، ص 586؛ مختار الاخضري،

وجود أمارات قوية على أنه يحوز أشياء تتعلق بالجريمة، ففي الجرائم العادية حضور كلا من المتهم أو من يحوز أشياء تتعلق بالجريمة لعملية التفتيش هو أمر وجوبي، إذا كانت هذه العملية ستتم في منازلهم[1]، فالعديد من الأحكام القضائية بينت موضوع تفتيش المساكن، ومنها الحكم الصادر عن محكمة النقض المصرية عام 2017، الذي جاء فيه: "إن القانون يحظر تفتيش المنزل إلا بناءً على أمر قضائي؛ وهذا يعني أن الأمر القضائي لازم لتفتيش المنزل في كل الأحوال وأنه لازم لتفتيش الشخص في غير حالة التلبس وهو من إجراءات التحقيق ويجب في كل أحواله أن يتم على وجه لا يتنافى والآداب العامة ولا يهدد الكرامة الإنسانية ولا يلحق بصحة الإنسان ضرراً وأن يلتزم منفذه بمحتواه"[2]، وجاء في حكم آخر أن: "التفتيش الذي يقوم به مأمور الضبط القضائي بناءً على ندبه لذلك من سلطة التحقيق تسري عليه أحكام المواد 92، و199، والمادة 200 من قانون الإجراءات الجنائية، والمادة الأولى منها تنص على إجراء تفتيش منزل المتهم وغير المتهم بحضوره، أو من ينيبه عنه إن أمكن ذلك، فحضور المتهم ليس شرطا جوهرياً لصحة التفتيش، ومن ثم، فلا يعيب الحكم التفاته عن الرد على دفاع الطاعنين في هذا الشأن"[3].

1- التلبس في الجريمة الإلكترونية:

تتسع سُلطات الضبطية القضائية في حالة التلبس لدى معظم التشريعات المقارنة[4]، بحيث يصبح بإمكانها مباشرة اختصاصات سلطة التحقيق[1]، كالتفتيش بحثاً عن أدلة الجريمة وتحديد

الإطار القانوني لمواجهة جرائم المعلوماتية وجرائم الفضاء الافتراضي، مجلة نشرة القضاة، المديرية العامة للشؤون القضائية والقانونية، مديرية الدراسات القانونية والوثائق، وزارة العدل، الجزائر، العدد 66، 2011، ص 61؛ **نقلاً عن:** مونة جنيح، أحمد الزعري، المرجع السابق، ص 30.

1 ثابت دنيازاد، مراقبة الاتصالات الإلكترونية والحق في حرمة الحياة الخاصة في القانون الجزائري، مجلة العلوم الاجتماعية والإنسانية، جامعة العربي التبسي، تبسة، الجزائر، المجلد الثالث (03)، العدد السادس (06)، ديسمبر 2012، ص 214؛ بوحليط يزيد، تفتيش المنظومة المعلوماتية وحجز المعطيات في التشريع الجزائري، مجلة التواصل في الاقتصاد والإدارة والقانون، تصدر عن جامعة باجي مختار، عنابة، العدد الثامن والأربعون (48)، ديسمبر 2016، ص 84؛ لدغش رحيمة، ضوابط تفتيش الحاسب الآلي، مجلة الحقوق والعلوم السياسية، جامعة زيان عاشور بالجلفة، الجزائر، العدد الرابع (04)، تاريخ النشر: 2015/12/15، ص 143.

2 حكم محكمة النقض، الدائرة الجنائية، في الطعن المقيد بجدول المحكمة برقم 29953 لسنة 86 القضائية، في الجلسة العلنية المنعقدة بدار القضاء العالي بمدينة القاهرة، في يوم الخميس 28 من ابريل سنة 2017.

3 حكم محكمة النقض المصرية، الدائرة الجنائية، الأربعاء (أ)، في الطعن المقيد بجدول المحكمة رقم 29658 لسنة 86 القضائية، السالف الذكر.

4 حالة تلبس نصت عليها المادة 41 من ق.إ.ج.ج: "توصف الجناية أو الجنحة بأنها في حالة تلبس إذا كانت مرتكبة في الحال أو عقب ارتكابها. كما تعتبر الجناية أو الجنحة متلبسا بها إذا كان الشخص المشتبه في ارتكابه إياها في وقت قريب جداً من وقت قريب

فاعلها، سواء تعلق الأمر بتفتيش المساكن أو الأشخاص، ويعد التلبس من الظروف العينية التي تلحق بالواقعة الإجرامية ذاتها، ذلك أن مشاهدة الجريمة عيناً يعد أقوى مظاهر إثباتها.

وينصرف التلبس في مدلوله القانوني إلى معنى التزامن بين ارتكاب الجريمة واكتشافها، وهو ما يستدل عليه من الحكم القضائي الصادر عن محكمة النقض المصرية عام 2017 بقولها: "وبفحص جهاز الحاسب الآلي المرتبط بشبكة الإنترنت المأخوذة من السنترال الصادر الإذن من النيابة العامة بتفتيشه، تبين أن الجهاز مدون ومنشور عليه عبارات تحريضية ضد مؤسسات الدولة ومنشورات تحث المواطنين ضد نظام الحكم في البلاد، وهي جرائم معاقب عليها قانوناً، فقاما بالقبض عليه والجريمة متلبس بها، والتلبس هنا ليس مرهوناً بمشاهدة الركن المادي للجريمة، بل مرهون بمظاهر خارجية لا تدخل في تكوين الركن المادي، لكنها تنبئ بذاتها عن وقوع الجريمة وعن انتسابها

جداً من وقت وقوع الجريمة قد تبعه العامة بالصياح. أو وجدت في حيازته أشياء أو وجدت آثار أو دلائل تدعو إلى افتراض مساهمته في الجناية أو الجنحة. وتتسم بصفة التلبس كل جناية أو جنحة وقعت ولو في غير الظروف المنصوص عليها في الفقرتين السابقتين، إذا كانت قد ارتكبت في منزل وكشف صاحب المنزل عنها عقب وقوعها وبادر في الحال باستدعاء أحد ضباط الشرطة القضائية لإثباتها."؛ **وتقابلها** المادة (30) من ق.إ.ج.م التي تنص: "تكون الجريمة متلبسا بها حال ارتكابها أو عقب ارتكابها ببرهة يسيرة. وتعتبر الجريمة متلبسا بها إذا اتبع المجني عليه مرتكبها أو تبعته العامة مع الصباح أثر وقوعها، أو إذا وجد مرتكبها بعد وقوعها بوقت قريب حاملا آلات أو أسلحة أو أمتعة أو أوراقا أو أشياء أخرى يستدل منها على فاعل أو شريك فيها، أو إذا وجدت به في هذا الوقت آثار أو علامات تفيد ذلك."؛ **وتقابلها كذلك** المادة (53) من ق.إ.ج.ف:

Article 53 du code de procédure pénale, (Modifié par Loi n°2004-204 du 9 mars 2004 - art. 77 JORF 10 mars 2004): « Est qualifié crime ou délit flagrant le crime ou le délit qui se commet actuellement, ou qui vient de se commettre. Il y a aussi crime ou délit flagrant lorsque, dans un temps très voisin de l'action, la personne soupçonnée est poursuivie par la clameur publique, ou est trouvée en possession d'objets, ou présente des traces ou indices, laissant penser qu'elle a participé au crime ou au délit. A la suite de la constatation d'un crime ou d'un délit flagrant, l'enquête menée sous le contrôle du procureur de la République dans les conditions prévues par le présent chapitre peut se poursuivre sans discontinuer pendant une durée de huit jours. Lorsque des investigations nécessaires à la manifestation de la vérité pour un crime ou un délit puni d'une peine supérieure ou égale à cinq ans d'emprisonnement ne peuvent être différées, le procureur de la République peut décider la prolongation, dans les mêmes conditions, de l'enquête pour une durée maximale de huit jours. »

1 تنص المادة 42 من ق.إ.ج.ج على أنه: "يجب على ضابط الشرطة القضائية الذي بلغ بجناية في حالة تلبس أن يخطر بها وكيل الجمهورية على الفور ثم ينتقل بدون تمهل إلى مكان الجناية ويتخذ جميع التحريات اللازمة. وعليه أن يسهر على المحافظة على الآثار التي يخشى أن تختفي. وأن يضبط كل ما يمكن أن يؤدي إلى إظهار الحقيقة ..."، ونصت المادة 56 من نفس القانون على أن: "ترفع يد ضابط الشرطة القضائية عن التحقيق بوصول وكيل الجمهورية لمكان الحادث. ويقوم وكيل الجمهورية بإتمام جميع أعمال الضبط القضائي المنصوص عليها في هذا الفصل. كما يسوغ له أن يكلف ضابط للشرطة القضائية بمتابعة الإجراءات". وتنص المادة 60 من نفس القانون على: "إذا حضر قاضي التحقيق لمكان الحادث فانه يقوم بإتمام أعمال ضباط الشرطة القضائية المنصوص عليها في هذا الفصل. وله أن يكلف احد ضباط الشرطة القضائية بمتابعة تلك الإجراءات...".

للمتهم، ومن ثم يكون دخول مأموري الضبط القضائي مسكن المتهم قد تم وفقـاً لصحيح القانون"[1].

ولكن قد لا يتصور المرء وجود حالة تلبس في الجريمة الإلكترونية، إلا أن هذه الحالة موجودة؛ ومن أمثلتها تواجد رجل الضبط القضائي في أحد مقاهي الإنترنت ولاحظ شخصاً يقوم بالإبحار عبر شبكة الإنترنت في المواقع الإباحية ويقوم بطباعة الصور بواسطة الطابعة، حينها تكون شروط حالة التلبس قد تحققت، ويكون بإمكانه القبض على ذلك الشخص وتفتيشه، ومن أمثلتها أيضاً: قيام الجاني بإعداد صفحة لترويج المخدرات أو الدعوة للقيام بأعمال إرهابية، وشاهده مأمور الضبط، أو أبلغ عن ذلك مزود خدمات الإنترنت، فرصدته شرطـة الإنترنت وقبضت عليه، أو أن المجني عليه أبلغ شرطة الإنترنت في الدائرة التي قام فيها الجاني بجريمته، كالسب والقذف، أو كما حدث حين قامت شركة (AOL) وهي شركة خدمات انترنت (ISP) بالولايات المتحدة الأمريكية باكتشاف أنشطة دعارة وترتيب لقاءات جنسية مع أطفال أثناء قيامها بمراقبة أنشطة المشتركين لديها، وعلى الفور قدمت أسماء المشتبه بهم للمباحث الفيدرالية الأمريكية التي تمكنت من القبض على العشرات منهم بعد مراقبة أنشطتهم[2].

وفي مثال آخر قام شخص بإبلاغ الشرطة الأمريكية بجريمة قتل وقعت خلال دردشة له مع امرأة بالفيديو عبر الإنترنت، وذكرت صحيفة "فيلادلفيا إنكوايارر أن الشخص شاهد جريمة قتل ميليني هاين (31) سنة من منطقة ليبانون بولاية بنسيلفانيا خلال محادثته معها على الإنترنت حيث قام على الفور بإبلاغ الشرطة بالجريمة، وقال مدير الشرطة في تلك المنطقة أن الضحية كانت تتحدث مع شخص على الإنترنت عندما أطلق عليها زوجها (33) سنة النار من مسدسه وأرداها قتيلة، وبعدها صعد القاتل إلى غرفة النوم في المنزل وانتحر بإطلاق النار على نفسه[3].

1 حكم محكمة النقض رقم 29953 لسنة 86 القضائية، السالف الذكر.

2 مرنيز فاطمة، المرجع السابق، ص.ص: 242-243.؛ علاء محمود يسن حراز، المرجع السابق، ص 352، **نقلاً عن**: عمر السعيد رمضان، مبادئ قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، 1985، رقم 175، ص 293؛ عـمر محمد أبو بكر يونس، المرجع السابق، ص 847.

3 فايز محمد راجع غلاب، الجريمة المعلوماتية في القانون الجزائري واليمني، أطروحة من اجل الحصول على شـهادة الدكتوراه في الحقـوق فرع القـانون الجنائي والعـلوم الجـنائية، كليـة الحقوق، جامعة الجزائر 01، السـنة الجـامعة 2009-2010، ص.ص: 288-289.

وبحسب قانون الإجراءات الجزائية الجزائري، يمكن لأي شخص شاهد جناية أو جنحة متلبس بها والمعاقب عليها بعقوبة الحبس، ضبط الفاعل واقتياده إلى أقرب ضابط للشرطة القضائية[1].

2- إذن التفتيش للوصول للدليل الإلكترونـــي.

إن تفتيش المتهم أو تفتيش منزله هو إجراء من الإجراءات الصارمة التي نصت عليها القوانين الإجرائية تجاه المتهم، لذلك وضع له المشرع شروطاً وضوابط وضمانات عند القيام به من قبل السلطات المختصة، ومن أهم تلك الضمانات صدور أمر أو إذن من تلك السلطة المختصة قانوناً[2]، ذلك أن الأعمال الإجرائية محكومة من جهة الصحة والبطلان بمقدماتها لا بنتائجها[3]، لذا يجب التقيد بالحدود المرجوة من التفتيش أثناء تنفيذه، فأغلب النصوص القانونيـة أوجبت ضرورة وجـوده في المواضـع التي يفرض فيها المشرع ذلك، ومنها المادة 09 من ق.إ.ج.م[4]، وتعتبر الشروط الموضوعية والشكلية[5] لإجراء التفتيش من أهم الضمانات القانونية التي تكفل مباشرة التفتيش في نطاق مفهوم قرينة البراءة التي يتمتع بها المتهم طوال فترة التحقيق في الدعوى[6].

إلا أنه في حالة اتصال التفتيش بجريمة إلكترونية تتم عن طريق الإنترنت، فلابد أن تشمل المذكرة القضائية ما مفاده جواز تفتيش أنظمة الكمبيوتر والقواعد التي تراعي التعامل عبر الإنترنت، إذ يجب أن يتضمن إذن التفتيش الإجازة بالبحث عن كيان البرنامج وأنظمة تشغيله والسجلات التي تثبت استخدام الأنظمة الآلية لمعالجة البيانات والسجلات المستخدمة في عملية الولوج في

1 المادة (61) من ق.إ.ج.ج: "يحق لكل شخص في حالات الجناية أو الجنحة المتلبس بها والمعاقب عليها بعقوبة الحبس، ضبط الفاعل واقتياده إلى اقرب ضابط للشرطة القضائية."، والمادة (37) من ق.إ.ج.م: "لكل من شاهد الجاني متلبسا بجناية أو جنحة يجوز فيها قانونا الحبس الإحتياطي، أن يسلمه إلى أقرب رجل من رجال السلطة العامة دون احتياج إلى أمر بضبطه."

2 مجيد خضر السبعاوي، مولان قادر أحمد، الضرورة الإجرائية في مرحلة التحقيق الابتدائي (تحليلية مقارنة)، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، مصر،2017، ص 111.

3 حكم محكمة النقض المصرية، الدائرة الجنائية، في الطعن المقيد بجدول المحكمة رقم 8426 لسنة 87 القضائية، السالف الذكر.

4 جاء في الفقرة الثانية من المادة 9 من ق.إ.ج.م: "... في جميع الأحوال التي يشترط فيه القانون لرفع الدعوى الجنائية تقديم شكوى أو الحصول على إذن أو طلب من المجنى عليه أو غيره لا يجوز اتخاذ إجراءات التحقيق فيها إلا بعد تقديم هذه الشكوى أو الحصول على هذا الإذن أو الطلب، ...".

5 عائشة بن قارة مصطفى، المرجع السابق، ص 108؛ سوزان نوري فقي محمد، المرجع السابق، ص 83.

6 ابراهيم محمد ابراهيم محمد، المرجع السابق، ص 161.

النظام الآلي لمعالجة البيانات[1]، فالتخصيص في إذن التفتيش هو أمر ضروري، حين ميزت الدائرة الاستئنافية الفيدرالية الخامسة في الولايات المتحدة الأمريكية في معرض تطبيقها لقانون خصوصية الاتصالات الإلكترونية ECPA، بين مصطلح تخزين الاتصالات الإلكترونية Stored E-Communications، والتي يتطلب القانون لتفتيشها أو مراقبتها إذن تفتيش Search Warrant مثلما هو متبع في التفتيش الصادر عن هيئة الإدعاء، والمبحوث فيه عن الجرائم، وذلك وفق ما جاء في القسم 18 USCode Sec.2703، والمصطلح الآخر هو مصطلح تخزين الاتصـالات السلكيـة Wire Communications، والـذي يتطلـب المشـــرع للقيـام بتفتيشـــه ومراقبته الحصول على إذن تفتيش من المحكمة Court Order، إذ لا يكفي مجرد إذن تفتيش عادي في هذه الحالة، وهو ما جاء في القسم 18 USCode Sec.2518[2].

ونظراً لأهمية الإذن في عملية التفتيش، لابد على القائم به احترام الإجراءات التي نص عليها المشرع في هذا الخصوص[3]، ذلك أن الكثير من القضايا تتعرض للطعن وترفض جميع التحقيقات التي تمت فيها رغم كل الجهد المبذول والإمكانيات المستعملة والخسائر المتكبدة بسبب عدم احترام الإجراء الذي يقضي بإصدار إذن بالتفتيش

وهو ما يتضح من خلال حكم محكمة النقض المصرية عام 2006، والذي جاء فيه: "ولما كان الحكم المطعون فيه قد عرض للدفع ببطلان التفتيش لإجرائه دون إذن مسبب بإجرائه أو طرحه في قوله: " وحيث أنه عن الدفع ببطلان أي دليل مستمد من تفتيش منزل ومكتب المتهم الأول، تبعاً لبطلان التفتيش في الحالين لعدم صدور أمر مسبب به طبقاً لما تنص عليه المادة 91 من قانون الإجراءات الجنائية، فمردود عليه بأن مفهوم المادة 91 من قانون الإجراءات الجنائية هو أن الأمر أو الإذن يقتضي أن يكون هناك أمر أو إذن ارتأى تنفيذ الإجراء ومأمور مأذون له ندباً

1 قرار محكمة الجنايات اللبنانية منشور في مجلة العدل اللبنانية، 2000، ص 375. **نقلاً عـــن**: عبد الله عبد الكريم عبد الله، المرجع السابق، ص 59، من:

2 Peter Schnaitman, Building a community through workplace E-mail : thenew privacy frontier op-cit at 06.

3 وحسب المادة 65 مكرر 5 من ق.إ.ج.ج فان الإذن هو الذي يعطي الجهة القائمة بالتفتيش مشروعية القيام بذلك الإجراء في غير المواعيد المحدد في المادة 47 من ذات القانون، كما ألزمت المادة 65 مكرر 15 من ذات القانون أن يكون الإذن مكتوباً ومـسبباً وذلك تحت طائلة البطلان، وأن يذكر في الإذن الجريمة التي تبرر اللجوء لهذا الإجراء، كما يجب أيضاً ذكر هوية ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته.

في تنفيذه، وفي هذه الحالة أوجب القانون تسبيب الأمر أو الإذن، وقد اشترط القانون في تلك الحالة أن يكون أمر التفتيش صادراً لمأمور ضبط قضائي، والثابت من التحقيقات أن تفتيش مسكن ومكتب المتهم الأول قد تم بمعرفة النيابة العامة صاحبة السلطة في ذلك انطلاقاً من مباشرتها التحقيق، ولم تر إسناد هذا الإجراء لأحد من مأموري الضبط القضائي بطريق الأمر أو الندب المشار إليه بالمادة 91 من قانون الإجراءات الجزائية، ومن ثم يكون قد تخلف عن النيابة العامة بصدد هذا الإجراء صفة الإذن أو الأمر حتى يكون هناك محل لوجوب التسبيب ومن نافلة القول أنه قد سبق إجراء تفتيش منزل المتهم الأول بمحضر تحريات المقدم (س) الضابط بالإدارة العامة لمباحث الأموال العامة المؤرخ../../..الذي تطمئنت المحكمة لجديتها والمحدد للجريمة واتهام المتهم الأول وآخرين بارتكابها، وكذا أقوال رئيسة مكتب توثيق (ع) السالف سردها تفصيلاً وكذا محضر الاطلاع على دفاتر ذلك المكتب، ومطابقته التوكيلات على ما أثبت فيها، وهي إجراءات قامت بها النيابـة العامـة بنفسها وتلك الإجراءات مسوغاً لقيام النيابة العامـة بتفتيش مسكـن المتـهم ومكتبه، ومن ثم يكون الدفع غير قائم على سند من صحيح القانون جديراً بالرفض، وهذا الذي أورده الحكم يتفق وصحيح القانون ويستقيم به إطراح الدفع المثار في هذا الشأن، ويكون منعى الطاعن الأول في هذا الخصوص غير سديد"[1].

من المؤكد أن وجود الاذن بالتفتيش أمر ضروري لصحة عملية التفتيش، ولكن قد يصادف القائم به جريمة أخرى غير تلك المنصوص عليها في الإذن، أو قد يسمح بتفتيش المتهم أو من له سلطة على موضع التفتيش، وبيان هاتين الحالتين كما يلي:

2-1) اكتشاف جريمة أخرى غير الجريمة المنصوص عليها في إذن التفتيش:

قد تُكتشف جريمة إلكترونية أخرى أثناء القيام بعملية التفتيش غير تلك التي صدر الإذن بشأنها، وهي الحالة التي نصت عليها الفقرة الأخيرة من المادة 44 من ق.إ.ج.ج، والفقرة الثانيـة من المادة 65 مكرر 6 من ذات القانـون، والفقرة الثانية من المادة 50 مـن ق.إ.ج.م، والفقرة

1 حكم محكمة النقض المصرية، في الطعن المقيد بجدول المحكمة رقم 13196 لسنة 76 القضائية، في الجلسة العلنية المنعقدة بدار القضاء العالي بمدينة القاهرة، في جلسة 18 مايو سنة 2006.

الرابعة من المادة 76 من ق.إ.ج.ف[1]، وهي الحالة المسماة في القضاء الأمريكي بالرؤيـة الكامـلة، حيث انقسم القضـاء الأمريكي إلى اتجـاهين في هـذه المسـالة؛ الاتجاه الأول أقر أن منهج الرؤية الكاملة لا يمكن أن يبرر الإعتداء على التوقع المعقول للخصوصية لدى الفرد، وأن هذا الإستثناء يسمح بشكل مجرد بضبط الدليل فقط دون الإطلاع على الملف غير المصرح برؤيته[2]، فحسب هذا الاتجاه على الضابط القائم بعملية التفتيش الذي وجد ملفاً يدل على جريمة أخرى غير تلك الصادر الإذن بالبحث عنها، إن يوقـف التفتـيش مؤقتاً لأجل الحصـول على إذن آخر للتفتيش، ومثالها ما جـاء في قضيـة في الولايات المتحدة الأمريكية التي تم فيها القبض على المتهم قبل أن يحضر الضابط الثاني الإذن بالتفتيش[3]، لذا قضت المحكمة بأنه لا يمكن أن تجرى عملية بحث شامل على القرص الصلب، لأن أجهزة الحاسبات الآلية يمكن أن تتضمن الكثير من المعلومات التي تمس حياة الشخص.

أما الاتجاه الثاني يرى أنه بمجرد البدء في إجراء التفتيش على جهاز الحاسب الآلي، فإن المتهم لم يعد يملك توقعاً معقولاً للخصوصية في المحتويات الباقية لحاسوبه أو جهاز التخزين خاصته، لذا قررت المحكمة الأمريكية أن منهج الرؤية الكاملة يجعل التوسع في تفتيش جهاز

1 تنص الفقرة الأخيرة من المادة 44 من ق.إ.ج.ج: "... إذا اكتشفت أثناء هذه العمليات جرائم أخرى غير تلك التي ورد ذكرها في إذن القاضي فان ذلك لا يكون سبباً لبطلان الإجراءات العارضة." (معدلة بالقانون 06-22)؛ وتنص الفقرة الثانية من المادة 65 مكرر 6 على: "...إذا اكتشفت جرائم أخرى غير تلك التي ورد ذكرها في إذن القاضي، فان ذلك لا يكون سبباً لبطلان الإجراءات العارضة."؛ وتنص الفقرة الثانية من المادة 50 من ق.إ.ج.م: "...لا يجوز التفتيش إلا للبحث عن الأشياء الخاصة بالجريمة الجاري جمع الاستدلالات أو حصول التحقيق بشأنها. ومع ذلك إذا ظهر عرضاً أثناء التفتيش وجود أشياء تعد حيازتها جريمة أو تفيد في كشف الحقيقة في جريمة أخرى، جاز لمأمور الضبط القضائي أن يضبطها."؛

Article 76 du Code de procédure pénale (modifié par LOI n°2019-222 du 23 mars 2019 - art. 49 (V)): «Toutefois, le fait que ces opérations révèlent des infractions autres que celles visées dans la décision ne constitue pas une cause de nullité des procédures incidentes. …»

2 مصطفى على خلف، المرجع السابق، ص 157، **نقلاً عن**:

- United States v.Maxwell, 45 M.j.406,417-19(C.A.A.f.1996) 4.plain. **See the following website :** http//www.cybertelecom.org/security/bbexceptions.htm#pla.

3 U.S. Supreme Court,Illinois v. Andreas, 463 U.S. 765 (1983), Illinois v. Andreas, No. 81-1843,Argued March 30, 1983,Decided July 5, 1983,463 U.S. 765 : « … When the other officer left to secure a warrant to search the apartment, the DEA agent maintained surveillance of the apartment. Some 30 or 45 minutes after the delivery, but before the other officer could return with a warrant, respondent emerged from the apartment with the shipping container and was immediately arrested and taken to the police station;… ». **See the following site :** https://supreme.justia.com/cases/federal/us/463/765/.

الحاسوب أمراً مشروعاً ولا ينتهك بذلك التعديل الرابع من الدستور الأمريكي[1]،كما أن الفترة التي يراد الحصول فيها على إذن مكتوب بالتفتيش عن الجريمة الثانية المكتشفة، قد تسمح للجاني بتدمير، أو محو البيانات، أو نقلها، أو تعديلها[2]، مما قد يتسبب في ضياع الدليل الإلكتروني نهائياً، لذا أجاز القانون لقاضي التحقيق القائم بعملية التفتيش حجز المواد أو الأشياء التي يعاقب القانون على حيازتها أو استعمالها، والتي اكتشفها عرضاً، ويبلغ عنها النيابة العامة فوراً لتتخذ ما تراه بشأنها باعتبارها جريمة في حالة تلبس تم اكتشافها بطريق مشروع وبشكل عرضي، ذلك أن التلبس حالة عينية تلازم الجريمة نفسها لا شخص مرتكبها[3].

"فالإذن بالتفتيش بعد الضبط إنما هو دفاع موضوعي يكفي للرد عليه اطمئنان محكمة الموضوع إلى وقوع الضبط بناءً على الإذن أخذاً بالأدلة التي أوردتها"[4].

2-2) التفتيش بناءً على رضا المتهم أو من له سلطة على موضع التفتيش:

رضا الشخص بالتفتيش أو ما يسمى بالتفتيش الإرادي[5]، هو حالة تتحقق حينما يعرض رجل الضبط القضائي على الشخص محل التفتيش صراحة أن يفتشه، أو أن يفتش المكان الذي لديه سلطة عليه، فيبدي ذلك الشخص رأيه بالموافقة على التفتيش بشكل إرادي وطوعي، دون تعرضه لأي إكراه أو أي نوع من أنواع العنف، ويلجأ رجل الضبط القضائي إلى هذا النوع من التفتيش في حالة وجود شك لديه بوقوع جريمة ما، ولم تتوفر لديه الأدلة الكافية للكشف عن وقوعها ونسبتها إلى شخص معين، وبالإسقاط على الجرائم الإلكترونية فإن التفتيش في هذه الحالة يكون الهدف منه البحث فيما إذا كان مالك الحاسـوب أو الشبكـة أو المؤسسة التي تدير الخادم أو الملقم أو المضيف أو البيانات الكامنة في الحاسوب مرتكباً أو ضالعاً في الجريمة، ومن الأمثلة على ذلك؛ القبض على متهماً –قد يكون متهم بجريمة أخرى غير الجريمة الكترونية– في مقهى الإنترنت وهو يستعمل حاسوباً ما، فيتراءى لمأمور الضبط القضائي تفتيش الحاسوب الذي ضبط

1 مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 158.

2 فايز محمد راجع غلاب، المرجع السابق، ص 297، **نقلاً عـــن**:

- Jean wifried noel, *Internet et enquéte judiciaire, le droit international de l'internet*; bruylant, 2002, p 245.

3 علي شملال، المرجع السابق، ص 67.

4 حكم محكمة النقض المصرية، رقم 8426 لسنة 87 القضائية، السالف الذكر.

5 مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق ، ص 172.

المتهم يستعمله، فهنا الضابط مطالب بسؤال مالك المقهى أو المدير المسئول فيما إذا كان يقبل بتفتيش الحاسوب المذكور.

ومن الأمثلة أيضاً قيام أحد مزودي الإنترنت بترديد عبارات أمام مرشد قضائي بأن لديه اشتراك بالبريد الإلكتروني مع أحد مروجي المخدرات والمؤثرات العقلية والذي يتم من خلاله عملية الترويج، فيتدخل المرشد القضائي بسؤاله لذلك المزود على إمكانية تفتيش جهازه للتحقق، فإن وافق ذلك الأخير، كان إيجاب صاحب المقهى أو المدير المسئول غير مشوب بضغط من أي نوع، عُد التفتيش حينها صحيحاً ولا يتطلب إذناً، وإن كان العكس فَقَدَ الدليل المستوحى من ذلك التفتيش قيمته الثبوتية، خاصة أمام القضاء[1]، ومن الأمثلة على ذلك ما جـاء في حكم محكمـة النقض المصرية الصادر في مارس 2018، والذي تتلخص وقائعه في قضية اتهمت فيها النيابة العامة امرأة مصرية –الطاعنة– من دائرة المنصورة محافظة الدقِلية بتاريخ: 2015/09/21 باستخدامها مواقع التواصل الاجتماعي "فيس بوك" للترويج لأفكـار مناهضة تحض على كراهية وازدراء النظام القائم بالبلاد، الشيء الذي كَدَّرَ السلـم والأمن العام، وكذا الدعوة لارتكاب أعمال إرهابية ضد هذا الأخير، كما حازت المعنية على جهاز حاسب آلي وملحقاته، ووسائل تسجيل وإصدارات لدعم تلك الأفكار، فأحيلت على إثرها إلى محكمة جنايات المنصورة أين حوكمت في 2015/12/30، وصدر ضدها حكم حضوري يقضي بإيداعها الحـبس لمدة سنة مع الشـغل، فـقام محـاميها بالطـعن بالنـقض بتاريخ 2016/02/25، وكان من بين أوجه الطعن التي استند إليها، أن عملية القبض والتفتيش تمت بدون إذن من النيابة العامة، وفي غير حالات التلبس، ودون تحقق رضاءها قانوناً بتفتيش مسكنها، ولكن جاء الرد على ذلك من محكمة النقض بما يلي: "...من المقرر أن التفتيش الذي يجريه رجال الشرطة في منزل بغير إذن من النيابة العامة ولكن بإذن صاحب المنزل هو تفتيش صحيح قانوناً، ويترتب عليه صحة الإجراءات المبنية عليه، وإذ أذنت الطاعنة لضابط الواقعة بالتفتيش على اعتبار أنها صاحبة المنزل والحائزة له في الفترة التي تم فيها التفتيش، وكان الحكم المطعون فيه قد خلص في استدلال سائغ إلى أن رضاء الطاعنة

1 عمر محمد ابوبكر بن يونس، المرجع السابق، ص 859، نقلاً عن:

- Greg Sergienko, United States v. Hubbell: Encryption and the Discovery of Documents, 7 Rich. J.L. & Tech 31 (2001)

بالتفتيش كان حراً حاصلاً فيما انتهى إليه من أن تفتيش مسكن الطاعنة تم صحيحاً قانوناً، ومن ثم فإن النعي عليه في هذا الخصوص لا يكون سديداً"[1].

وهو ذات الأمر الذي يمكن استنتاجه من حكم محكمة النقض المصرية الصادر في شهر أبريل سنة 2017، والذي جاء فيه: "وقد بان من الأوراق أن دخول ضابطي الواقعة مسكن المتهم كان برضاء من هذا الأخير، وما قاله الحكم من ذلك سائغ وصحيح في القانون، ذلك بأن الرضا بدخول المسكن وتفتيشه يكفي فيه أن تكون المحكمة قد استبانته من وقائع الدعوى وظروفها واستنتجته من دلائل مؤدية إليه، ومن ثم فإن دخول الضـابطـين مسكن الطاعــن وضبـط جهاز الكمبيوتر المستخدم يكون صحيحـاً ومشروعـاً، وتكون المحكمة إذا اعتبرته كذلك ودانت الطاعن استناداً إلى الدليل المستمد منه لم تخالف القانون"[2].

ولأن عملية التفتيش الإرادي قد تمس بخصوصية الأفراد كما هو الحال في التفتيش العادي؛ كان لابد من إحاطتها ببعض الضمانات، ومنها أن تكون صيغة الموافقة على التفتيش بشكل صريح وليس ضمني، وأن تكون مكتوبة، إلا إذا كان الشخص المعني لا يعرف الكتابة، فيجب حينها ذكر ذلك في محضر التفتيش، وهو ما نصت عليه المادة (64) من ق.إ.ج.ج، والفقرة الثانية من المادة (76) من ق.إ.ج.ف[3]، وقد يثور التساؤل هنا حول من يمكنه إبداء الموافقة، هل هو الشخص المراد تفتيشه أم يمكن أن ينوب عنه شخص آخر؟

1 حكـم محكمـة النقض المصرية، الدائرة الجنائيـة، الأربعاء (أ)، في الطعن المقيد بجدول المحكمـة رقم 9680 لسنـة 86 القضائيـة، في الجلسة العلنية المنعقدة بدار القضاء العالي بمدينة القاهرة، في يوم الأربعاء 03 رجب سنة 1439هـ الموافق 21 مارس 2018.

2 حكم محكمة النقض المصريـة، الدائرة الجنائية، الخميس (ج)، في الطعن المقيد بجدول المحكمة رقم 29953 لسنـة 86 القضائيـة، في الجلسة العلنية المنعقدة بدار القضاء العالي بمدينة القاهرة، في يوم الخميس الأول من شعبان سنة 1438هـ الموافق 27 ابريل 2017، ص 04.

3 تنص المادة (64) من ق.إ.ج.ج: "لا يجوز تفتيش المساكن ومعاينتها وضبط الأشياء المثبتة للتهمة إلا برضا صريح من الشخص الذي ستتخذ لديه هذه الإجراءات. ويجب أن يكون هذا الرضا بتصريح مكتوب بخط يد صاحب الشأن، فان كان لا يعرف الكتابة فبإمكانه الاستعانة بشخص يختاره بنفسه، ويذكر ذلك في المحضر مع الإشارة صراحة إلى رضاه..."؛ والمادة (76) من ق.إ.ج.ف، السالف الذكر:

« Les perquisitions, visites domiciliaires et saisies de pièces à conviction ou de biens dont la confiscation est prévue à l'article 131-21 du code pénal ne peuvent être effectuées sans l'assentiment exprès de la personne chez laquelle l'opération a lieu. Cet assentiment doit faire l'objet d'une déclaration écrite de la main de l'intéressé ou, si celui-ci ne sait écrire, il en est fait mention au procès-verbal ainsi que de son assentiment »

نجد أن القضاء الأمريكي لا يشترط هذا الشرط، بل يكتفي في حالة غياب ذلك الأخير أن يحل محله أشخاص آخرون يبدون موافقتهم، وهو ما يمكن أن يتحقق في حالة الآباء حين تفتيش أغراض أبنائهم وكذا غرفهم إذا كانوا صغاراً كقاعدة عامة، الأزواج، أو اشترك شخصان أو أكثر في استخدام أو امتلاك ذات الحاسب الآلي، والذي لم تكن ملفاته محمية بكلمة سر خاصة بمالكه، حينها يمكن لرجال الضبط القضائي الإعتماد على إرادة أحدهما، طالما أن لذلك الأخير السلطة على الحاسب الآلي للقيام بالتفتيش[1]، وهذا ما قضى به القضاء الأمريكي في قضية United States V.Smith؛ وتتلخص وقائع هذه القضية في أن المدعو Smith كان يعيش مع سيدة تدعى Ushman وابنتها، ولما أثير ضده ادعاء التحرش الجنسي بالأطفال، وافقت السيدة Ushman على تفتيش الحاسوب الخاص بالمدعى عليه الموجود داخل المنزل في تجويف مرتبط بحجرة النوم الرئيسية، بالرغم من أن تلك السيدة استعملت حاسوب Smith مرات قليلة، فقررت حينها محكمة المقاطعة بأن السيدة Ushman يمكنها إبداء الموافقة على تفتيش الحاسوب الخاص بالمتهم، حتى وإن كانت تنقصها السلطة الفعلية على الموافقة، وذلك على أساس أنها لم تكن ممنوعة من الدخول إلى المكان الذي كان موجوداً به الحاسوب، كما أن المتهم لم يضع كلمة سر يحمي بها حاسوبه[2].

وعلى إثر ذكر كلمة السر أو كلمة المرور، فإن مواقف التشريعات تباينت في هذا الشأن، في إمكانية إجبار المتهم من عدمها على تزويده سلطات التحقيق المختصة بكلمة مرور، أو كلمة السر التي يكون النظام المعلوماتي المراد تفتيشه مزوداً بها، فالقانون الياباني مثلاً يحظر على الأجهزة المختصة إكراه مالك الحاسب الآلي على الإفصاح عن كلمة المرور، كما يوجد في المجر وبولندا قوانين خاصة بجرائم الحاســب الآلي والإنترنت، والتي توضـح كيفية التعامل مـع تلك الجرائـم والمتهمــين فـيها، ويمكن للمتهم بموجبها عدم طبع سجلات الحاسب الآلي أو إفشاء كلمات السر أو الاكواد الخاصة بالبرنامج[3].

1 نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات"دراسة مقارنة"، دار الفكر الجامعي، الإسكندرية، مصر، 2013، ص.ص: 248-249، **نقلاً عـــن**: عمر محمد بن يونس، الإجـراءات الجنائيـة عـبر الانتــرنت في القانون الأمريكي، الطبعة الأولى، دار النهضة العربية، مصر، 2005، ص 89.

2 نبيلة هبة هروال، المرجع نفسه، ص 251، **نقلاً عن**: عمر محمد بن يونس، نفس المرجع، ص 91.

3 عبد العالي الديربي، محمد صادق إسماعيل، الجرائم الإلكترونيـة دراسـة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والانترنت، الطبعة الأولى، المركز القومي للإصدارات القانونية، مصر، 2012، ص 173.

وفي المقابل هناك رأي آخر يذهب إلى القول بأنه حتى وإن كان لا يجوز إجبار الشخص على الإدلاء بأقواله ضد نفسه، إلا أن ذلك لا يجب إن يكون حائلاً دون إجباره على تقديم معلومات تقتضيها متطلبات التحقيق لإمكانية الولوج للنظام المعلوماتي متى كانت هذه المعلومات بحوزته[1]، ولكن هذا الرأي الأخير لا يستقر مع مقتضيات الأصول المستقرة في الإثبات الجنائي، ويتنافى مع مقتضيات حق الدفاع أمام القضاء الجنائي، كما أن المتهم في الجريمة الإلكترونية قد يعطي كلمة سر معينة يتمكن من خلالها تخريب النظام المعلوماتي المراد تفتيشه، لذا من الأفضل ألا يقحم في هذا الأمر أساساً، مما يدفعنا للقول أن الرأي الأول أقرب إلى الصواب من الرأي الثاني، وإن كان يمكن أن يلزم غير المتهم بإفصاح عن كلمة السر التي بحوزته، كما هو الحال في كلمة السر التي بحوزة مقدم الخدمة، والتي يمكن من خلالها الوصول إلى مصدر أو شبكة الاتصالات التي تمت من خلالها الجريمة الإلكترونية.

وقد لا يكون رضا المتهم بالتفتيش ضرورياً إذا اقتضت ذلك ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في الجرائم الإلكترونية، خاصة إذا صدر إذن من السلطة المختصة بغرض وضع ترتيبات تقنية بالدخول إلى المحـلات السكنية أو غـيرها ولو خـارج المواعيد المحددة في المادة 47 من ق.إ.ج.ج[2].

هذا ويعد التفتيش في الجريمة الإلكترونية حلقة مهمة في دائرة التحقيق الجنائي، التي يمكن من خلالها الحصول على الدليل الإلكتروني لإثبات أو نفي تلك الجريمة، ولأن الأماكن التي تتواجد فيها الأدلـة الإلكترونيـة متعددة، فقد وضعت عدة طرق لتفتيش المنظومة المعلوماتية، كما جـاء في المرشد الفيدرالي الأمريكي، الذي وضع أربع طرق أساسية ممكنة التحقق:

1 أحمد يوسف أحمد حسين الطحطاوي، المرجع السابق، ص 283.

2 جاء في المـادة 65 مكرر 5 من ق.إ.ج.ج، السالف الذكر: "إذا اقتـضت ضرورات التحـري في الجريمة المتلبس بهـا أو التحقيـق الابتـدائي في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو...، ويجوز لوكيل الجمهورية المختص أن يأذن بما يلي:- اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكيـة واللاسلكية. - وضع الترتيبات التقنية، دون موافقـة المعنيـين، من أجـل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو ســرية من شــخص أو عـدة أشخـاص في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص. يسمح الإذن المسلم بغرض وضع الترتيبات التقنية بالدخول إلى المحلات السكنية أو غيرها ولو خارج المواعيد المحددة في المادة 47 من هذا القانون وبغير علم أو رضا الأشخاص الذين لهم الحق عل تلك الأماكن...".

1- تفتيش الحاسب الآلي وطبع نسخة ورقية من ملفات معنية في ذات الوقت.
2- تفتيش الحاسب الآلي وعمل نسخة الكترونية من ملفات معينة في ذات الوقت.
3- عمل نسخة إلكترونية طبق الأصل من جهاز التخزين بالكامل في الموقع، وبعد ذلك يتم إعادة عمل نسخة تعمل من جهاز التخزين خارج الموقع للمراجعة.
4- ضبط الجهاز وإزالة ملحقاته ومراجعة محتوياته خارج الموقع. [1]

أكيد أنه بعد كل إجراء تقوم بها الجهة المختصة، إلا وتدون ما تم التوصل إليه من أدلة ونتائج في محضر[2]، والذي يجب أن يستوفي الشروط التي نص عليها القانون، تطبيقاً لما ورد في المادة 18 من ق.إ.ج.ج والتي أوجبت على ضباط الشرطة القضائية أن يحرروا محاضر بأعمـالهم وأن يبادروا بـغير تمهل إلى إخطار وكيل الجمـهورية بالجنايات والجنح التي تصل إلى علمهم. وعليهم بمجرد إنجاز أعـمالهم أن يوافوه مباشرة بأصول المحاضر التي يحررونها مصحوبة بنسخة منها مؤشر عليها بأنها مطابقة لأصول تلك المحاضر التي حرروها وكذا بجميـع المستندات والوثائق المتعلقة بها وكذا الأشياء المضبوطة. وترسل المحاضر الخاصة بالمخالفات والأوراق المرفقة بها إلى وكيل الجمهورية لدى المحكمة المختصة. ويجب أن ينوه في تلك المحاضر عن صفة الضبط القضائي الخاصة بمحرريها.

كما أن المحاضر التي يضعها ضابط الشرطة القضائية طبقاً للقانون ينبغي تحريرها في الحال وعليه أن يوقع على كـل ورقـة مـن أوراقـها[3]؛ مع الأخذ بعين الإعتبار مسألة رضا الشخص الذي ستتخذ ضـده الإجراءات[4]، كما يتعين على ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص أن يحرر محضراً عن كل عملية اعتراض وتسجيل المراسلات وكذا عن عمليات وضع الترتيبات التقنية وعمليات الالتقاط والتثبيت والتسجيل الصوتي أو السمعي

1 حسين بن سعيد الغافري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الانترنت، ص 14، مقال متاح على الموقع الإلكتروني الموالي: *http://previous.eastlaws.com/Uploads/Morafaat/33.pdf*، والذي تم تصفحه يوم 2018/07/30.

2 نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت- في مرحلة جمع الاستدلالات دراسة مقارنة-، دار الفكر الجامعي، الطبعة الأولى، الإسكندرية، 2007، ص 263.

3 المادة 54 من ق.إ.ج.ج، السالف الذكر.

4 المادة 64 من نفس القانون.

البصري. يذكر بالمحضر تاريخ وساعة بداية هذه العمليات والانتهاء منها[1]، كما يجب أن يكون الإذن المسلم مكتوباً ومسبباً، وذلك تحت طائلة البطلان، وأن تذكر في الإذن الجريمة التي تبرر اللجوء إلى هذا الإجراء وهوية ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته. ويحدد هذا الإذن مدة عملية التسرب التي لا يمكن أن تتجاوز أربعة (4) أشهر[2]. وذلك لكي تكون لهذه المحاضر القوة الثبوتية أمام القضاء[3].

البند الثاني: التفتيش داخل وخارج الدولة.

للتطرق لمحتويات هذه الجزئية من الدراسة، ستكون انطلاقتنا من الفقرة الثانية من المادة الخامسة (05) من القانون 09-04 الخاص بقواعد الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والتي أجاز بموجبها المشرع الجزائري تمديد التفتيش إلى منظومة معلوماتية ثانية غير المنظومة المعلوماتية الأولى؛ مثلما يحدث عندما يكون جهاز الحاسب الآلي للمتهم موضوع التفتيش متصلاً بجهاز حاسب آخر مملوك للغير أو متصـلاً بنهاية طرفيـة أخـرى، ووجدت أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى غير المنظومة المبحوث فيها، وأن هذه المعطيات يمكن الدخول إليها انطلاقاً من المنظومة الأولى، على أن يتم ذلك بعد إعلام السلطة القضائية المختصة مسبقاً بذلك، وبكل سرعة[4]؛ لأن المعطيات في المنظومة المعلوماتية يمكن تغييرها أو محوها بكل سهولة، مما قد يتسبب في ضياع الدليل الإليكتروني المبحوث عنه[5].

1 المادة 65 مكرر 9 من نفس القانون.

2 المادة 65 مكرر 9 من نفس القانون.

3 ممـدوح حسن مانع العدوان، نادر عبد الحليم السلامات، المرجع السابق، ص 64؛ أبو عامر محمد زكى، الإثبات في المـواد الجنائية، الفنية للطباعة والنشر، الإسكندرية، مصر، 1985، ص 156 وما بعدها.

4 محمودي سماح، مشكلات التفتيش الجنائي عن المعلومات في الكمبيوتر والانترنت، مجلة الحقوق والعلوم السياسية، جامعة عباس لغرور خنشلة، الجزائر، الجزء الأول، العدد الثامن، جوان 2017، ص 337، ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة دكتـوراه العلـوم في الحقوق تخصص قانون العقوبات والعلوم الجنائية، قسم الحقوق،كلية الحقوق والعلـوم السياسـية، جامعـة باتنـة 01، الموسم الجامعي 2015-2016، ص 205.

5 تنص الفقرة الأولى من المادة (1/23) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحرّرة بالقاهرة بتاريخ 21 ديسمبر سنة 2010، المصادق عليها بالمرسوم الرئاسي رقم 14-252، السالفة الذكر على أن: "تلتزم كل دولة طرف بتبني الإجراءات الضروريـة لتمكين السلطات المختصة من إصدار الأمر أو الحصول على الحفظ العاجل للمعلومـات المخزنة بما في ذلك معلومات تتبع معلومات

ولأن التفتيش في منظومة معلوماتية أخرى غير المنظومة المبحوث فيها يتسم بطابع الخصوصية، فرض المشرع الجزائري ضرورة إعلام السلطة القضائية المختصة مسبقاً قبل البدء في الإجراء، كذلك فعل المشرع المصري من خلال المادة السادسة (6) من القانون رقم 175 لسنة 2018 الخاص بمكافحة جرائم تقنية المعلومات، والتي أشارت إلى ضرورة إصدار أمر مسبب من قبل جهة التحقيق المختصة لمأموري الضبط القضائي المختصين من أجل البحث والتفتيش والدخول والنفاذ إلى برامج الحاسب الآلي وقواعد البيانات، وغيرها من الأجهزة والنظم المعلوماتية، أو سحب أو جمع أو التحفظ على البيانات والمعلومات، أو تتبع تلك الأنظمة المعلوماتية في أي مكان أو حاسب آلي أو دعامة الكترونية أو نظام تكون فيه، وهو الأمر المقصود في مواد المرسوم الرئاسي رقم 14-252، المتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة في 2010، والقرار الرئاسي رقم 276 لسنة 2014، بشأن الموافقة على انضمام جمهـورية مصر العربية إلى الاتفاقـية العربية لمكافحة جرائم تقنية المعلومات الموقعة في القاهرة بتاريخ 21 ديسمبر 2010[1]، كالمادة 22، والمادة 26 منهما، واللتان تلزمان كل دولة طرف بتبني الإجراءات الضرورية، التي تتمكن من خلالها سلطاتها المختصة من التفتيش لأجل الوصول إلى معلومات موجودة أو مخزنة في نظام تقنية معلومات، أو بيئة أو وسيط تخزين معلومات؛ أو الوصول إلى جزء منها.

ولأجل التنفيذ الجيد لهذه الإجراءات وللمحافظة على سرية التحقيقات وسرعتها، فقد مدد المشرع الجزائري من الاختصاص المحلي لجهـات التحقيق في الجرائم الإلكترونية،كما جاء في المواد: 16، 37، و40 من ق.إ.ج.ج.

المستخدمين والتي خزنت على تقنية معلومات وخصوصا إذا كان هناك اعتقاد أن تلك المعلومات عرضة للفقدان أو التعديل"، خاصة وأن الفقرة الثانية (2-ج) من المادة (22) من نفس المرسوم نصت على أن جمع الأدلة عن الجرائم الإلكترونية يجب أن يكون بشكل إلكتروني.

1 الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحرّرة بالقاهرة بتاريخ 21 ديسمبر سنة 2010، المصادق عليها بالمرسوم الرئاسي رقم 14-252، السالفة الذكر؛ القرار الرئاسي رقم 276 لسنة 2014، بشان الموافقة على انضمام جمهورية مصر العربية إلى الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الموقعة في القاهرة بتاريخ 21 ديسمبر 2010، الصادرة في الج.ر للجمهورية مصر العربية، العدد 46 الصادرة في 13 نوفمبر سنة 2014.

وبالنسبة إلى امتداد التفتيش في الجرائم الإلكترونية إلى خارج الإقليم المنفذ فيه إجراء التفتيش هي احتمالية واردة جداً، لأنه وكما رأينا فإن الجريمة الإلكترونية تتسم بكونها جريمة عابرة للحدود يُعد أو يشرف؛ أو يخطط لها المجرم الإلكتروني في بلد وتنفذ في بلد آخر أو عدة بلدان أخرى، وقد تمول من مجرمين متواجدين في عدة بلدان وتنفذ في بلـد من تلك البلـدان أو في بلد مختلف عنها، لذا فإن هذا النوع من التفتيش تفرضه مقتضيات إيجاد سبل مكافحة الجريمة الإلكترونية عبر سائر التشريعات الدولية والعالمية، فلا غنى عن آليات تعاونية دولية لتصدي لهذه الجريمة، لهذا نجد مختلف التشريعات نصت في جانب من قوانينها الداخلية على مـواد تخدمها في هـذا المجـال، فالتشريع الجزائري ومن خلال الفقرة الثالثة (3) من المادة الخامسة (5) من القانون 09-04 بَيَّنَ بأنه، إذا كانت المعطيات المبحوث عنها مخزنة في منظومة معلوماتية موجودة خارج الإقليم الوطني، فإن عملية الحصول عليها تكون بمساعدة السلطات الأجنبية المختصة طبقاً للاتفاقيات الدولية ذات الصلة، أو وفقاً لمبدأ المعاملة بالمثل، إذا لم يوجد مثل هذا النوع من الاتفاقيات[1].

ونصت المادة 16 من ذات القانون أنه يمكن للسلطات المختصة قبول طلبات المساعدة القضائية وتقديم تلك المساعدات في إطار الاتفاقيات الدولية والمعاملة بالمثل من أجل القيام بالتحريات أو التحقيقات القضائية الضرورية لمعاينة الجرائم الإلكترونية المنصوص عليها في هذا القانون وكشف المجرمين الضالعين في ارتكابها.

ونجد أن المشرع المصري هو الآخر أشار إلى نفس الجزئية من خلال الفقرة الأولى من المادة الرابعة (4) من القانون رقم 175 لسنة 2018، كما حثت على ذلك مواد الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، كالمادة 32 التي دعت الدول الأطراف إلى تبادل المساعدات فيما بينهم من أجل تسهيل التحقيقات أو الإجراءات أو جمع الأدلة الإلكترونية، أما المادة 40 من ذات الاتفاقية[2] فلقد بينت أنه بإمكان أي دولة طرف، وبدون الحصول على تفويض من الدولة الطرف

1 ناجية شيخ، حول مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسيـة، جامعـة الشهيد حمه لخضر بالوادي، المجلد التاسع (09)، العدد الثاني (02)، جوان 2018، ص 698؛ براهيمي جمـال، مكافحة الجرائم الالكترونيـة في التشريع الجزائري، المجلة النقدية للقانون والعـلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، العدد الأول، 2017، ص 154.

2 المادة 32، والمادة 40 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحرّرة بالقاهرة بتاريخ 21 ديسمبر سنة 2010، المصادق عليها بالمرسوم الرئاسي رقم 14-252، السالفة الذكر؛ ونفس المادة من القرار الرئاسي رقم 276 لسنة 2014، بشأن الموافقة على

الأخرى، أن تصل إلى معلومات تقنية المعلومات المتوفرة للعامة، وأن تصل أو تستقبل من خلال أنظمتها المعلوماتية للمعلومات الموجودة لدى الدولة الطرف الأخرى، إذا ما حصلت على الموافقة الطوعية والقانونية من الشخص الذي يملك السلطة القانونية لكشف تلك المعلومات إلى الدولة الطرف، وهي ذات الأحكام التي نجدهـا في نص المادة 32 من اتفاقيـة بودابست[1]، ذلك لأن هذه الاتفاقية تعد مرجعاً يُقْتدى به في مجال مكافحة الجريمـة الإلكترونيـة، الشيء الذي دفع العديد من الدول للمصادقة على هذه الاتفاقية، كما فعلت المملكة المغربية، والتي أصبحت منذ تاريخ: 2018/10/01 جزءاً من القانون الوطني المغربي، لذا يستوجب على المشرع المغربي اتخاذ جميع الإجراءات اللازمة للقيام بالإصلاحات التي تمكنه من التماشي وبنود اتفاقية بودابست، خاصة وكما رأينا سابقاً أن الدستور المغربي يمنح السمو للاتفاقيات الدولية على التشريعات الوطنية فور المصادقة عليها[2]. ولكن في انتظار ذلك يطبق القانون المغربي نص المادة 713 من قانون المسطرة

انضمام جمهورية مصر العربية إلى الاتفاقية العربية لمكافحـة جرائم تقنية المعلومـات، السالف الذكر، إذ نصـت المادة 40 على:"يجـوز لأي دولة طـرف، وبدون الحصول على تفويض من دولة طـرف أخرى : 1- أن تصل إلى معلومات تقنية المعلومات المتوفرة للعامة (مصدر مفتوح) بغض النظر عن المـوقع الجـغرافي للمعلومات. 2- أن تصل أو تستقبل- من خلال تقنية المعلومات في إقليمها- معلومات تقنية المعلومات الموجودة لدى الدولة الطرف الأخرى وذلك إذا كانت حاصلة على الموافقة الطوعية والقانونية من الشخص الذي يملك السلطة القانونية لكشف المعلومات إلى تلك الدولة الطرف بواسطة تقنية المعلومات المذكورة."

1 Conseil de l'Europe, **Convention sur la cybercriminalité (STE n° 185)**; Budapest, 23.XI.200, Article 32 : « Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au publicUne Partie peut, sans l'autorisation d'une autre Partie, :a. accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données; oub. accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre Etat, si la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique. »

- **لتفاصيل أكثر حول الموضوع يمكن الاطلاع على:** إيهاب السنباطي، الترجمة الجديدة والكاملة للاتفاقية المتعلقة بالجريمة الإلكترونية (بودابست 2001) والبروتوكول الملحق بها، دار النهضة العربية، القاهرة، 2009، ص.ص: 56-57.

2 لأجل مناقشة تلك الإصلاحات تم عقد يوم دراسي حول: "إجراءات التعاون الدولي وفقاً لأحكام اتفاقية بودابست المتعلقة بالجريمة المعلوماتية"، بمدينة مراكش يوم الاثنين 03 ديسمبر 2018، برئاسة الوكيل العام للملك رئيس النيابة العامة، **المصـــدر:** عبد الكبير الميناوي، لقاء بمراكش يتدارس إجراءات التعاون الدولي لمكافحة الجريمة المعلوماتية، دعا إلى اعتماد التقنيات الحديثة في التحقيق الجنائي والارتقاء بقدرات المحققين، جريدة الشرق الاوسط، العدد 14616، بتاريخ: 04 ديسمبر 2018، متاحة على الرابط الإلكتروني التالي: *https://aawsat.com/home/article/1489666/* تاريخ الإطلاع: 2020/06/15.

الجنائية المغربية فيما يخص التعاون القضائي الدولي، والذي يكون على أساس الاتفاقيات الدولية أو المعاملة بالمثل[1].

وبالعودة إلى التشريعات الغربية المقارنة، نجدها هي الأخرى سمحت بإمكانية امتداد التفتيش إلى نظام معلوماتي آخر غير النظام محل التفتيش؛ ومنها التشريع الألماني بمقتضى القسم 103 من قانون الإجراءات الجزائية الألماني[2]، وكذا القانون البلجيكي من خلال المادة 88 التي أضيفت في قانون تحقيق الجنايات بمقتضى القانون الصادر في 23 نوفمبر سنة 2000، التي تنص على أنـه: "إذا أمر قاضي التحقيق بالتفتيش في نظام معلوماتي، أو في جزء منه، فإن هذا البحث يمكن أن يمتد إلى نظام معلوماتي آخر يوجد في مكان آخر غير مكان البحث الأصلي، ويتم هذا الامتداد وفقاً لضابطين: 1- إذا كان ضرورياً لكشف الحقيقة بشأن الجريمة محل البحث، 2- إذا وجدت مخاطر تتعلق بضياع بعض الأدلة، نظراً لسهولة عملية محو أو إتلاف، أو نقل البيانات محل البحث إلى موقع آخر"[3]، ونص مشروع قانون جرائم الحاسوب بهولندا على أنه يجوز لجهات التحقيق مباشرة التفتيش داخل الأمـاكن، وتفتيش نظـم الحاسوب المرتبطة حتى وإن كانت في دولـة أخرى، بشرط أن يكون التدخل مؤقتا وأن تكون البيانات المفتش عنها لازمة لإظهار الحقيقة[4].

---

1 ظهير شريف رقم 1.02.255 صادر في 25 من رجب 1423، الموافق 03 أكتوبر 2002، الخاص بتنفيذ القانون رقم 22.01 المتعلق بالمسطرة الجنائية المغربية، الصادر في الج.ر عدد 5078 بتاريخ 30 يناير2003، ص 315، معدل ومتمم بالقانون رقم 32.18، الصادر بتنفيذه الظهير الشريف رقم 1.19.92 بتاريخ 5 ذي القعدة 1440، الموافق 8 يوليو 2019، الصادر في الج.ر عدد 6796 بتاريخ 18 يوليو 2019، ص 5036، تقضي المادة 713 من ق.م.ج.م على أن: "تكون الأولوية للاتفاقيات الدولية على القوانين الوطنية فيما يخص التعاون القضائي مع الدول الأجنبية. لا تنطبق مقتضيات هذا الباب، ألا في حالة عدم وجود اتفاقيات أو في حالة خلو تلك الاتفاقيات من الأحكام الواردة به".

2 أحمد محمود مصطفى، جرائم الحاسبات الآلية في التشريع المصري (دراسة مقارنة)، دار النهضة العربية، الطبعة الأولى، القاهرة، 2010، ص 140؛ محمد أبو العلا عقيدة، التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، المنعـقدة بإمارة دبي بدولة الإمارات العربية المتحدة في الفترة من 26-28 ابريل 2003، ص 34 وما بعدها؛ **كما ورد لدى:**

- Kaspersen (W. K. Henrik), Computer crime and other crime against information Technology in nether lands .R.I. D .P, 1993 , pp :479 -498.

3 حسين بن سعيد الغافري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الانترنت، موجود على الموقع الإلكتروني الموالي: http://previous.*eastlaws.com/Uploads/Morafaat/33.pdf*، تاريخ الإطلاع: 2018/08/04، وكذلك عن:

- Kaspersen (W.K.Henrik), computer crime and other crime against Information Technology In Netherlands, R.I.D.P 1993, p 479

4 **نقلاً عـن:**

وفي مثال عن هذا النوع من أنواع التفتيش، ما حدث في ألمانيا أثناء التحقيق عن جريمة غش وقعت على بيانات حاسب آلي متواجد في ألمانيا، وحين القيام بذلك الإجراء تبين وجود اتصال بين الحاسوب محل التفتيش وشبكة اتصالات في سويسرا أين يتم تخزين البيانات، وعندما أرادت سلطات التحقيق الألمانية ضبط تلك البيانات، لم تتمكن من ذلك، إلا بعد التماس المساعدة من السلطات السويسرية[1].

أما في القانون الفرنسي فإن الفقرة الاولى من المادة (57-1) من ق.إ.ج.ف هي التي تجيز التفتيش خارج الحدود الإقليمية شرط مراعاة بنود الاتفاقيات الدولية السارية المفعول التي توضح كيفية الوصول إلى المعطيات والبيانات المبحوث عنها[2]، وهو ما بينه حكم لمحكمة النقض الدائرة الجنائية، والذي أكد أن عملية التفتيش التي تمت بموجب الاتفاقيات الدولية وخاصة أحكام المادة (32) من اتفاقية بودابست بشأن الجريمة الإلكترونيـة، والمؤرخة في 23 نوفمبر 2001، والتي بموجبها يجوز لأي طرف دون إذن من الطرف الآخر، الوصول إلى بيانات الحاسب الآلي المخزنة والموجودة في دولة أخرى إذا ما حصل على الموافقة القانونية والطوعية من الشخص المخول له قانوناً بالإفصاح عنها[3].

أما في الولايات المتحدة الأمريكية، إذا ثبت لرجال الضبط القضائي قبل القيام بالتفتيش أن بعض أو جميع البيانات مخزنة بعيداً خارج الأراضي الأمريكية، فإنه يتعين عليه القيام بأعمال تتراوح ما بين الملاحظة غير الرسمية إلى طلب رسمي للمساعدة موجه إلى الدولة المعنية، وأكثر من ذلك فإن بعض الدول قد تعترض على محاولات السلطات الأمريكية الاطلاع على حواسيب موجودة

- Durham (COLO) The emergingstrures of criminal information law.trcing the contours of anew pardigm general report for the A.I.D.P collwium R.I.D.P. 1993 p.15.

- **وقد أشار إلى ذلك:** طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي، ورقة عمل مقدمـة للمؤتمر المغاربي الأول حول: المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، ليبيا، يومي 28 و29 اكتوبر 2009، ص 63.

1 خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجريمة الإلكترونية (دراسة مقارنة)، المرجع السابق، ص.ص: 205-206.

2 l'article 57-1 du code de procédure pénale français,Op.Cit : « …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... » ; Voir :Myriam Quéméner, Les nouvelles dispositions de lutte contre la cybercriminalité issues de la loi du 13 novembre 2014 renforçant la lutte contre le terrorisme, La base de données juridique des Éditions Dalloz, France, AJ Pénal 2015, p:32, p 03.

3 Cour de cassation, chambre criminelle, Audience publique du 6 novembre 2013, N° de pourvoi: 12-87130, ECLI:FR:CCASS:2013:CR05362(Publié au bulletin).

داخل حدودها، رغم أنه قد يتراءى لرجل الضبط الأمريكي القائم بتنفيذ تفتيش داخل الولايات المتحدة وفقاً لإذن التفتيش، أنه يقوم بالتفتيش ضمن حدود بلده، ولكن الواقع أن التفتيش يتم خارج الحدود الإقليمية الأمريكية، لذا يجب طلب المساعدة القضائية قبل القيام بالتفتيش، وإلا اعـتبر ذلك الإجراء من قبيل انتهاك السيادة والجوسسة الإلكترونية التي تمس بالأمن القومي لأي دولة[1].

وفي قضية للولايات المتحدة الأمريكيـة ضـد غورشكوف (Wl 1024026 2001) في عـام 2000، والتي تتلخص وقائعها حول سلسلة من الاختراقات مست أنظمة الحواسب الآلية لمجموعة من الشركات في الولايات المتحدة، وبعد قيام مكتب التحقيقات الفيدرالي (FBI) بالتحقيق في الموضوع، تمكن من تحديد الأشخاص المسؤولين على ذلك، وهما الروسيان: فاسيلي غورشكوف وأليكسي إيفانوف (Vasiliy Gorshkov and Alexey Ivanov)، ولأجل القبض عليهما قام مكتب التحقيقات الفيدرالي (FBI) برسم خطة لإغرائهم للقدوم للولايات المتحدة، فقام هذا الأخير بإنشاء شركة تدعى إنفيتا (Invita)، ثم تمت دعوة غورشكوف وإيفانوف إلى الشركة لإجراء مقابلة؛ خلال المقابلة طُلب من غورشكوف وإيفانوف إثبات مهاراتهما في اختراق أجهزة الحواسيب الآلية، ولأجل ذلك زودهما مكتب التحقيقات الفيدرالي (FBI) بحاسوب محمول للوصول إلى حواسيبهم المنزلية حيث يحتفظان بأدوات القرصنة الخاصة بهما، ولم يكونا يعرفان أن مكتب التحقيقات الفيدرالي استخدم ذلك الجهاز كأداة للحصول على هوية المستخدم وكلمة المرور للمتسللين، وعلى أثر ذلك تم القبض عليهما فوراً، وفي وقت لاحق استخدم مكتب التحقيقات الفيدرالي دون أمر تفتيش اسم المستخدم وكلمة المرور اللتين تم التقاطهما من الحاسوب المحمول لتنزيل المعلومات من أجهـزة الحواسيب المنزلية لجورشكوف وأيفانوف في روسيـا، والتي استخدموها كدليل ضد المتهمين. فقام المتهمون بالدفع في عدم مشروعية الأدلة لأنه تم الحصول عليها من أجهزتهما الخاصة في روسيا انتهاكا للتعديل الرابع، كما يعد ذلك تعدٍ على سيادة روسيا، وبالتالي كان على الولايات المتحدة كمسألة مجاملة، أن تسعى للحصول على إذن من السلطات الروسية للبحث في أجهزة الحاسوب الخاص بكل من غورشكوف وإيفانوف.

وعلى الجانب الآخر، جادل مكتب التحقيقات الفيدرالي بأنه نظراً لأن عملية التنزيل من

1 مصطفى على خلف، المرجع السابق، ص.ص: 96-97.

مصدر الحاسوب لا تشكل عملية بحث، فمن غير الضروري أن يحصل مكتب التحقيقات الفيدرالي على موافقة السلطات الروسية، وعليه رفضت المحكمة اقتراح الروس، واعتمدت على حقيقة أن التعديل الرابع لا يجوز التذرع به إلا عندما يكون هناك تفتيش وضبط في المعنى المتوخى في التعديل الرابع، ومع ذلك؛ فإن عملية تنزيل المعلومات من جهاز الحاسوب في بلد آخر من قبل عملاء مكتب التحقيقات الفيدرالي لا يشكل بحثاً أو ضبطاً؛ نظراً لأن نسخ البيانات على أجهزة الحاسوب الروسية لم تتداخل مع المصلحة الخاصة للمدعى عليهما، لأن البيانات ظلت سليمة وبدون تغيير ويمكن الوصول إليها من قبل المدعى عليهما علاوة على ذلك،لم يكن من الممكن لوكلاء مكتب التحقيقات الفدرالي (FBI) تأمين مذكرة اعتقال قبل أن يتمكنوا من تنزيل البيانات حيث كان من الممكن أن يقوم المتآمرون بتدمير تلك الأدلة[1].

وكما وضحنا سابقاً فإن امتداد عملية التفتيش إلى خارج الحدود الإقليمية الوطنية لابد منها في الجريمة الإلكترونية، إلا أن ذلك يجب أن يتم وفق المعايير القانونية المنصوص عليها في القوانين الداخلية أو في الاتفاقيات الدولية، أو حتى بموجب المعاملة بالمثل، رغم أن مثل هذا الإجراء قد يستغرق وقتاً طويلاً وغير مضمون النجاح بسبب التنوع التشريعي الخاص بالجريمة الإلكترونية بين مختلف الدول[2]. ولهذا فإن الدول تسعى دائماً إلى إيجاد حلول قانونية للعراقيل التي تواجهها في هذا المجال، لذا نجدها تبرم العديد من الاتفاقيات الثنائية التي تتمكن من خلالها تسهيل عملية التفتيش عن الجرائم ومرتكبيها[3].

1 DR. Adel Azzam Saqf Al- Hait, *Jurisdiction in Cybercrimes: A Comparative Study*, Journal of Law, Policy and Globalization, *www.iiste.org*, ISSN 2224-3240 (Paper) ISSN 2224-3259 (Online), Vol.22, 2014, p.p: 77-76.

2 Anastasios Papathanasiou1, Alexandros Papanikolaou, and others, *Legal and Social Aspects of Cyber Crime in Greece*, Conference Paper, October 2014, p 10-11, **On the website**: *https:// www. researchgate.net /publication /260390705_Legal_and_Social_Aspects_of_Cyber_Crime_in_Greece*. Date Viewing : 04/09/2019.

3 ولأجل تسهيل عملية البحث والتفتيش عن الجرائم ومرتكبيها فقد صادقت الجزائر على العديد من الاتفاقيات، والتي تطرقت في بعض بنودها لعملية البحث والتفتيش عن الجرائم ومرتكبيها، منها على سبيل المثال: المادة 40 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحرّرة بالقاهرة بتاريخ 21 ديسمبر سنة 2010، المصادق عليها بالمرسوم الرئاسي رقم 14-252، السالفة الذكر ، المادة الأولى (1) والمادة 14 من الاتفاقية المتعلقة بالتعاون القضائي في المجال الجزائي بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وحكومة الجمهورية الفرنسية، المؤرخة في 9 جمادى الثانية عام 1439 الموافق 25 فبراير سنة 2018، الموقعة بباريس في 5 اكتوبر سنة 2016، المصادق عليها بالمرسوم الرئاسي رقم 18-73، الصادرة في الج.ر.ج رقم 13 المؤرخة في 28 فبراير سنة 2018؛ المادة 16 من الاتفاقية المتعلقة بالتعاون القضائي في المجال الجزائي بين الجمهورية الجزائرية الديمقراطية الشعبية وفيدرالية روسيا، مؤرخة

الفرع الثاني: الضبط أو الحجز في الجريمة الإلكترونية.

تكملة لحلقة التحقيق الجنائي في الجريمة الإلكترونية، يأتي الدور للحديث عن ضبط أو حجز الأدلة الإلكترونية التي توصلت إليها الجهات المختصة، وهو العثور على أدلة الجريمة التي بوشر بشأنها التحقيق والتحفظ عليها، والضبط هو الغاية من التفتيش ونتيجته المباشرة، لأن بطلان التفتيش يؤدي إلى بطلان الضبط[1]، كون هذا الأخير لا يجوز أن يقع على شيء إلا لاعتباره دليلاً من أدلة الجريمة التي يجري التفتيش بشأنها، ولذلك فإنه يباشر من أجل الحقيقة المطلقة[2]، فالضبط في الجريمة الإلكترونية هو استخدام البرامج المهمة من أجل الولوج للبيانات المراد ضبطها إلى جانب وضع اليد على تلك الدعائم المادية[3].

نظم المشرع الجزائري ضبط أو حجز الأدلة الإلكترونية في عدة مواد قانونية؛ أولها المادة السادسة (6) من القانون 09-04 الخاص بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والتي تتمكن من خلالها السلطة التي تباشر التفتيش في منظومة معلوماتية، من ضبط –أو حجز– معطيات تكون مفيدة في كشف الجرائم، أو مرتكبيها[4]، والمادة 27 من المرسوم الرئاسي رقم 14-252، المتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة في 2010، والتي تلزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من ضبط وتأمين معلومات تقنية المعلومات التي يتم الوصول إليها بعد القيام بعملية التفتيش، والتي نصت عليها الفقرة الأولى من المادة 26 من ذات المرسوم، حيث يتم الضبط؛ إما بضبط تقنية المعلومات كاملة، أو جزء منها، أو عمل نسخة من المعلومات التي توجد بها والاحتفاظ بها، وإما إزالة أو منع الوصول إلى تلك المعلومات.

في 18 جمادى الثانية عام 1440 الموافق 23 فبراير سنة 2019، الموقعة بالجزائر في 10 اكتوبر سنة 2017، المصادق عليها بالمرسوم الرئاسي رقم 19-78، الصادرة في الج.ر.ج رقم 14 المؤرخة في 28 فبراير سنة 2019.

1 أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال في ضوء القانون رقم 09-04، مذكرة مقدمة لنيل شهادة الماجستير، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح بورقلة، الجزائر، 2013، ص 94، **نقلاً عن**: محمد سعيد نمور، أصول الإجراءات الجزائية (شرح لقانون أصول المحاكمات الجزائية)، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2005، ص 359.

2 مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص.ص 208-209.

3 نبيل محمد عثمان عرعارة، المرجع السابق، ص 156؛ نبيلة هبة هروال، المرجع السابق، ص 266.

4 بوحليط يزيد، المرجع السابق، ص 91.

وجاء في الفقرة الرابعة من المادة 15 من المرسوم الرئاسي رقم 20-183، الذي يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها على أن مديرية المراقبة الوقائية واليقظة الإلكترونية تتولى مهمة "جمع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها وتتبعها بغرض استعمالها في الإجراءات القضائية"[1]، ودون أن ننسى مواد قانون الإجراءات الجزائية، وخاصة المادة 45، والمادة 47، والمادة 84 من ذات القانون[2]، والتي أشارت إلى ضرورة أن لا يتعدى الضبط الأشياء والوثائق النافعة في إظهار الحقيقة، أو التي قد يضر إفشاؤها بسير التحقيق، ومن المواد أيضاً المادة 394 مكرر 06 من قانون العقوبات[3]، وكذلك المادة 146 من قانون حقوق المؤلف والحقوق المجاورة، والتي يمكن بموجبها للأعوان المحلفون التابعون للديوان الوطني لحقوق المؤلف والحقوق المجاورة القيام بصفة تحفظية بحجز نسخ دعائم المصنفات أو الأداءات المقلدة، كما يمكن للجهة القضائية المختصة أن تأمر بحجز كل عتاد استخدام أساساً لصنع الدعائم المقلدة[4].

1 مرسوم رئاسي رقم 20-183، المؤرخ في 21 ذي القعدة عام 1441 الموافق 13 يوليو سنة 2020، المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الصادر بالج.ر.ج رقم 40 المؤرخة في 18 يوليو سنة 2020، ونفس النص جاء ضمن الفقرة الثانية من المادة 12 من المرسوم الرئاسي رقم 19-172، المؤرخ في 3 شوال عام 1440، الموافق 2 جوان سنة 2019، الذي يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها، الصادر في الج.ر.ج العدد 37، المؤرخة في 09 جوان سنة 2019 (الملغى).

2 تنص المادة 45 من ق.إ.ج.ج على: "... تغلق الأشياء أو المستندات المحجوزة ويختم عليها إذا أمكن ذلك، فإذا تعـذرت الكتابة عليها فانها توضع في وعـاء او كيس يضـع عليه ضابـط الشـرطـة القضائيـة شـريطا من ورق ويختم عليه..."، وجاء في المادة 47 من ذات القانون أنه: "يجوز إجراء الحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار والليل بناءً على إذن مسبق من وكيل الجمهورية المختص، كما يمكن لقاضي التحقيق القيام بعملية الحـجز ليلا ونهاراً وفي أي مكان من التراب الوطني، أو يأمر بذلك ضباط الشرطة القضائية المختصين"؛ تنص المادة 84 من ذات القانون: "يجب إحصاء الأشياء والوثائق المضبوطة ووضعها في أحراز مختومة، وانه لقاضي التحقيق أو ضابط الشرطة القضائية المنوب عنه وحدهما الحق في الاطلاع على المستندات قبل ضبطها".

3 تنص المادة 394 مكرر 06 من الأمر رقم 66-156، المتضمن قانون العقوبات المعدل والمتمم، السالف الذكر: "مع الاحتفاظ بحقوق الغير حسن النية، يحكم بمصادرة الأجهزة والبرامج والرسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها".

4 جـاء في المادة 146 من الأمر رقم 03-05، المؤرخ في 19 يوليو 2003 والمتعلق بحقـوق المؤلف والحقوق المجاورة، السالف الذكر، ص 03 أنه: "فضلاً عن ضباط الشرطة القضائية، يؤهل الأعوان المحلفون التابعون للديوان الوطني لحقوق المؤلف والحقوق المجاورة للقيام بصفة تحفظية بحجز نسخ دعائم المصنفات أو الاداءات المقلدة، شريطة وضعها تحت حراسة الديوان. يخطر فوراً رئيس الجهة القضائية المختصة بناءً على محضر مؤرخ وموقع قانوناً يثبت النسخ المقلدة المحجوزة. تفصل الجهة القضـائية في طلب الحجز التحفظي خلال

أما المشرع المصري فقد تطرق للضبط في الجريمة الإلكترونية من خلال الفقرة الأولى من المادة السادسة (06) من قانون رقم 175 لسنة 2018 المتعلق بمكافحة جرائم تقنية المعلومات، إذ يمكن بمقتضاها لمأموري الضبط القضائي المختصين بموجب أمر مسبب من جهة التحقيق المختصة، ولمدة ثلاثين يوماً قابلة للتجديد مرة واحدة، ضبط أو سحب أو جمع أو التحفظ على أنظمة المعلومات أو على البيانات والمعلومات أو تتبعها في أي نظام أو برنامج أو دعامة الكترونية، أو حاسب آلي أو برامجه وقواعد بياناتـــه، وغيرها من الأجهزة والنظـم المعلوماتيـة، وفي أي مكان تكون موجودة فيه، مع الحرص على ألا يؤثر ذلك في استمرارية النظم المعلوماتية وتقديم الخدمة إن كانت تستعمل لذلك؛ كل ذلك من أجل الوصول إلى حقيقة ارتكاب الجرائم الإلكترونية والحصول على الأدلة الإلكترونية التي تسلم للجهة مصدرة الأمر بالضبط.

يلاحظ هنا أن المشرع المصري حدد للقائم بعملية الضبط في الجريمة الإلكترونية مدة ثلاثين يوماً قابلة للتجديد مرة واحدة؛ لأن الضبط في هذه الجريمة يجب أن يتسم بالسرعة وإلا ضاعت الأدلة الإلكترونية المراد ضبطها، كما نصت المادة 27 من القرار الرئاسي رقم 276 لسنة 2014، المتعلق بالموافقة على انضمام جمهورية مصر العربية إلى الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الموقعة في القاهرة بتاريخ 21 ديسمبر 2010، على ذلك على النحو المبين سابقاً في

ثلاثة (3) أيام على الأكثر من تاريخ إخطارها". والمادة 147 من نفس القانون: "يمكن رئيس الجـهة القضائية المختصة أن يأمر بناءً على طلب من مالك الحقوق أو ممثله بالتدابير التحفظية الآتية: -إيقاف كل عملية صنع جارية ترمي إلى الاستنساخ غير المشروع للمصنف أو للأداء المحمي أو تسويق دعائم مصنوعة بما يخالف حقوق المؤلفين و الحقوق المجاورة. – القيام ولو خارج الأوقات القانونية بحجز الدعائم المقلدة والإيرادات المتولدة من الاستغلال غير المشروع للمصنفات والاداءات. – حجز كل عتاد استخدام أساساً لصنع الدعائم المقلدة ..."، لأنه وبحسب المادة 152 من نفس القانون فإنه: "يعتـبر مرتكباً لجنحة التقليد كل من ينتهك الحقوق المحمية بموجب هذا الأمر فيبلغ المصنف أو الأداء عن طريق التمثيل أو الأداء العلني، أو البث الإذاعي السمعي البصري، أو التوزيع بواسطة الكبل أو أية وسيلة نقل أخرى لإشارات تحمل أصواتاً أو صوراً وأصواتاً أو بأي منظومة معالجة معلوماتية"، وبحسب المادة الرابعة (04) من معاهدة المنظمة العالمية للملكية الفكرية (الويبو) بشان حق المؤلف، المؤرخة في 22 جمادى الأولى عام 1434 هـ، الموافق 03 أبريل سنة 2013، المنعقدة بجنيف بتاريخ 20 ديسمبر سنة 1996، المصادق عليها بالمرسـوم الرئـاسي رقم 13-123، الصادر في الج.ر.ج العدد 27، الصـادر في 22 مايو 2013، فإن برامج الحاسوب تعد من المصنفات الأدبية والتي يجب أن تحظى بالحماية بقولها: "تتمتع برامج الحاسوب بالحماية باعتبارها مصنفات أدبية بمعنى المادة 2 من اتفاقية برن، وتطبق تلك الحماية على برامج الحاسوب أياً كانت طريقة التعـبير عنها أو شكلها". **للمزيد يمكن الرجوع إلى:** عبد الوهاب ملياني، إشكالية التوازن بين حرية تداول المعلومات الإلكترونية والحماية القانونية من الاعتداء عليها، مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور بالجلفة، الجزائر، المجلد الثاني (02)، العدد (22)، تاريخ النشر: 2015/03/15، ص 41.

ذات المادة من المرسوم الرئاسي رقم 14-252 السالف الذكر، كما بينت مواد من ق.إ.ج.م، على أن عملية الضبط تشمل كل ما يحتمل أن يكون قد استعمل في ارتكاب الجريمة أو نتج عن ارتكابها أو ما وقعت عليه الجريمة، وكل ما يفيد في كشف الحقيقة، من خلال نصوصه، ومنها المادة 53، والمادة 55، والمادة 91[1].

وبحثاً عن كيفية تعامل القوانين الأخرى مع عملية ضبط الأدلة الإلكترونية، نجد المادة 251 من قانون الإجراءات الجنائي اليوناني تعطي لسلطات التحقيق إمكانية القيام بأي شيء يكون ضرورياً لجمع وحماية الدليل، وبمقدور المحقق أن يعطي أمراً للخبير لجمع البيانات، والتي يمكن أن تقبل كدليل في المحاكمة الجنائية، كما تمنح المادة 487 من القانون الجنائي الكندي سلطة إصدار إذن لضبط أي شيء طالما تتوفر أسس معقولة للاعتقاد بأن الجريمة ارتكبت أو يشتبه في ارتكابها، أو أنه سوف ينتج دليلاً على وقوع الجريمة، أو أن هناك نية في أن يستخدم ذلك الشيء في ارتكاب الجريمة[2].

أما المشرع الألماني فقد خصص المادة 92 وما يليها للضبط رغم أنه لم ينص صراحة على ضبط المعطيات الإلكترونية، وإنما اكتفى بالنص على ضبط أو تسجيل أي معلومات تظهر مفيدة لكشف الحقيقة[3]. وفي التشريع الفرنسي فالمادة 56 من ق.إ.ج.ف كما رأينا سابقاً، تعد مادة من المواد التي تطرق من خلالها المشرع الفرنسي إلى إجراء عملية الضبط[4]، فحسب هذه المادة يجوز

1 المادة 53 من ق.إ.ج.م، السالف الذكر: "لمأموري الضبط القضائي أن يضعوا الأختام على الأماكن التي بها آثار أو أشياء تفيد في كشف الحقيقة ولهم أن يقيموا حراساً عليها. ويجب عليهم إخطار النيابة العامة بذلك في الحال، وعلى النيابة إذا ما رأت ضرورة ذلك الإجراءات أن ترفع الأمر إلى القاضي الجزئي لإقراره."، والمادة 55 من نفس القانون: "لمأموري الضبط القضائي أن يضبطوا الأوراق والأسلحة وكل ما يحتمل أن يكـون قد استعـمل في ارتكـاب الجريمة أو نتج عن ارتكابها أو ما وقعت عليها الجريمة وكل ما يفيد في كشف الحقيقة، وتعرض هذه الأشياء على المتهم، ويطلب منه إبداء ملاحظاته عليها ويعمل بذلك محضر يوقع عليه من المتـهم أو يذكر فيه امتـناعه عن التوقيع"، الفـقرة الثانية من المادة 91 من نفس القانـون أيضاً: "...، ولقاضي التحقيـق أن يفتـش أي مكان ويضبـط فيه الأوراق والأسلحـة وكل ما يحتمل أنه استعمل في ارتكاب الجريمة أو نتج عنها أو وقعت عليه وكل ما يفيد في كشف الحقيقة، وفي جميع الأحوال يجب أن يكون أمر التفتيش مسبباً".

2 رابحي عزيزة، المرجع السابق، ص 281؛ **نقلاً عن**: علي عدنان الفيل، إجراءات التحري وجمع الأدلـة والتحـقيق الابـتدائي في الجريمة المعلوماتية دراسة مقارنة، المكتب الجامعي الحديث، الإسكندرية، مصر، 2012، ص 42.

3 إحسان طبال، المرجع السابق، ص.ص 165-166.

4 Article 56 du Code de procédure pénale française **(**Modifié par LOI n°2016-731 du 3 juin 2016 - art. 58), Op. Cit.

لضابط الشرطة القضائية المرخص له من قبل النائب العام الانتقال دون تأخير للقيام بعملة الضبط إذا كانت طبيعة الجريمة تسمح بالحصول على الأدلة عن طريق الاستيلاء على الأوراق، أو المستندات أو بيانات الحاسوب أو الأشياء الأخرى الموجودة في حوزة أشخاص يبدو أنهم شاركوا في الجريمة، أو يحتفظون بوثائق أو معلومات أو أشياء تتعلق بالوقائع المدانة.

وفي القانون البلجيكي تطرق المشرع البلجيكي إلى قابلية المكونات المعنوية للضبط بموجب المادة 39 من القانون تحقيق الجنايات البلجيكي[1]، حين أصدر تعديل قانون التحقيق الجنائي بالقانون المؤرخ في 28 نوفمبر2000 مضيفا المادة 39 مكرر[2]، في الفقرات من الثانية إلى السادسة Les paragraphes 2 à 6 du nouvel article 39bis C.I.C Belge ، كما أشار المشرع الأمريكي إلى الضبط من خلال المرشد الفيدرالي، والذي حدد من خلال أساليب الضبط المختلفة وفقاً لطبيعة كل مخالفة والقانون الصادر بشأنها، إذ أجاز القانون الأمريكي مصادرة القـطع الصلبة، كالحاسوب ككل؛ كما هو الحال في وجود انتهاك لحقوق النسخ أو العدوان على العلامات التجارية عبر الإنترنت، بحسب ما هو مقرر في قانون حق المؤلف Copy Right Act، وقانون العلامات التجارية Lanham Act في القسم (d) 34 منه[3].

في بعض الأحيان قد تتطلب عملية ضبط الأدلة الإلكترونية، أو الأدلة بصفة عامة وجود تعاون بين الدول لتسهل العملية ونجاحها، والمادة 17 من القانون 09-04 السالف الذكر أشارت إلى هذه النوع من أنواع التعاون بشرط عدم المساس بالسيادة الوطنية أو النظام العام، وعلى ألا تستعمل المعلومات المتحصل عليها في غير ما هو موضح في الطلب؛ إضافة إلى المحافظة على سرية

1 صالح شنين، الحماية الجنائية للتجارة الإلكترونية "دراسة مقارنة"، رسالة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقـوق، جامعة أبو بكر بلقايـــد، تلمسان، الجزائر، السنة الجامعية 2012-2013، ص 256، **وقد أشار إلى ذلك أيضاً**: هلالي عبد الله، التـفتيش في نظم الحاسب الآلي وضمانات المتهم المعلوماتي دراسة مقارنة، دار النهضة العربية، القاهرة، مصر، 1993، ص 202.

2 Code D'instruction Criminelle. SECTION II. – Mode de Procedeur du Roi dans L'exercice de leurs Fonctions.: Art. 39 bis.Iinséré par L 2000-11-28/34, art. 7; En vigueur : 13-02-2001 1er. Sans préjudice des dispositions spécifiques de cet article, les règles de ce code relatives à la saisie, y compris l'article 28sexies, sont applicables aux mesures consistant à copier, rendre inaccessibles et retirer des données stockées dans un système informatique 2 ou une partie de celui-ci.

3 عمر محمد ابوبكر بن يونس، المرجع السابق، ص 870.

المعلومات المبلغة[1]، كما سعت الجزائر وكغيرها من الدول إلى عقد اتفاقيات في المجال الجزائي لأجل الوصول إلى نتائج أفضل، والحصول على أدلة تفيد في كشف الجرائم ومرتكبيها، ومنها على سبيل المثال؛ اتفاقياتها مع جمهورية الصين الشعبية، وحكومة المملكة المتحدة لبريطانيا العظمى وإيرلندا الشمالية، وحكومة دولة الكويت[2].

ومن أهم ما جاء أيضاً في الاتفاقيات بخصوص ضبط الأدلة، ما ورد في المادة 16 من اتفاقية بودابست[3]، والمادة 29 من نفس الاتفاقية على أن يكون الضبط في شكل طلب تقدمة دولة طرف إلى دولة أخرى طرف بغية الحصول على الحفظ العاجل للبيانات المخزنة في نظام معلوماتي يقع ضمن إقليمها، ويكون طلب الحفظ متعلقاً بما تود الدولة الطالبة أن تقدم طلباً بشأنـه للمساعدة المتبادلة للبحث وضبط وتأمين وكشف المعلومات[4]، وتطبق نفس الأحكام في التشريع الفرنسي بموجب المرسوم رقم 2006-580 المؤرخ 23 ماي 2006 بشأن نشر اتفاقية الجريمة الإلكترونية، التي تمت في بودابست في 23 نوفمبر 2001[5].

1 المادة 17 من القانون 09-04، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، السالف الذكر:" تتم الاستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظية وفقا للاتفاقيات الدولية ذات الصلة والاتفاقيات الدولية الثنائية ومبدأ المعاملة بالمثل".

2 الاتفاقية بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وجمهورية الصين الشعبية المتعلقة بالتعاون القضائي في المجال الجزائي، المؤرخة في 20 جمادى الأولى عام 1428 الموافق 06 جوان 2007، الموقعة ببيكين في 06 نوفمبر سنة 2006، المصادق عليها بالمرسوم الرئاسي رقم 07-175، الصادر في الج.ر.ج رقم 38 المؤرخة في 10 جوان سنة 2007. الاتفاقية المتعلقة بالتعاون القضائي في المجال الجزائي بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وحكومة المملكة المتحدة لبريطانيا العظمى وإيرلندا الشمالية، المؤرخة في 20 ذي القعدة عام 1427 الموافق 11 ديسمبر 2006، الموقع بلندن في 11 جويلية سنة 2006، المصادق عليها بالمرسوم الرئاسي رقم 06-465، الصادر في الج.ر.ج رقم 81 المؤرخة في 13 ديسمبر سنة 2006. واتفاقية التعاون القانوني والقضائي في المجال الجزائي بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وحكومة دولة الكويت، المؤرخة في 21 ذي الحجة عام 1436 الموافق 5 اكتوبر سنة 2015 الموقعة بالجزائر في 12 اكتوبر سنة 2010، المصادق عليها بالمرسوم الرئاسي رقم 15-255، الصادر في الج.ر.ج رقم 53 المؤرخة في 8 اكتوبر سنة 2015.

3 Bertrand Warusfel, *Procédure pénale et technologies de l'information: de la convention sur la cybercriminalité à la loi sur la sécurité quotidienne*, Revue droit et défense, Numéro 2002/1, (pp.17-22), France, p :03.

4 إلهام بن خليفة، الحماية الجنائية للمحررات الإلكترونية من التزوير، أطروحة مقدمة لنيل درجة دكتوراه علوم في العلوم القانونية والإدارية تخصص قانون جنائي، قسم الحقوق،كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، الموسم الجامعي 2015-2016، ص ص 353-354.

5 Décret n° 2006-580 du 23 mai 2006 portant publication de la Convention sur la cybercriminalité, faite à Budapest le 23 novembre 2001, JORF n°120 du 24 mai 2006 page 7568 texte n° 2.

البند الأول: الأشياء محل الضبط فـــي الجريمة الإلكترونية.

قد يتساءل المرء عن الأشياء التي يمكن أن تضبط أو تحرز في الجريمة الإلكترونية، خاصة وأن أكثر الأدلة التي قد نتحصل عليها هي عبارة عن نبضات كهربائية، فإذا كان التفتيش ينتهي بتحديد موضع ومكان البيانات التي كانت موضوع التفتيش، فإن المعالجة التي تجرى عليها لجعلها مرئية للاطلاع عليها وإثباتها، أو إخراجها من الحاسوب في صورة مستندات مطبوعة لا تعد تفتيشاً عن أدلة الجريمة، ولكنها تمثل وصلاً إلى هذه الأدلة، ومن ثم ضبطاً لها، فتلك الكيانات المعنوية تكون بذلك قد تحولت إلى أشياء مرئية مقروءة تكتسب كياناً مادياً يمكن بواسطته ضبطها ونقلها من مكان لآخر، فالضبط ينصب على الأشياء المادية وغير المادية، والتوغل داخل المنظومة المعلوماتية، والعثور على المعطيات والبيانات المخزنة في النظام أو النظم المرتبطة بالنظام محل الاشتباه هدفه ضبط ما يعد ذو فائدة من بيانات ليكون دليل يتحدد بها الركن المادي للجريمة[1].

كما يمكن أن يكون العقار محل ضبط، ومثالها أن يعتقد مأمور الضبط القضائي أو عضو النيابة العامة، أن الجريمة الإلكترونية قد تركت آثاراً بمكان ما، وخلفت به أشياء تفيد التحقيق وتقتضي مقتضياته الكشف عنها، وهو ما أجازته المادة 53 من ق.إ.ج.م[2]، وقد يشمل الضبط العقار بالتخصيص كالحاسب الآلي بمقهى الإنترنت وملحقاته من طابعة أو آلات تصوير مثل السكانير، وكذلك الأشياء الثابتة إذا نزعت من أصلها المثبتة به مثل الكابلات الموصلة للحاسب الآلي، وقد يطال الضبط الأشياء الموجودة في عقار كأثاث مقهى الإنترنت مثلاً.

نصت بعض الأحكام القضائية كما سيتضح منها على أشياء تكون محل للضبط لأجل الوصول إلى الأدلة، ومنها ما ورد في حكم محكمة النقض بتاريخ: 2015/12/03، ومما جاء فيه أنه

1 خالد عياد الجلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، المرجع السابق، ص 170؛ على جبار الحسيناوي، جرائم الحاسوب والانترنت، دار اليازوري العلمية للنشر والتوزيع، عمان، الأردن، 2009، ص 108، **نقلاً عـن**: يونس عرب، جرائم الكمبيوتر والانترنت، ورقة عمل مقدمة إلى مؤتمر الأمن العربي، تنظيم المركز العربي للدراسات والبحوث الجنائية، أبوظبي، من 10 إلى 12 فيفري 2002.

2 المادة (53) من ق.إ.ج.م: "لمأموري الضبط القضائي أن يضعوا الأختام على الأماكن التي بها آثار أو أشياء تفيد في كشف الحقيقة ولهم أن يقيموا حراساً عليها. ويجب عليهم إخطار النيابة العامة بذلك في الحال، وعلى النيابة إذا ما رأت ضرورة ذلك الإجراءات أن ترفع الأمر إلى القاضي الجزئي لإقراره"، كما أجازت المادة (54) من ذات القانون بالتظلم من ذلك الإجراء بقولها:"لحائز العقار أن يتظلم أمام القاضي من الأمر الذي أصدره بعريضة إلى النيابة العامة، وعليها رفع التظلم إلى القاضي فوراً".

في شهري أوت وسبتمبر من سنة 2013 قام ضباط من قطاع الأمن الوطني، ونفاذاً لإذن النيابة العامة بتفتيش مساكن ومجموعة من الأماكن التي كانت تابعة لمجموعة من المتهمين، حيث عثر فيها على عدة أشياء منها على سبيل المثال: عدد من الأوراق التنظيمية والاسطوانات المدمجة وخمسة حواسب آلية محمـولة، وتسعة عشر (19) هاتفاً محمولاً مختلفي الأنواع، وهاتف ثريا، وكاميرتي فيديو ولاب توب وعدد USB 02، وبطاقة ذاكرة وأربع وسائط تخزين، وفلاشه وقناع غاز، وثمان عشرة (18) وحدة معالجة مركزية وماسح ضوئي، وعدد أجهزة صوتيات وإضاءة ومقويات إشارة، وعدد من أجـهزة الاتصال، وثلاث وحـدات معالجـة مركزيـة، وعدد من شرائط الفيديو وأخـتام خاصة، وبعض الأجهزة التقنية الخاصة بالتصوير والإضاءة، وغيرها من الأشياء[1].

وفي حكم آخر بتاريخ: 2017/06/07، في قضية أُتُّهِمَ فيها أربعة وعشرين (24) شخص من بينهم طفل لم يتجاوز الثامنة عشرة من عمره بتكوين جماعة إرهابية، حيث تم العثور لديهم على عدة أشياء؛ منها: مجموعة من الحواسب الآلية، ووحدات معالجة آلية، ووحدات تخزين، وهواتف محمولة، وأقراص صلبة، وثماني وعشرين (28) اسطوانة مدمجة، وجهازين لتشغيلهما، وعثر في موضع آخر من السيـارة على ثلاثـة حواسيب آلية محمـولة، وجهاز لوحي وحقيبة تحوي وحـدة تخـــزين، ومجموعة من الأسلاك، والتوصيلات، وجهاز للاتصال بشبكـة المعلومات الدولية[2].

ولكن في كثير من الأحيان قد يتعذر الوصول إلى الأجزاء الصلبة المراد ضبطها، لذا اتجه التشريع المقارن إلى إيجاد أساليب أخرى تصلح لكي يتم الضبط بمقتضاها، مثل نسخ المواد التي تحتاج إلى فك شفرتها لكي يتم التعرف على محتوياتها، أو نسخ البيانات التي تم وضعها في إطار برمجة تحتوي على قنبلة زمنية أو موقوتة، إضافة إلى أسلوب تجميد التعامل بالحاسوب أو أحد القطع المكونة له، والتي تم استخدامها في ارتكاب الجريمة، والتي تفيد في استخراج دليل على ارتكاب الجريمة الإلكترونية، ومن أمثلتها الخوادم التي تحتوي على مواقع دعارة، أو حلقـات نقـاش، أو مواقع هكرز، أو ملفات فيروسية[3]، كما يمكـن أن تثار صعوبـة عند ضبط النظام كله

1 حكم محكمة النقض المصرية، في الطعن المقيد بجدول المحكمة برقم 21819 لسنة 85 القضائية، السالف الذكر.

2 حكم محكمة النقض المصرية، الدائرة الجنائيـة، الأربعاء (أ)، في الطعن المقيد بجدول المحكمـة رقم 29658 لســنة 86 القضـائية، السالف الذكر، ص 10.

3 عمر محمد أبوبكر بن يونس، المرجع السابق، ص 870، **نقلاً عــن**:

- Id.See also, Sega Enterprises, Ltd v.Maphia, 857 F.Supp.679 (N.D.Cal 1994).

أو الشبكة كلها، كونُها تحتوي على عناصر لا يمكن فصلها، ولأنها تتضمن على عناصر مهمة لإثبات الجريمة الإلكترونيـة، لذا يتعين إعمال مـبدأ التناسب من أجل إقامة التوازن بين مصلحتين؛ مصلحة الدولة في كشف الحقيقة ومصلحة صاحب النظام في تسيير أعماله وعدم ضياع فرص الربح خاصة في المشاريع الاقتصادية، ومبدأ التناسب (Principe de Proportionnalité) يرمي إلى اقتصار الضبط على الأدلة التي تفيد في كشف الحقيقة، دون أن يؤدي ذلك إلى تعطيل كل العمل في النظام والشبكات المتصل به، ومن التطبيقات القضائية ما قضت به المحكمة الفيدرالية الألمانيـة بإلغاء قرار الضبط الذي ورد على (220) دسك بالإضـافة إلى الوحـدة المركزيـة، لمخالفته مبدأ التناسب[1].

ولأن الضبط يجب أن يتم بمقتضى إذن من الجهـة المختصـة[2]، اعتمدت الشرطة التابعة للإدارة الأمنية لمركز المعلوماتية الكندي على نموذج استخلصته من واقع الخبرة العملية لديها، والذي يتضمن في صيغته الأمور الآتية:

- البحث وضبط برنامج أو كيان الحاسب المنطقي، والذي يدخل فيه برنامج التطبيق ونظم التشغيل وما يتفرع عنه من نظم.
- البيانات المستخدمة بواسطة برنامج الحاسب أو كيانه المنطقي.
- السجلات التي تثبت استخدام الأنظمة الآلية لمعالجة البيانات.
- السجلات المستخدمة في عملية الولوج في النظام الآلي لمعالجة البيانات"[3].

1 شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، الإسكندرية، مصر، 2007، ص 358.

2 حكم محكمة النقض المصرية، الدائرة الجنائية، الخميس (ج)، في الطعن المقيد بجدول المحكمـة رقم 29953 لسنـة 86 القضـائية، مرجع سابق، ص 04: "... لما كان ذلك، وكان البين من مدونات الحكم أن ضابطي الواقعة قد استصدرا إذناً من النيابة العامة بتفتيش سنترال... والمملوك ... لضبط أجهزة الحاسب الآلي الثابتة والمحمولة ووحدات تخزين المعلومات وكذلك تتبع كافة الوصلات الصادرة من السنترال لأي أجهزة استخدمت في ارتكاب الواقعة فانتقلا إلى مكانه وتقابلا مع مالكه ومديره المسؤول، فقرر أن المتهم ينتمي لجماعة ... ولديه وصلة انترنت مأخوذة منه فصعدا لمسكنه لتتبع تلك الوصلة وبالطرق على بابه فتح لهما المتهم الباب وسمح بدخولهما وقام الشاهد الثاني بفحص جهاز الحاسب الآلي الخاص بالطاعن مما مفاده أن تفتيشاً ما لم يتم ولم يحصل من مأمور الضبط ثمة إجراء بمسكن المتهم ينم بذاته عن أنهما قاما بالبحث والتقصي داخله بحثاً عن المضبوطات. ولما كان ذلك، فإن ما ينعاه الطاعن في هذا الصدد يكون على غير أساس ...".

3 فتوح الشاذلي، عفيفي كامل عفيفي، المرجع السابق، ص 367.

كما أكدت القوانين والأحكام القضائية على أن الضبط يجب أن يقتصر بشكل صارم على ما هو ضروري وبشكل واضح، ويجب ألا يتجاوز الحدود المبينة في تصريح الزيارة[1].

البند الثانـــي: الإستعانة بالخبرة من أجل ضبط الأدلـة الإلكترونـيـة.

بسبب طبيعة مسرح الجريمة الإلكترونية، وعدم وجـود دليل رقمي مـرئي يمكن فهمـه بالـقراءة، وسهولة محو ذلك الدليل أو تدميره في زمن قصير جداً، وكذا قلة الآثار المادية الناتجة عن هذه الجريمة، وضخامة البيانات التي يجب فحصها من قبل المحقق الجنائي، وكذا قلة خبرة بعض العاملين في الأجهزة الأمنية[2]، خاصة أن عملية استعادة البيانات الأصلية التي تم العبث بها يمكن أن يؤدي إلى إلغاء الدليل الرقمي، مثلما حدث عندما طلبت إحدى دوائر الشرطة بالولايات المتحدة الأمريكية من شركة تعرضت للقرصنة أن تتوقف عن تشغيل الحاسب الآلي خاصتها لتتمكن من وضعه تحت المراقبة بهدف كشف مرتكب الجريمة، ونتيجة لذلك أتلف ما كان قد سُلم من ملفات وبرمجيات. وفي واقعة أخرى تدور وقائعها حول إبلا غ إحدى الشركات عن وضع قنبلة منطقية بنظام حاسبها الآلي من قبل أحد الأشخاص، وعند التدقيق والتحقيق في الأمر تبين أن الشركة وقبل إبلا غ السلطات المختصة كانت قد استدعت خبيراً للتحقق من صحة ادعاء ذلك الشخص وإبطال مفعول القنبلة إن وجدت، وبالفعل نجح الخبير في اكتشاف القنبلة وإزالتها من

1 Cour de cassation, chambre criminelle, Audience publique du 24 avril 2013, N° de pourvoi: 12-80331, ECLI:FR:CCASS:2013:CR01858: « alors que la saisie doit être strictement limitée à ce qui est évidemment nécessaire et ne doit pas dépasser les limites strictes fixées par l'autorisation de visite».

2 هناك أسلوبان يعمل بهما الخبير التقني، الأسلوب الأول: القيام بتجميع وتحصيل لمجموعة المواقع التي تشكل جريمة في حد ذاتها كما هو الشأن في التهديد Intimidation أو النصب Fraud أو السب Defamation أو جرائم النسخ Infringement of Copyrights وبث صور فاضحة بقصد الدعاية للتحريض على ارتكاب جرائم الدعارة والرقيق ودعارة الأطفال وغيرها من الجرام الإلكترونية، وبعدها يقوم الخبير بعملية تحليل رقمي لهذه المواقع لمعرفة كيفية إعدادها البرمجي ونسبتها إلى مسارها الذي أعدت فيه، كما يقوم بتحديد عناصر حركتها، وكيف تم التوصل إلى معرفتها، وليصل بعدها لمعرفة بروتوكول الانترنت IP الذي ينسب إلى جهاز الحاسوب الذي صدر عنه هذا الموقع. والأسلوب الثاني: هو قيام الخبير بعملية تجميع وتحصيل لمجموعة المواقع التي لا يشكل موضوعها جريمة في ذاته، وإنما تؤدي حال تتبع موضوعاتها إلى قيام الإفراد بارتكاب جرائم كما هو الحال في المواقع التي تساعد الغير على القيام بتحديد مسار الدخول على مواقع دعارة من أماكن متفرقة دون لزوم القيام بالدخول من مكان ثابت، وأيضاً معلومات عن كيفية صنع فيروسات معلوماتية، أو بث بعض الثغرات البرمجية الموجودة في نظام معلوماتي ما. **ينظر فـــي ذلك:** نواف بن نايف بن دبيان الحربي، الضبط والتفتيش في الجريمة المعلوماتية في النظام السعودي (دراسة تحليلية تطبيقية)، رسالة مقدمة استكمالاً لمتطلبات الحصول على درجة الماجستير في العدالة الجنائية تخصص التشريع الجنائي الإسلامي، قسم العدالة الجنائية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، 2011، ص 73؛ حسين بن سعيد بن سيف الغافري، السياسة الجنائية في مواجهة جرائم الانترنت"دراسة مقارنة"، دار النهضة العربية، القاهرة، مصر، سنة 2009، ص 445.

البرنامج الموضوعة فيه، وعندما تولت الشرطة التحقيق اتضح أنه بإزالة القنبلة أتلفت كل الأدلة الرقمية الدالة على وجود الجريمة[1].

مما سبق يتبين أن الاستعانة بالخبرة الفنية لضبط الأدلة الرقمية –الإلكترونية– والمحافظة عليها حتى تصلح لأن تكون أدلة إثبات مقبولة أمام الجهات القضائية أمر ضروري، فمن حيث المبدأ يجب أن يعامل الدليل المستمد من الحاسب الآلي أو من أي نظام معلوماتي بعناية، وبطريقة يحافظ بها على قيمته الاستدلالية، إذ يجب حماية البيانات التي قد تكون عرضة للضرر أو التغيير بسبب وجود مجالات كهرومغناطيسية أو أجهزة الإرسال وغيرها من أنواع التشويش[2]. ولقد أجاز المشرع الجزائري الاستعانة بالخبرة في الجريمة الإلكترونية من خلال الفقرة الرابعة (04) من المادة الخامسة (05) من القانون 09-04 المتضمن القواعد الخاصة بالوقايـة من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ومن خلال المادة 27 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة في 2010، والمصادق عليها بالمرسوم الرئاسي رقم 14-252[3]، إضافة إلى مواد من ق.إ.ج.ج؛ بداية بالمادة 143 إلى غاية المادة 156 منه[4]، كما جاء في الفقرة الثالثة من

1 فاديا سليمان، الجرائم المعلوماتية وأثرها على العمليات المالية والمصرفية، مجلة الدراسات المالية والمصرفية، السنة الثالثة والعشرون، العدد الأول، الأردن، مارس 2015، ص ص 07-08.

2 John Ashcroft, Electronic Crime Scene Investigation:A Guide for First Responders, Written and Approved by the Technical Working Group for Electronic Crime Scene Investigation, Washington, July 2001, p : 29.

- **ينظر في ذلك أيضاً**: عبد الناصر محمد فرغلي، محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية دراسة تطبيقية مقارنة، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف لعربية للعلوم الأمنية، الرياض، السعودية، الأيام من 12 إلى 14 نوفمبر 2007، ص 33، **نقلاً عن**: هشام فريد رستم، الجـوانب الإجـرائية للجـرائم المعلوماتية – دراسـة مقـارنة –، مكتبة الآلات الحـديثة، أسيوط، مصر، سنة 1994، ص.ص: 142-143.

3 المادة الخامسة (05) من القانون رقم 09-04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، السالف الذكر جاء فيها: "... يمكن السلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها"؛ والمادة 27 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة في 2010، والمصادق عليها بالمرسوم الرئاسي رقم 14-252، السالفة الذكر: "...2- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى أي شخص لديه معرفة بوظيفة تقنية المعلومات، أو الإجراءات المطبقة لحماية تقنية المعلومات من أجل تقديم المعلومات الضرورية لإتمام تلك الإجراءات المذكورة في الفقرتين (1، و2) من المادة 26 من الاتفاقية".

4 نذكر على سبيل المثال المادة 143 من ق.إ.ج.ج التي جاء فيها: "لجهات التحقيق أو الحكم عندما تعرض لها مسالة ذات طابع فني أن تأمر بندب خبير إما بناءً على طلب النيابة العامة وإما من تلقاء نفسها أو من الخصوم. وإذا رأى قاضي التحقيق انه لا موجب للاستجابة لطلب الخبرة فعليه أن يصدر في ذلك أمراً مسبباً في أجل ثلاثين (30) يوماً للفصل في الطلب، تسري من تاريخ

المادة 15 من المرسوم الرئاسي رقم 20-183، الذي يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، على تولي مديرية المراقبة الوقائية واليقظة الإلكترونية مهمة مساعدة السلطات القضائية ومصالح الشرطة القضائية بناءً على طلبها، بمدها بالخبرات اللازمة لمكافحة الجريمة الإلكترونية[1]، وخصص المشرع الأردني للخبرة المواد 39، 40، و41، من قانون أصول المحاكمات الجزائية[2].

كما نص قانون تحقيق الجنايات البلجيكي بموجب نص المادة 88 منه على جواز الاستعانة بالخبرة من قبل مأمور الضبـط وقاضي التحقيـق[3]، ومن خلال الفصـول من 194 إلى 209 من قانون المسطرة الجنائية، تطرق المشرع المغربي إلى إجراء الخبرة، خاصة إذا كان موضوع الانتقال يحتاج إلى معلومات لا تتوفر للقاضي، لكون الخبرة إجراء يرمي إلى استخدام احد الفنيين لتوضيح مسألة غامضة يحتاج حلها إلى كفاءة فنية لا يملكها القاضي [4]، وبالعودة للتشريع المصري نجده أشار من خلال الفقرة 21 من المادة الأولى من القانون رقم 175 لسنة 2018 الخاص بمكافحة جرائم تقنية المعلومات إلى أن الخبرة هي: " كل عمل يتصل بتقديم الاستشارات أو الفحـص أو المراجعـة أو التقييم أو التحليـل في مجالات تقنية المعلومـات"، وبينت المادة 10 من ذات القانون أن هناك سجلان لقيد الخبراء؛ الأول مخصص للفنيون والتقنيون العاملون بالجهاز القومي لتنظيم الاتصالات، والثاني يخصص للخبراء من خارج الجهاز، كما نظمت المواد من 85 إلى 89 من

إخطارها. ويكون قرارها غير قابل لأي طعن. ويقوم الخبراء بأداء مهمتهم تحت مراقبة قاضي التحقيق أو القاضي الذي تعينه الجهة القضائية التي أمرت بإجراء الخبرة".

1 المرسوم الرئاسي رقم 20-183، الذي يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، السالف الذكر.

2 قانون أصول المحاكمات الجزائية الأردني رقم: 328 بتاريخ 07 آب 2001، المعدل بالقانون رقم: 359 بتاريخ: 2001/08/16: محمد نافع فالح رشدان العدواني، حجية الدليل الإلكتروني كوسيلة من وسائل الإثبات في المسائل الجزائية "دراسة مقارنة بين القانونين الكويتي والأردني"، قدمت هذه الرسالة استكمالاً لمتطلبات الحصول على درجة الماجستير في القانون العام، قسم القانون العام، كلية الحقوق، جامعة الشرق الأوسط، الأردن، تشرين الثاني 2015، ص 87.

3 رابحي عزيزة، المرجع السابق، ص 272.

4 تنص المادة 194 من ق.م.ج.م على: "يمكن لكل هيئة من هيئات التحقيق أو الحكم كلما عرضت مسألة تقنية، أن تأمر بإجراء خبرة إما تلقائيا وإما بطلب من النيابة العامة أو من الأطراف. يقوم الخبير أو الخبراء بمهمتهم تحت مراقبة قاضي التحقيق أو المحكمة المعروضة عليها القضية أو القاضي الذي تعينه المحكمة عند الاقتضاء. إذا ارتأى قاضي التحقيق أنه لا موجب للاستجابة للطلب الخاص بإجراء الخبرة، فعليه أن يصدر في ذلك أمرًا معللاً قابلاً للاستئناف، طبق الكيفيات وضمن الآجال المنصوص عليها في المادتين 222 و223".

ق.إ.ج.م عملية ندب الخبراء[1]، ومواد أخرى يتضح من خلالها اهتمام المشرع المصري والمشرع الإماراتي بتنظيم أعمال الخبرة، فقد أجاز كلا القانونين لكل من مأموري الضبط والنيابة العامة وقاضي التحقيق الاستعانة بالخبراء في المادتين 29 من ق.إ.ج.م، والمادة 40 من قانون الإجراءات الجزائية الإماراتي.

إن الاستعانة بالخبير من أجل إثبات الجريمة الإلكترونية هو شيء حتمي تفرضه طبيعة هاته الجريمة، إذ تتضح تلك الأهمية عند غياب الخبير، فقد يعجز حينها رجال الشرطة أو جهات التحقيق عن كشف غموض الجريمة الإلكترونية ويصعب جمع الأدلة حولها، والتي قد تمحى أو تدمر أو تتلف نتيجة لجهل أو إهمال المتعامل معها، فانتداب الخبراء ذوي المعرفة بتقنيات المنظومة المعلوماتية ومناقشتهم في كيفية وقوع الجريمة، ومواجهة المتهم بتقرير الخبرة وما ورد فيه، قد ينهي التحقيق إما بثبوت واقعة الجريمـة قبل المتهم وإحالته إلى المحكمة المختصـة، أو بصدور أمر بألا وجه لإقامة الدعـوى الجـنائية، لأن الخبرة تنير الطريق للقاضي الذي يهتدي بها لتحقيق العـدالة خاصة في المجال الجنائي، لذا فإنه يمكن للمحكمة تعيين الخبراء سواء من تلقاء نفسها أو بناءً على طلب الخصـوم، ولا يرفض طلب الخصوم إلا إذا كان عديم الفائدة، لأنه أمر يعود لتقدير القاضي، لذا عليه تسبيبه عند الرفض[2]، وهو ما يبينه حكم محكمة النقض الذي جاء فيه: "... فضلاً عما

1 تنص المادة 85 من ق.إ.ج.م على: "إذا استلزم إثبات الحالة الاستعانة بطبيب أو غيره من الخبراء يجب على قاضي التحقيق الحضور وقت العمل وملاحظته وإذا اقتضى الأمر إثبات الأدلة بدون حضور قاضي التحقيق نظراً إلى ضرورة القـيام بأعمال تحضيرية أو تجارب متكررة، أو لأي سبب آخر وجب على قاضي التحقيق أن يصدر أمراً يبين فيه أنواع التحقيقات وما يرد إثبات حالته. ويجوز في جميع الأحـوال أن يؤدى الخبير مأموريته بغير حضور الخصوم".

2 تنص المادة (29) من ق.إ.ج.م: "لمأموري الضبط القضائي أثناء جمع الاستدلالات أن يسمعوا أقوال من يكون لديه معلومات عن الوقائع الجنائية ومرتكبها وأن يسألوا المتهم عن ذلك، ولهم أن يستعينوا بالأطباء وغيرهم من أهل الخبرة ويطلبوا رأيهم شفهيا أو بالكتابة. ولا يجوز لهم تحليف الشهود أو الخبراء اليمين إلا إذا خيف ألا يستطاع فيما عد سماع الشـهادة بيمين"، كما تنص المـادة (40) من قـــانون إ.ج.إ: "لمأموري الضبط القضائي أثناء جمع الأدلة أن يسمعوا أقوال من تكون لديهم معلومات عن الوقائع الجنائية ومرتكبيها وأن يسألوا المتهم عن ذلك، ولهم أن يستعينوا بالأطباء وغيرهم من أهل الخبرة ولا يجوز لهم تحليف الشهود أو الخبراء اليمين إلا إذا خيف ألا يستـــطاع فيما بعد سماع الشهادة."، كما نصت المواد من (96) إلى (98) من ق.إ.ج.إ على ندب الخبراء. **للمزيد بخصوص هذه المسألة ينظر:** كحيل حياة، حجية الإثبات الإلكتروني، مجلة البحوث والدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة لونيسي علي، البليدة 02، الجزائر، العدد التاسع (09)، أوت 2016، ص 241، **نقلاً عـن:** عن مراد محمود الشنيكات، الإثبات بالمعاينة والخـبرة في القانون المـدني"دراسـة مقارنة"، دار الثقافة للنشـر والتوزيـــع، الطبعة الأولى، عمـان، الاردن، 2008، ص 99؛ **ونقلاً كذلك عن:** محمد حسين منصور، الإثـبات التقليـدي والإلكتروني، دار الفكـر

هو مقرر من أن طلب ندب لجنة من خبراء الكمبيوتر المختصين إذا كان لا يتجه إلى نفي الفعل المكون للجريمة، ولا إلى إثبات استحالة حصول الواقعة كما رواها الشهود، بل كان مقصوداً به إثارة الشبهة في الدليل الذي اطمأنت إليه المحكمة – كما هو الحال في الدعوى المطروحة – فإن مثل هذا الطلب يعد دفاعاً موضوعياً لا تلتزم المحكمة بإجابته ولا يستلزم منها رداً صريحاً، بل يكفي أن يكون الرد عليه مستفاداً من قضائها بالإدانة"[1]، وجاء في حكم آخر أنه: "من المقرر أن تقدير آراء الخبراء والفصل فيما يوجه إلى تقاريرهم من اعتراضات ومطاعن مرجعه إلى محكمة الموضوع التي لها كامل الحرية في تقدير القوة التدليلية لتلك التقارير، شأنها في ذلك شأن سائر الأدلة لتعلق الأمر بسلطتها في تقدير الدليل، وأنها لا تلتزم بالرد على الطعون الموجهة إلى تقارير الخبراء، ما دامت قد أخذت بما جاء بها؛ لأن مؤدى ذلك أنها لم تجد في تلك الطعون ما يستحق التفاتها إليها، كما أن لمحكمة الموضوع أن تورد في حكمها من تقرير الخبير ما يكفي لتبرير اقتناعها بالإدانة، وما دامت قد اطمأنت إلى ما أوردته منها واعتمدت عليه في تكوين عقيدتها، فإن إغفالها الرجوع إلى محاضر أعمال تقارير لجنة الخبراء المرفق وما تقدم لها من مستندات ومذكرات يعتبر اطراحاً لها"[2].

وبصفة عامة فإن وظيفة الخبراء هي تقديم تقاريرهم للمحكمة بما تم التوصل إليه من أدلة وحقائق، وليس من دورهم الدفاع عن جانب واحد من القضية، لأن هذا العبء يقع على عاتق المحامين، لذا وضعت الشرطة البريطانية قواعد إجرائية، تحدد مهام وواجبات الخبراء وتبين مهام عملهم، ومنها:

1- على الخبير أن يساعد المحكمة لأجل الوصول إلى الحقيقة، بعيداً عن أي رأي متحيز في الأمور الداخلة في مجال تخصصه وخبرته.
2- يتجاوز هذا الواجب أي التزام شخصي.

الجامعي، الإسكندرية، مصر، 2006، ص 403؛ سوزان نوري فقي محمد، المرجع السابق، ص131؛ عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر الانترنت، دار الكتب القانونية، مصر، 2007، ص 407.

1 حكم محكمة النقض المصرية، في الطعن المقيد بجدول المحكمة رقم 27735 لسنة 72 القضائية، في الجلسة العلنية المنعقدة بدار القضاء العالي بمدينة القاهرة، في يوم 07 ديسمبر سنة 2003، ص 29.

2 حكم محكمة النقض المصرية، في الطعن المقيد بجدول المحكمة رقم 132 لسنة 78 القضائية، في الجلسة العلنية المنعقدة بدار القضاء العالي بمدينة القاهرة، جلسة 12 ابريل سنة 2014، ص 108.

3- على الخبير إبلاغ جميع الإطراف والمحكمة، أو يسلم ذلك في بيان، إذا رأى أن التقرير الذي قدمه طرأ عليه تغيير"[1].

وحسب المادة 06 من القانون 09-04 الخاص بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، فإنه بعد الحصول على المعطيات التي تكون مفيدة في كشف الجرائم أو مرتكبيها، يتم حجز المنظومة المعلوماتية أو جزء منها، أو نسخ المعطيات محل البحث، وكذا المعطيات اللازمة لفهمها على دعامة إلكترونية لتكون بذلك قابلة للحجز والتحريز؛ أي وضعها في أحراز مختومة، لا تفتح إلا بحضور المتهم مصحوباً بمحاميه، أو بعد استدعائهما قانوناً، كما يستدعى من ضبطت لديه الأشياء المضبوطة لعملية فتح الأحراز، كما أجاز القانون لقاضي التحقيق أو ضابط الشرطة القضائية الذي ينوب عنه، وحدهما الحق في الاطلاع على المستندات قبل ضبطها، وذلك تفادياً للادعاء بتغيير الأحراز، وهي شروط قالت بها معظم التشريعات الحديثة كالتشريع المصري بموجب المواد 55، 56، و57 من ق.إ.ج.م، والمادة 56 من ق.إ.ج.ف[2].

1 أحمد محمد عبد الباقي، المرجع السابق، ص 66.

2 المادة 84 من ق.إ.ج.ج؛ المادة 55 من ق.إ.ج.م: "لمأموري الضبط القضائي أن يضبطوا الأوراق والأسلحة وكل ما يحتمل أن يكون قد استعمل في ارتكاب الجريمة أو نتج عن ارتكابها أو ما وقعت عليه الجريمة وكل ما يفيد في كشف الحقيقة. وتعرض هذه الأشياء على المتهم، ويطلب منه إبداء ملاحظاته عليها ويعمل بذلك محضر يوقع عليه من المتهم، أو يذكر فيه امتناعه عن التوقيع."؛ والمادة 56 من ذات القانون: "توضع الأشياء والأوراق التي تضبط في حرز مغلق وتربط كلما أمكن، ويختم عليها، ويكتب على شريط داخل الختم تاريخ المحضر المحرر بضبط تلك الأشياء، ويشار إلى الموضوع الذي حصل الضبط من أجله."؛ والمادة 57 من نفس القانون:"لا يجوز فض الأختام الموضوعة طبقا للمادتين 53 و56 إلا بحضور المتهم أو وكيله، ومن ضبطت عنده هذه الأشياء أو بعد دعوتهم لذلك"؛ وكذلك المادة 56 من ق.إ.ج.ف التي جاء فيها

- **Article 56 du Code de procédure pénale, Op. Cit : « …**Tous objets et documents saisis sont immédiatement inventoriés et placés sous scellés. Cependant, si leur inventaire sur place présente des difficultés, ils font l'objet de scellés fermés provisoires jusqu'au moment de leur inventaire et de leur mise sous scellés définitifs et ce, en présence des personnes qui ont assisté à la perquisition suivant les modalités prévues à l'article 57. Il est procédé à la saisie des données informatiques nécessaires à la manifestation de la vérité en plaçant sous main de justice soit le support physique de ces données, soit une copie réalisée en présence des personnes qui assistent à la perquisition».

- **أشار إلى ذلك:** بوقرين عبد الحليم، قانون مكافحة جرائم تقنية المعلومات الكويتي: دراسة مقارنة، مجلة كلية القانون الكويتية العالمية، السنة الخامسة، العدد 04، العدد التسلسلي 20، الكويت، ديسمبر 2017، ص.ص: 316– 317.

يستخلص من المواد السابقة أن مختلف التشريعات حرصت على أن تتم عملية الضبط وفقاً للشروط المقررة قانوناً ضماناً للحقوق، وحفاظاً على الأدلة المضبوطة؛ لأن ضبط الأدلة وتحريزها يحميها من الضياع ومن أن تصل إليها أيادٍ أخرى غير تلك التي قامت بتحريزها، وكذلك يساعد على تنظيمها حتى تحافظ على قوتها الثبوتية، والأمر في الأخير متروك للمحكمة في تقرير ذلك، فبهذا الخصوص جاءت مجموعة من الأحكام القضائية مؤكدة على ذلك، منها حكم محكمة النقض بتاريخ 23 فبراير 2015 الذي جاء فيه: "هذا إلى أنه من المقرر أن إجراءات التحريز، إنما قُصد بها تنظيم العمل للمحافظة على الدليـل، خشية تـوهينه، ولم يرتب القانون على مخالفتها بطلاناً، بل ترك الأمر في ذلك إلى اطمئنان المحكمة إلى سلامة الدليل، وأن يد العبث لم تصل إلى الأحراز المضبوطة، ولما كانت المحكمة قد أقامت قضاءها على عناصر صحيحة وسائغة، واطمأنت إلى عدم حصول عبث بالمضبوطات، فإنه لا يقبل من الطاعن الأول ما يثيره في هذا الصدد"[1].

وفي حكم آخر بتاريخ: 2015/10/10، جاء فيه: "كما أن ما يثيره الطاعن بشان تقاعس النيابة العامة لعدم تحريزها وحدة الحاسب الآلي المضبوط لا يعدو أن يكون تعييباً للإجراءات السابقة على المحاكمة، مما لا يصح أن يكون سبباً للنعي على الحكم، هذا فضلاً عن أن إجراءات التحريز إنما قصد بها تنظيم العمل للمحافظة على الدليل، ولم يرتب القانون البطلان على مخالفتها، بل ترك الأمر في ذلك إلى اطمئنان المحكمة إلى سلامة الدليل المستمد منها فإن ما يثيره الطاعن في هذا الشأن لا يعدو أن يكون جدلاً موضوعـاً في تقديـر الدليل الذي اطمأنت إليه المحكمـة، ولا يجوز مجادلتها فيه أو مصادرتها في عقيدتها، ومن ثم فإن ما ينعاه الطاعن في هذا الصدد لا يكون قويماً"[2]، ما دامت المحكمة قد عرضت المضبوطات "على بساط البحث وكانت المحكمة قد فضـت الأحراز المحتويـة عليها في حضـور الخصـوم ومدافعيهم وصرحـت لهم بالاطلاع عليها وأجلت نظر الدعوى لذلك واستمروا في مرافعتهم دون إثارة هذا الدفاع"[3].

1 حكم محكمة النقض المصرية، الدائرة الجنائية، في الطعن المقيد بجدول المحكمة رقم 15854 لسنة 84 القضائية، في الجلسة العلنية المنعقدة بدار القضاء العالي بمدينة القاهرة، في يوم الاثنين 23 فبراير سنة 2015.

2 حكم محكمة النقض المصرية، الدائرة الجنائية، في الطعن المقيد بجدول المحكمة رقم 24908 لسنة 84 القضائية، السالف الذكر.

3 حكم محكمة النقض المصرية، في الطعن المقيد بجدول المحكمة رقم 13196 لسنة 76 القضائية، السالف الذكر، ص 240.

وعليه فإن التفتيـش عن الأدلـة وضبطها وتحريزها وفقاً للقانـون والإجراءات التي نص عليـها وبمعرفة الخبراء حين الحاجة إليهم أَمرُ ضروري جداً، وذو أهمية بالغة في آليات مكافحة الجريمة الإلكترونية، والحصول على الأدلة التي يمكننا الاعتداد بها أمام المحكمة، والتي لها في الأخير كامل النظر في مدى قبول أو نفي حجية تلك الأدلة.

الفصل الثانـــــي:
الآليات الإجرائية الحديثة المعتمدة للحصول على الدليل الإلكتروني

الفصل الثاني:

الآليات الإجرائية الحديثة للحصول على الدليل الإلكترونـي.

لقد ارتأينا أن يكون مدخل هذا الفصل ما تضمنه حكم المحكمة الدستورية العليا المصرية لسنة (1995) عـن حرمة الحياة الخاصة للفرد، وهي أنه: "ثمة مناطق من الحياة الخاصة لكل فرد تمثل أغواراً لا يجوز النفاذ إليها، وينبغي دوماً- ولاعتبار مشـروع- ألا يقتحمها أحد ضماناً لسريتها، وصوناً لحرمتها، ودفعاً لمحاولة التلصص عليها أو اختلاس بعض جوانبها، وبوجه خاص من خلال الوسائل العلمية الحديثة التي بلغ تطورها حداً مذهلاً، وكان لتنامي قدراتها على الاختراق، أثر بعيد على الناس جميعهم، حتى في أدق شؤونهم، وما يتصل بملامح حياتهم، بل وبياناتهم الشخصية التي غدا الإطلاع عليها وتجميعها نهباً لأعينهم ولآذانهم. وكثيراً ما ألحق النفاذ إليها الحرج أو الضرر بأصحابها"[1]، ولهذا فقد خصصت لحرمة الحياة الخاصة حماية دولية ودستورية وتشريعية وقضائية، وفقهية[2] من الاعتداء عليها، حيث يمثل ذلك العدوان خرقاً لمبادئ عامة تسود

1 حكم المحـكمة الدستورية العليا المصرية، لجلسة 18 مارس سنة 1995، في القـضية رقم 23 لسنة 16 قضـائية "دسـتورية"، ص 587، القـــرار موجود على الموقع الموالي: *http://www.cc.gov.eg.Images/L/378444.pdf/*، والذي تم تصفـحه في: 2018/07/6.

2 إذ جاء في المادة 47 من التعديل الدستوري الجزائري لسنة 2020: "لكل شخص الحق في حماية حياته الخاصة وشرفه. لكل شخص الحق في سرية مراسلاته واتصالاته الخاصة في أي شكل كانت. لا مساس بالحقوق المذكورة في الفقرتين الأولى والثانية إلا بأمر معلل من السلطة القضائية. حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي. يعاقب القانون على كل انتهاك لهذه الحقوق."؛ ونـصت الـمادة 57 من دستـور جمهورية مصر على:"للحيـاة الخاصة حرمة، وهي مصونة لا تمس. وللمراسـلات البريدية، والبرقية، والإلكترونيـة، والمحادثـات الهـاتفية، وغيرهـا من وسائل الاتصـال حرمـة، وسريتـها مكفولة، ولا تجوز مصادرتها، أو الاطـلاع عليها، أو رقابتها إلا بأمر قضائي مسبب، ولمدة محدودة، وفي الأحوال التي يبينها القانون. كما تلتزم الدولة بحماية حق المواطنين في استخدام وسائل الاتصال العامة بكافة أشكالها، ولا يجوز تعطيلـها أو وقفها أو حرمان المواطنـين منها، بشكل تعسـفي، وينظـم القانون ذلك."، وتنص المادة 164 من القانون رقم 18-04، الذي يحدد القواعـد العامة المتعلقة بالبريد والاتصالات الإلكترونية، السالف الذكر عـلى أن: "يعاقب بالحـبس من سنة (1) إلى خمس (5) سنوات وبغرامة من 500.000 دج إلى 1.000.000 دج، كـل شخـص ينتهك سرية المراسـلات المرسلة عن طريـق البريـد أو الاتصالات الإلكترونيـة أو يفشي مضمونها أو ينشره أو يستعمله دون ترخيـص من المـرسل أو المرسل إليه أو يخبر بوجودها". **للمزيد يمكن الرجوع إلى:** جميلة محلق، اعتراض المراسلات، تسجيل الأصوات والتقاط الصور في قانون الإجراءات الجزائية الجزائري، مجلة التواصل في الاقتصاد والإدارة والقـانون، كلية الحقـوق والعلوم السياسيـة، جامعة باجي مختـار عنابة، الجزائر، العدد (42)، جوان 2015، ص 177؛ محمد أميـن الخـرشة، مشروعية الصوت والصورة في الإثبات الجنائي"دراســة مقارنة"، دار الثقافة للنشر والتوزيع، عمان، 2011، ص 97.

النظام القانوني ككل، والنظام الإجرائي خصوصاً، وفي مقدمتها النزاهة في البحث عن الأدلة، فالتنصت على محادثات المتهم أو المشتبه فيه وتسجيلها ثم مفاجأته بها، يعد في الواقع نوعاً من الغش والخداع تأباه العدالة[1]، فلا يجوز تعريض أي شخص على نحو تعسفي أو غير قانوني للتدخل في خصوصيته أو شؤون أسرته أو بيته أو مراسلته، ولا لأي حملات غير قانونية تمس شرفه أو سمعته، وأنه من حق كل شخص أن يحميه القانون من مثل هذا التدخل أو هذا المساس، ولكن لمقتضيات الحال ولخطورة بعض الجرائم؛ كما هو الشأن في الجريمة الإلكترونية يكون من المحتم المساس بحرمة الحياة الخاصة للأفراد، وفرض رقابة على اتصالاتهم والتنصت عليها، وأخذ الصور، أو تسلل بعض الأشخاص لمكنونات الأسرار للحصول على أدلة يمكن من خلالها إثبات الجريمة أو نفيها خاصة إذا لم تُجدي طرق التحقيق المعتادة نفعاً. ولأن الحياة الخاصة لها حرمتها، فقد أحاطتها معظم التشريعات بضمانات تكفل لها تلك الحرمة، وجعلت عملية المساس بها في حدود ضيقة وفي جرائم محددة على سبيل الحصر وبتوفر شروط خاصة[2]، تحرص الجهات القضائية على مراقبة مدى تطبيقها.

وعلى هذا الأساس قسمنا هذا الفصل إلى ثلاث مباحث؛ تم تخصيصها لاعتراض المراسلات وتسجيل الأصوات والتقاط الصور (البحث الأول)، ولدراسة التسرب أو الاختراق (المبحث الثاني)، وصولاً لدور مقدم الخدمات في كشف الجريمة الإلكترونية وجمع الأدلة الإلكترونية (المبحث الثالث).

1 محمد أبو العلا عقيدة، المرجع السابق، ص 43.

2 هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 2003، ص.ص: 253-254.

المبحث الأول:

اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

على الرغم من كل ما تمت الإشارة إليه بخصوص حرمة الحياة الخاصة للأفراد، إلا أن طبيعة الجريمة الإلكترونية وخطورتها، فرضت على المشرعين وضع نصوص قانونية يكون بموجبها للسلطات المختصة الباحثة عن حقيقة الجرائم، مراقبة جانب من تصرفات الأفراد الخاصة للوصول إلى الأدلة المطلوبة، والمشرع الجزائري واحد من أولئك المشرعين، إذ أوجد أساليب بحث[1] وتحَري خاصة نصت عليها بعض المواد القانونية من نصوص مختلفة، كالمادتين الثالثة (3) والرابعة (4) من القانون 09-04 المتضمـن القواعـد الخاصة للوقايـة مـن الجرائم المتصلة بتكنولوجيات الإعلام والاتصـال ومكافحتها، واللتان نصتا على إمكانية إجراء المراقبة الإلكترونية ووضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها، إذا استدعت ذلك مقتضيات حماية النظام العـام، من احتمال الاعتـداء على منظومـة معلوماتيـة على نحـو يهـدد الـدفاع الـوطني أو مؤسسات الدولة أو الاقتصاد الوطني، أو للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، أو في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة[2]، وكان من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى تلك المراقبة الإلكترونية، كما نصت المادة 56 من القانون 06-01[3] المتعلق بالوقاية من الفساد ومكافحته على إمكانية اتباع أساليب تحري خاصة كالترصد الإلكتروني والإختراق من أجل تسهـيل جمع الأدلـة.

---

1 البحث يعني طلب الشيء والتفتيش عنه واستقصائه من أجل التعرف عليه، وهنا يعني طلب الجريمة والتفتيش عنها وعن الآثار التي تخلفت عنها، واستقصاؤها من أجل التعرف على حقيقتها، وحقيقة وجودها وحقيقة مرتكبها أو مرتكبيها إذا تعددوا". **انظر في ذلك:** محمد حماد مرهج الهيتي، أصول البحث والتحقيق الجنائي (موضوعه أشخاصه والقواعد التي تحكمه)، دار الكتب القانونية، مصر 2008، ص 26.

2 تنص المادة 17 من الاتفاقية المتعلقة بالتعاون القضائي في المجال الجزائي بين حكومة الجمهورية الجزائرية الديمقراطية الشعبيـة وحكومة الجمهورية الفرنسية، المصادق عليها بالمرسوم الرئاسي رقم 18-73، السالفة الذكر، على أن:"طلبات اعتراض الاتصالات السلكية واللاسلكية: يجوز أن يتقدم أي من الطرفين، في إطار تحقيق جزائي، بطلب تعاون من أجل الحصول على معلومات حول اتصالات سلكية ولا سلكية أو اعتراضها وتسجيلها وإرسالها إلى الطرف الطالب".

3 جاء في المادة 56 من القانون رقم 06-01، المؤرخ في 20 فبراير 2006، المتعلق بالوقاية من الفساد ومكافحته ، الصادر في الج.ر.ج، عدد 14، مـؤرخة في 08 مارس 2006، الصـفحة 4، متمم بالأمر رقم 10-05 ممضي في 26 غشت 2010،

وجـاءت المواد من 65 مكرر05 إلى 65 مكرر 18 من قانون الإجراءات الجزائية[1]، مبينة كيفية القيام بإجراءات اعتـراض المراسلات وتسجيل الأصوات والتقاط الصور، وكذا إجراء التـسرب، وحددت الجرائم التي تجوز فيها مثل هاته الإجراءات، والتي كما أُشير إليها سابقاً هي على سبيل الحصر، وبينت تلك المواد الضمانات التي يفرضها القانون لمثل هكذا إجراءات، بحيث حاول المشرع الجزائري التوفيق بين أمن البلاد واستقرارها والحفاظ على النظام العام، وبين الحرية الشخصية أو ما يسمى بالحق في الخصوصية[2]؛ لكن عند تعارض هاتين المصلحتين لا بد من تغليب المصلحة العامة على المصلحة الفردية أو الحرية الشخصية؛ لأنه وبكل تأكيد فإن المصلحة العامة تعلو على المصلحة الخاصة والحريات العمومية[3]. ولأكثر تفاصيل حول موضوع اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، قسم هذا المبحث إلى شقين؛ تم التطرق في الأول إلى اعتراض المراسلات (المطلب الأول)، ولتسجيل الأصوات والتقاط الصور (المطلب الثاني).

الصادر بالج.ر.ج، عدد 50، مؤرخة في 01 سبتمبر 2010، الصفحة 16، القانون رقم 10-11 ممضي في 27 أكتوبر 2010، الصادر في الج.ر.ج، عدد 66 مؤرخة في 03 نوفمبر 2010، الصفحة 5، يتضمن الموافقة على الأمر رقم 10-05 الذي يتمم القانون رقم 06-01، المتعلق بالوقاية من الفساد ومكافحته، القانون رقم 11-15، يعدل ويتمم القانون رقم 06-01، المتعلق بالوقاية من الفساد ومكافحته، مؤرخ في 02 رمضان عام 1432، الموافق 02 غشت سنة 2011، الصادر في الج.ر.ج، عدد 44، بتاريخ 10 غشت سنة 2011: "من أجل تسهيل جمع الأدلة المتعلقة بالجرائم المنصوص عليها في هذا القانون، يمكن اللجوء إلى التسليم المراقب أو إتباع أساليب تحري خاصة كالترصد الإلكتروني والاختراق على النحو المناسب بإذن من السلطة القضائية المختصة، تكون للأدلة المتوصل إليها بهذه الأساليب حجيتها وفقا للتشريع والتنظيم المعمول به".

1 الأمـر رقم 66-155، المتضمن قانون الإجراءات الجزائية، السالف الذكر، المعدل والمتمم (خاصة بالقانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المنشور بالج.ر.ج رقم 84 ص 08، القانون 06-22 هو الذي تمت بموجبه إضافة هذه المواد).

2 تتعدد صور الحق في الحياة الخاصة، وهناك جملة من العناصر المكونة لهذا الحق وقع إجماع بين الفقه والقانون عليها وهي حرمة المسكن، حرمة محادثات المكالمات الشخصية، حرمة المراسلات، حرمة الحياة الصحية وكذا حرمة الحياة العائلية في مختلف مكوناتها. **انـظر**: صالح شنين، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور في قانون الإجراءات الجزائية الجزائري، المجلة الاكادمية للبحث القانوني، مجلة سداسية، عدد 02، جامعة عبد الرحمان ميرة – بجاية–، 2010، ص 67؛ صفية بشاتن، الحماية القانونية للحياة الخاصة (دراسة مقارنة)، رسالة لنيل شهادة الدكتوراه في العلوم تخصص قانون، جامعة مولود معمري، تيزي وزو، الجزائر، السنة الجامعية 2011-2012، ص 207؛ محمود على السرطاوي، موقف الشريعة الإسلامية من استعمال الوسائل العلمية في تعذيب المتهم، الندوة العلمية (الجوانب الشرعية والقانونية لاستخدام الوسائل العلمية في التحقيق الجنائي)، مركز الدراسات والبحوث قسم الندوات واللقاءات العلمية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2007، ص 01؛ أوشن حنان، وادي عماد الدين، الإثبات الجنائي والوسائل العلمية الحديثة، دار الخلدونية للنشر والتوزيع، الجزائر، 2015، ص 128.

3 المجلس الشعبي الوطني، السنة الثالثة رقم 122، الفترة التشريعية السادسة، الدورة العادية الرابعة، الجلسة العلنية المنعقدة يوم السبت 27 يونيو 2009، المنشورة بالج.ر.ج للمناقشات، الجزائر، 06 يوليو سنة 2009، ص.ص: 21 -22.

المطلب الأول: اعتراض المراسلات.

إن الاعتراض والتسجيل والالتقاط والتسرب هي عدة تسميات يمكن اختزالها في مصطلح واحد هو "المراقبـة" التي لا تخرج عن كونها رقابة مشروعة لشخص أو مكان أو أحاديث أو مراسلات مكتوبة أو مرئية نتيجة الاشتباه في تصرفات غير قانونية وذلك بصورة لا يحس معها الغير بمباشرتها نظراً لطابع السرية الذي يكتنفها"[1].

واعتراض المراسلات[2] هو نوع من أنواع المراقبة الإلكترونيـة، وهو القيـام باعتـراض كل المراسـلات التي تتم عن طريق وسائـل الاتصـال السلكية واللاسلكية، التي يقصـد بها التنصت التليفـوني، ولم يعرف المشـرع الجزائـري هذه التقنية شأنه في ذلك شأن المشرع الفرنسي غير أن القضاء الفرنسي عرفها على أنها: تقنية يتم من خلالها الاعتراض عن طريق ربط خط هاتفي للمشتبه فيه مع اللجوء إلى تسجيل المكالمات في أشرطة مغنطيسية[3].

كما يعرفها بعضهم بأنها عملية مراقبة سرية المراسلات السلكية واللاسلكية في إطار البحـث والتحري عن الجريمـة وجمـع الأدلـة أو المعلومـات حـول الأشخـاص المشتبه في ارتـكابهم أو مـشاركتهم في ارتكاب الجريمة، وتعتبر المراقبة الإلكترونية على الاتصالات الشخصية تعدياً على الحياة الخاصة للأفراد، إذا لم تَجْرِ وفقاً لمقتضيات القـانون[4]، وتعد الولايات المتحدة من أوائل الدول

1 فوزي عمارة، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور كإجراء تحقيق قضائي في المواد الجزائية، مجلة العلوم الإنسانية كلية الحقوق والعلوم السياسية، جامعة منتوري قسنطينة، عدد 33، جوان 2010، ص 236.

2 شيخ ناجية، خصوصيات جريمة الصرف في القانون الجزائري، رسالة لنيل شهادة الدكتوراه في العلوم تخصـص قانون،كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، الجزائر، 2012، ص210؛ سامية بولافة، مبروك ساسي، الأساليب المستحدثة في التحريات الجزائية، مجلة الباحث للدراسات الأكاديمية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر (جامعة باتنة 1)، الجزائر، العدد الحادي عشر (11)، جوان 2017، ص 396.

3 وعلى جمال، حقوق المشتبه فيه عند اللجوء إلى إجراءات البحث والتحري الخاصة، كلية الحقوق والعلوم السياسية، جامعة تلمسان، مجلة الدراسات الحقوقية، جامعة الدكتور الطاهر مولاي، سعيدة، الجزائر، العدد الثالث، جوان 2015، ص 177.

4 تنص الفقرة الثالثة من المادة (22) من المرسوم التنفيذي رقم 20-62، المؤرخ في 20 رجب عام 1441 الموافق 15 مارس سنة 2020، المتضمن الموافقة على تجديد رخصة لإقامة واستغلال شبكة مفتوحة للجمهور، عبر الساتل V.SAT، ولتوفير خدمات الاتصالات الإلكترونية للجمهور، الممنوحة لشركة "اتصالات الجزائر الفضائية، شركة ذات أسهم"، الصادر في الج.ر.ج العدد 17، المؤرخة في 28 مارس سنة 2020، على أنه:يلتزم صاحب الرخصة باتخاذ التدابير التي من شأنها أن تضمن سرية المعلومات التي يحوزها عن مشتركيه، وكذا سرية مكالماتهم وألا يسمح بوضع أي ترتيبات بغرض اعتراض الاتصالات أو مراقبة المكالمات الهاتفية والوصلات والمحادثات والمبادلات الإلكترونية دون إذن مسبق من السلطة القضائية وفقاً للتشريع المعمول به...".

التي أثيرت فيها المناقشات حول مدى مشروعية مراقبة المحادثات التليفونية والدليل الناجم عنها، حيث صدر القانون الفيدرالي 19 جوان 1968 ونظم مراقبة المحادثات التليفونية من قبل الشرطة الفيدرالية أو المحلية في الولايات، وأحاطها المشرع الأمريكي بالعديد من الضمانات التي تهدف إلى منع التعسف وتصون حرمة الحياة الخاصة[1].

وبعد أحداث الحادي عشر (11) من شهر سبتمبر سنة 2001، صدر في الولايات المتحدة الأمريكية قانون يبيح التنصت على المكالمات الهاتفية وتسجيلها، كما أجاز ذات القانون اعتراض المراسلات بجميع أنواعها، ويعتبر المشرع الأمريكي هذا القانون بمثابة وسيلة إجرائية وقائية ضد جرائم الإرهاب الدولي، وليس انتهاكاً للخصوصية[2]، كما منح التشريع الأمريكي حق الاختصاص لمراقبـة مدى صلاحيـة الإدارة في القيام بعمـليات اعـتراض المراسلات أو التنصت لبعض الجهات؛ كمحكمة الاستخبارات الأجنبية FISC، والتي تبحث في مدى توفر شروط مشروعية المراقبة، وخاصة ضرورة توافر ثلاثة مستندات إجرائية هي الطلب والشهادة المكتوبة والإذن[3].

وفي هولندا لقاضي التحقيق الحق في إصدار أمره بالتنصت على شبكات الحاسب الآلي متى كانت هناك جريمة خطيرة، وكان ذلك التنصت على قدر عالٍ من الأهمية للكشف عن تلك الجريمة،كما يجيز القانون الفنلندي لمأمور الضبط القضائي حق التنصت على المكالمات الخاصة بشبكات الحاسب الآلي. كما سمحت القوانين الألمانيـة للقاضي بإصـدار أمره بمراقبـة اتصـالات الحاسب الآلي وتسجيلها والتعامل معها وذلك خلال مدة أقصاها ثلاثة أيام، أما في اليابان فقد وضعت قانوناً خاصاً سنة 1991 أقـرت من خلاله شرعية التنصت على شبكات الحاسب الآلي إذا كان ذلك في مجال البحث عن الأدلة الخاصة بإحدى الجرائم الإلكترونية[4]، كما "يجيز المشرع

1 عاقلي فضيلة، الحمايـة القانونيـة للحـق في حرمة الحياة الخاصة (دراسة مقارنة)، بحث مقدم لنيل شهادة الدكتـوراه علوم في القانون الخاص، جامعة الإخوة منتوري، قسنطينة، الجزائر، 2011-2012، ص 196.

2 كاظم عبد الله نزال المياحي، حجية المراقبـة الإلكترونيـة للصوت والصورة في الإثبات الجنائي"دراسة في القانـون العراقي والمقارن"، رسالة مقدمة لنيل درجة الدكتوراه في الحقوق، قسم القانون الجنائي، كلية الحقوق، جامعة عين شمس، مصر، 2016، ص 134، **نقلاً عـن:** مقني بن عمار، التنصت على المكالمات الهاتفية واعتراض المراسلات كآلية لمكافحة الفساد في الجزائر، بحث منشور في مجلة مصر المعاصرة، العدد 507، السنة 104، القاهرة، يوليو 2012، ص 422.

3 فؤاد أمين السيد محمد، المرجع السابق، ص 129.

4 عبد العالي الديربي، محمد صادق إسماعيل، المرجع السابق، ص 173؛ منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، المرجع السابق، ص189.

الإيطالي انتهاك الحق في سرية المراسلات لمصلحة العدالة في المادتين 226 و338 من قانون الإجراءات الجنائية الإيطالي رقم 517 لسنة 1955، حيث أعطت هاتان المادتان للقضاء حق إصدار قراره بالاطلاع على المراسلات بين الأفراد والتنصت على المكالمات الهاتفية في حالة ما إذا كان ذلك من شأنه أن يفيد القائمين بالتحقيق من رجال الشرطة في كشف الحقيقة والحد من الجريمة"[1]، كما أقرت محكمة مقاطعة "كوفر" سنة 1991 بمشروعية التنصت على شبكات الحاسب الآلي في سبيل البحث عن الدليل[2]، وأجاز المشرع المصري هو الآخر لقاضي التحقيق بأن يأمر بمراقبة المحادثات السلكية واللاسلكية أو إجراء تسجيـلات لأحاديث تجري في مكان خاص، بموجب المادة 95 من ق.إ.ج.م، متى كان لذلك فائدة في إظهار الحقيقة حول جنايـة أو جنحة معاقب عليها بالحبس لمدة تزيد على ثلاثة أشهر، وأيضاً المادة 206 من نفس القانون[3].

فمما سبق يتضح أن مشروعية مراقبة المحادثات الهواتف المحمولة تجد أساسها في عدة مـواد قانونية من القانون المصري[4]. وفي القانون الفرنسي تم النص على عملية اعتراض وتسجيل ونسخ

1 عمار غالي عبد الكاظم العيساوي، المسئولية الجنائية عن جرائم انتهاك الحق في سرية المراسلات "دراسة في القوانين المقارنة"، رسالة مقدمة لنيل درجة الدكتوراه في الحقوق، قسم الدراسات العليا، كلية الحقوق، جامعة عين شمس، مصر، سنة 2016، ص 444.

2 **أشار إلى ذلك:** موسى مسعود أرحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، ورقة بحثية مقدمة في إطار اشغال المؤتمر المغاربي الأول حول: المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، الفترة بين 28 و29 اكتوبر 2009، ص 13، **نقلاً عـــن:** هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي –دراسة مقارنة ، الطبعة الأولى، دار النهضة العربية، القاهرة، 1997، ص.ص: 79–80؛ أسامة أحمد المناعسة وآخرون، جرائم الحاسب الآلي والإنترنت –دراسة تحليلية مقارنة–، الطبعة الأولى، دار وائل للنشر، عمان، الأردن، 2000، ص.ص: 283–285، **ونقلاً عن:**

- Yamaguchi (Atsushi), *Computer crimes and others crimes against information Technology in Japan*, Rev. int. de dr. pén. 1993. P. 448.

3 نصت المادة 95 من ق.إ.ج.م على: "لقاضي التحقيق أن يأمر بضبط جميع الخطابات والرسائل والجرائد والمطبوعـات والطـرود لدى مكاتب البريد وجميع البرقيات لدى مكاتب البرق وأن يأمر بمراقبة المحادثات السلكية وللاسلكية أو إجراء تسجيلات لأحاديث جرت في مكان خاص متى كان لذلك فائدة في ظهور الحقيقة في جناية أو جنحة معاقب عليها بالحبس لمدة تزيد على ثلاثة أشهر. وفي جميع الأحوال يجب أن يكون الضبط أو الإطلاع أو المراقبة أو التسجيل بناء على أمر مسبب ولمدة لا تزيد على ثلاثين يوما قابلة للتجديد لمدة أو لمدد أخرى مماثلة"، وتنص المادة (206) من نفس القانون على أنه يجوز للنيابة العامة: "... ويجوز لها أن تضبط لدى مكاتب البريد جميع الخطابات والرسائل والجرائد والمطبوعات والطرود ولدى مكاتب البرق وجميع البرقيات وأن تراقب المحـادثات السلكية واللاسلكية وأن تقوم بتسجيلات لمحادثات جرت في مكان خاص متى كان لذلك فائدة في ظهور الحقيقة في جنايـة أو في جنحة معاقب عليها بالحبس لمدة تزيد على ثلاثة أشهر. ويشترط لاتخاذ أي إجراء من الإجراءات السابقة الحصول مقدما على أمر مسبب بذلك من القاضي الجزئي بعد اطلاعه على الأوراق".

4 محمد أمين الخرشة، مشروعية الصوت والصورة في الإثبات الجنائي دراسة مقارنة، الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2015، ص 56.

المراسلات المرسلة بواسطة الاتصالات الإلكترونية بموجب عدة مواد؛ منها المادة 100، والمادة 706- 95 من ق.إ.ج.ف، وما يلاحظ في التشريع الفرنسي أنه وبمقتضى القانون رقم 2019-222 الصادر في 2019/03/23، والذي عدلت بموجبه عدة مواد منها المادة 100، أصبح بإمكان الضحية طلب مراقبة اتصالاتها الإلكترونية إذا كانت عقوبة الفعل المجرم الواقع عليها السجن، وتخضع تلك المراقبة حينها لنفس الإجراءات التي تطبق في حالة الجرائم الأخرى التي نص القانون على جواز المراقبة فيها[1].

وبـالرجوع للمشرع المغربي نجده أشار إلى إمكانية مراقبة الإتصالات؛ وذلك بمقتضى المادة 108 من قانون المسطرة الجنائية[2]، وخاصة في حالة الجرائم التي تمس بأمن الدولة والجرائم الإرهابيـة، وجرائم أخرى نصـت عليها ذات المـادة[3]، وهـو ما أكـده القرار رقم: 7/319 المـؤرخ في 2009/02/04، ملف جنائي عدد 15938/2008، والذي أشار إلى أن التقاط المكالمات الهاتفية، التي أجريت من طرف القضاء الأجنبي- يجوز قبولها: "حيث من جهة أولى فإنه لما كان قانون المسطرة الجنائية، وبموجب المادة 108 منه يجيز لقاضي التحقيق، وكذا للوكيل العام للملك بعد التماس هذا الأخير من الرئيس الأول بمحكمة الاستئناف إذا اقتضت ضرورة البحث إصدار الأمر

1 Article 100 du **Code de procédure pénale**, Modifié par LOI n°2019-222 du 23 mars 2019 - art. 44 (V) du Code de procédure pénale**,** OP.CIT : « En matière criminelle et en matière correctionnelle, si la peine encourue est égale ou supérieure à trois ans d'emprisonnement, le juge d'instruction peut, lorsque les nécessités de l'information l'exigent, prescrire l'interception, l'enregistrement et la transcription de correspondances émises par la voie des communications électroniques. Ces opérations sont effectuées sous son autorité et son contrôle.… »; Article 706-95 du **Code de procédure pénale** , Modifié par Ordonnance n°2016-1636 du 1er décembre 2016 - art. 2 , OP.CIT : « 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 des articles 706-73 et 706-73-1 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 communications électroniques 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 ».

2 المادة 108 من ق.م.ج.م: "يمنع التقاط المكالمات الهاتفية أو الاتصالات المنجزة بوسائل الاتصال عن بعد وتسجيلها أو أخذ نسخ منها أو حجزها. غير أنه يمكن لقاضي التحقيق إذا اقتضت ضرورة البحث ذلك، أن يأمر كتابة بالتقاط المكالمات الهاتفية وكافة الاتصالات المنجزة بواسطة وسائل الاتصال عن بعد وتسجيلها وأخذ نسخ منها أو حجزها"، شملت هذه المادة بعض الأحكام المشابهة لما ورد في المادة 706- 73 من ق.إ.ج.ف، للمزيد من المعلومات يمكن الاطلاع على المادة السالفة الذكر:-Article 706 . 73, Modifié par LOI n°2017-1510 du 30 octobre 2017 - art. 9

3 عبد الكافي الورياشي، المرجع السابق، ص 108.

بالتقاط المكالمات الهاتفية، أو الاتصالات المنجزة بواسطة وسائل الاتصال عن بعد وتسجيلها وأخذ نسخ منها وحجزها إذا تعلق الأمر بإنجاز عمليات تخص المخدرات، أو غيرها من الأفعال المحظورة كما أوردتها المادة المشار إليها أعلاه، على أن تحرر الجهة المعنية المختصة طبقاً للمادة 111 من نفس القانون المذكور، ما يمنع القضاء المغربي من الأخذ بعمليات التنصت عن طريق الإتصال الهاتفي المنجزة من طرف السلطة الأجنبية المختصة والمحاضر المحررة والمنجزة بشأن تلك العمليات، طالما أن الهدف من هذا الإجراء كما ترمي إليه المـادة 108 المشـار إليها أعلاه هو الحيلولـة دون اندثار وسائـل الإثبات في مواجهـة الفـاعل أو المشتبه فيه، وهو ما ينطبق على العارض في نازلة الحال"[1].

وقبل التطرق للمطلب الثاني من هذا المبحث، وجب الإشارة إلى مسألة مهمة وهي موقف التشريعات المقارنة من مراقبة الاتصالات التي تتم بين المحامي وموكله؛ أي من يدافع عنه ذلك المحامي، إذ شملت الإجراءات المنصوص عليها في المادة 65 مكرر 05 جميـع الأشخاص المشتبـه في ارتكابهم جريمة من الجرائم المشار إليهـا في ذات المـادة[2]، دون أن تخص هذا النوع من المراسلات والاتصالات بإجراءات خاصة، وذلك حفاظاً على حقوق الـدفاع، غير أن تطبيق مبدأ عدم انتهاك تلك المراسلات يجد حدوده فقط في المراسلات المتبادلة بين الزبون والمحامي الذي يضمن دفاعه[3]، وهو الأمر الذي أخذت به محكمة الجنح بباريس في حكمها الصادر بتاريخ:

1 تقرير عن المركز الوطني للدراسات والعلوم القانونية، مجلة القضاء الجنائي، العدد الثاني، السنة الأولى، مطبعة المعارف الجديدة وتوزيع دار الأفاق المغربية، الرباط، المغرب، صيف/خريف 2014، ص 137.

2 بن سعيد صبرينة، حماية الحق في حرمة الحياة الخاصة في عهد التكنولوجيا" الإعلام والاتصال"، أطروحة مقدمة لنيل شهادة الدكتوراه العلوم في العلوم القانونية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، الجزائر، السنة الجامعية 2014-2015، ص 266.

3 جاء في المادة 24 من القانون رقم 13-07، المؤرخ في 24 ذي الحجة عام 1434 هـ الموافق 29 أكتوبر سنة 2013، المتضمن تنظيم مهمة المحاماة، الصادر في الج.ر.ج عدد 04، بتاريخ 30 أكتوبر 2013، ص 03: يستفيد المحامي بمناسبة ممارسة مهنته من: – الحماية التامة للعلاقات ذات الطابع السري القائمة بينه وبين موكله، – ضمان سرية ملفاته ومراسلاته، ..."؛ وجاء في المادة 96 من ق.إ.ج.م: "لا يجوز لقاضي التحقيق أن يضبط لدى المدافع عن المتهم أو الخبير الاستشاري الأوراق والمستندات التي سلمها المتهم لهما لأداء المهمة التي يعهد إليهمـا بها، ولا المراسلات المتبادلة بينهما في القضيـة"؛ وفي نفس المعنى جاءت المادة 100-5 من ق.إ.ج.ف التي تنص:

Article 100-5 du **Code de procédure pénale,** Modifié par LOI n°2010-1 du 4 janvier 2010 - art. 6 (V): « … A peine de nullité, ne peuvent être transcrites les correspondances avec un avocat relevant de l'exercice des droits de la défense. . ».

1984/04/24، والذي جاء على إثر الحكم في قضة جرى خلالها تفتيش مسكن شخص يعمل مسيراً لأحد البنوك كان مشتبهاً فيه بارتكاب جريمة غش، فقامت الشرطة القضائية بحجز المراسلات الموجهة لهذا الأخير من طرف محامي البنك، غير أن المحكمة قضت برفض الدفع ببطلان الحجز المثار من طرف المتهم، وبررت رفضها على أساس أن المحامي المشار إليه يُعد وكيلاً عن البنك ولم يكن مدافعاً عن المتهم، وبالتالي فإن حجز هذه الرسائل لا يشكل أي انتهاك لسرية المراسلة المتبادلة بين المحامي وزبونه[1]؛ لأن القانون الفرنسي لا يجيز التنصت على هاتف المحـامي أو مسكنه، إلا بعد إخطار نقيب المحامين من طرف قاضي التحقيق[2]، ما لم يتعلق الأمر بجريمة مرتكبـة من المحامي نفسه[3]، وعملية إخطار مجلس نقابـة المحامـين يجب أن تتـم قـبل التحقـيق في الشكوى المقدمة ضد المحامي؛ لأن هذا الإجراء يعتبر تنظيمياً لا يرتب على مخالفته البطلان[4]، وإنما قد يستتبع ذلك استعادة تلك الوثائق بأثر رجعي[5].

وبذلك يكون المشرع الفرنسي قد أجاز التنصت شريطة أن يكون بناءً على تكليف، ودون اللجوء إلى أية حيلة أو انتهاكاً لحقوق الدفاع[6]، فقد قامت محكمة النقض الفرنسية في قرارها

1 **أشار إلى الحكم**: نويري عبد العزيز، الحماية الجزائية للحياة الخاصة –دراسة مقارنة–، أطروحة لنيل شهـادة دكتوراه العلوم، شعبة القانون الجنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، السنة الجامعة 2010-2011، ص 369.

2 **Article 100-7** du **Code de procédure pénale,** Modifié par Loi n°2004-204 du 9 mars 2004 - art. 5 JORF 10 mars 2004, OP.CIT: « … Aucune interception ne peut avoir lieu sur une ligne dépendant du cabinet d'un avocat ou de son domicile sans que le bâtonnier en soit informé par le juge d'instruction.. » ; Article 706-95-3, du **Code de procédure pénale ,** Créé par LOI n°2016-731 du 3 juin 2016 - art. 2: « … Lorsque l'identifiant informatique est associé au compte d'un avocat, d'un magistrat, d'un sénateur ou d'un député, l'article 100-7 est applicable. »

3 **Cour de cassation**, **chambre criminelle,** Audience publique du 24 avril 2013, OP.CIT: « alors que quelle qu'en soit la forme, les correspondances échangées entre un avocat et son client sont insaisissables ce qui interdit à l'administration de prendre connaissance de tels documents ; que la saisie de correspondances couvertes par le secret professionnel concernant directement l'enquête en cours porte une atteinte irrémédiable aux droits de la défense devant être sanctionnée par la nullité de la procédure;… . »

4 حكم محكمة النقض المصرية، في الطعن المقيد بجدول المحكمة رقم 13196 لسنة 76 القضائية، السالف الذكر، ص 238.

5 معمري عبد الرشيد، ضوابط مشروعية أساليب التحري الخاصة، المجلة الأكاديمية للبحث القانوني، كلية الحقوق والعلوم السياسية لجامعة عبد الرحمان ميره، بجاية، المجلد 11، العدد الأول، 2015، ص 475؛

6 زوزو زوليخة، مشروعية أساليب التحري الحديثة، مجلة الحقوق والعلوم السياسية، جامعة عباس لغرور خنشلة، الجزائر، العدد الثامن (08)، الجزء الثاني (02)، جوان 2017، ص 766، **نقلاً عن**: نزيه نعيم شلالا، دعاوى التنصت على الغير، الاتصالات السلكية واللاسلكية والمكالمات الهاتفية، دراسة مقارنة من خلال الفقه والاجتهاد والنصوص القانونية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2010، ص.ص: 16-17.

الصادر بتاريخ: 01/26/ 2016 باستبعاد مراسلات خاصة تم الحصول عليها من بريد أحد العمال كدليل على إدانته على اعتبار انتهاك سرية المراسلات والحصول عليها بطريقة غير مشروعة[1]. كذلك فعل المشرع الايطالي من خلال نص الفقرة الخامسة (05) من المادة 103 من قانون الإجـراءات الجنائية الإيطالي، والذي حـظر مراقبة المحـادثات التليفونية التي تتم بين المحامي والمتهم، واستبعدت الفقرة السابعة من نفس المادة كل الأدلة المتحصلة من الحديث بين المتهم ومحاميه[2].

المطلب الثانـــي: تسجيل الأصوات والتقاط الصور.

يتم تسجيل الأصوات عن طريق وضع أجهزة تنصت في أمكنة أو مركبات خاصة أو عمومية وإخفائها لتلقي أحاديث يمكن أن تفيد في التعرف على الحقيقة وتسجيلها[3]، أما التقاط الصورة فيقصد به تثبيت صورة شخص على مادة خاصة مما يسهل الاطلاع عليها ونسخها وذلك باستخدام الوسائل المعدة لذلك[4].

فبفضل التطور العلمي والتكنولوجي لوسائل الاتصالات وكذا التصوير، لم يعد تسجيل الأصوات والتقاط الصور عملاً صعباً، فقد يتم ذلك على مسافات بعيدة دون الحاجة إلى البقاء قريباً من المكان المراد التسجيل منه، ومثال ذلك؛ تقنية التجسس على الهاتف النقال التي يطلق عليها تسمية السن الأزرق (Blue tooth) وهي الطريقة التي تسمح بالتقاط التسجيلات والمحادثات المارة من وإلى الهـاتف النقال التابع للغير داخل مسافة معينة. فبعـد انتشـار المحـمول سـنة 1990، كان الإعتقاد السائد أنه لا يمكن مراقبة هذا الأخير والتنصت عليه، إلا أن شركة ألمانية تدعى International Mobile Scbscr طورت نظاماً سمته Schwarz Identity، يمكن من خلاله اصطـياد جميع الإشارات الصـادرة من هاته الهواتـف وقلبها إلى كلمات مسموعة، ولم تَكتفِ

1 عبد السلام بنسليمان، الإجرام المعلوماتي في التشريـع المغربي دراسة نقدية مقارنة في ضوء آراء الفقه وأحكـام القضـاء، الطبعة الأولى، دار الأمان، الرباط، 2017، ص250.

2 مجرب الدوادي، الأساليب الخاصة للبحث والتحري في الجريمة المنظمة، أطروحة لنيل شهادة دكتوراه علوم في القانون العام،كلية الحقوق، جامعة الجزائر 01 يوسف بن خدة، السنة الجامعية 2015-2016، ص 273.

3 وعلى جمال، المرجع السابق، ص 177.

4 بن حيدة محمد، النظام القانوني لحق الإنسان في صورته، مجلة القانون والمجتمع، مخبر القانون والمجتمع، جامعة أحمد دراية أدرار، العدد الخامس، 2015، ص 224؛ حسيني مراد، إجراءات التحقيق المستحدثة في قانون الإجراءات الجزائية الجزائري (عملية التسرب)، قراءات في المادة الجنائية، الجزء الأول، الإصدار السادس عشر، الطبعة الأولى، مجلة الحقوق (R.D) سلسلة المعارف القانونية والقضائية، دار نشر المعرفة، الرباط، المغرب، 2013، ص 172.

تلك الشركة بذلك بل تمكنت من معرفة مكان المتحدثين، كما طورت جهاز إلكترونياً تستطيع بواسطته استخدام الميكروفون الموجود في الهاتف المحمول لكي ينقل جميع الأصوات[1].

ولكن ورغم أن عملية التنصت والمراقبة الإلكترونية بمختلف أنواعها أصبح من السهل القيام بها، إلا أن مختلف التشريعات فرضت للقيام بها مجموعة من الشروط، ولعل من أهمها صدور إذن من قبل السلطة المختصة للقيام بالإجراء أو العملية المزمع انجازها، وهو شرط نصت عليه المواد الدستورية؛ كالمادة 47 مـن التعديل الدستوري الجزائري لسنة 2020، والمادة 57 من الدستور المصري كما تمت الإشارة إليه سابقاً ونصت عليه أيضاً المواد القانونية السالفة الذكر؛ كالمادة: 56 من القانون رقم 06-01، والمادة 04 من القانون 09-04، والمادة 65 مكرر 5 من ق.إ.ج.ج، والمادة 65 مكرر 15 من ق.إ.ج.ج، والمادة 95 من ق.إ.ج.م، وكذا المادة 206 من نفس القانون، والمادة 108 من ق.إ.ج.م، والمادة 100 من ق.إ.ج.م، والأمثلة كثيرة على ذلك.

هذا إضافة إلى أن الإذن يـجب أن يتضمن كل العناصر[2] التي يمكن من خلالها التعرف على الإتصـالات المـراد التقاطها، والأماكن المعنية بالمراقبة، وكذا الجريمة التي تبرر اللجـوء لهـكذا إجـراء، والمدة التي سيستغرقها هذا الأخير[3]، ومن الأمثلة على ضرورة وجود إذن للقيام بعملية التنصت، ما ورد في مسجلة لدى محكمة الجنايات بمصر منطقة الجيزة، والتي تمثلت وقائعها في قيام المتهم (يعمل طبيباً بمستشفى القصر العيني) ببعث رسائل عبر الإنترنت للمدعوة (س) (تعمل محاسبة بأحد البنوك الأجنبية في مصر) مهدداً إياها بوضع صورتها الحقيقية على صور جنسية مخلة ونشرها عبر تلك الشبكة، إن لم تدفع له مبلغ خمسة آلاف دولار أمريكي، وأن تباشر الجنس معه لقاء عدم قيامه بتنفيذ تهديده لها، مع العلم أنهما تعرفا على بعضهما البعض في المركز الثقافي البريطاني في إطار الدراسة من أجل تحسين مستواهم في اللغة الانجليزية، حيث قاما بتبادل أرقام الهاتف المحمول والبريد الإلكتروني، وهو الأمر الذي ساعد المتهم على الاتصال بها أولاً، ثم تنفيذ تهديده بعد أن رفضت الضحية الإنصياع لمطالبه، حيث قام بإنشاء موقع باسمها ضمنه دعوى كاذبة بأنها تقدم جسدها لمن يرغب لقاء مبلغ مادي، وأثبت ذلك بوضع رقم هاتفها على الموقع.

1 نويري عبد العزيز، المرجع السابق، ص 106؛ محمد أمين الخرشة، المرجع السابق، ص 51.

2 معمري عبد الرشيد، المرجع السابق، 477؛ المجلس الشعبي الوطني، السنة الثالثة رقم 122، السالف الذكر، ص.ص: 21-22.

3 لأكثر تفاصيل يمكن الاطلاع على: المادة (65 مكرر 7) من ق.ا.ج.ج، و المادة (100- 1) من ق.ا.ج.ف.

وبالفعل تلقت الضحية مكالمات هاتفية يطلب أصحابها إقامة علاقة جنسية معها مؤكدين لها بوجود موقع لها على شبكة الإنترنت مما دفع الضحية لإبلاغ الشرطة؛ والتي قامت بدورها بالتحريات اللازمة حول الموضوع وتأكدت من وجود موقعاً عليه بيانات شخصية للمعنية ورقمها الهاتفي، وكذا عبارات خطية تفيد رغبتها في إقامة العلاقة الجنسية، كما توصل العقيد (ع) رئيس قسم المساعدات الفنية بإدارة مكافحة جرائم الحاسبات وشبكـات المعلومات لرقم تلفون المتهم وحدد شخصيتـه وعنـوانه، كما أثبت التقرير أنه بعد تفتيش مسكن المتهم تم العثور على حاسبه الشخصي الذي وجد فيه صورة المجني عليها، وكذا بعض الآثار والدلائل على الرسائل- حوالي تسع عشرة (19) رسالة- التي أُرسلت من جهاز المتهم للمجني عليها.

أنكر المتهم التهم المنسوبة إليه، ودفع محاميه بأن الإجراءات شابها البطلان لعدم استئذان القاضي الجزائي لتسجيل المحادثات، وفي المقابل قدم الدفاع تقريراً فنياً استشارياً، تم رد الدفع ببطلان الإجراء لم يراقب تلفون المتهم، وإنما خاطبه على رقم البريد الإلكتروني الخاص به، وهو أمر متاح لمأمور الضبط وللكافة كأن يهدف مأمور الضبط من خلاله الوصول لرقم الهاتف الأرضي المرتبط بحاسوب المتهم، من أجل معرفة شخصيته والتوصل إلى ما هو مسجل عليه من مكالمات، وهو إجراء تفتيش للبحث عن أدلة جريمة وقعت فعلاً وليس تصنتاً على هاتف، ذلك أن هناك فرق فني كبير بين مراقبة الاتصالات الصوتية الهاتفية والتنصت عليها، وبين البحث عن أدلة الجريمة في مكمن السر وهذا لا يستلزم سوى استئذان النيابة العامة، كما أن التنصت يستلزم فرض رقابة ايجابية على الهاتف المراد مراقبته وحماية لحريات الأفراد استلزم المشرع أن يكون ذلك بإذن من القاضي المختص، أما ما لا يستلزم رقابة ايجابية على هاتف الشخص فهو لا يستلزم استئذان القاضي. ثبتت التهمـة على المتهم وحكمت عليه المحكمة بالحبس مع الشغل لمـدة سـنة، حيث صدر الحكم وتلي علناً بجلسة يوم الأحد الموافق 2004/01/18[1].

1 القضية رقم 6854 لسنة 2003، المسجلة لدى محكمة الجنايات بالجيزة. **أشار إلى ذلك:** محمد على قطب، المرجع السابق، ص.ص: 151-160.

المبحث الثاني:
التسرب أو الاختراق.

تكملة للحالات التي نصت عليها المادتان الثالثة (03) والرابعة (04) من القانون 09-04 المتضمـن القواعـد الخاصة للوقايـة من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، يأتي الدور للحديث عن وسيلة أخرى من الوسائل الحديثة للحصول على الدليل الإلكتروني، ألا وهو التسرب أو ما يسمى بالاختراق[1]، والذي خصص له المشرع الفصل الخامس من الباب الثاني من قانون الإجراءات الجزائية، وتحديداً المواد من 65 مكرر 11 إلى المادة 65 مكرر 18 منـه، ويعتبر التسرب أسلوباً جديداً من أساليب البحث والتحري الخاصة[2] التي جاء بها القانون 06-22 المعدل والمتمم لقانون الإجراءات الجزائية، وذلك لأن الأساليب التقليدية لم تعد تجدي نفعاً أمام تطور الجرائم واستفحالها، فهو عملية إجرائية تتميز بالاستمرار النسبي وتتم بشروط معينة ومحددة قانوناً يقوم بها شخص مخول أو مجموعة أشخاص، يستعينون بوسائل مختلفة غايتها الوصول إلى حقائق معينة تتعلق بالمشتبه بهم في ارتكاب جرائم معينة[3] واردة على سبيل الحصر[4].

فالتسرب يعد واحداً من أهم وأخطر طرق البحث والتحري وأكثرها تعقيداً، حيث يعتمد على المهارات والقدرات الشخصية لضباط وأعوان الشرطة القضائية القائمين بالعملية، والتي تعتمد

1 وداعي عز الدين، التسرب كأسلوب البحث والتحري الخاصة على ضوء قانون الإجراءات الجزائية الجزائري والمقارن، المجلة الأكاديمية للبحث القانوني، كلية الحـقوق والعلوم السياسية، جامعة عبد الرحمن ميرا بجاية، الجزائر، المجلد (16)، العدد الثاني (02)، 2017، ص 204.

2 يقصد بها العمليات أو الإجراءات أو التقنيات التي تستخدمها الضبطية القضائية من أجل البحث والتحري عن الجرائم الخطيرة وجمع الأدلة عنها والكشف عن مرتكبيها وذلك دون علم أو رضا الأشخاص المعنيين بها. **انظر في ذلك:** لوجاني نور الدين، أساليب البحث والتحري الخاصة وإجراءاتها، يوم دراسي حول علاقة النيابة العامة بالشرطة القضائية (احترام حقوق الإنسان ومكافحة الجريمة)، المركز الجامعي بإيليزي 12 ديسمبر 2007، ص 02.

3 تنص المادة 26 من القانون رقم 20-05، المؤرخ في 05 رمضان عام 1441 المـوافق 28 أبريل سنة 2020، المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما، الصادرة في الج.ر.ج رقم 25، المؤرخة في 29 أبريل سنة 2020، أنه: "مع مراعاة أحكام قانون الإجراءات الجزائية، يمكن وكيل الجمهورية أو قاضي التحقيق، بعد إخطار وكيل الجمهورية، أن يأذن، تحت رقابته، لضابط الشرطة القضـائية، بالتسـرب الإلكتروني إلى منظـومة معلوماتية أو نظام للاتصالات الإلكترونية أو أكثر، قصـد مراقبة الأشـخاص المشتبه في ارتكابهم لأي جريمة من الجرائم المنصوص عليها في هذا القانون، وذلك بإيهامهم أنه فاعل معهم أو شريك لهم...".

4 شرف الدين وردة، المرجع السابق، ص 545، **نقلاً عن:** باسم محمد شـهاب، عمليـة التـسرب: الحقيقة التشـريعية، مجلة الحقوق، مجلس النشر العلمي، جامعة الكويت، العدد الرابع (04)، السنة 37، ديسمبر 2013، ص 522.

على الكفاءة والخبرة والحيلة والذكاء، وتُستخدم فيها مختلف الأساليب من أجل كسب ثقة المشتبه فيهم وتحديد طبيعة ومدى النشاط الإجرامي[1]، ويتطلب ذلك ربط علاقات مع الأشخاص المشتبه فيهم بالاتصال بهم بطريق مباشر أو غير مباشر حسب مقتضيات العملية مع ضرورة الاحتفاظ بالسر المهني إلى حين تحقق الغاية من العملية وهو ما يستلزم المشاركة المباشرة في نشاط الخلية الإجرامية[2].

وقد عرف المشرع الجزائري التسرب في المادة 65 مكرر 12 بقوله: "يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف".

ويمكن أن تتجسد عمليـة التسرب في الجرائم الإلكترونيـة باشـتراك ضـابط أو عون الشرطة في محادثات غرف الدردشة أو حلقات النقاش حول دعارة الأطفال، أو كلام يدور حول قيام أحدهم باختراق شبكات أو بث فيروسات، فيتخذ المتسرب أسماء مستعارة ويحاول الإستفادة حول كيفية اقتحام الهاكر لموقع ما حتى يتمكن من اكتشاف وضبط الجرائم[3]. ولأن التسرب يعد إجراءً من الإجراءات التي تساعد في كشف الجرائم[4]، نصت عليه بعض التشريعات كما فعلا المشرع الفرنسي في المواد من 706-81 إلى 706-87 من ق.إ.ج.ف[5]، حيث وضع المشرع

1 معزيز أمينة، التسرب في قانون الإجراءات الجزائية، مجلة القانون والمجتمع، مخبر القانون والمجتمع، جامعة أحمد دراية أدرار، العدد الخامس، 2015، ص 246.

2 علاوة هوام، التسرب كآلية للكشف عن الجرائم في قانون الإجراءات الجزائية الجزائري، مجلة الفقه والقانون، جامعة الحاج لخضر- باتنة -، ديسمبر 2012، ص02.

3 بوعناد فاطمة الزهرة، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة الندوة للدراسات القانونية،كلية الحقوق والعلوم السياسية، جامعة الجيلالي ليابس، سيدي بلعباس، الجزائر، العدد الأول، 2013، ص 70؛ خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2010، ص 191؛ عبد الرحمن بن عبد الله السند، أحكام تقنية المعلومات "الحاسب الآلي وشبكة المعلومات(الإنترنت)"، رسالة مقدمة لنيل درجة الدكتوراه في الفقه المقارن، المعهد العالي للقضاء، قسم الفقه المقارن، جامعة الإمام محمد بن سعود الإسلامية، المملكة العربية السعودية، 1424-1425 هـ، ص 35.

4 Myriam Quéméner, *Concilier la lutte contre la cybercriminalité et l'éthique de liberté*, Revue des directeurs sécurité d'entreprise (Club des Directeurs de Sécurité des Entreprises, Sécurité et stratégie), N°5, France, Mars 2011, p: 63.

5 Les Articles 706-81 a 706-87 du Code de Procédure Pénale.

الفرنسي هذا الإجراء من أجل جمع الأدلة والبحث عن الفاعلين فيها[1]، لأنه أسلوب من أساليب التحري الجنائية التي توسع من صلاحيات الضبط القضائي ليصل إلى إمكانية استخدام أسلوب التخفي من قبل رجال الضبط القضائي بقصد ضبط الجناة، فقد تمكنت المباحث الفيدرالية الأمريكية (FBI) من ضبط أفراد عصابة باستخدام أسلوب التسلل (Infiltrate)، وذلك بدس عضو الضبطية القضائية، مما مكنهم من ضبط تشكيل (Fastlane) المكون من أعضاء منتشرين حول العالم امتهنوا قرصنة البرمجيات وتحميلها على المواقع (هكرة) عبر الإنترنت (Warez)، محققين بذلك أرباحاً وصلـت إلى مليـون دولار في فتـرة وجيـزة، إذ تمكنت المباحـث الفيدراليـة من ضبط تسعة منهم في الولايات المتحدة الأمريكية[2].

ولأن موضوع التسرب كما بينا سابقاً يعد من بين العمليات المهمة في الكشف عن الجرائم الإلكترونية ومكافحتها، فقد حددت له مجموعة من الشروط (المطلب الأول)، وخصصت للقائم به حماية قانونية (المطلب الثاني).

1 روابح فريد، الأساليب الإجرائية الخاصة للتحري والتحقيق في الجريمة المنظمة، أطروحة لنيل شهادة الدكتوراه في القانون العام، تخصـص القانون الجنائي والعلوم الجنائية، كلية الحـقوق، جامعـة بن يوسـف بن خدة، الجزائر 01، 18 فبراير 2016، ص 176؛ بوكر رشيـدة، الحماية الجزائية للتعـامـلات الإلكترونيـة، أطروحة مقدمة لنيل شهادة دكتوراه علوم، تخصص قانـون جـزائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الجيلالي اليابس، سيدي بلعباس،2017، ص 308.

2 عمـر محمد ابوبكـر بن يونس، المـرجع السابق، ص.ص: 832-833.

المطلب الأول: شروط التسرب.

حتى تكون عملية التسرب ناجحة، ونتائجها مقبولة كأدلة أمام القضاء، فرض لها المشرع مجموعة من الشروط، والتي إذا لم تتوفر لا يمكن اللجوء لعملية التسرب أساساً، فبحسب المادة 65 مكرر 11، يمكن القيام بالتسرب إذا اقتضت ذلك ضرورات التحري أو التحقيق في إحدى الجرائم المبينة في المادة 65 مكرر 5 من ق.إ.ج.ج، والتي عددت الجرائم على سبيل الحصر كما رأينا سابقاً.

وعلى اعتبار الجريمة الإلكترونية إحدى تلك الجرائم التي نصت عليها المادة السالفة الذكر، فالتسرب فيها جائز إذا فرضت ذلك ضرورة التحقيق والتحري، وأثبتت الجهة القائمة بالتسرب عدم نجاعة الأساليب العادية للتحقيق والتحري في جمع الأدلة، خاصة الإلكترونية منها، على أن تتم تلك العملية تحت رقابة وكيل الجمهورية أو قاضي التحقيق الذي أذن بها، والذي يصدر إذنه بناءً على تقرير يحرره ضابط الشرطة القضائية المكلف بتنسيق عملية التسرب، مُضمناً إياه كل العناصر الضرورية لمعاينة الجريمة محل العملية في ظروف تؤمن عدم تعرض الضابط أو العون المتسرب للخطر، مع ذكر هويته وصفته، إذ وحسب المادة 65 مكرر11 من ق.إ.ج.ج فإنه قبل إجراء عملية التســرب يتعين إصدار إذن بالعمليـة مكتوباً ومسبباً من الجهات القضائية –المتمثلة في وكيل الجمهورية أو قاضي التحقيق–، كما يتعين ذكر المدة التي تستغرقها العملية والتي لا يمكن أن تتجاوز أربعة (04) أشهر، قابلةً للتجديد حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكليـة والزمنية، كما يمكن للقاضي الذي رخـص بها أن يأمر بوقفها قبل انقـضاء المدة، على أن توضع الرخصة بالتمديد أو الوقف في الملف[1]، وهو ذات الحكم نصت عليه المادة 706-83 من ق.إ.ج.ف[2].

1 المادة 65 مكرر 15 من ق.إ.ج.ج، السالف الذكر.

2 Article 706-83, Créé par Loi n°2004-204 du 9 mars 2004 - art. 1 JORF 10 mars 2004 en vigueur le 1er octobre 2004, OP.CIT : « A peine de nullité, l'autorisation donnée en application de l'article 706-81 est délivrée par écrit et doit être spécialement motivée. Elle mentionne la ou les infractions qui justifient le recours à cette procédure et l'identité de l'officier de police judiciaire sous la responsabilité duquel se déroule l'opération. Cette autorisation fixe la durée de l'opération d'infiltration, qui ne peut pas excéder quatre mois. L'opération peut être renouvelée dans les mêmes conditions de forme et de durée. Le magistrat qui a autorisé l'opération peut, à tout moment, ordonner son interruption avant l'expiration de la durée fixée. L'autorisation est versée au dossier de la procédure après achèvement de l'opération d'infiltration ».

المطلب الثاني: الحماية القانونية للمتسرب.

نظراً للمهمة الخطيرة التي يقوم بها العون المتسرب، فقد أحاطه القانون بجملة من التدابير التي تكفل له الحماية حفاظاً على حياته وحياة عائلته، وتسهل مهمته، وتساعد على نجاحها؛ بداية بالهوية المستعارة التي يحملها، إذ لا يسمح له بالكشف عن هويته الحقيقية، وهو ما أوضحته المادة 65 مكرر 16 من ق.إ.ج.ج، بقولها:"لا يجوز إظهار الهوية الحقيقية لضابط أو أعوان الشرطة القضائية الذين يباشروا عملية التسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات"، رغم أن مسألة إعطاء الشخص المتسرب هوية مستعارة يعتريها الكثير من المخاطر والصعاب في وقتنا الحالي، خاصة مع وجود الأرقام الإلكترونية الوطنية لكل مواطن، أو ما نسميه بالوثائق البيومترية.

ولكن وعلى الرغم من ذلك فقد وضع المشرع عقاباً جزائياً قد يصل إلى عشرين (20) سنة، إذا تسبب شخص ما في وفاة أحد الأشخاص المذكورين في نفس المادة أعلاه[1]، كما أُعفي المتسرب بحكم القانون من المسؤولية الجزائية إذا اضطر للقيام بأفعال مجرمة حسب ما ورد في نص المادة 65 مكرر14 من ق.إ.ج.ج، ونص المادة 706-82 من ق.إ.ج.ف[2]، مع ملاحظة أنه لا يجوز تحت طائلة البطلان أن تشكل هذه الأفعال تحريضاً على ارتكاب الجرائم[3]؛ والمقصود

1 الأشخاص المعنيون هنا هم الضباط أو أعوان الشرطة القضائية الذين يباشرون عملية التسرب، وأزواجهم، وأبائهم، وأصولهم المباشرين.

2 جاء في المادة 65 مكرر14 من ق.إ.ج.ج، السالف الذكر: "يمكن ضباط وأعوان الشرطة القضائية المرخص لهم بإجراء عملية التسـرب والأشخـاص الذين يسخرونهم لهذا الغـرض، دون أن يكـونوا مسؤولين جـزائيا، القيام بما يلي: – اقتناء أو حيازة أو نقل أو تسليم أو إعطاء أموال أو منتوجات أو وثائق أو معلـومات متحصل عليهـا مـن ارتكاب الجرائـم أو مستعملة في ارتكابها.– استعمال أو وضع تحت تصرف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل أو التخزين أو الإيـواء أو الحفظ أو الاتصال"؛

Article 706-82**,** Créé par Loi n°2004-204 du 9 mars 2004 - art. 1 JORF 10 mars 2004 en vigueur le 1er octobre 2004, OP.CIT : « Les officiers ou agents de police judiciaire autorisés à procéder à une opération d'infiltration peuvent, sur l'ensemble du territoire national, sans être pénalement responsables de ces actes : 1° Acquérir, détenir, transporter, livrer ou délivrer des substances, biens, produits, documents ou informations tirés de la commission des infractions ou servant à la commission de ces infractions ; 2° Utiliser ou mettre à disposition des personnes se livrant à ces infractions des moyens de caractère juridique ou financier ainsi que des moyens de transport, de dépôt, d'hébergement, de conservation et de télécommunication. L'exonération de responsabilité prévue au premier alinéa est également applicable, pour les actes commis à seule fin de procéder à l'opération d'infiltration, aux personnes requises par les officiers ou agents de police judiciaire pour permettre la réalisation de cette opération. »

3 الفقرة الأخيرة من المادة 65 مكرر 12 من ق.إ.ج.ج، والفقرة ما قبل الأخيرة من المادة 706-81 من ق.إ.ج.ف؛ قضائياً:

Cour de cassation, chambre criminelle, Audience publique du 7 février 2007, N° de pourvoi: 06-87753 **(**Publié au bulletin) ; Audience publique du 7 février 2007, N° de pourvoi: 06-87753 **,** Bulletin criminel

بالتحريض البوليسي هو أنه لأجل اكتشاف سلوكيات إجرامية واقعية أو مفترضة، يقوم ضابط الشرطة القضائية بالتنكر في صورة أو أخرى ويضع المشتبه فيه تحت التجريب، فإذا ما انساق هذا الأخير وراء التحريض أو وقع في الفخ المنصوب له ألقي عليه القبض بسبب ارتكابه جريمـة[1]، لهذا قضت محكمة النقض المصرية بأن "تصرفات رجال الضبط أثناء قيامهم بالبحث والتحري يجب ألا تتجاوز الإجراءات المشروعة لاستقصاء الجريمة وجمع الاستدلالات المتعلقة بها، فكل إجراء يقومـون بـه في سبيل كشف ملابسات الجريمة والبحث عن أدلتها يعتبر صحيحاً، طالما أنهم لم يتدخلوا في خلق الجريمة أو التحريض عليها"[2].

وفي قضيـة بهذا المعنى قـام ضباط من دائرة شـرطة نيويـورك، بإنشاء موقع يسمح لمتصفحي الإنترنت بتبادل أرائهم، ومختلف التصرفات حول الممارسات الاحتيالية التي تقع على البطاقات المصرفية، حيث كان الهدف من وراء إنشائه ذلك الموقع هو جمع أدلة على ارتكاب الجرائم الإلكترونية الواقعة على البطاقات المصرفية، وتحديد مرتكبيها، ولم يكن المقصود تشجيع أولئك الذين دخلوا الموقع، على ارتكاب تلك الجرائـم الإلكترونيـة، لذا اعتبر القضـاء الفرنسي أن هذا النـوع من المواقـع لا يعد استفزازاً، أو تحريضاً على ارتكاب الجرائم[3]، لهذا فقد استحدثت المحكمة العليا الأمريكية وسيلة للدفاع مستمدة من تقنية التحريض البوليسي على ارتكاب الجريمة، والتي تستند –وسيلة الدفاع– على فكرتين؛ الأولى هي منع الشرطة من أن يجتذبوا مواطنين شرفاء لارتكاب الجريمة، حيث لو تركوا لأنفسهم لما ارتكبوها، والفكرة الثانية هي احترام أخلاقيات المهنة لدى الشرطـة القضائيـة حتى في مواجهة الجناة، إذ قال أحد قضاة المحكمة العليا في الولايات

2007 N° 37 p. 241: Sur la définition de la provocation à la commission d'une infraction par agent public, constitutive d'une atteinte au principe de la loyauté de la preuve, à rapprocher :Crim., 7 février 2007, pourvoi n° 06-87.753, Bull. crim. 2007, n° 37 (cassation), et les arrêts cités ;Crim., 16 janvier 2008, pourvoi n° 07-87.633, Bull. crim. 2008, n° 14 (rejet), et les arrêts cités ;Crim., 7 janvier 2014, pourvoi n° 13-85.246, Bull. crim. 2014, n° 1 (cassation).

1 محمد مروان، وضعية الشخص المشتبه فيه أثناء المرحلة البوليسية في الدعوى الجنائية في القانون الجزائري والمقارن، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية، كلية الحقوق والعلوم الإدارية، جامعة الجزائر، الجزء تسعة وثلاثون (39)، العدد رقم 02، سنة 2001، ص 138.

2 حكم محكمة النقض المصرية بتاريخ: 1967/01/14، نقلا عن: علاوة هوام، المرجع السابق، ص05.

3 Cour de cassation, chambre criminelle, Audience publique du 30 avril 2014, N° de pourvoi: 13-88162, ECLI:FR:CCASS:2014:CR02211(Publié au bulletin).

المتحدة الأمريكية بأن الحكومة يمكنها أن تضع طعما للقبض على المجرمين، ولكن لا يمكنها خلق جريمة من أجل محاكمة مجرم هو من خالص صنعها[1].

ومنه يمكننا القول أن مشروعية أي إجراء من الإجراءات السابقة يستوجب عدم مخالفتها للقواعد القانونية المنظمة لها، أي الشروط الموضوعية والشكلية اللازمة لممارستها مع مراعاة المواثيق الدولية وحقوق الإنسان[2]، وإلا نكون إزاء إجراء غير مشروع، ينجم عنه طرح كل دليل جنائي ناجم عنه وغير معتد به، وفي كثير من الأحيان يقع باطلاً بطلاناً مطلقاً ويتم استبعاده من أدلة الإثبات[3].

1 روابح فريد، المرجع السابق، ص ص 198-199، **نقلاً عـن**:

- Jean Pradel, *Le Crime organisé après la loi française du 09 Mars 2004 dite loi de Perben II* **,** Revue de droit pénal et de criminologie, éd la charte, Bruxelles, n° 02, 2005, p : 311.

2 تنص المادة 159 من ق.إ.ج.ج: "يترتب البطلان أيضاً على مخالفة الأحكام الجوهرية المقررة في هذا الباب خلاف الأحكام المقررة في المادتين 100 و105 إذا ترتب على مخالفتها إخلال بحقوق الدفاع أو حقوق أي خصم في الدعوى. وتقرر غـرفة الاتهام ما إذا كان البطلان يتعين قصره على الإجـراء المطعون فيه أو امتداده جزئيا أو كليا على الإجـراءات اللاحقة له..."، والمادة 336 من ق.إ.ج.م: "إذا تقرر بطلان أي إجراء فإنه يتناول جميع الآثار التي تترتب عليه مباشرة، ولزم إعادته متى أمكن ذلك".

3 جميلة محلق، المرجـع السابق، ص 182، **نقلاً عـن**: أحمد الشافعي، البطلان في قانـون الإجراءات الجزائيـة "دراسة مقارنة"، دار هومـة، الجزائر، الطبعة الرابعـة، 2007، ص 30؛ رويس عبد القادر، أساليب البحث والتحري الخاصة وحجيتها في الإثبات الجـنائي، المجلـة الجـزائرية للحقوق والعلوم السياسية، معهد العلوم القانونيـة والإداريـة، المركز الجـامعي احمد بن يحي الونشريسي، تيسمسيلت، الجزائر، العدد الثالث (03)، جوان 2017، ص 44؛ نقادي حفيظ، أساليب البحث والتحري الخاصـة، المجلة الجزائرية للعلوم القانونيـة والسـياسية، كليـة الحقـوق، جامعة الجزائر 01 بن يوسف بن خدة، المجلد (50)، العدد الرابع (4)، 2013/12/01، ص 467.

المبحث الثالث:

دور مقدم الخدمات في كشف الجريمة الإلكترونية وجمع الأدلة الإلكترونية.

لدى مقدم الخدمات من المعلومات ما يُمكِّن الجهات المختصة سواء كانت جهات تحقيق أو تحري، أو جهات قضائية وطنية أو حتى دولية من الحصول والوصول إلى معلومات تفيد في كشف الجرائم الإلكترونية، وإيجاد مرتكبيها، لذا أوجبت عليه مختلف التشريعات بعض الإلتزامات التي تسهل عملية الحصول والوصول لتلك المعلومات أو البيانات التي يمكن أن تستخلص منها الأدلة الإلكترونية المبحوث عنها.

ولأن ميولات الأشخاص واحتياجاتهم واستعمالاتهم للانترنت تختلف، نجد أن ذلك ينعكس على وظائف مـزودي خدمات الإنترنت فتتـنوع بذلك الخدمـات التي يقدمونها لمستعملي الشبكـة العنكبوتيـة، فمنهم من يقتصر دوره في مساعدة مستخدمي تلك الشبكة في الدخول إليها وتصفح مواقعها، والاطلاع على ما تحتويـه من معلومـات، دون أن يكـون لذلك المـزود أي دور في تحـرير محتـوى الشبكـة، أو تعديله، أو حتى تخزينه، وهم من يطلق عليهم تسمية مزودي خدمة الدخول، وهناك نوع أخر من مزودي خدمات الإنترنت، والذي يقوم بتخزين المحتوى مهما كان نوعه؛ كالنصوص والصور والفيديوهات، وهو المسمى بمـزود خدمـات الاستضافـة على الشبكة، وإلى جانبهما هناك مزود المحتوى، والذي يملك سلطة الرقابة الكاملة على المحتوى الذي يضعه على الشبكة، إذ تتوفر لديه إمكانية تصحيـح أو تغيير ذلك المحتـوى[1].

ومن أجل الوصل للدور الذي يلعبه مقدم الخدمات في الكشف عن الجريمة الإلكترونية وجمع الأدلة الإلكترونية، تم تقسيم هذا المبحث إلى مطلبين؛ يتم التطرق فيهما إلى مقدم خدمة الإنترنت في القانون الوطني والمقارن (المطلب الأول)، وإلى التزام مقدم خدمة الإنترنت اتجاه المحتوى غير المشروع (المطلب الثاني).

1 أروى محمد تقوى، التزامات مزودي خدمات الانترنت في مجال حماية الأطفال من المواد الضارة على الشبكة في النظام القانـوني السـوري"دراسـة مقارنـة"، مجلـة جامعـة الخليـل للبحـوث، فلسطيـــن، المجـلد الثـــامن (08)، العـــدد الثاني (02)، 2013، ص.ص: 155-156؛ باسم السيد، النظـــام القانوني لمزود خدمة الانترنت في سوريـــة، مجلة جامعـة البعث، سورية، المجلد التاسع والثلاثون (39)، العدد الخمسون (50)، 2017، ص 71.

المطلب الأول: مقدم خدمة الإنترنت في القانون الوطني والمقارن.

يطلق على مقدم خدمة الإنترنت عـدة تسميات مثل متعهـد الوصـول، متعهد الخدمة[1] أو مقدم الخدمة، كما سماه المشرع الجزائري في القانون رقم 09-04 الخاص بقواعد الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، من خلال الفقرة (د) من المادة الثانية (02)[2] والمادة 11 من نفس القانون، أين بَيَّنَ الإلتزامات التي تقع على هذا الأخير، لِيُبقي على ذات التسمية خلال القوانين اللاحقة مثلما جاء في الفقرة الثانية من المادة الثانية (02) من المرسوم الرئاسي رقم 14-252، المتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، السالف الذكر[3]، وكذا ما ورد في الفقرة (19) من المادة الثالثة (03) من القانون رقم 18-07، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي[1].

---

1 متعهد الإيواء: "يعمل على تخزين البيانات والمعلومات التي يبثها أصحاب المواقع الإلكترونية على حساباته الآلية المرتبطة على المودم بشبكة الانترنت بحيث يتمكن أصحاب هذه المواقع من اطلاع الجمهور على مضمون المعلومات على مدار الساعة". **انظر**: زينة حازم خلف الجبوري، القانون الواجب التطبيق على مسؤولية مزود خدمـة الانترنت، مجلـة جامعـة تكـريت للحقوق، العـــراق، السـنة الأولى (01)، المجلد الأول (01)، العدد الرابع (04)، الجزء الثاني (02)، جوان 2017، ص 390، **نقلاً عن**: أحمد فرح، النظام القانوني لمقدمي خدمات الانترنت، مجلة المنارة، المجلد 13، العـدد 9، الأردن، 2007، ص 324.

أما مقدم الإيواء:"أو خادم الإيواء هو الشخص الطبيعي أو المعنوي الذي يضع رهن إشارة مقدمي الخدمات على الانترنت المعدات التقنية التي تمكن مستعمليها من النفاذ إلى تلك الخدمات على الانترنت المعـدات التقنيـة التي تمكـن مستعمليها من النفـاذ إلى تلك الخدمـــات، فمهمته إذن مختلفة عن مهمة مقدم الولوج وإن كان بإمكانه أن يجمع المهام كلها. فهو يوفر فضاء للذاكرة على خوادمه الشخصية"، كتقديم الجامعات لصفحات أو مشغل لفائدة مستخدميه، أو شركة تزاول الخدمات على الخط. **انظر**: العربي جنان، الأنظمة المعلوماتية والانترنت بين التنظيم وأحـــكام المسؤولية – النظرية والتأصيل-، أطـــروحة لنيل الدكتـــوراه في الحقوق، كلية العلوم القانونية والاقتصادية والاجتماعية، جامعة القاضي عياض، مراكش، المغرب، 2010، ص 421.

2 جاء في الفقرة (د) من المادة الثانية من القانون 09-04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، السالف الذكر:"مقدم الخدمات: 1- أي كيان عام أو خاص يقدم لمستعملي خدماته، القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام للاتصالات، 2- وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصـال المذكورة أو لمستعمليها". وهـذا التعريف في النص باللغة الفرنسية للقانون 09-04، نجده في المادة الأولى (1) من الفصل الأول من اتفاقية بودابست لسنة 2001 الخاصة بمكافحة الجريمة الإلكترونية كما يلي:

Conseil de l'Europe - **Convention sur la cybercriminalité (STE n° 185)** ; Conseil de l'Europe - Convention sur la cybercriminalité (STE n° 185) , Budapest, 23.XI.2001, sur le site : https://rm.coe.int/168008156d: « c- l'expression «fournisseur de services» désigne: (i) toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique, et (ii) toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs… »

3 الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر سنة 2010، المصادق عليها بالمرسوم الرئاسي رقم 14-252، السالفة الذكر، جاء في الفقرة الثانـية من المادة الثانية (02) منه أن:"... 2- مزود الخدمة: أي شخص طبيعي أو

أما بالنسبة للمشرع المصري فهو الآخر استعمل نفس المصطلح سنة 2003 في الفقرة السابعة (7) من المادة الأولى (01) من القانون رقم 10 لسنة 2003 الخاص بإصدار قانون تنظيم الاتصال[2]، كما حافظ عليه خلال القوانين اللاحقة، كالقرار الرئاسي رقم 276 لسنة 2014، المتعلق بالموافقة على انضمام جمهورية مصر العربية إلى الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الموقعة في القاهرة بتاريخ 21 ديسمبر 2010، وما ورد في القانون رقم 175 لسنـة 2018 الخاص بمكافحـة جرائم تقنيـة المعلومات من خلال الفقرة الثامنة (08) من المادة الأولى[3]، إلا أن المشرع المصـري في هذا القانون وسـع من مهام مقدم خدمة الإنترنت، بحيث أصبح تعريف مقـدم خـدمة الإنترنت يشمـل كل شخص طبيعي أو معنوي يزود المستخدمين بخدمات تقنيات المعلومات والاتصالات سواء قام بمعالجة أو تخزين المعلومات بذاته أو قام بها من ينوب عنه في أي من تلك الخدمات أو تقنية المعلومات.

وما يلاحظ أن المشرعين الجزائري والمصري لم يبينوا الأصناف المختلفة لمـزودي الخدمات كما فعل المشرع السوري من خلال فقرات المادة الأولى من القانـون الخاص بتنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية، إذ أوضح من هو مقدم الخدمات على الشبكة، ومقدم

معنوي عام أو خاص يزود المشتركين بالخدمات للتواصل بواسطة تقنية المعلومات، أو يقوم بمعالجة أو تخزين المعلومات نيابة عن خدمة الاتصالات أو مستخدميها."

1 جاء في الفقرة (19) من المادة الثالثة (03)، القانون رقم 18-07، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، السالف الذكر: "مقدم الخدمات": 1- أي كيان عام أو خاص يقدم لمستعملي خدماته، القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام للاتصالات، 2- أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكور أو للمستعملين،...".

2 جاء في الفقرة السابعة (7) من المادة الأولى (01) من القانون رقم 10 لسنة 2003، الخاص بإصدار قانون تنظيم الاتصالات المصري، الصادر في الج.ر العدد 5 مكرر(أ)، في 04 فبراير سنة 2003، ص 03 بأن: "بمقدم خدمة الاتصالات: أي شخص طبيعي أو اعتباري، مرخص له من الجهاز بتقديم خدمة أو أكثر من خدمات الاتصالات للغير". في هذا القانون كانت الخدمة مقتصرة على الاتصالات فقط، بينهما في القانون رقم 175 لسنة 2018 أضاف المشرع المصري لمهام مقدمي الخدمات خدمات تقنية المعلومات.

3 نصت الفقرة الثامنة من المادة الأولى (08/01) على أن: "مقدم الخدمة: أي شخص طبيعي أو اعتباري يزود المستخدمين بخدمات تقنيات المعلومات والاتصالات، ويشمل ذلك من يقوم بمعالجة أو تخزين المعلومات بذاته أو من ينوب عنه في أي من تلك الخدمات أو تقنية المعلومات".

خدمات التواصل، ومقدم خدمات الاستضافة، وكذا مقدم خدمات النفاذ إلى الشبكة[1]، بينما هناك بعض التشريعات العربية التي لا يوجد بها تنظيم قانوني ينظم العلاقة بين مزود الخدمة والمتعامل كما هو الحال في العراق[2].

أما بالنسبة للتشريعات الغربية، نجد المشرع الفرنسي تطرق لتعريف مقدم الخدمة في المجتمع المعلوماتي من خلال الفقرات (أ)، (ب)، (ج) من التوجـيه EC 31/2000 الصادر عن البرلمـان والمجلس الأوروبي[3]، وتطرق لمقدم الخدمات أيضاً في الفقرات الأولى (1) والثانية (2) من المادة السادسة (6) من القانون رقم 2004-575 والخاص بالثقة في الاقتصاد الرقمي[4]، والذي تعرض من خلاله لتعريف كل من متعهد الإيواء، وكذا مقدم خدمات الاستضافة.

1 قانون تنظيـم التواصل على الشبكة ومكافحة الجريمة المعلوماتيـة، الصادر بموجب المرسـوم التشريعي رقم 17 لعام 2012، والصادر بموجـب القـرار رقـم 290 بتاريخ 08 ماي 2012، والمتضمن التعليمات التوضيحية والتنفيذية، لقانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية السوري.

نصت الفقرات (12، و14، و15، و16) من المادة الأولى من هذا القانون على أن:" **مقدّم الخدمات على الشبكة** on-line service provider أي من مقدمي الخدمات الذين يعملون في إطار التواصل على الشبكة؛ ومن أصنافهـم: مقدم خدمات النفـاذ إلى الشبكـة، ومقدم خدمات التواصل على الشبكة، ومقدم خدمات الاستضافة على الشبكة. **مقّدم خدمات التواصل على الشبكة** on-line communication provider مقّدم الخـدمات الذي يتيح التواصل على الشبكـة، وذلك عن طريـق مـوقع إلكتروني أو أكثـر، أو أي منظومة معلوماتية مشابهة." ت9 ." مقّدم التواصل على الشبكة يدل على كل من يقّدم معلومات أو خدمات على الشبكة، أياً كان نوعها، لعامة الجمهور أو فئة منه، على موقع إلكتروني أو أكثر، أو أي منظومة معلوماتية مشابهة، سواء أكان ذلك يتطلب اشتركاً أم لا يتطلب، أو كان مجاناً أم في مقابل أجر، أو كان تفاعلياً أم لم يكن". "**مقّدم خدمات الاستضافة على الشبكة** on-line hosting provider: مقّدم الخدمات الذي يوفّر، مباشرة أو عن طريق وسيط، البيئة والموارد المعلوماتية اللازمة لتخزين المحتوى، بغية وضـع موقـع إلكتروني على الشبكة؛ وُيسّمى اختصارا المضيف host. **مقّدم خدمات النفاذ إلى الشبكة** on-line access provider: مقّدم الخدمات الذي يتيح للمشتركين لديه النفاذ إلى الشبكة والوصول إلى المعلومات والخدمات المتوفّرة عليها".ت 10. من أهم أشكـال مقّـدمي خدمـات النفـاذ إلى الشبكة: مقّدمو خدمات الإنترنت Internet Service Provider (ISP)".

2 زينة حازم خلف الجبوري، المرجع السابق، ص 381.

3 التوجـيه EC 31/2000 / الصادر عن البرلمـان والمجلس الأوروبي في 8 يونيو 2000، بشأن بعـض الجوانـب القانـونية لخدمـات مجتمع المعلومات، ولاسيما التجارة الإلكترونية، في السوق الداخلية، موجود على الموقع الإلكتروني الموالي والخاص بالمنظمة العالمية للملكية الفكرية (WIPO).

4 L'Article 6 (Modifié par LOI n°2018-898 du 23 octobre 2018 - art. 29) du la Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique: « I.-1. Les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne informent leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner et leur proposent au moins un de ces moyens. … 2. Les personnes physiques ou morales qui assurent, même à

أما المشرع الأمريكي فقد خصص الباب الثاني من قانون حقوق المؤلف للألفية الرقمية[1] (DMCA) لمزودي خدمة الإنترنت ومختلف الالتزامات المفروضة عليهم، وقد ورد في الصفحة التاسعة منه تعريف لمختلف أنـواع مزودي الخدمة[2]، وقد عُرف مـزود الخدمة على أنه: "أي كيان يعرض إرسال، توجيه، أو توفيـر الاتصالات، للاتصالات الرقمية على الشبكة، بين نقطتين أو نقاط محددة من قبل المستخدم، لمدة يختارها المستخدم، دون تعديل محتوى المادة التي يتم إرسالها أو استقبالها"[3].

إن مسألة التعرف على الأنواع المختلفة لمزودي الخدمات هي خطوة يسهل معها معرفة الدور الذي يلعبه كلاً منهم في الاتصالات الإلكترونية التي تتم بمساعدتهم في المجتمع المعلوماتي، وبالأخص ما قد يتم من جرائم في العالم الافتراضي المترامي الأطراف، كما يمكن تحديد من منهم لديه إمكانية الوصول إلى البيانات والمعلومات غير المشروعة أكثر من الآخر.

المطلب الثاني: التزام مقدم خدمة الإنترنت اتجاه المحتوى غير المشروع.

لحسن سير الخدمات المقدمة للجمهور واستمراريتها، أوجدت التشريعات مجموعة من المبادئ والشروط التي على مقدمي الخدمات مراعاتها، كنوعية الخدمة ووفرتها والحرص على عدم المساس بالأمن والنظام العام، واحترام خصوصية حياة الأشخاص، خاصة البيانات والمعلومات التي

titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature . »

1 قانون الألفية الجديدة لحقوق طبع ونشر للمواد الرقمية (DMCA) هو تشريع سنه كونغرس الولايات المتحدة في أكتوبر 1998 والذي أدخل تغييرات كبيرة على قانون حقوق النشر في الولايات المتحدة. كانت هذه التغييرات ضرورية جزئيًا لجعل قانون حقوق النشر الأمريكي يتوافق مع معاهدة حقوق الملكية الفكرية للمنظمة العالمية للملكية الفكرية (WIPO)، كما عزز هذا القانون الحماية القانونية لحقوق الملكية الفكرية في أعقاب تكنولوجيات الاتصالات المعلوماتية الجديدة الناشئة، أي الإنترنت، للمزيد بخصوص ذلك يمكن الإطلاع على الموقع الإلكتروني لجامعة إنديانا الأمريكية: *https://kb.iu.edu/d/alik*.

2 The Digital Millennium Copyright Act (DMCA) OF 1998 U.S. Copyright Office Summary, Pub. L. No. 105-304, 112 Stat. 2860 (Oct. 28, 1998) , p :09 « Service Provider is defined in section 512 (k) (1) (A) as "an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received." For purposes of the other three limitations, "service provider" is more broadly defined in section 512(k)(l)(B) as "a provider of online services or network access, or the operator of facilities therefor."

3 أروى محمد تقوى، مدى مسؤولية مشغلي الهاتف النقال عن إساءة استخدامه في الاتصال بالانترنت دراسة مقارنة، مجلة الحقوق، جامعة البحرين، البحرين، المجلد الحادي عشر (11)، العدد الثاني (02)، 2014، ص 362.

يتم إيصالها عن طريق شبكات الإتصال الإلكترونية[1]، لأن مزود خدمة الإنترنت يساعد في تقليص الصعوبات وتشخيص الجاني أو على الأقل إيجاد الأداة التي ارتكبت بواسطتها الجريمة، والتي قد تكون قرينة أو دليل لإثبات تلك الجريمة، حيث يمكنه معرفة بعض البيانات التي تساعد في كشفها كمصدر الاتصال ووجهته، من خلال رقم الهاتف وبروتوكول الإنترنت IP، ومن الأمثلة على دور مزود الخدمة في كشف الجريمة، ما حدث في مصر عام 2014، حينما بُث فيلم عبر شبكات الإنترنت لمجموعة من الجنود، تم اختطافهم وتصويرهم كأسرى، وبمساعدة مزود الخدمة تمكن المحققون من تتبع مصدر ذلك الفيلم، وتوصلوا إلى تحديد الموقع الذي بث منه لأول مرة، والذي

1 تنص المادة 97، والمادة 117 على التوالي من القانون رقم 18-04، المتضمن القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، السالف الذكر: "يخضع إنشاء واستغلال شبكات الاتصالات الإلكترونية المفتوحة للجمهور وتقديم خدمات الاتصالات الإلكترونية للجمهور إلى احترام ما يأتي: – شروط المداومة ونوعية الخدمات والوفرة وأمن وسلامة الشبكات والخدمات، وكذا جميع المتطلبات الأخرى الجوهرية كما هي محددة في دفاتر الشروط، – شروط خصوصية البيانات والمعلومات التي تم إيصالها بواسطة شبكات الاتصالات الإلكترونية، شروط حماية الحياة الخاصة للمشتركين والبيانات ذات الطابع الشخصي، ..."، "يجب ألا يمس استعمال شبكات و/أو خدمات الاتصالات الإلكترونية بما يلي: – النظام العـام والدفـاع الوطني والأمـن العمومي، – الكرامة وحفظ الحياة الخاصة للآخرين، – حماية الأطفال، خصوصاً فيما يتعلق باستعمال خدمات الانترنت". وعرفت الفقرة 21 و22 من المادة 10 من ذات القانون بأن: "شبكة الاتصالات الإلكترونية: كل منشأة أو مجموعة منشآت تضمن إما إرسالا، أو إرسال و إيصال إشارات إلكترونية، وكذا تبادل معلومات التحكم والتسيير المتصلة بها، ما بين النقاط الطرفية لهذه الشبكة، وعند الاقتضاء، الوسائل الأخرى التي تضمن إيصال الاتصالات الإلكترونية، وكذا التحويل والتوجيه. تعـد شبكات اتصالات إلكترونية خصوصا: شبكات الأقمار الصناعية والشبكات الأرضية والأنظمة التي تستعمل الشبكة الكهربائية شريطة أن تستعمل لإيصال الاتصالات الإلكترونية."، شبكة الاتصالات الإلكترونية المفتوحة للجمهور: "كل شبكة للاتصالات الإلكترونية منشأة أو مستعملة لتقديم خدمات الاتصالات الإلكترونية أو خدمات اتصالات للجمهور بطريقـة إلكترونيـة". أما الفقرة 40 من نفس المادة ونفس القانون فقد وصفت منشآت الاتصالات الإلكترونية بأنها:"تجهيزات أو أجهزة أو كوابل أو أنظمة إلكترونية أو لاسلكية كهربائية أو بصرية أو كل آلية تقنية يمكن استخدامها لإرسال علامات أو إشارات أو بيانات أو كتابات أو صور أو صوت عبر أمواج كهرومغناطيسية أو أي عملية أخرى متصلة مباشرة بها". كما تنص المادة 160 من نفس القانون على أنه: "يلتزم المتعاملون وكذا مستخدموهم، باحترام سرية المراسلات الصادرة عن طريق الاتصالات الإلكترونية وشروط حماية الحياة الخاصة والمعلومات الاسمية للمشتركين"؛ وتنص المادة 26 من القانون رقم 18-05، المؤرخ في 24 شعبان عام 1439 الموافـق 10 مـاي سنة 2018، المتعلق بالتجارة الإلكترونية، المنشور بالج.ر.ج رقـم 28، الصادرة يوم 16 ماي 2018: "ينبغي للمورد الإلكتروني الذي يقوم بجمع المعطيات ذات الطابع الشخصي ويشكل ملفات الزبائن المحتملين، ألا يجمع إلا البيانات الضرورية لإبرام المعاملات التجارية.كما يجب عليه: – الحصول على موافقة المستهلكين الإلكترونيين قبل جمع البيانات، – ضمان امن نظم المعلومات وسرية البيانات، – الالتزام بالأحكام القانونية والتنظيمية المعمول بها في هذا المجال...".

كان لأحد مقاهي الإنترنت الموجودة بمحافظة شمال سيناء، مما ساعد في التوصل إلى مرتكبي تلك الجريمة، وتحرير الجنود المُختطفين[1].

ولأن مُقدمي الخدمات لهم دور مهم في كشف الجرائم والوصول لمرتكبيها، فقد فرضت عليهم مختلف التشريعات التزامات يتعين عليهم القيام بها، كتقديم المساعدة للسلطات المكلفة بالتحريات القضائية سواء كانت داخلية أو خارجية من أجل جمع وتسجيل المعطيات المتعلقة بمحتوى الإتصالات في حينها ووضع المعطيات التي يتعين عليهم حفظها تحت تصرف السلطات المحددة في القانون والاتفاقيات الدولية، وكذا التدخل الفوري والسريع من أجل سحب المحتويات غير المشروعة بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين أو جعل الدخول إليها غير ممكن، ووضع الترتيبات التقنية الضرورية التي تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام والآداب العامة وإخبار المشتركين لديهم بوجودها[2]، لذا أكد مكتب الشرطة الفيدرالية في سويسرا أنه على مقدم الإيواء إذا كانت تتوفر لديه معلومات دقيقة ومفصلة

1 محمد عبد الكريم حسين، المسؤولية الجنائية لمورد خدمة الانترنت، منشـورات الحلبي الحقوقيـة، بيروت، 2017، ص 116.

2 جاء في المادة 10، والمادة 11، والمادة 12 على التوالي من القانون 09-04 السالف الذكـر ما يلي: "في إطار تطبيق أحكام هذا القانون، يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها وفقاً للمادة (11) أدناه، تحت تصرف السلطات المذكورة. ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق."، وكذلك: "مع مراعاة طبيعة ونوعية الخدمات، يلتزم مقدمو الخدمات بحفظ: أ- المعطيات التي تسمح بالتعرف على مستعملي الخدمة، ب- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال، ج- الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال، د- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها، هـ- المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها. بالنسبة لنشاطات الهاتف، يقوم المتعامل بحفظ المعطيات المذكورة في الفقرة "أ" من هذه المادة وكذا تلك التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه..."، "زيادة على الالتزامات المنصوص عليها في المادة (11) أعلاه، يتعين على مقدمي خدمات"الانترنت" ما يأتي: أ- التدخل الفوري لسحب المحتويات التي يتيحون الاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن، ب- وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام والآداب العامة وإخبار المشتركين لديهم بوجودها"، كما تنص المادة (119) من نفس القانون على:"يلزم متعاملو الاتصالات الإلكترونية باتخاذ التدابير التي من شأنها أن تضمن سرية المكالمات والمعلومات التي يحوزونها عن مشتركيهم، وألا يسمحوا بوضع أي ترتيبات بغرض اعتراض الاتصالات أو مراقبة المكالمات الهاتفية والوصلات والمحادثات والمبادلات الإلكترونية دون إذن مسبق من السلطة القضائية وفقا للتشريع المعمول به. ويجب عليهم أن يطلعوا أعوانهم على الالتزامات التي يخضعون لها وعلى العقوبات التي يتعرضون لها في حالة عدم احترامهم لهذه الأحكام".

عن مضامين تقع تحت طائلة العقاب موجودة على أحـد خوادمه، فعليه أن يعمل على حذفها أو الحيلولـة دون الوصول والنفـاذ إليها"[1].

كما طلب قاضي تحقيق السويسري سنة 2002 في قضية جنائية من موفري الوصول منع وصول عملائهم إلى بعض المواقع التشهيرية لاسيما عن طريق تعديل خوادم (DNS) لتوجيه أولئك المستخدمين لصفحة فارغة حتى لا يستطيعوا تصفح تلك المواقع المحتوية على أشياء مخالفة للقانون[2]، وكذلك فعل المدَّعي العام في ايطاليا حين طلب من مزودي خدمة الإنترنت منع وصول المشتركين إلى الموقع المسمى "خليج القراصنة"، نظراً لما يحويه هذا الأخير من معلومات مخالفة للقانون، إذ يعد الالتزام الذي يقع على عاتق مقدم خدمات الإنترنت في هذا المجال هو الالتزام ببذل العناية اللازمة لمعرفة الأشخاص الذين يشتركون في البث على شبكة الإنترنت عن طريق المدخل الذي يقدمه لهم، ففي ذلك تدرك أن حقيقة ما يجنيه مقدم الخدمات من أربـاح يبرر ما يمكن أن يتكبده من نفقـات لمتابعة ما يتم بثه عن طريق المنفـذ الذي يقدمـه[3].

ويذهب جانب من الفقه[4] إلى القول بأنه من منطلق الالتزامات التي تقع على عائق مزود خدمة الإنترنت، فهو ملزم بإفشاء أسرار الاتصالات التي تتم عبر شبكة الإنترنت لرجال الضبط القضائي، إذا كانت تلك المعلومات تفيد في الكشف عن بعض الجرائم القائم التحقيق الجنائي بشأنها، وهو الأمر الذي أكدته مختلف التشريعات والأحكام القضائية في هذا الشأن؛ لأن أول الأمور التي يضمنها مزود الخدمة هي صحة المعلومـات، لهذا ذهبت المحكمة الابتدائية بباريـس إلى القول بأن:"مزودي الخدمات ملزمون بحكم القانون بتمكين الجهات القضائية من البيانات والمعطيات التي تدخل في إطار حوزتهم وذلك لأغراض بحث مدنية أو جنائية، وأن الجهات

1 العربي جنان، المرجع السابق، ص 446.

2 François Charlet**,** *Responsabilité en droit d'auteur des intermédiaires : de l'hébergeur aux plateformes interactives***,** Mémoire en vue de l'obtention de la Maîtrise universitaire en Droit, criminalité et sécurité des technologies de l'information, Faculté de droit et des sciences criminelles, Université de Lausanne, Année académique, Université de Lausanne , 2011-2012, p32.

3 غانم محمد غانم، المرجع السابق، ص 236.

4 شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، الإسكندرية، مصر، 2007، ص 211؛ زيبحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والـدولي، دار الهـدى، عين مليلة، الجزائـر، 2011، ص 153؛ عبد الله الكرجي، صليحة حاجي، الإثبـات الرقمي، الطبعـة الأولى، مطبعة الأمنيـة، الرباط، 2015، ص 109.

المذكورة لا تتحـمل أية مسؤولية قانونيـة ما دام القانون الفرنسي والقوانين الأوربية تجيز لها ذلك"[1]. كما تضمن القانون الأمريكي (ECPA) حالات أجاز فيها لمزودي خدمة الإنترنت الكشف الاختياري عن محتوى ملفات العملاء لديهم، خاصة إذا تعلقت هذه المعلومات بارتكاب جريمة ما، كالجرائم التي تقع إخلالاً بقانون حماية الطفل، أو أفعال جنسيـة شاذة، أو كـان هناك خطر بالموت، أو إيذاء جسماني يهدد الأشخاص. وأجاز أيضاً القانون الأمريكي لرجال الضبط القضائي الاطلاع على البيانات الموجودة بحوزة موردي الخدمات، والتي لا يتمتع فيها المشترك بالحق في الخصوصية، وهذه المعلومات هي:

- المعلومات الشخصية كالاسم والعنوان ورقم الهاتف،
- المعلومات الخاصة بالمتعامل مع المشترك،
- المعلومات الخاصة بمحتوى الملفات؛ كمضمونها أو ما تضمنته المحادثات[2].

وهي معلومات لا تمانع قوانين عدة الكشف عنها عند طلبها من طـرف السلطـات المختصة كما رأينا في المادة 11 من القانون 09-04 الخاص بقواعد الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وما تضمنته المادة الثانية (02) والفقرة الثالثة من المادة السادسة (3/6) من القانون رقم 175 لسنة 2018 الخاص بمكافحة جرائم تقنية المعلومات[3].

---

1 حكم المحكمة الابتدائية بباريـس بتاريخ 30 يناير 2013، **نقلاً عـن**: عبد الحكيم الحكماوي، المرجع السابق، ص 152.

2 محمد عبد الكريم حسين، المرجع السابق، ص.ص: 125-127. وللمزيد حول إفصاح مزودي خدمة الانترنت عن اتصالات العملاء وسجلاتهم في حالة صدور أمر من السلطة المختصة، يمكن الاطلاع على القانون الموالي:

- 18 U.S.C. 2703 - U.S. Code - Unannotated Title 18. Crimes and Criminal Procedure 2703. Required disclosure of customer communications or records.

3 المادة الثانية (02) من القانون رقم 175 لسنة 2018، السالف الذكر، التزامات وواجبات مقدم الخدمة: "أولاً: مع عدم الإخلال بالأحكام الواردة بهذا القانون وقانون تنظيم الاتصالات رقم 10 لسنة 2003 المشار إليه، يلتزم مقدمو الخدمة بما يلي (1): حفظ وتخزين سجل النظام المعلوماتى أو أي وسيلة لتقنية المعلومات لمدة مائة وثمانين (180) يوماً متصلة وتتمثل البيانات الواجب حفظها وتخزينها فيما يلي: أ-البيانات التي تمكن من التعرف علي مستخدم الخدمة. ب- البيانات المتعلقة بمحتوي ومضمون النظام المعلوماتي المتعامل متى كانت تحت سيطرته. ج - البيانات المتعلقة بحركة الاتصال. د- البيانات المتعلقة بالأجهزة الطرفية للاتصال. هـ- أي بيانات أخرى يصـدر بتحديدها قرار من مجلس إدارة الجهاز. 2- المحافظة علي سرية البيانات التي تم حفظها وتخزينها، وعدم إفشائها أو الإفصاح عنها بغير أمر مسبب من إحدى الجهات القضائية المختصة، ويشمل ذلك البيانات الشخصية لأي من مستخدمي خدمته، أو أي بيانات أو معلومات متعلقة بالمواقع والحسابات الخاصة التي يدخـل عليها هؤلاء المستخدمون، أو الأشخاص والجهات التي يتواصـلون معهـا. 3-تأمين البيانات والمعلومات بما يحافظ على سريتها، وعدم اعتراضها أو اختراقها أو تلفها. ثانياً: مع عدم الإخلال بأحكام قانون حماية المستهلك الصادر بالقانون رقم 67 لسنه 2006، يجب علي مقدم الخدمة أن يوفر لمستخدمي

وباستقصاء مختلف التشريعات يتبين أن دور مزود الخدمات لا يتوقف على إمداد السلطات المختصة بالمعلومات التي تطلبها فقط، بل لابد عليه أن يُعلِمها بالمحتوى غير المشروع، وأن يوقف إذاعة ذلك المحتوى ويتخذ الإجراءات الضرورية والسريعة لإزالة أو تعطيل الوصول إلى تلك المعلومات، خاصة إذا كان من مزودي الخدمات الذين بحكم إمكانياتهم ومهامهم يمكنهم الإطلاع على المحتوى غير المشروع[1]، ولقد بينت المواد: 12، و13، و14، و15 من التوجيه الأوربي EC 31/2000 الحالات التي يكون فيها مزود الخدمة مسؤولاً عن المعلومات غير المشروعة، وكيف عليه التصرف حين العلم بعدم مشروعيتها[2]، أما في إيطاليا فقد أصدر المشرع الايطالي في 19 أبريل 2003 مرسوم يتعلق بنقل نصوص التوجه الأوربي للتجارة الإلكترونية لقانونه الداخلي ونص في المادة 14 منه على نفس الأحكام التي تضمنتها المادة 14 من التوجه الأوربي، أما في ألمانيا فقد نص المشرع الألماني في الفقرة الخامسة من المادة الأولى (5/1) من القانون الخاص بالشروط

خدماته ولأي جهة حكومية مختصة، بالشكل والطريقة التي يمكن الوصول إليها بصورة ميسرة ومباشرة ومستمرة، البيانات والمعلومات الآتية: 1- اسم مقـدم الخدمة وعنوانه. 2- معلومات الاتصال المتعلقة بمقـدم الخدمة، بما في ذلك عنوان الاتصال الإلكتروني. 3- بيانات الترخيص لتحديد هوية مقدم الخدمة، وتحديد الجهة المختصة التي يخضع لإشرافها. 4- أية معلومات أخرى يقدر الجهـاز أهميتها لحمايـة مستخـدمي الخدمـة، ويصدر بتحددها قرار من الوزير المختص. ثالثا: مع مراعاة حرمـة الحياة الخاصة التي يكفلها الدستور، يلتزم مقدمو الخدمة والتابعون لهم، أن يوفروا حال طلب جهات الأمن القومي، ووفقا لاحتياجاتها كافة الإمكانيات الفنية التي تتيح لتلك الجهات ممارسة اختصاصاتها وفقا للقانون. رابعاً: يلتزم مقدمو خدمات تقنية المعلومات ووكلائهم وموزعيهم التابعون لهم المنوط بهم تسويق تلك الخدمات بالحصول علي بيانات المستخدمين، ويحظر على غيرهم القيام بذلك".

1 حدة بوخالفة، النظام القانوني لمتعهد الإيواء عبر الانترنت، مجلة المفكر، كليـة الحقوق والعلوم السياسية بجامعة محمد خيضر ببسكرة، الجزائر، 2017/01/19، ص 296.

ويعرف مزود خدمة الاتصالات الإلكترونية (Electronic Communication Service ECS) بأنه من يقوم بتسهيل إرسال واستقبال الاتصالات السلكية والإلكترونية، فهو بمثابة ناقل فقط، فعمله فني بحث، هذا ما أكده القانون والقضاء الأمريكي في القضية الشهيرة المرفوعـــة من Religious technology ضـد شركة Net com، حيث أوضح القضاء أن متعهد الوصول لا علاقة له بالمحتوى؛ "يكون مقدم خدمة الدخول للانترنت مسؤول عن محتوى الصفحات وموزعات المعطيات التي يستخرجها أو يأويها، إذا ساهم في تقديم المعلومات عبر الانترنت، ولم يقتصر دوره على الأداء الفـني للخدمة فقط". **انظر في ذلك:** أكسوم عيلام رشيـدة، المركز القانوني للمستهلك الإلكتروني، أطروحة لنيل درجة الدكتوراه الطور الثالث (ل.م.د) في القانون تخصص: قانون خاص داخلي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة مولود معمري بتيزي وزو، الجزائر، 12 جوان 2018، ص 71، **نقلاً عـن:** الجمال سمير حامد عبد العزيز، التعاقد عبر تقنيات الاتصال الحديثة –دراسة مقارنة–، الطبعة الثانيـة، دار النهضة العربية، القاهرة، 2005، ص 300.

2 DIRECTIVE 2000/31/EC, op.cit, Article 15: « … Recipients of the service upon their request, on condition that: (e) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.… ».

الأساسية لخدمة الاتصالات والمعلومات (TDG أو Tele Dienst Gesetz) أنه:"لا يعد مزود الخدمة مسؤولاً عن المحتوى غير المشروع، إلا إذا كان عالما بعدم مشروعية ذلك المحتوى وكان يستطيع من الناحية الفنية تجنب الوصول إليه أو كان من العدل أن يطلب منه ذلك"[1].

يعد الإلتزام بالتصرف اتجاه المحتوى غير المشروع من أهم الالتزامـات التي تقع على عاتـق مـزود خـدمات الإنترنت، ففي 08 ديسمبر 1999 حددت محكمة بداية (نانتير)، في حكم لها مضمون الالتزامات التي تقع على عاتـق متعهدي الإيواء، وحصرتـها في ثلاثة التزامات؛ أولها الالتزام بالإعـلام، وثانيها الالتزام باليقظة، وثالثها الالتزام بوقف بث المضمون المعلوماتي غير المشروع، أو على حـد تعبيرها، وجوب اتخـاذ موقـف إيجـابي[2].

إن العلم بالمحتوى غير المشروع شرط أساسي حتى تقوم مسؤولية مزود الخدمة، لاسيما إذا لم تكن عدم المشروعية ظاهرة بما يكفي[3]، فحسب القسم 512 (ج) من قانون حقوق المؤلف للألفية الرقمية (DMCA)، فإن مسؤولية مزودي خدمة الإستضافة تقوم عن إنتهاك المواد الموجودة على مواقع الويب خاصتهم أو مستودعات المعلومات الأخرى على أنظمتهم، ولا يمكنهم التنصل من المسؤولية إلا إذا اثبتوا استيفاء الشروط التالية:

- يجب ألا يكون لدى المزود معرفة فعلية بالانتهاك، أو ليس على دراية بالوقائع أو الظروف التي يكون النشاط المخالف أو غير المشروع فيها ظاهرًا،
- كما عليهم أو عليه أن يثبت عدم القدرة على التحكم في النشاط المخالف،
- ويجب ألا يتلقى المزود منفعة مالية مرتبطة وبشكل مباشر بالنشاط المخالف،

---

1 عبد الفتاح محمود كيلاني، مدى المسئولية القانونية لمقدمي خدمة الانترنت، المرجع السابق، ص 480، **عـــن**: شريف محمـد غانم، التنظيم القانوني للإعلانات التجارية عبر شبكة الانترنت، دار الجامعة الجديدة، الإسكندرية، 2008، ص 102.

2 TGI de Nanterre, 1re ch., sect. A, 8 décembre 1999, Comm. Com. Électr., mars 2000, p. 29, note A. LEPAGE, disponible également à l´adresse: www.droit-technologie.org, rubrique jurisprudence, Th. VERBIEST et É. WÉRY, Le droit de l´internet et de la société d´information, précité, n° 411, p. 225.

أحمد قاسم فرح، النظام القانوني لمقدمي خدمات الانترنت –دراسة مقارنة–، مجلة المنارة للبحوث والدراسات، عمادة البحث العلمي، جامعة آل البيت، المملكة الأردنية الهاشمية، المجلد الثالث عشر (13)، العدد التاسع (09)، 2007، ص 334.

3 باسم السيد، المرجع السابق، ص 80؛ **نقلاً عن**:

- Maurizio De Arcangelis, *La responsabilité des « fournisseurs d'hébergement*, Etude de droit comparé entre la France et l'Italie, *http://www.droit-technologie.org*, Date de mise en ligne :7 novembre 2001, p :17.

– كما عليه وبوجه السرعة أن يمنع الوصول إلى المواد والمعلومات المخالفة حين تلقيه الإخطار المناسب بذلك الانتهاك المزعوم.

إضافة إلى ذلك، يجب أن يكون مقدم الخدمة قد قدم إلى مكتب حقوق الطبع والنشر طلبه بتعيين وكيل لاستلام الإخطارات الخاصة بالانتهاكات المبلغ عنها وفقاً للنموذج الذي يوفره مكتب حقوق الطبع والنشر على موقعه الإلكتروني. وأضافت المادة الرابعة 04 (أ/ت2) من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتيـة السوري حالة أخرى يكون فيها مقدم الخدمة غير مسؤول عن المحتوى غيـر المشـروع وهي؛ إذا حدث تغيير في المحتوى المخزن لديه، وكان ذلك التغيير لسبب خارج عن إرادته، كما في حالة اختراق منظوماته المعلوماتية أو قرصنتها[1]، بينما اقتصر المشرع المغربي في مسؤولية مقدمي الخدمات على مجال واحد هو حقوق المؤلف والحقوق المجاورة على الإنترنت وذلك في الباب الرابع المكرر، وحدد فيه الوظائف والمهام التي يتولى مقدمو الخدمات القيام بها من جهة، ونطاق مسؤولياتهم وحالات الإعفاء من هذه المسؤولية من جهة أخرى[2].

في حين نجد المشرع الجزائري قد تطرق للالتزامات المفروضة على مقدمي الخدمات من خلال الفصل الرابع من القانون رقم 09-04 الخاص بقواعد الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، في مواده: 10، و11، و12، ومواد أخرى من قوانين متفرقة[3]، إلا أنه لم يشر إلى الالتزام بالإعلام عن المحتوى غير المشروع في حالة علمه به، وهو أمر في غاية الأهمية

1 قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية السوري السالف الذكر: "لا يكون المضيف مسؤولاً عن حدوث تغيير في المحتوى المخزن لديه إذا كان ذلك لسبب خارج عن إرادته، كما في حالة اختراق منظوماته المعلوماتية أو قرصنتها".

2 الباب الرابع المكرر المعدل والمتمم بمقتضى القانون رقم 05-34 المؤرخ في 20 فبراير 2006.

3 تنص المادة 28 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر سنة 2010، المصادق عليها بالمرسوم الرئاسي رقم 14-252، السالفة الذكر على:"... ب) إلزام مزود الخدمة ضمن اختصاصه الفني بأن: – يجمع أو يسجل بواسطة الوسائل الفنية على إقليم الدولة الطرف، أو – يتعاون ويساعد السلطات المختصة في جمع وتسجيل معلومات تتبع المستخدمين بشكل فوري مع الاتصالات المعنية في إقليمها والتي تثبت بواسطة تقنية المعلومات..."؛ كما نصت المادة 43 من القانون رقم 18-07، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، السالف الذكر بأنه: "إذا أدت معالجة المعطيات ذات الطابع الشخصي في الشبكات الاتصالات الإلكترونية المفتوحة للجمهور إلى إتلافها أو ضياعها أو إفشائها أو الولوج غير المرخص إليها، يعلم مقدم الخدمات فورا السلطات الوطنية والشخص المعني، إذا أدى ذلك إلى المساس بحياته الخاصة، ما لم تقرر السلطة الوطنية أن الضمانات الضرورية لحماية المعطيات قد تم اتخاذها من قبل مقدم الخدمات. يجب على كل مقدم خدمات أن يمسك جرداً محينا حول الانتهاكات المتعلقة بالمعطيات ذات الطابع الشخصي والإجراءات التي اتخذها بشأنها".

لأن ذلك قد يساعد في كشف الجرائم الإلكترونية قبل وقوعها، وإن وقعت فيمكن حينها على الأقل الحد من انتشارها وتدارك ما قد تتسبب فيه من نتائج وخيمة، بينما تطرقت المادة السادسة (06) من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية السوري للإخبار عن الطابع غير المشروع للمحتوى على شبكة الإنترنت، والتي أجازت لأي متضـرر أن يُخبر مقدم الخدمة بذلك المحتوى وأن يطالبه بحذفه أو تعديله أو تصحيصه، على أن يتضمن البلاغ جميع المعلومات التي تسمح بالتعرف على المُبَلِّغ، وكذا وصف واضح لذلك المحتوى غير المشروع المطلوب اتخاذ الإجراء بشأنه[1].

وقد تكون المعلومات الموجودة عند مزودي الخدمات هي السبيل الوحيد للحصول على الأدلة الإلكترونيـة، ومع ذلك يمتنـع مزودي خدمات الإنترنت عن القيـام بالالتزامـات المفروضـة عليهـم؛ كتزويد السلطات المختصة بالمعلومات التي تَطلُبُها، لذلك فرض المشرع عقوبات جزائية وإدارية على كل ممتنع؛ والتي قد تصل للسجن في بعض الحالات[2]، ولعدم التحجج بكثرة

1 تنص المادة (06) من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية، السالف الذكر على أن: "الإخبار عن الطابع غير المشروع للمحتوى على الشبكة: يحق لأي متضرر إخبار مقدم خدمات التواصل على الشبكة أو مقدم خدمات الاستضافة على الشبكة بالطابع غير المشروع، كما يمكنه المطالبة بحذفه أو تعديله أو تصحيحه، على أن يتضمن البلاغ المعلومات التي تسمح بالتعرف على المبلغ؛ مثل اسمه وعنوانه ومحل إقامته ورقم هاتفه وطبيعة عمله، أو عنوانه ورقم هاتفه وسجله التجاري وطبيعة نشاطه في حالة الشخص المعنوي. ووصف المحتوى المفترض انه غير مشروع، ومكان وتاريخ نشره، والأسباب التي دعت إلى الاعتقاد بعدم مشروعيته، طلب الحذف أو التعديل أو التصحيح".

2 هناك عدة مواد قانونية تطرقت لهذه النقطة، منها على سبيل المثال: المادة 394 مكرر 08 من القانون رقم 16-02 الذي يعدل ويتمم قانون العقوبات، مرجع سابق على: "دون الإخلال بالعقوبات الإدارية المنصوص عليها في التشريع والتنظيم الساري المفعول، يعاقب بالحبس من سنة إلى ثلاث (3) سنوات وبغرامة من 2.000.000 دج إلى 10.000.000 دج، أو بإحدى هاتين العقوبتين فقط، مقدم خدمات "الإنترنت" بمفهوم المادة 2 من القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام الاتصال ومكافحتها، الذي لا يقوم رغم إعذاره من الهيئة الوطنية المنصوص عليها في القانون المذكور أو صدور أمر أو حكم قضائي يلزمه بذلك: أ- بالتدخل الفوري لسحب أو تخزين المحتويات التي يتيح الاطلاع عليها أو جعل الدخول إليها غير ممكن عندما تتضمن محتويات تشكل جرائم منصوص عليها قانونا، ب-بوضع ترتيبات تقنية تسمح بسحب أو تخزين المحتويات التي تتعلق بالجرائم المنصوص عليها في الفقرة (أ) من هذه المادة أو لجعل الدخول إليها غير ممكن"؛ وتنص المادة (11) القانون 09-04 السالف الذكر:"... تحدد مـدة حفـظ المعـطيات المذكورة في هذه المادة بسنة واحدة ابتداء من تاريخ التسجيل. دون الإخلال بالعقوبات الإدارية المترتبة على عدم احترام الالتزامات المنصوص عليها في هذه المادة، تقوم المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية، ويعاقب الشخص الطبيعي بالحبس من ستة (6) أشهر إلى خمس (5) سنوات وبغرامة من 50.000 دج إلى 500.000 دج. يعاقب الشخص المعنوي بالغرامة وفقا للقواعد المقررة في قانون العقوبات..."؛ والمادة 61 من القانون رقم 18-07، المتعلق

المعلومات وعدم القدرة على الاحتفاظ بها طويلاً حُددت القوانين لها مدة زمنية معينة تتراوح بين ثلاثة أشهر وسنة، ففي لبنان اصدر المدعي العام بتاريخ 07 جوان 2013 قراراً طلب فيه من موردي خدمة الإنترنت الاحتفاظ بسجل نشاطات مستخدمي الإنترنت لمدة عام واحد[1].

وهناك جزئية أخرى لم يُشِر إليها المشرع الجزائري رغم أهميتها، خاصة لما لها من تأثير على الحياة الخاصة للأفراد؛ وهي مصير البيانات والمعلومات المتعلقة بالاتصالات التي يجريها مختلف الأشخاص والتي يكون مزودي الخدمات قد احتفظوا بها بناءً على طلب من سلطة مختصة بغرض التحري والتحقيق حول جريمة من الجرائم الإلكترونية، بينما لم يُغفل المشرع الفرنسي هذه الجزئية إذ تناولها في المادة (32-3-1) من قانون البريـد والاتصالات الإلكترونيـة الفرنسـي، والذي يلزم من خلاله مزود الخدمات بإزالة البيانات التي يتم تخزينها تلقائياً وكذا المعلومات المذكورة في المادة السادسة (6) من القانون رقم 2004-575 المتضمن الثقة في الاقتصاد الرقمي، كما نصت ذات المادة على بعض الاستثناءات التي ترد على عملية محو تلك البيانات، ومنها الاحتفاظ بها لمدة عام بغرض إجراء التحقيق والكشف عن الجرائم الجنائية وملاحقة مرتكبيها، أو لأجل الفوترة[2].

بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، السالف الذكر؛ وكذلك المواد: 30، 31، 32، و33 على التوالي من القانون رقم 175 لسنـة 2018 الخاص بمكافحـة جرائم تقنيـة المعلومات، مرجع سابق.

1 محمد عبد الكريم حسين، المرجع السابق، ص.ص: 118-119. وهي المـدة التي تضمنتها المادة 11 من القانون 09-04، السالف الذكر، بينما حددتها الفقرة الثانية من المادة 2/23 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر سنة 2010، المصادق عليها بالمرسوم الرئاسي رقم 14-252، السالفة الذكر، بمدة أقصاها تسعين يوماً (90) قابلة للتجديد، ولم تحدد مواد الاتفاقية عدد حالات التجديد.

2 Article L32-3-1(Modifié par Loi n°2003-239 du 18 mars 2003 - art. 20 et Modifié par Loi n°2004-575 du 21 juin 2004 - art. 56 JORF 22 juin 2004, Transféré par Loi n°2004-669 du 9 juillet 2004 - art. 10 JORF 10 juillet 2004) du **Code des postes et des communications électroniques**: « I. - Les opérateurs de télécommunications, et notamment ceux mentionnés au 1° du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, sont tenus d'effacer ou de rendre anonyme toute donnée relative à une communication dès que celle-ci est achevée , sous réserve des dispositions des II, III et IV. II. - Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire d'informations, il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques. Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, détermine, dans les limites fixées par le IV, ces catégories de données et la durée de leur conservation, selon l'activité des opérateurs et la nature des communications ainsi que les modalités de compensation, le cas échéant, des surcoûts identifiables et spécifiques des prestations assurées à ce titre, à la demande de l'Etat, par les opérateurs. III. - Pour les besoins de la facturation et du paiement des prestations de télécommunications »

الباب الثانـــــي:
الآليات المؤسساتية لمكافحة الجريمة الإلكترونية

الباب الثاني:
الآليات المؤسساتية لمكافحة الجريمة الإلكترونية.

إن تنامي التوجه نحو التحول الرقمي، وتبني التكنولوجيات العالمية الحديثة عاد بالكثير من الفائدة على الدول وكذا شعوبها، ولكن في المقابل نشأ عنه شق إجرامي يسعى إلى خلق عالم رقمي يستنزف العديد من ايجابيات التكنولوجيا الحـديثة الخيـرة، وهو الأمر الذي دفع العديد من الدول والمنظمات والهيئات إلى رفع التحديات لمواكبة التطورات العالمية المتلاحقة، محاولةً اعتماد سياسات رامية إلى تطوير استراتيجيات عملها وجعلها تقدمية، وإعادة صياغة دورها من أجل توثيق أواصر التعاون والعمل المشترك فيما بينها، وتبادل الخبرات بما يساعدها على إيجاد آليات لمكافحة مختلف أنواع الجرائم الإلكترونية التي لم يسلم منها أي ميدان من ميادين الحياة.

فإلى جانب الآليات الإجرائية التي شملها الباب الأول من الدراسة، لا بد من تعزيز تلك الآليات بأخرى مؤسساتية وطنية، وإقليمية، ودولية فعالة تعمل كل منها في المحيط المخصص لها، مع إلزامية أن يكون بينها اتصال وتنسيق وتعاون للحصول على المعلومات التي تسمح بالقبض على مرتكبي الجرائم الإلكترونية وتسليمهم للمحاكمة؛ لأن التعاون المتبادل بين كل تلك الآليات المؤسساتية سيساعد على احترام الحدود الإقليمية، وكذا السيادة الدولية التي تعد الجريمة الإلكترونية أكثر الجرائم انتهاكً لها، فهي جريمة لا تشكل أمامها الحدود الإقليمية الجغرافية والسياسية أي عائق، بل قد ترتكب جرائم إلكترونية في مختلف أنحاء العالم في دقائق معدودة، كما أن وجود آليات مؤسساتية متخصصة في مكافحة الجريمة الإلكترونية، سيشكل وسيلـة ردعيـة مهمة في وجه الأفعال الإجرامية المرتكبة في المجتمـع المعلومـاتي، فإحساس المجرم الإلكتروني بأنه لن يكون في مأمن من الملاحقة أينما وجد يعد عاملاً لإدخال الخوف في قلوب أولئك المجرمين، الشيء الذي قد يقلل من ارتكاب الجرائم الإلكترونية ويساهم في الحد منها، هذا دون أن ننسى الدور الذي تلعبه الآليات المساعدة في الحد من الجريمة الإلكترونية والوقاية منها حتى قبل وقوعها.

لذلك نحاول في هذا الباب دراسة المكافحة المؤسساتية الوطنية للجريمة الإلكترونية (الفصل الأول)، على نحو يمكننا من دراسة الآليات المؤسساتية الخارجية لمكافحة الجريمة الإلكترونية (الفصل الثاني)، وذلك على النحو التالي:

الفصل الأول:
المكافحة المؤسساتية الوطنية للجريمة الإلكترونية

الفصل الأول:
المكافحة المؤسساتية الوطنية للجريمة الإلكترونية

لقد خصصت مختلف التشريعات الوطنية والدولية مؤسسات ومصالح ووحدات من أجل مكافحة الجريمة الإلكترونية، فعلى المستوى الوطني في الجزائر مثلاً نجد؛ الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والمصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمـديرية الأمن الوطني (SCLCTIC)، ومركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية التابع للدرك الوطني (CPLCIC/GN)، وكذا المعهد الوطني للأدلة الجنائية وعلم الإجرام التابع هو الآخر للدرك الوطني (INCC/GN)، كما قام المشرع الجزائري باستحداث منظومة لأمن الأنظمة المعلوماتية، حتى يتمكن من تحقيق الإستراتيجية الوطنية في أمن أنظمة المعلومات التي تفرضها عمليات حماية تلك الأنظمة، والتي أصبحت تشكل في معظم الأحيان الإستعمالات اليومية للتكنولوجيا المعلوماتية وشبكات الإنترنت.

ولأكثر تفاصيل حول ما سبق ذكره أعلاه، قسم هذا الفصل إلى أربع مباحث؛ تم التطرق فيها للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها (المبحث الأول)، ثم السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي (المبحث الثاني)، كما تم التطرق للمنظومة الوطنية لأمن الأنظمة المعلوماتية (المبحث الثالث)، وصولاً لوحدات الأمن الوطني المتخصصة في مكافحة الجريمة الإلكترونية (المبحث الرابع).

الـمبحث الأول:

الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها

في إطار الإصلاحات التي تنتهجها الجزائر مؤخراً ذات الطابع القانوني والأمني والسياسي، وإصلاح العدالة لتعزيز دولة القانون ولمكافحة الجريمة الإلكترونية، أصدرت عدة نصوص قانونية، والتي تم من خلالها إنشاء مصالح وهيئات، تضم مجموعة من الموارد البشرية والإمكانات المادية والتقنية التي تُسهل عملية البحث عن مرتكبي الجرائم الإلكترونية، وتمكن من القبض عليهم، وتسليمهم للجهات القضائية المختصة، الوطنية منها أو الدولية، ومن بينها: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

فبموجب المادة الثالثة عشرة (13) من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، نص المشرع الجزائري على إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[1]، والتي كانت محط أنظار العديد من وسائل الإعلام التي تحدثت عنها، ولكن بعدها اختفت أخبارها، حتى اعتقد الجميع أنها ستبقى حبراً على ورق كغيرها من الكيانات القانونية التي كان مصيرها البقاء حبيسة المواد والنصوص القانونية، إلا أنه وفي الثامن (08) من شهر أكتوبر سنة 2015 تم إصدار المرسوم الرئاسي رقم 15-261[2] والذي تم من خلاله تحديد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[3].

1 جاء في المادة 13 من القانون رقم 09-04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام الاتصال ومكافحتها، السالف الذكر أنه:"تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها. تحدد تشكيلتها وتنظيمها وكيفية سيرها عن طريق التنظيم".

2 المرسوم الرئاسي رقم 15-261، المؤرّخ في 24 ذي الحجة عام 1436، الموافق 8 أكتوبر سنة 2015، الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المنشور بالج.ر العدد 53 بتاريخ 08 أكتوبر 2015، ص 16 (الملغى).

3 بارة سمير، الدفاع الوطني والسياسات الوطنية للأمن السيبراني (Cyper Security) في الجزائر: الدور والتحديات، ورقة بحثية مقدمة في إطار أشغال الطبعة الثانية من الملتقى الدولي حول: سياسات الدفاع الوطني بين الالتزامات السيادية والتحديات الإقليمية، كلية الحقوق والعلوم السياسية ومخبر التحولات السياسية والاقتصادية والاجتماعية والقانونية في التجربة الجزائرية، جامعة قاصدي مرباح، ورقلة، يومي الاثنين والثلاثاء 30 و31 جانفي 2017، ص 437.

وعلى غير العادة قام المشرع الجزائري بعدها بأربع سنوات تقريباً بإصدار مرسوم رئاسي آخر تحت رقم 19-172 والخاص بتشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها، والذي يتكون من خمسٍ وعشرين (25) مادة، نصت المادة الرابعة والعشرين (24) منه على إلغاء المرسوم الرئاسي 15-261 الصادر سنة 2015 السالف الذكر[1]، ثم بعد حوالي (13) شهراً قام المشرع بإصدار مرسوم رئاسي تحت رقم 20-183، والمتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، متكون من (38) مادة، ألغت المادة (37) منه المرسوم الرئاسي رقم 19-172 السالف الذكر[2].

ولأكثر تفاصيل حول الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، تم تقسيم هذا المبحث إلى مطلبين، تم التطرق فيهما لتشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها (المطلب الأول)، ثم لمهامها (المطلب الثاني).

1 نصت المادة 24 من المرسوم الرئاسي رقم 19-172، الذي يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها، السالف الذكر، على: "تلغى جميع الأحكام المخالفة لهذا المرسوم لاسيما أحكام المرسوم الرئاسي رقم 15-261، المؤرّخ في 24 ذي الحجة عام 1436 الموافق 8 أكتوبر سنة 2015 الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها".

2 تنص المادة 37 من المرسوم الرئاسي رقم 20-183، المؤرخ في 21 ذي القعدة عام 1441 الموافق 13 يوليو سنة 2020، المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الصادر بالج.ر رقم 40 المؤرخة في 18 يوليو سنة 2020، أنه: "تُلغى جميع الأحكام المخالفة لهذا المرسوم، لاسيما أحكام المرسوم الرئاسي رقم 19-172 المؤرخ في 3 شوال عام 1440 الموافق 6 يونيو سنة 2019 الذي يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها".

المطلب الأول: تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

حسب المادة الأولى من المرسوم الرئاسي رقم 20-183، فإن هذا المرسوم جاء ليعيد تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، فمن خلاله يمكن معرفة تشكيلة هذه الهيئة وكذا طريقة وكيفية سيرها.

وبمقتضى المادة 02 و03 من ذات المرسوم، تعد الهيئة:"سلطة إدارية مستقلة تمتع بالشخصية المعنوية والاستقلالية المالية، توضع تحت سلطة رئيس الجمهورية"، "يحدد مقر الهيئة بمدينة الجزائ، ويمكن نقله إلى أي مكان آخر من التراب الوطني بموجب مرسوم رئاسي"، وبمقارنة هاتين المادتين بالمادتين الثانية والثالثة من المرسوم الرئاسي رقم 19-172 الملغى، والذي كان يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها، وكذا المرسوم الرئاسي 15-261 الذي سبقه، يتبين أن هناك تغيير جوهري يستوجب الوقوف عنده، فالمشرع الجزائري ومن خلال المادة الثانية من المرسوم الرئاسي رقم 19-172، جرد الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال من صفتين مهمتين كانتا موجودتين في المرسوم الذي سبقه؛ ألا وهما: الاستقلالية الإدارية والسلطة الإدارية التي تخضع لها الهيئة.

إذ تعد الاستقلالية الإدارية إحدى أهم الخصائص التي تميز السلطات الإدارية؛ ذلك أنها الصفة البارزة في تنميتها، كما أنها تمثل المحرك الرئيسي في أداء هذه السلطات لوظائفها. ويقصد بالاستقلالية تحرر السلطات من الخضوع لأية وصاية أو سلطة تسلسلية لجهة ما[1]، وهذا لا يتعارض مع تبعيتها للدولة، لأنها تعمل باسم الدولة ولحسابها، فهي من سلطات الدولة، في حين أبقى المشرع على تميز الهيئة بالشخصية المعنوية، واستقلالها المالي؛ لتتمكن من أداء وظائفها، ليعود

1 بن زيطة عبد الهادي، ضرورة إنشاء سلطة إدارية مستقلة كآلية للحماية القانونية للبيانات الشخصية في مواجهة استخدامات المعلوماتية، مجلة الحقيقة، جامعة أحمد دراية أدرار، العدد 39، سنة 2016، ص 64، **نقلاً عـــن**:
- René Chapus, *Droit administratif général*, Montchrestien, 9eme édition, France,1995,T1, p:190.

المشرع في سنة 2020 ويعيد صفة الاستقلالية للهيئة بموجب نص المادة الثانية (02) من المرسوم الرئاسي رقم 20-183 السالف الذكر[1].

والمسألة الثانية التي تثير التساؤل ما جاء في المادة الثانية من المرسوم الرئاسي رقم 19-172 الملغى، والتي كانت تخضع فيها الهيئة الوطنية لسلطة وزارة الدفاع الوطني، بعدما كانت خاضعة للوزير المكلف بالعدل في ظل المرسوم الرئاسي رقم 15-261 الملغى، فهذا التحول أرجعه بعضهم إلى أن وزارة الدفاع الوطني لها إمكانيات تقنية حديثة متطورة تمكنها من إدارة تلك الهيئة[2]، إلا أننا نعتقد أن الأوضاع التي كانت تمر بها بلادنا في تلك الفترة قد تكون إحدى الأسباب وراء هذا الأمر، على الرغم من أن إخضاع الهيئة لوزارة الدفاع الوطني، كان استناداً إلى القانون رقم 91-23، المتعلق بمساهمة الجيش الوطني الشعبي في مهام حماية الأمن العمومي خارج الحالات الاستثنائية[3]،

1 نصت أيضاً المادة الثانية (02) من المرسوم الرئاسي رقم 15-261، **الملغى** والذي كان يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، السالف الذكر، على استقلالية الهيئة بقولها: "الهيئة سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي، توضع لدى الوزير المكلف بالعدل." ويحدد مقر الهيئة بمدينة الجزائر".

2 بقلم: بهية.ب، جريدة الخبر، العدد 2462، ليوم الخميس 27 جوان 2019، ص 02، متاح على الموقع الإلكتروني الموالي: *https://elikaaonline.com/wp-content/uploads/2019/06/likaa-n-2462.pdf*؛ بقلم: آمال.ش.د، جريدة المغرب الأوسط، العدد 2737، ليوم الأربعاء 26 جوان 2019، ص 03، متاح على الموقع الإلكتروني الموالي: *https://elmaghrebelawsat.com/wp-content/uploads/2019/06/site-journel-14.pdf*.

3 تنص المادة الثالثة (03) من القانون رقم 91-23، المؤرخ في 29 جمادى الأولى عام 1412 الموافق 6 ديسمبر سنة 1991، المتعلق بمساهمة الجيش الوطني الشعبي في مهام حماية الأمن العمومي خارج الحالات الاستثنائية، المنشور في الج.ر.ج العدد 63، الصادرة بتاريخ 7 ديسمبر سنة 1991، ص 239، على: "يمكن تجنيد وحدات الجيش الوطني الشعبي وتشكيلاته في الحالات التالية: ...ب- عندما يكون حفظ الأمن العمومي وصيانته وإعادته خارج عن نطاق السلطات والمصالح المختصة عادة، ج- بسبب المخاطر الجسيمة أو توقعها التي قد يتعرض لها أمن الأشخاص والممتلكات، د- في حالة المساس المستمر بالحريات الجماعية أو الفردية"، وأضافت المادة الأولى من الأمر رقم 11-03، المؤرخ في 20 ربيع الأول عام 1432 الموافق 23 فبراير سنة 2011، والمتعلق بمساهمة الجيش الوطني الشعبي في مهام حماية الأمن العمومي خارج الحالات الاستثنائية، والذي يعدل ويتمم القانون رقم 91-23، المؤرخ في 29 جمادى الأولى عام 1412 الموافق 6 ديسمبر سنة 1991، المنشور في الج.ر العدد 12، الصادرة في 23 فبراير سنة 2011، إلى المادة الثانية من القانون رقم 91-23، المرجع السابق -مطة رابعة- لإمكانية استخدام وحدات الجيش الوطني الشعبي وتشكيلاته في مكافحة الإرهاب والتخريب، بقولها: "تعدل وتتمم أحكام المادة 2 من القانون رقم 91-23 المؤرخ في 29 جمادى الأولى عام 1412 الموافق 6 ديسمبر سنة 1991 والمذكور أعلاه، وتحرر كما يأتي: " المادة (2): دون المساس بأحكام المادتين 91 و93 من الدستور، يمكن استخدام وحدات الجيش الوطني الشعبي وتشكيلاته للاستجابة إلى المتطلبات الآتية: - ... (بدون تغيير)...، - مكافحة الإرهاب والتخريب...".

إلا أنه يعد سبباً غير كافٍ لإخضاع هيئة بهذه الأهمية لوزارة الدفاع بدل وزارة العدل التي لها دراية أكثر من غيرها بالجرائم وكذا القوانين الواجب تطبيقها.

ويبقى التساؤل مطروحاً بعد صدور المرسوم الرئاسي 20-183، السالف الذكر، حول سبب وضع الهيئة تحت سلطة رئيس الجمهورية بدل وزارة العدل، كما أن وجود ممثل واحد عن قطاع العدالة –الوزير المكلف بالعدالة- في مجلس التوجيه يعد عدد غير كافٍ في تسيير مثل هكذا هيئات، بل حبذا لو أن المشرع أضاف بعض الشروط التي يجب توفرها في ممثل وزارة العدل، كالتخصص في القضاء الجنائي، والمعرفة بالتقنية الحديثة، والكفاءة في مجال مكافحة الجريمة الإلكترونية.

وبالرجوع للمادة الثالثة (03) من المرسوم الرئاسي رقم 20-183 السالف الذكر، نجد المشرع حدد مقر الهيئة بمدينة الجزائر، وأضاف أنه يمكن نقل مقرها إلى أي مكان آخر من التراب الوطني بموجب مرسوم رئاسي، وهو الأمر الذي لم يكن منصوصاً عليه في المادة الثالثة (03) من المرسوم الرئاسي رقم 15-261 الملغى، بل كان مقرر إنشاء ملحقات جهوية وذلك بمقتضى المادة 11 من ذات المرسوم[1].

1 حسب المادة 11 من المرسوم الرئاسي رقم 15-261، السالف الذكر والملغى فإنه يتم تشكيل ملحقات جهوية يتم تشغيلها من طرف مديرية المراقبة والوقاية واليقظة الإلكترونية التي تكون تابعة لها، وعلى حسب المادة 08 من القرار الوزاري المشترك، المؤرخ في 28 ربيع الأول عام 1439، الموافق 17 ديسمبر سنة 2017، والذي يحدد التنظيم الداخلي لهياكل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الصادر في الج.ر.ج العدد 14، المؤرخة في 04 مارس سنة 2018: تتكون الملحقة الجهوية من أربعة مكاتب؛ مكتب الإدارة العامة، المراقبة الإلكترونية، مكتب المتابعة والتحليل، وأخيرا مكتب العمليات التقنية. ولقد كانت مديرية المراقبة والوقاية واليقظة الإلكترونيـة، مديرية مهمة جداً في تسيير الهيئة؛ لأنها تتكفل بالقيام بالعديد من المهام لضمان فعالية الهيئة نذكر منها على وجه الخصوص: القيام بتنفيذ عمليات المراقبة الوقائية للاتصالات الإلكترونية، من أجل الكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال- الجرائم الإلكترونية-، بناءً على رخصة مكتوبة تُمنح لها من طرف السلطة القضائية وتحت مراقبتها طبقا للتشريع الساري المفعول، إرسال المعلومات المحصل عليها من خلال المراقبة الوقائية إلى السلطات القضائية ومصالح الشرطة القضائية المختصة، كما تقوم بتزويد تلك السلطات والمصالح تلقائيا أو بناءً على طلبها بالمعلومات والمعطيات المتعلقة بالجرائم الإلكترونية، وكانت أيضاً تضع مركز العمليات التقنية والملحقات الجهوية قيد الخدمة وتسهر على حسن سيرها والحفاظ على الحالة الجيدة لمنشاتها وتجهيزاتها ووسائلها التقنية، وتنفذ توجيهات اللجنة المديرة، مع المحافظة في كل ذلك على قواعد السر في نشاطاتها، وعلى المستوى الدولي فإنها تنفذ طلبات المساعدة القضائية الأجنبية في مجال تدخل الهيئة وجمع المعطيات المفيدة في تحديد مكان تواجد مرتكبي الجرائم الإلكترونية والتعرف عليهم.

أما بالنسبة لتشكيلة الهيئة فحسب المرسوم الرئاسي رقم 20-183، السالف الذكر، فإنها تتكون من مجلس توجيه ومديرية عامة، يديرها مدير عام يتم تعيينه بموجب مرسوم رئاسي، وتنتهي مهامه بحسب الأشكال نفسها[1]. تضم المديرية العامة؛ مديرية للمراقبة الوقائية واليقظة الإلكترونية، ومديرية للإدارة والوسائل، ومصلحتين، مصلحة للدراسات والتلخيص، ومصلحة للتعاون واليقظة التكنولوجية[2]. يَضُم مجلس التوجيه مجموعة من الأعضاء، هم: الوزير المكلف بالعدل، الوزير المكلف بالداخلية، الوزير المكلف بالمواصلات السلكية واللاسلكية، المدير العام للأمن الداخلي، قائد الدرك الوطني، المدير العام للأمن الوطني، ممثل عن رئاسة الجمهورية، ممثل عن وزارة الدفاع الوطني[3].

بينما وحسب المادة 05 من المرسوم الرئاسي 19-172، الملغى، كان مجلس التوجيه يتكون من ممثلي أربع وزارات، وفي ظل المرسوم الرئاسي 15-261، الملغى،كانت تتكون اللجنة المديرة من وزراء وممثلي مصالح أخرى، وقاضيان من المحكمة العليا يعينهما المجلس الأعلى للقضاء، وهو الأمر الايجابي الذي كان يميز تشكيلتها الإدارية، إضافة إلى أن رئاسة تلك اللجنة كانت للوزير المكلف بالعدل.

كما نص المشرع من خلال المادة 13 من مرسـوم رئاسي رقم 20-183، السالف الذكر على أنه يتم تعيين مستخدمي الهيئة وفق التشريع والتنظيم المعمول به في هذا المجال، ليبقى مصير كل أولئك العمال الذين تم تعيينهم للعمل في الهيئة، طبقاً للإعلانات التي تم الإعلان عنها في هذا الصدد مجهولاً، هل يبقون في مناصبهم ؟ أم يسرحون ؟ أو يتم إدماجهم في إدارات أخرى؟

1 المادة 09 من المرسوم الرئاسي رقم 20-183، الذي يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، السالف الذكر.

2 المادة 11 من نفس المرسوم الرئاسي.

3 المادة 06 من نفس المرسوم الرئاسي.

المطلب الثانـــي: مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

بالنسبة لمهام الهيئة فقد نصت عليها في البداية المادة 14 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المشار إليه سابقاً كما يلي: "تتولى الهيئة الذكورة في المادة 13 أعلاه، خصوصاً المهام الآتية: أ- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ب- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيا الإعلام والإتصال، بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية، ج- تبادل المعلومات مع نظيراتها في الخارج قصد جمع المعلومات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم".

ونصت بعدها المادة الرابعة (04) من المرسوم الرئاسي 15-261 الملغى على المهام الموكلة للهيئة؛ بأنها المهام المنصوص عليها في المادة 14 من القانون 09-04، المشار إليه سابقاً، وأضافت مهام أخرى، تمارسها الهيئة تحت رقابة السلطة القضائية، وفي ظل احترام أحكام التشريع الساري المفعول، لاسيما قانون الإجراءات الجزائية والقانون 09-04. وفي سنة 2019 نص المشرع الجزائري على مهام الهيئة في المرسوم الرئاسي 19-172، الذي يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها، بمنح كل هيكل من هياكل الهيئة مهاماً خاصة به، فقد أوضحت المادة السادسة (06) من المرسوم المهام الموكلة لمجلس التوجيه، أما عن مهام المديرية العامة، فقد تضمن القسم الثاني من الفصل الثاني من المرسوم الرئاسي 19-172 تسع مواد؛ من المادة 09 إلى المادة 15، تمت الإشارة خلالها إلى المديرية العامة بفرعيها؛ المديرية التقنية ومديرية الإدارة والوسائل، والمهام الموكلة لكل منها.

وبالعودة للمرسوم الرئاسي رقم 20-183، والذي يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، نجد المشرع الجزائري قد نص في المادة الرابعة (04) من ذات المرسوم، على أن بعض المهام المنوطة بالهيئة هي ذاتها المنصوص عليها في المادة 14 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وهذه المهام هي كالآتي: "1-اقتراح عناصر الإستراتيجية الوطنية

للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، 2- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، 3- مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، لاسيما من خلال جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية، 4- ضمان المراقبة والوقاية للاتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة، 5- تجميع وتسجيل وحفظ المعطيات الرقمية للأنظمة المعلوماتية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية؛ 6- السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها، 7- تطوير التعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال، 8- المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيا الإعلام والاتصال، 9- المساهمة في تحيين المعايير القانونية في مجال اختصاصها"[1].

وأضافت المادة السابعة (07) من المرسوم 20-183، السالف الذكر المهام الموكلة لمجلس التوجيه والمتمثلة فيما يلي: أول تلك المهام مستمد من تسميته؛ فهو الموجه والمشرف والمراقب لعمل الهيئة، ومن مهامه أيضاً دراسة كل مسألة تخضع لمجال اختصاص الهيئة، خاصة ما تعلق بالشروط الواجب توفرها للقيام بالمراقبة الوقائية للاتصالات الإلكترونية، التي نصت عليها المادة الرابعة (04) من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، كما يقوم مجلس التوجيه أيضاً بالتداول حول الإستراتيجية الوطنية للوقاية من الجرائم الإلكترونية -الجرائم المتصلة بتكنولوجيا الإعلام والاتصال- ومكافحتها، والتباحث حول مسائل تطوير التعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم الإلكترونية، والقيام بتقييم دوري لحالة التهديد التي تسببها الجرائم الإلكترونية من أجل تحقيق الأهداف المنشودة من عمليات المراقبة، واقتراح كل نشاط من شأنه تسهيل البحث والتقييم المباشر في مجال الوقاية من الجرائم الإلكترونية، هذا إضافة إلى مهام إدارية كالموافقة على برنامج عمل الهيئة، ودراسة

1 المادة الرابعة (04) من المرسوم الرئاسي رقم 20-183، الذي يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، السالف الذكر.

التقرير السنوي لنشاطات هذه الأخيرة والمصادقة عليه، كما يبدي مجلس التوجيه رأيه ويقدم اقتراحات في كل ما له علاقة بمهام الهيئة، ويتولى دراسة مشروع ميزانيتها والموافقة عليه، ويقوم مجلس التوجيه أيضاً بإعداد نظامه الداخلي والمصادقة عليه، ويضبط المعايير القانونية في مجال اختصاصه.

وللقيام بالمهام الموكلة إليه فإن مجلس التوجيه يجتمع مرتين (02) في السنة في دورة عادية، بناءً على استدعاء من رئيسه، كما يمكنه أيضاً الاجتماع في دورة غير عادية بناءً على استدعاء من رئيسه أو بطلب من أحد أعضائه، أو من المدير العام للهيئة[1].

أما الشق الثاني من المهام التي تعنى بها الهيئة، فهي تلك التي تتولاها المديرية العامة، كسهرها على حسن سير الهيئة، وإعداد وتنفيذ برنامج عملها، وميزانيتها لعرضها على المجلس التوجيه للموافقة، كما تعمل المديرية على تنشيط ومتابعة ومراقبة أنشطة مكونات المديرية والتنسيق بين هياكلها، وتنشيط وتنسيق عمليات الوقاية من الجرائم الإلكترونية، والتحضير لاجتماعات مجلس التوجيه، وإعداد التقرير السنوي لأنشطة الهيئة، ومن أهم المهام الموكلة للمديرية العامة قيامها بتبادل المعلومات مع مثيلاتها في الخارج بغرض جمع كل المعطيات التي من شأنها التعرف على مرتكبي الجريمة الإلكترونية وتحديد مكان تواجدهم[2].

وحسب المادة 15 وما بعدها، فإن المديرية العامة تتولى مهام أخرى من خلال ما تضمه من مديريات ومصالح[3]، كمديرية المراقبة الوقائية واليقظة الإلكترونية، التي تكلف بمهمة المراقبة الوقائية للاتصالات الإلكترونية من أجل الوقاية من جرائم معينة؛ كالجرائم الموصوفة بالأفعال الإرهابية والتخريبية والاعتداء على أمـن الـدولة، كما أُوكلت لها مـهام أخرى منها: مساعدة السلطات

1 المادة 08 من المرسوم الرئاسي رقم 20-183، الذي يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، السالف الذكر.

2 Voir : BOUASRIA OmarMAR, *lutte contre les atteintes aux systèmes de traitements automatisés de données à la lumière de la loi 09/04*, les actes de la 14ème Conférence internationale sur la Cybercriminalité, Tripoli, Lebanon , 25 - 24 mars 2017, p 238.

3 جاء في المادة (11) من المرسوم الرئاسي رقم 20-183، الذي يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المرسوم نفسه، بأن المديرية العامة تضم: مديرية للمراقبة واليقظة الإلكترونية، مديرية للإدارة والوسائل، مصلحة للدراسات والتخليص، مصلحة للتعاون واليقظة التكنولوجية.

القضائية ومصالح الشرطة القضائية في حالة ما إذا طُلب منها ذلك،كما تقدم المساعدات في مجال الخبرات القضائية التي تتطلب أساليب تحرٍ خاصة لأجل مكافحة الجرائم الإلكترونية، وتعمل أيضاً على جمع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها وتتبعها بغرض استعمالها في الإجراءات القضائية، كما عليها أن تتحلى باليقظة الإلكترونية في مجال الجرائم الإلكترونية[1]. ولأجل كل ذلك تضع مديرية المراقبة الوقائية واليقظة الإلكترونية كل التجهيزات والوسائل والأجهزة التقنية الضرورية من أجل تنفيذ مهامها على مستوى المنشآت القاعدية للمتعاملين ومقدمي الخدمات، والذين هم ملزمون بحكم القانون على تقديم المساعدات الضرورية لها للقيام بتنفيذ مهامها على أحسن وجه[2]، إذ يمكن للهيئة أن تطلب من أي جهاز أو مؤسسة أو مصلحة كل وثيقة أو معلومة تراها ضرورية لإنجاز مهامها[3].

كما تقوم كل من؛ مديرية الإدارة والوسائل، ومصلحة الدراسات والتخليص، ومصلحة التعاون واليقظة التكنولوجية، بأداء مجموعة من المهام نصت عليها المواد: 18، و19، والمادة 20 على التوالي، فمن بين المهام الموكلة لمديرية الإدارة والوسائل اهتمامها بالجانب الإداري وتقديمها للمساعدات المادية، حيث تُكلف بتسيير الموارد البشرية والوسائل والمنشآت القاعدية، وصيانتها وصيـانة العتاد لأنها تُكلف بالإسناد التمويني والتقني الخاص بالهيئة، كما تقوم بإعداد احتياجات الهيئة حين دراستها للتقديرات الميزانية[4]، ومن أهم المهام الأخرى الموكلة لباقي المصالح، جمع ومراقبة الإجراءات المتعلقة بالطلبات القضائية، وإعداد محاضر للمراقبة الوقائية وفقاً للقواعد المنصوص عليها في قانون الإجراءات الجزائية؛ وهي مهمة موكلة لمصلحة الدراسات والتلخيص، ومهمة أخرى في غاية الأهمية تكلف بها مصلحة التعاون واليقظة التكنولوجية، وهي مسألة التعاون مع الشركاء لتنفيذ عمليات الوقاية من الجرائم الإلكترونية ومكافحتها.

1 المادة 15 من المرسوم الرئاسي رقم 20-183، الذي يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، السابق الذكر.

2 المادة 17 من نفس المرسوم الرئاسي رقم 20-183.

3 المادة 21 من نفس المرسوم الرئاسي.

4 المادة 18 من نفس المرسوم الرئاسي.

من خلال التطرق إلى كل تلك المهام الموكلة للهيئة، يتبين الدور المهم الذي يجب أن تلعبه هذه الأخيرة في إطار الوقاية من الجرائم الإلكترونية ومكافحتها وطنياً و/أو دولياً، فعلى المستوى الوطني أعطاها المشرع سلطة التداول حول الإستراتيجية الوطنية للوقاية من الجرائم الإلكترونية[1]، والتحديد والتقييم الدوري لحالة التهديد التي تشكلها تلك الجرائم، وكذا وضع الخطط والبرامج لتحقيق الأهداف المرجوة منها، وعلى رأسها تنشيط وتنسيق الوقاية من الجرائم الإلكترونية ومكافحتها، كما تعد الهيئة أداة فعالة في مراقبة الاتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والماسة بأمن الدولة، إذ تعد عمليات جمع المعلومات والتزويد بها، وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أهم الأشياء التي قد تساعد الشرطة القضائية، والسلطات القضائية في اتخاذ الإجراءات المناسبة من أجل الوقاية من الجرائم الإلكترونية ومكافحتها والقبض على مرتكبيها.

دون أن ننسى الدور المهم الذي ستلعبه الهيئة في تطوير التعاون مع نظيراتها بالدول الأخرى، إذ ستكون الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال همـزة وصل مهمــة جداً في تطوير تبادل المعلومات والتعاون الدولي[2]، خاصة عندما يتعلق الأمر بتنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية، وكذا التعاون مع المؤسسات والهيئات الوطنية المعنية بمكافحة الجرائم الإلكترونية، ومن الأمثلة على تلك المؤسسات والهيئات: المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات، التابع للجهاز القومي لتنظيم الاتصالات المصري[3]، والمركز الفرنسي

1 آمال بن صويلح، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام خطوة هامة نحو مكافحة الإرهاب الإلكتروني بالجزائر، ورقة بحثية مقدمة في إطار الملتقى الدولي حول "الإجرام السيبراني المفاهيم والتحديات"، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعريرج، يومي 11-12 أفريل 2017، ص 04.

2 Bouder Hadjira**,** *Les dispositifs légaux de lutte contre la cybercriminalité*, Bulletin d'information trimestriel, Centre de recherche sur l'information scientifique et technique– CERIST, Treizième numéro, Alger, Juin 2013, p 25.

3 تم تشكيل المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات بالجهاز القومي لتنظيم الاتصالات في أبريل عام 2009. يقدم المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات الدعم اللازم لحماية البنية التحتية القومية للمعلومات الهامة خاصة في قطاع تكنولوجيا المعلومات والاتصالات والقطاع المالي والاستعداد لطوارئ الحاسبات والشبكات ومراقبة الأمن السيبراني والاستجابة للحوادث والتنبؤ بالأخطار وإصدار تحذيرات مبكرة عن انتشار البرمجيات الخبيثة والهجمات واسعة النطاق التي تهدد البنية التحتية للاتصالات في جمهورية مصر العربية. معلومات من الموقع الإلكتروني الخاص بالمركز الوطني للاستعداد لطوارئ الحاسبات والشبكات متاحة عبر الموقع الإلكتروني التالي: *http://www.tra.gov.eg/ar/industry/eg-cert*

لمكافحة جرائم تكنولوجيا المعلومات والاتصالات (OCLCTIC)[1]، والذي يعد هو الآخر نقطة اتصال مهمة مع الخارج، وفي الولايات المتحدة الأمريكية نجدها هي الأخرى قد وَضعت عدداً كبيراً من الوحدات المتخصصة، والأجهزة الخاصة للبحث والتحري في الجريمة الإلكترونية، ومن بين تلك الوحدات نجد المكتب المركزي لمكافحة الجريمة المرتبطة بتكنولوجيا المعلومات والإتصالات، وكذلك قسم جرائم الحاسوب وجرائم حقوق الملكية الفكرية الذي تم إنشاؤه سنة 1991، ونجد أيضاً معهد أمن الحواسيب، ووحدة جرائم الإنترنت وهي وحدة مختصة في الجرائم المرتبطة بالتقنية العالية؛ والتي يترأسها مدير مساعد مكتب التحقيقات الفدرالية[2].

كما أبدت بعض الدول العربية جاهزيتها لإنشاء مراكز لمكافحة الجرائم الإلكترونية، مثلما هو الحال في الأردن التي أعلنت عن إنشاء مركز وطني للاستجابة لحوادث الكمبيوتر يَتْبع هذا المركز لمركز تكنولوجيا المعلومات الوطني الذي يعتبر مرجعية لأمـن وسلامة المعلومـات والشبكات في المملكة، وتتمثل المهمة الرئيسية للمركز في دعم البنية التحتية للاتصالات ونظم المعلومات والمحافظة عليها من تهديدات الجرائم الإلكترونية[3]، على الرغم من أن الأردن أنشأت قسم الجرائم المعلوماتية عام 2008 التابع لمديرية الأمن العام الأردني، والذي ثم تطويره ليصبح وحدة الجرائم

1 Décret n° 2000-405 du 15 mai 2000 **portant création d'un office central de lutte contre la criminalité liée aux technologies de l'information et de la communication** (JORF 16 mai 2000): « L'OCLCTIC est chargé : d'animer et coordonner la mise en œuvre opérationnelle de la lutte contre les auteurs d'infractions liées aux technologies de l'information et de la communication ;… . » ; Chilstein David , **Législation sur la cybercriminalité en France, Revue internationale de droit comparé, Vol. 62 N°2,2010. pp. 553-606, France, 2010, p 46/47 :** « L'office constitue, pour la France, le point de contact central dans les échanges internationaux. Il contribue au niveau national à l'animation et à la coordination des travaux préparatoires nécessaires et participe aux activités des organismes et enceintes internationaux. Sans préjudice de l'application des conventions internationales, il entretient les liaisons opérationnelles avec les services spécialisés des autres pays et avec les organismes internationaux en vue de rechercher toute information relative aux infractions ainsi qu'à l'identification et à la localisation de leurs auteurs ».

2 **أشار إلى ذلك:** عمر عبد العزيز موسى الدبور، آليات تفعيل الحماية والوقاية من الجرائم الإلكترونية (إنشاء ضبطية خاصة بالجرائم الإلكترونية)، المؤتمر الدولي الرابع عشر حول الجرائم الإلكترونية، طرابلس، 24-25 مارس 2017، ص 225، نبيلة هبة هروالة، الجوانب الإجرائية لجرائم الانترنت، دار الفكر الجامعي، مصر، 2008، ص 110؛ درار نسيمة، الأمن المعلوماتي وسبل مواجهته مخاطره في التعامل الإلكتروني – دراسة مقارنة–، رسالة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة ابوبكر بلقايد، تلمسان، الجزائر، السنة الجامعية 2015-2016، ص 299.

3 ثامر على النويران، الجرائم الإلكترونية وطرق الحد منها: تجربة الأردن، ورقة بحثية مقدمة في إطار أشغال المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية ICACC، كلية علوم الحاسب والمعلومات، جامعة الإمام محمد بن سعود الإسلامية، الرياض، المملكة العربية السعودية، نوفمبر 2015، ص.ص: 181-182.

الإلكترونية عام 2015. وفي البحرين تم إنشاء إدارة الجرائم الإلكترونية المختصة في متابعة كل القضايا والجرائم المتعلقة بالمعلوماتية والإنترنت[1].

بينما هنالك دول عربية لم تنص أصلاً على مثل هذه الهيئة، كالمشرع الكويتي، بل أوكل مهمة تلقي البلاغات عن الجرائم الإلكترونية إلى موظفين يتم تحديدهم بموجب قرار من الوزير المختص، يقومون بتحرير المخالفات، وإحالتها إلى النيابة العامة، وذلك وفقاً لما جاء في المادة 15 من القانون رقم 63 لسنة 2015 المتعلق بمكافحة جرائم تقنية المعلومات الكويتي[2]، وكذلك هو الأمر في المملكة العربية السعودية، حيث يتم التبليغ عن الجرائم الإلكترونية إلى هيئة الاتصالات السعودية أو المراكز الأمنية التابعة لوزارة الداخلية السعودية، وفي الإمارات العربية المتحدة أيضاً لا يوجد جهاز متخصص لمكافحة هذا النوع من الجرائم، وهو ما يستدعي من هذه الدول الإسراع لإنشاء أجهزة أمنية متخصصة لمكافحة هذا النوع من الجرائم[3].

ما يمكن استنتاجه من خلال دراستنا لهذه الهيئة أنها سلطة إدارية مهمة جداً في مكافحة الجريمة الإلكترونية، لذا فإنه جدير بالمشرع الإسراع في إدخالها حيز العمل وأن لا يتركها مجرد هيئة على ورق، كما أن إنشاء منصات أو مراكز إلكترونية لتلقي البلاغات والشكاوى المتعلقة بالجرائم الإلكترونية، يعد أمراً لابد منه، فالإبلاغ هو إعلام السلطات المتخصصة عن وقوع الجريمة سواء من الضحية أو من شخص آخر شاهدها أو علم بها، وبالنسبة للجريمة الإلكترونية فإنه يتم التبليغ عنها سواءً بالشكل التقليدي أو من خلال التبليغ الإلكتروني[4]، لذا فقد قامت بعض الدول بإنشاء مراكز وإدارات للقيام بهذه المهمة، كإدارة مكافحة الحاسبات وشبكات المعلومات[5] بوزارة

1 لورنس سعيد الحوامدة، المرجع السابق، ص 27.

2 المادة (15) من قانون مكافحة جرائم تقنية المعلومات رقم (63) لسنة 2015، السالف الذكر.

3 بوقرين عبد الحليم، المرجع السابق، ص 311؛ لورنس سعيد الحوامدة، المرجع السابق، ص 27.

4 حاحة عبد العالي، قلات سمية، المكافحة الإجرائية للجرائم الإلكترونية دراسة حالة الجزائر، مجلة المفكر، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، العدد السادس عشر (16)، ديسمبر 2017، ص 229.

5 تختص الإدارة بالمتابعة اليومية للشبكات العاملة لضبط الحالات الخارجة عن القانون، والإجراءات تتخذ فورا اتجاه المخالفين، حيث يتم تدمير المواقع إذا ثبت إضرارها بمصلحة الأمن القومي أو الآداب العامة، **انظر في ذلك:** تركي بن عبد الرحمن المويشير، المرجع السابق، ص 109.

الداخلية المصريـة، بالإضافة إلى مـراكز وأقسام الشـرطة المعنية بتلقي بلاغات وشكاوي جرائم الحاسبات وجــرائم الإنترنت في العديد من الدول العربية[1].

الجزائر وعلى الرغم من وجــود موقع الكتروني للإبــلاغ عن الجـرائم المختلفة[2]، ومنها الجريمة الإلكترونية، إلا أن ذلك يعد غير كافٍ نظراً لطبيعة هذه الجريمة، فإنشاء منصة أو موقع إلكتروني خاص بها يعد أمراً ضرورياً، لهذا أنشأت فرنسا موقعاً إلكترونياً يتم من خلاله الإبلاغ عن أي محتوى غير قانوني على شبكة الإنترنت، مثل المواد الإباحية المتعلقة بالأطفال، أو الخطاب الذي يحض على الكراهية، الاحتيال الإلكتروني، وذلك على البوابة الإلكترونية (PhAROS)[3]، خاصة في ظل التزايد المستمر لهذا النوع من الجرائم، وأن عملية الإبلاغ عنها بدأت تشهد تحسناً؛ وهو الشيء الذي سيساعد في مكافحتها، والقبض على مرتكبيها في الوقت المناسب[4].

1 محمد محمد الألفي، التعاون الدولي في مجال مكافحة المخدرات عبر الفضاء المعلوماتي، المركز القومي للدراسات القضائية، وزارة العدل المصرية، مصر، ص 32، ورقه بحثية متاحة على الموقع الإلكتروني الموالي: *http://www.jp.gov.eg/img/8d21d88e -ad6b-4139-bdb8-fee981af466c.pdf* ، والذي تم الاطلاع عليه يوم: 2018/06/04.

2 تم معالجة 1843 قضية من طرف وحدات الدرك الوطني على مستوى 48 ولاية، بما فيها 722 شكوى مسبقة و1121 معلومة، أي ما يعادل 307 قضية شهريا، ومنها طبعا جرائم إلكترونية: موقع الإلكتروني للشكاوي المسبقة والاستعلام عن بعد *https:\\ppgn.mdn.dz*، والموجود على الموقع الإلكتروني للدرك الوطني: *http://www.mdn.dz/site_cgn/index*

3 متاحة عبر الموقع الإلكتروني التالي: *www.internet-signalement.gouv.fr*

4 Stéfan Lollivier et Christophe Soullez, *La criminalité en France (L'activité des offices centraux de police judiciaire de la police et de la gendarmerie nationales)*, Rapport annuel 2015 de l'ONDRP, France, octobre 2015, p 35 : En 2014, la plate-forme a reçu 137456 signalements (contre 123987 en 2013).

المبحث الثاني:
السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي.

تعزيزاً للمنظومة الحقوقية[1]، وتكريساً لمبدأ حماية حقوق الإنسان وحافظاً على الحياة الخاصة والكرامة الإنسانية، وتجسيداً للمبادئ الدستورية مثلما جاء في المادة 47 من التعديل الدستوري الجزائري سنة 2020[2]، ومكافحةً للجريمة الإلكترونية، خاصة منها تلك التي تمس المعطيات ذات الطابع الشخصي[3]، ولأجل إعطاء حماية أكثر لتلك المعطيات من الاعتداءات التي قد تقع عليها، قام المشرع الجزائري بإصدار قانون في العاشر (10) من شهر جوان سنة 2018[4]، تضمن 76 مادة بها قواعد قانونية تتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي[5]، كما قام بموجب ذات القانون بإنشاء سلطة وطنية لحماية هذه المعطيات[6].

ولتفصيل ذلك سنتطرق لنشأة وتشكيلة السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي (المطلب الأول)، ولمهام السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي (المطلب الثاني)، وصولاً لحماية البيانات الشخصية في التشريع الجزائري والمقارن (المطلب الثالث).

---

1 أكد الجميع أن مشروع هذا القانون سيعزز المنظومة الحقوقية أكثر وسيشكل نقلة نوعية تقضي على الفوضى في الحصول على البيانات الشخصية للمواطنين، من الموقع الرسمي للمجلس الشعبي الوطني: *http://www.apn.dz/ar/plus-ar/actualite-ar/* ، تاريخ الإطلاع: 2018/02/15.

2 جاء في الفقرة الرابعة من المادة 47 من تعديل الدستور الجزائري لسنة 2020 أن: "حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي. ... ".

3 مريم لوكال، الحماية القانونية الدولية والوطنية ذات الطابع الشخصي في الفضاء الرقمي: في ضوء قانون حماية المعطيات رقم 18-07، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمة لخضر بالواد، الجزائر، المجلد العاشر (10)، العدد الأول (01)، افريل 2019، ص.ص: 1313-1314.

4 القانون رقم 18-07، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، السالف الذكر.

5 جاء في الفقرة الأولى من المادة الثالثة (01/03) من القانون رقم 18-07، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، أن: "المعطيات ذات الطابع الشخصي:كل معلومة بغض النظر عن دعامتها متعلقة بشخص معرف أو قابل للتعرف عليه والمشار إليه أدناه، "الشخص المعني" بصفة مباشرة أو غير مباشرة، لاسيما بالرجوع إلى رقم التعريف أو عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية".

6 الفقرة 18 من المادة الثالثة (03) من القانون رقم 18-07 نفسه، والتي تنص: "السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي المنصوص عليها في هذا القانون".

المطلب الأول: نشأة وتشكيلة السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي.

بمقتضى القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، تم إنشاء سلطة وطنية لحماية المعطيات ذات الطابع الشخصي لدى رئيس الجمهورية، مقرها بالجزائر العاصمة، تتمتع بالشخصية المعنوية والاستقلال المالي والإداري[1].

وحسب المادة 23 من ذات القانون فإن السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي تتشكل من ثلاث (3) شخصيات من بينهم الرئيس، يتم اختيارهم من قبل رئيس الجمهورية من ذوي الاختصاص في مجال عمل السلطة الوطنية، وتضم أيضاً ثلاثة (3) قضاة يتم اقتراحهم من قبل المجلس الأعلى للقضاء من بين قضاة المحكمة العليا ومجلس الدولة، وعضو من كل غرفة من غرفتي البرلمان يتم اختيار كل منهما من قبل رئيس كل غرفة بعد التشاور مع رؤساء المجموعات البرلمانية، وكذا ممثل (01) عن المجلس الوطني لحقوق الإنسان، وممثل (01) عن وزير الدفاع الوطني، وممثل (01) عن وزير الشؤون الخارجية، وممثل (01) عن الوزير المكلف بالداخلية، وممثل (01) عن وزير العدل حافظ الأختام، وممثل (01) عن الوزير المكلف بالبريد والمواصلات السلكية وللاسلكية والتكنولوجيات والرقمنة، وعضوين آخريين عن كل من الوزير المكلف بالصحة، ووزير العمل والتشغيل والضمان الاجتماعي[2].

ويتم اختيار أعضاء السلطة الوطنية بناءً على كفاءتهم في الميادين القانونية والتقنية في مجال المعطيات ذات الطابع الشخصي، كما يمكنها –السلطة الوطنية– الإستعانة بأي شخص مؤهل، من شأنه مساعدتها في أشغالها. ويتم تعيين رئيس وأعضاء السلطة الوطنية بموجب مرسوم رئاسي لعهدة قابلة للتجديد، وهنا لم يحدد المشرع عدد مرات التجديد إن كانت مرة واحدة أو عدة مرات، ذلك أن اكتساب الخبرة يعد عاملاً مُهماً في التسيير الجيد لهذه السلطة، تلك الخبرة التي قد يكتسبها العضو من خلال ممارسته لمهامه داخل السلطة الوطنية، خاصة بالنسبة للقضاة، وهناك نقطة أخرى لابد من الإشارة إليها وهي مسألة اختيار عضوين من البرلمان اللَّذَيْنِ يتم

1 المادة (22) من القانون رقم 18-07، السالف الذكر.

2 حزام فتيحة، الضمانات القانونية لمعالجة المعطيات ذات الطابع الشخصي دراسة على ضوء القانون رقم 18-07، مجلة الاجتهاد للدراسات القانونية والاقتصادية، كلية الحقوق والعلوم السياسية، المركز جامعي تمنراست، الجزائر، المجلد الثامن (08)، العدد الرابع (04)، 2019، ص 293.

اختيارهما من قبل رئيسي غرفتي البرلمان، بعد التشاور مع رؤساء المجموعات البرلمانية، والإشكال هنا يكمن في كيفية حساب عهدة الخمس سنوات، خاصة إذا تم تعيينهما في منتصف العهدة فهل يكملان عهدة الخمس (05) سنوات في حالة حل البرلمان أو في حالة انتهاء عُهدتيهما البرلمانية؟ أم يتم استبدالهما؟ خاصة وأن رئيس السلطة الوطنية وأعضائها ملزمون بالحفاظ على الطابع السري للمعطيات ذات الطابع الشخصي والمعلومات التي اطلعوا عليها بهذه الصفة ولو بعد انتهاء مهامهم، وفي المقابل يحظون بحماية الدولة ضد أي تهديدات أو إهانات أو اعتداءات من أي طبيعة كانت بمناسبة أو أثناء تأدية مهامهم[1]، طبعاً ما لم يوجد نص قانوني يقضي بخلاف ذلك[2].

المطلب الثاني: مهام السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي.

أوكل المشرع الجزائري للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي عدة مهام مهمة، خاصة وأنها ستلعب دوراً كبيراً في حماية المعطيات ذات الطابع الشخصي، هذه المعطيات التي تعد بمثابة جزء لا يتجزأ من الحياة الخاصة للأفراد، والتي لا يجوز الاعتداء عليها، لذا تسهر السلطة الوطنية على مطابقة معالجة المعطيات ذات الطابع الشخصي لأحكام القانون 18-07، وضمان عدم انطواء استعمال تكنولوجيات الإعلام والاتصال على أي خطر تجاه حقوق الأشخاص والحريات العامة والحياة الخاصة[3]، خاصة وأن الجريمة الإلكترونية أصبحت تهدد الحياة الخاصة للأفراد بشكل خاص، إذ يستعمل الهاكرز تلك المعطيات الشخصية في ارتكاب مختلف أنواع الجرائم الإلكترونية، ومن أجل ذلك فإنها –السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي– تقوم بـ:

1 العيداني محمد، يوسف زروق، حماية المعطيات الشخصية في الجزائر على ضوء القانون رقم 18-07 (المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي)، مجلة معالم للدراسات القانونية والسياسية، المركز الجامعي علي كافي تندوف، الجزائر، العدد الخامس (05)، ديسمبر 2018، ص 123؛ طباش عزالدين، الحماية الجزائية للمعطيات الشخصية في التشريع الجزائري دراسة في ظل قانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، المجلة الأكاديمية للبحث القانوني، جامعة عبد الرحمان ميرة، بجاية، الجزائر، العدد الثاني (02)، ديسمبر 2018، ص 48.

2 المادة 26 من القانون رقم 18-07، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، السالف الذكر.

3 المادة 25 من نفس القانون.

1- تلقي التصريحات المتعلقة بمعالجة المعطيات ذات الطابع الشخصي[1]، وتمنح التراخيص[2] عند الاقتضاء، إذا تبين لها أن المعالجة المعتزم القيام بها تتضمن أخطارا ظاهرة على احترام وحماية الحياة الخاصة والحريات والحقوق الأساسية للأشخاص.

2- تقوم السلطة الوطنية بإعلام الأشخاص المعنيين والمسؤولين عن المعالجة بحقوقهم وواجباتهم، كما تقدم الاستشارات للأشخاص والكيانات التي تلجأ لمعالجة المعطيات ذات الطابع الشخصي أو التي تقوم بتجارب أو خبرات من طبيعتها أن تؤدي إلى مثل هذه المعالجة[3].

3- تلقي الاحتجاجات والطعون والشكاوي بخصوص تنفيذ معالجة المعطيات ذات الطابع الشخصي وإعلام أصحابها بمآلها.

4- الترخيص بنقل المعطيات ذات الطابع الشخصي نحو الخارج وفقاً للشروط المنصوص عليها في هذا القانون، خاصة المادتين 44 و45 منه[4].

5- الأمر بإجراء التغييرات اللازمة من أجل حماية المعطيات ذات الطابع الشخصي المعالجة، والأمر بإغلاق معطيات أو سحبها أو إتلافها، خاصة إذا كانت معالجة تلك المعطيات غير مطابقة للقانون 18-07.[5]

6- تقديم أي اقتراح من شأنه تبسيط وتحسين الإطار التشريعي والتنظيمي لمعالجة المعطيات ذات الطابع الشخصي.

---

1 المادة 17 من القانون رقم 18-07، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، السابق الذكر.

2 المادة 13 من نفس القانون.

3 الفقرة الثانية (02) والثالثة (3) من المادة 25 من نفس القانون.

4 تنص المادة 44 من القانون 18-07 القانون نفسه:"لا يجوز لمسؤول عن معالجة نقل المعطيات ذات طابع شخصي إلى دولة أجنبية إلا بترخيص للسلطة الوطنية وفقاً لأحكام هذا القانون، وإذا كانت هذه الدولة تضمن مستوى حماية كاف للحياة الخاصة والحريات والحقوق الأساسية للأشخاص إزاء المعالجة التي تخضع لهذه المعطيات أو التي قد تخضع لها. تقدر السلطة الوطنية المستوى الكافي من الحماية الذي تضمنه دولة معينة، لاسيما وفقاً للمقتضيات القانونية المعمول بها في هذه الدولة ولإجراءات الأمن المطبقة فيها، وللخصائص المتعلقة بالمعالجة مثل غاياتها ومدتها وكذا طبيعة وأصل ووجهة المعطيات المعالجة. وفي جميع الأحوال، يمنع إرسال وتحويل معطيات ذات الطابع الشخصي إلى دولة أجنبية عندما قد يؤدي ذلك إلى المساس بالأمن العمومي أو المصالح الحيوية للدولة". أما المادة 45 فقد تضمن استثناءات على أحكام المادة 44 التي سبقتها، كالموافقة الصريحة للشخص المعني، تنفيذاً لإجراء يتعلق بالتعاون القضائي الدولي.

5 المادة 35 من القانون رقم 18-07، المذكور سابقاً.

7- نشر التراخيص الممنوحة والآراء المدلى بها في السجل الوطني المشار إليه في المادة الثامنة والعشرين (28) من القانون 18-07.

8- تطوير علاقات التعاون مع السلطات الأجنبية المماثلة مع مراعاة المعاملة بالمثل[1].

9- إصدار عقوبات إدارية وفقاً لأحكام المادة 46 من القانون 18-07، والتي جاء فيها:"تتخذ السلطة الوطنية في حق المسؤول عن المعالجة في حال خرقه لأحكام هذا القانون، الإجراءات الإدارية الآتية:

- الإنذار، الإعذار، السحب المؤقت لمدة لا تتجاوز سنة، أو السحب النهائي لوصل التصريح أو الترخيص، الغرامة. تكون قرارات السلطة الوطنية قابلة للطعن أمام مجلس الدولة وفقا للتشريع الساري المفعول".

10- وضع معايير في مجال حماية المعطيات ذات الطابع الشخصي، ووضع قواعد السلوك والأخلاقيات التي تخضع لها معالجة المعطيات ذات الطابع الشخصي، وتعد تقريراً سنوياً حول نشاطاتها ترفعه إلى رئيس الجمهورية.كما تقوم السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي بإعلام النائب العام المختص فوراً، في حالة معاينة وقائع تحتمل الوصف الجزائي[2].

ولحسن سير السلطة الوطنية فقد زودت بأمانة تنفيذية، يسيرها أمين تنفيذي ويساعده في مهامه مستخدمون، وهم ملزمون بالحفاظ على سرية المعلومات التي يطلعون عليها أثناء أو بمناسبة ممارسة مهامهم[3]. كما سيتم إنشاء سجل وطني لحماية المعطيات ذات الطابع الشخصي، يمسك من طرف السلطة الوطنية، وتقيد فيه:

- الملفات التي تكون السلطة العمومية مسؤولة عن معالجتها، وكذا الملفات التي يكون الخواص مسؤولين عن معالجتها،
- مراجع القوانين أو النصوص التنظيمية المنشورة المتضمنة إحداث ملفات عمومية،
- التصريحات المقدمة للسلطة الوطنية والتراخيص التي تسلمها،

1 الفقرة العاشرة (10) من المادة 25 من القانون 18-07، السالف الذكر.

2 المادة 25 من نفس القانون.

3 المادة 27 من نفس القانون.

– المعطيات المتعلقة بالملفات الضرورية للسماح للأشخاص المعنيين بممارسة حقوقهم المنصوص عليها في القانون 18-07.

وتعفى من التقييد في السجل الوطني الملفات التي يكون الغرض الوحيد من معالجتها مسك سجل موجه بموجب مقتضيات تشريعية أو تنظيمية لاطلاع العموم، غير أنه تدرج بالسجل الوطني المذكور وجوباً هوية الشخص المسؤول عن المعالجة حتى يتمكن الأشخاص المعنيون من ممارسة الحقوق المنصوص عليها في القانون 18-07.[1]

المطلب الثالث: حماية البيانات الشخصية في التشريع الجزائري والمقارن.

أصبحت الخصوصية المعلوماتية، وبالذات حماية البيانات الشخصية محل اهتمام العديد من المنظمات الدولية[2]، والدول الغربية منها والعربية على حد سواء[3]، ومقارنة للتشريع الجزائري بالتشريعات الأخرى، نجد أنه تأخر كثيراً في إصدار القانون الخاص بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، لأن بعض الدول وخاصة العربية منها، وبالأخص الدول المجاورة، كتونس والمغرب، قد سبقته في ذلك، حيث أصدر المشرع التونسي القانون رقم 63 لسنة 2004، والمتعلق بحماية المعطيات الشخصية، وأحدث من خلاله الهيئة الوطنية لحماية المعطيات الشخصية بموجب الفصل 75 من الباب السادس من ذات القانون[4]، ولحسن سير هذه

1 المادة 28 من نفس القانون.

2 Catherine CHABERT, *Fiche pratique : RGPD (le règlement européen relatif a la protection des personnes physiques a l'égard du traitement des données a caractère personnel et a la libre circulation de ces données)*, Saint-Étienne Roanne, France, Rédigée en Avril 2017, Mise à jour en Juin 2018, p 01 : "Après plusieurs années d'attente, le Règlement européen relatif à la protection des données à caractère personnel a été adopté le 27 avril 2016 et est entré en vigueur le 25 mai 2018. Cette entrée en vigueur différée a permis aux organismes concernés de se mettre en conformité avec cette nouvelle réglementation. L'objectif consiste à « assurer un niveau cohérent et élevé de protection des personnes physiques et lever les obstacles aux flux de données au sein de l'Union Européenne ."

3 بن قارة مصطفى عائشة، الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية القانونية، مجلة الفقه والقانون (مجلة إلكترونية شهرية تعنى بنشر الدراسات الشـرعية والقانونية)، العدد الثاني والأربعون (42)، المملكة المغربية، ابريل 2016، ص ص 78 - 82.

4 قانون أساسي عدد 63 لسنة 2004، يتعلق بحماية المعطيات الشخصية، مؤرخ في 27 جويلية 2004، الصادر بالرائد الرسمي للجمهورية التونسية، بتاريخ 30 جويلية 2004، العدد 61، ص 2084، حيث جاء في الفصل 75 من الباب السادس من هذا القانون: "أُحدثت بموجب هذا القانون هيئة تسمى: "الهيئة الوطنية لحماية المعطيات الشخصية"، وتتمتع بالشخصية المعنوية والاستقلال المالي ويكون مقرها بتونس العاصمة. وتلحق ميزانية الهيئة بميزانية الوزارة المكلفة بحقوق الإنسان. وتضبط طرق سير الهيئة بمقتضى أمر".

الهيئة، صدر في سنة 2007 أمرين؛ الأول يتعلق بضبط طرق سير الهيئة الوطنية لحماية المعطيات الشخصية[1]، والثاني يتعلق بضبط شروط وإجراءات الترخيص لمعالجة المعطيات الشخصية[2].

أما في المملكة المغربية فقد صار المشرع المغربي مع التوجه التشريعي، الذي يهدف إلى تحقيق حماية فعلية للبيانات الشخصية التي يتم تبادلها إلكترونياً، فأُصدر القانون رقم: 09-08 المتعلق بالأشخاص الذاتيين اتجاه المعطيات ذات الطابع الشخصي[3]، والذي يهدف إلى حماية هؤلاء الأشخاص من الاطلاع على بياناتهم الاسمية والشخصية التي يدلون بها عبر الشبكة العنكبوتية[4]، وبذاتِ القانون تم إحداث اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي[5] بموجب المادة 27 من الفرع الأول من الباب الرابع منه، كما أحدث المشرع المغربي السجل الوطني لحماية المعطيات الشخصية وبين حدود إحداث أو استعمال سجلات مركزية أو ملفات بموجب المادة 45 من الباب السادس من ذات القانون، وفي شهر ماي من نفس السنة، أصدر مرسوماً لتطبيق القانون 09-08[6]، وفي السنة الموالية لإصدار القانون؛ أي في سنة 2010، تم تنصيب اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي[7]، والتي تتألف من سبعة

1 أمر عدد 3003 لسنة 2007، يتعلق بضبط طرق سير الهيئة الوطنية لحماية المعطيات الشخصية، مؤرخ في 27 نوفمبر 2007، الصادر بالرائد الرسمي للجمهورية التونسية، بتاريخ 30 نوفمبر 2007، العدد 96، ص 4214.

2 أمر عدد 3004 لسنة 2007، يتعلق بضبط شروط وإجراءات التصريح والترخيص لمعالجة المعطيات الشخصية، مؤرخ في 27 نوفمبر 2007، الصادر بالرائد الرسمي للجمهورية التونسية، بتاريخ 30 نوفمبر 2007، العدد 96، ص 4215.

3 القانون رقم 09-08، المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، الصادر بتنفيذه الظهير الشريف رقم 1.09.15، صادر في 22 من صفر 1430(18 فبراير 2009)، بالج.ر للمملكة المغربية، عدد 5711 بتاريخ 27 صفر 1430 (23 فبراير 2009)، ص 552.

4 خالد عثماني، مكافحة الجريمة الإلكترونية في ضوء التشريع المغربي، مجلة العلوم الجنائية، مطبعة الأمنية، العدد الأول، الرباط، 2014، ص 46؛ عبد المنعم ابقال، الإطار القانوني لمكافحة الجريمة الإلكترونية دراسة مقارنة، مجلة المنارة للدراسات القانونية والإدارية، عدد خاص، مركز المنارة للدراسات والأبحاث بالرباط، المغرب، 2017، ص 192.

5 Ali ElAZZOUZI, OP.CIT, p 129.

6 مرسوم رقم 2.09.165، لتطبيق القانون رقم 09-08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، صادر في 25 من جمادى الأولى 1430(21 ماي 2009)، بالج.ر للمملكة المغربية، عدد 5744 بتاريخ 24 جمادى الأخيرة 1430 (18 يونيو 2009)، ص 3571.

7 مقرر للوزير الأول رقم 3.62.10، بشان تنصيب اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي، صادر في 20 من رمضان 1431 (31 أغسطس 2010) ، بالج.ر للمملكة المغربية، عدد 5891 بتاريخ 08 ذو الحجة 1431 (15 نوفمبر 2010)، ص 5007.

أعضاء؛ رئيس يعينه الملك، وستة أعضاء يعينهم الملك كذلك لكن باقتراح من الوزير الأول ورئيس مجلس النواب ورئيس مجلس المستشارين، وتحدد مدة العضوية بخمس سنوات قابلة للتجديد مرة واحدة، أما شروط التعيين فيحددها مرسوم[1]. ولا ندري متى سيقوم المشرع الجزائري بتنصيب السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي؟ ومتى سيقوم بإصدار اللوائح التنظيمية الخاصة بالقانون 18-07[2] ؟

أما في التشريع المصري فلم تكن تحظَ الخصوصية والبيانات الشخصية قبل سنة 2020 بالعناية الكافية، حيث خلت البنية التشريعية من قانون خاص يحمي سرية البيانات الخاصة سواء للأفراد أو للشركات[3]، وإنما اكتفى المشرع المصري حينها بالإشارة إلى التزام الدولة بحماية الحياة الخاصة للإفراد من خلال المادة 57 من الدستور المصري لسنة 2014، ولكنه –أي المشرع المصري– تدارك هذا الأمر في سنة 2020، حيث أصدر القانون رقم 151 لسنة 2020[4].

وبالنسبة للدول الغربية فلقد كانت السباقة في إصدار مثل هكذا قوانين، حيث وضعت ألمانيا عدة قوانين لحماية الخصوصية المعلوماتية، وكان من بينها؛ قانون لحماية البيانات في سنة 2000 والذي كان يهدف إلى الانسجام مع القانون الأوربي بالأخص اتفاقية 1995.[5]

1 العربي جنان، المرجع السابق، ص 82.

2 القانون رقم 18-07، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، السالف الذكر.

3 عثمان بكر عثمان، المسئولية عن الاعتداء على البيانات الشخصية لمستخدمي شبكات التواصل الاجتماعي، كلية الحقوق، جامعة طنطا، القاهرة، 2016، ص 06، بحث متاح على الموقع الإلكتروني الموالي: http://*law.tanta.edu.eg/files/conf4/*، جلسة رابعة يوم ثاني/المسئولية عن الاعتداء على البيانات الشخصية، والذي تم الاطلاع عليه يوم: 2018/07/15.

4 القانون رقم 151 لسنة 2020، المتعلق بإصدار قانون حماية البيانات الشخصية، الصادر في الجريدة الرسمية المصرية، العدد 28 مكرر (هـ)، بتاريخ 15 يولية سنة 2020، جاء في الفقرة الأولى من المادة الأولى أن البيانات الشخصية هي: " أي بيانات متعلقة بشخص طبيعي محدد، أو يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بين هذه البيانات وأي بيانات أخرى كالاسم، أو الصوت، أو الصورة، أو رقم تعريفي، أو محدد للهوية عبر الإنترنت، أو أي بيانات تحدد الهوية النفسية، أو الصحية، أو الاقتصادية، أو الثقافية، أو الاجتماعية."

5 بن قارة مصطفى عائشة، الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية القانونية، المرجع السابق، ص 81.

وكذلك كان الحال بالنسبة لفرنسا، حيث أصـدرت سنة 1978 قانـوناً خاصاً بالمعلومات والحريات[1]، وبموجب المادة السادسة (06)[2]منه تم إنشاء "اللجنة الوطنية للمعلومات والحريات"[3]، كما تم تعديل القانون السابق عدة مرات، ومنها تعديل 20 جوان 2018[4]، وبموجبه تم تعديل مهام اللجنة الوطنية للمعلـومات والحريات[5]، بحـيث تتـماشى مـهامها مع اللائحة رقم 679/2016 الصـادرة عن (الاتحاد الأوروبي)، أو بالأحرى المجلس والبرلمان الأوروبي بشأن حماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية وحرية حركة هذه البيانات[6]، حيث تقوم اللجنة (CNIL) بإخطار السلطات العامـة والكيانات المهنية القائمة بمعالجة البيـانات الشخصية بواجبـاتها في هـذا الشـأن، كما تسمح للمواطنين بالـنفاذ المباشر إلى تلك الملفات، وتجري مراقبة الإلتزام بالقانون من خلال إعلانات فحص، ومن خلال زيارات إلى الشركات والكيانات التجارية سواء بصورة عشوائية أو أثناء التحقيق في شـكوى. كما منـحها المشـرع الفرنسي سـلطات عقابية تتمثل في الإنذارات والدعاوى القضائية والغرامات المالية، ويجوز لها أيضاً أن تحيل القضايا الشديدة الخطورة إلى مـكتب النائب العام[7]. ولتسهيل التـعامل مع اللجنة الوطنية للـمعلومات والحريات[8]، فقد وُضعت لها عدة مواقع الكترونية[1] زيـادة على موقـعها الرسمي[2].

1 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés .

2 Loi n° 78-17, Ibid, Art.06 : "La Commission Nationale de l'Informatique et des Libertés :Une commission nationale de l'Informatique et des libertés est instituée. Elle est chargée de veiller au respect des dispositions de la présente loi."

3 Pierre PEREZ, Jean DUCHAINE, *La Commission Nationale de l'Informatique et des Libertés Principes de la protection des données à caractère personnel*, École supérieure de l'éducation nationale, de l'enseignement supérieur et de la recherche (ESENESR), France, 2009 – actualisation : 2013, p 01 : P 03: La Commission Nationale de l'Informatique et des Libertés (CNIL) est une autorité administrative indépendante née de l'adoption de la loi précitée. La mission générale de la CNIL est, face aux dangers de l'informatique, de protéger la vie privée et les libertés individuelles ou publiques. Elle est chargée de veiller au respect de la loi Informatique et libertés.

4 LOI n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, Modifie Loi n° 78-17 du 6 janvier 1978 - art. 11 (V).

5 Article 11, Modifié par LOI n°2018-493 du 20 juin 2018 - art. 1 :" I. - La Commission nationale de l'informatique et des libertés est une autorité administrative indépendante. Elle est l'autorité de contrôle nationale au sens et pour l'application du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité...."

6 Kristiina Milt, La protection des données à caractère personnel, Fiches techniques sur l'Union européenne - 2018 , Strasbourg, France, 06/2018, p 04.

7 حسين محمد الغول، جرائم شبكة الانترنت والمسؤولية الجزائية الناشئة عنها (دراسة مقارنة في التشريع اللبناني والمصري والفرنسي والأمريكي)، الطبعة الأولى، مكتبة بدران الحقوقية، صيدا، لبنان، 2017، ص.ص: 560-561.

8 Société Financière de la Nef, RGPD - Notice d'information sur la Protection des Données Personnelles, France, Version du 05/06/2018, Sur le Site Souvent : *https://www.lanef.com/wp-content/uploads /2018 /06 /2018 _06_06_Notice-RGPD.pdf.*

لقد كان ولازال المشرع الجزائري في كثير من الأحيان يتتبع خطى المشرع الفرنسي في إصدار تشريعاته، إلا أنه هذه المرة تأخر كثيراً في ذلك، ولا نعلم إن كان إصداره لقانون حماية المعطيات ذات الطابع الشخصي جاء استجابة لاحتياجات مواطنيه، أم أنه جاء نتيجة الضغوطات الدولية في هذا المجال؟

إن الأوضاع التي مر بها العالم بسبب جائحة كورونا، ساهم وبشكل كبير على الاستعمال واسع النطاق لتقنيات المعلوماتية والوسائل الإلكترونية، فأصبح العمل يدار باجتماعات الفيديو عن بعد، وكذا التعليم، والتسوق يتم عبر الانترنت، وكثرة معه الإشاعات والأخبار حول هذه الجائحة، الأمر الذي سهل مهمة مجرمي المعلوماتية للحصول على مختلف أنواع البيانات، مما تسبب في حدوث انتهاكات كثيرة مست البيانات الشخصية خاصة منها الرقمية، وهو ما تداولته مختلف المواقع والهيئات والمركز على غرار ما أشار اليه، المركز الوطني للأمن الإلكتروني (NCSC) بالمملكة المتحدة، حيث بين أن مجرمو شبكات الإنترنت تمكنوا "من انتحال صفة موقع المركز الأمريكي لمكافحة الأمراض (CDC) بخلق نطاق إلكتروني بأسماء مماثلة للعنوان الإلكتروني للمركز وقرصنة كلمات المرور بالإضافة إلى قيامهم بطلب تبرعات "بيتكوين" لتمويل لقاح مزور."[3]

1 La Commission nationale de l'informatique et des libertés, 31e rapport d'activité 2010, Direction de l'information légale et administrative – Paris, 2011, P 16: L'année 2010 marque l'entrée de la CNIL sur les réseaux sociaux. Elle est présente sur Facebook, Twitter, Dailymotion et les réseaux professionnels Viadéo et LinkedIn.

2 الموقع الرسمي للجنة الوطنية للمعلومات والحريات الفرنسية: *https://www.cnil.fr/* .

3 مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC)، كوفيد-19: تحليل التهديدات الإلكترونية، برنامج مكافحة الجرائم الإلكترونية بالمكتب الإقليمي للشرق الأوسط وشمال إفريقيا، 01 مايو 2020، على الموقع الإلكتروني الموالي: *https://www.unodc.org/documents/middleeastandnorthafrica/2020/COVID19/COVID19_MENA_Cyber_Report_AR2.pdf*، تاريخ الاطلاع: 2021/02/07، ص 05.

المبحث الثالث:

المنظومة الوطنية لأمن الأنظمة المعلوماتية

أصبح السعي إلى تحقيق أمن المعلومات ضرورة ملحة، كونها تشكل ثروة حقيقية، تسعى جميع الأطراف، من دول ومؤسسات وشركات وأفراد وجميع المستفيدين من الخدمات الإلكترونية إلى حمايتها من كل ما يضر بها، وبالأخص من الهجمات الإلكترونية، وما قد تتسبب فيه الجرائم الإلكترونية بكل أشكالها[1].

واستجابة لمتطلبات العصر التكنولوجي التي أصبحت تفرض ضرورة حماية الأنظمة المعلوماتية، ووفاءً للعهود التي قطعتها الجزائر في هذا المجال[2] ، تم في العشرين (20) من شهر يناير من السنة الحالية 2020 إصدار مرسوم رئاسي تحت رقم 20-05، لوضع منظومة وطنية لأمن الأنظمة المعلوماتية موضوعة لدى وزارة الدفاع الوطني[3]، والتي تعد –المنظومة– أداة الدولة وإطارها التنظيمي ووسيلتها لإعداد إستراتيجيتها الوطنية في مجال أمن الأنظمة المعلوماتية، وتشتمل

1 الأمن المعلوماتي يعرف بأنه حماية المعلومات المختلفة والأدوات التي تتعامل معها وتعالجها كالأجهزة ووسائط التخزين من كل اعتداء كالسرقة، والتزوير، والتلف، والضياع، أو هو وسيلة حماية فنية تهدف للوقاية من الجرائم المعلوماتية والحد منها من إيجاد أنظمة وتقنيات فنية كفيلة بذلك. **انظر في ذلك:** ذيب بن عايض القحطاني، أمن المعلومات، إصدارات مدينة الملك عبد العزيز للعلوم والتقنية (KACST)، الرياض، المملكة العربية السعودية، 2015، ص.ص: 59-60؛ أحمد نوري دخيل، سعد عبد السلام طلحة، اختراقات أمن المعلومات وطرق تفاديها، المجلة الدولية المحكمة للعلوم الهندسية وتقنية المعلومات، جامعة مصراتة، ليبيا، المجلد الثاني (02)، العدد الثاني (02)، يونيو 2016، ص19؛ مانع سلمى، دور الأمن المعلوماتي في مكافحة الجرائم المعلوماتية، مداخلة في إطار أشغال الملتقى الوطني المتعلق بالجريمة المعلوماتية بين الوقاية والمكافحة، المنظم من قبل قسم الحقوق ومخبر الحقوق والحريات في الأنظمة المقارنة، بجامعة بسكرة يومي 16-17 نوفمبر2015، ص 09.

2 جاء في المادة (21) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر سنة 2010، المصادق عليها بالمرسوم الرئاسي رقم 14-252، السالفة الذكر، بأن:"تتعهد كل دولة طرف أن تتخذ ما يلزم من تدابير في إطار قانونها الداخلي، لتجريم ارتكاب أو المشاركة في ارتكاب الأفعال الآتية التي تقوم بها جماعة إجرامية منظمة في نطاق الاستعمال غير المشروع لتقنية أنظمة المعلومات: 1- الاختراق غير المشروع أو تسهيل الاختراق غير المشروع على نحو كلي أو جزئي لأحد نظم المعلومات. 2- تعطيل أو تحريف تشغيل احد نظم المعلومات. 3- إدخال بيانات بطرق غير مشروعة في احد نظم المعلومات أو مسح أو تعديل أو نسخ أو نشر البيانات التي يحتويها هذا النظام بطريق غير مشروع. 4- استراد، أو حيازة، أو اعتراض، أو ترك، أو إتاحة إحدى المعدات أو الأدوات أو برامج تقنية المعلومات، بدون سبب مشروع بهدف ارتكاب إحدى الجرائم المنصوص عليها في الفقرات الثلاث السابقة، 5- أي جريمة من الجرائم التقليدية ترتكب بإحدى وسائل تقنية أنظمة المعلومات".

3 مرسوم رئاسي رقم 20-05، المؤرخ في 24 جمادى الأول علم 1441 الموافق 20 جانفي سنة 2020، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، المنشور بالج.ر.ج العدد 04، بتاريخ 26 جانفي سنة 2020، ص 05.

المنظومة الوطنية لأمن الأنظمة المعلوماتية على مجلس وطني لأمن الأنظمة المعلوماتية، والذي يتكلف بإعداد الإستراتيجية الوطنية لأمن تلك الأنظمة والموافقة عليها وتوجيهها، ووكالة لأمن الأنظمة المعلوماتية تتكلف بتنسيق تنفيذ تلك الإستراتيجية[1]،كما تتكـفل هـذه المنظومة بإجراء تحقيقات في حالة حـدوث هجمات إلكترونية، بالإضافة إلى تقييم وجمع المعطيات، وتقديم المشورة للهيئات العمومية، بالإضافة إلى مهام أخرى متعلقة بالأمن الإلكتروني للمؤسسات العمومية.

ومن أجل معالجة أدق لهاته الهيئات، يتم التطرق للمجلس الوطني لأمن الأنظمة المعلوماتية (المطلب الأول)، ثم لوكالة أمن الأنظمة المعلوماتية (المطلب الثاني).

1 المواد الأولى والثانية والثالثة من المرسوم الرئاسي رقم 20-05، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، السالف الذكر.

المطلب الأول: المجلس الوطني لأمن الأنظمة المعلوماتية.

يعد المجلس الوطني لأمن الأنظمة المعلوماتية أحد العناصر المكونة للمنظومة الوطنية لأمن الأنظمة المعلوماتية يترأسه وزير الدفاع الوطني أو ممثله، ويتكون المجلس من: – ممثل عن رئاسة الجمهورية، – ممثل عن الوزير الأول، – الوزير المكلف بالشؤون الخارجية، – الوزير المكلف بالداخلية، – الوزير المكلف بالعدل، – الوزير المكلف بالمالية، – الوزير المكلف بالطاقة، – الوزير المكلـف بالاتصالات، – الوزير المكلف بالتعليم العالي.

يمـكن أن يستعين المجلس بأي شخص أو مؤسسة من شأنه تنويره في أعماله[1]، ولكي يقوم المجلس بأداء مهامه على أحسن وجه، فإنه يتوفر على أمانة تقنية يسيرها أمين عام توضع تحت سلطة رئيس المجلس، تقوم بعدة مهام منها: إعداد مشروع القواعد الداخلية المنظمة للمجلس، وجمع الوثائق والمعلومات اللازمة لتحضير أعماله من أي إدارة أو مؤسسة أو هيئة؛ وهي خاصية جد مهمة وخطيرة في نفس الوقت مُنحت للأمانة التقنية، لأنها ستتمكن من خلالها الاطلاع على معلومات قد تمس خصوصية وحرمة الحياة الخاصة، لذا يجب أن ترفق هذه المهمة بآليات لحماية تلك الحرمة وتكفل لها عدم الانتهاك باسم القانون. ومن مهام الأمانة التقنية أيضاً أنها تتولى تسيير الموارد البشرية والمادية وحفظ الوثائق والأرشيف، وتعمل كمنسق بين المجلس والوكالة[2].

يتولى المجلس الوطني لأمن الأنظمة المعلوماتية عدة مهام وضحتها المادة الرابعة (04) من المرسوم الرئاسي رقم 20-05 والمتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، وبداية تلك المهام قيامه بتحديد عناصر الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية المقترحة من قبل الوكالة والبث فيها، كما يقوم بدراسة التقارير المتعلقة بتنفيذ تلك الإستراتيجية والموافقة عليها، ومن مهامه أيضاً تقرير نشاط الوكالة ودراسة مخطط عملها والموافقة عليه، وللمجلس الوطني لأمن الأنظمة المعلوماتية دور مهم في الموافقة على اتفاقيات التعاون والاعتـراف المتـبادل مـع الهيئات الأجنبية في مجال أمن الأنظمة المعلوماتية، فالتعاون في هذا المجال لابد منه، نظراً للتطور المخيف الذي وصل وسيصل إليه الإجرام الإلكتروني.

1 المادة 05 من المرسوم الرئاسي رقم 20-05، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، السالف الذكر.
2 المواد 7، و8، و9 من نفس المرسوم الرئاسي.

ومن مهام المجلس كذلك صلاحية الموافقة على سياسة التصديق الإلكتروني التي تنجزها السلطة الوطنية للتصديق الإلكتروني[1]، والموافقة على تصنيف الأنظمة المعلوماتية، والتي يوجد منها أنواع كثيرة، منها على سبيل المثال؛ نظم المعلومات الإدارية، وهي الأنظمة المسؤولة عن تقديم المعلومات الضرورية للإدارة حتى تستطيع تحديد المشكل وحله، وهناك أيضاً أنظمة دعم القرار، والتي تسمح باتخاذ القرار المناسب لحل المشكل المطروح وخلق فرصٍ للإبتكار والتطوير، والحصول على نتائج أفضل[2]، فالمجلس الوطني لأمن الأنظمة المعلوماتية يمكنه أن يقترح ملاءمة الإطار الهيكلي أو التنظيمي الخاص بأمن تلك الأنظمة عند الحاجة، كما له أن يبدي رأيه في أي مشروع لنص تشريعي أو تنظيمي ذي صلة بأمن الأنظمة المعلوماتية.

المطلب الثاني: وكالة أمن الأنظمة المعلوماتيـــة.

وكالة أمن الأنظمة المعلوماتية هي مؤسسة عمومية ذات طابع إداري، تتمتع بالشخصية المعنوية والإستقلال المالي، مقرها في مدينة الجزائر، تتوفر الوكالة على مركز وطني عملياتي لأمن الأنظمة المعلوماتية ومديريات ومصالح تقنية وإدارية موضوعة تحت سلطة المدير العام الذي يسيرها، كما تدير الوكالة لجنة توجيه مزودة بلجنة علمية، وتتكون لجنة التوجيه من ممثلي عدة

1 عرفت الفقرة 15 من المادة الثانية (02) من القانون رقم 15-04، المؤرخ في 11 ربيع الثاني عام 1436 الموافق أول فبراير سنة 2015، الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، المنشور بالج.ر.ج عدد 6 مؤرخة في 10 فبراير 2015، الصفحة 6، سياسة التصديق الإلكتروني على أنها:"مجموع القواعد والإجراءات التنظيمية والتقنية المتعلقة بالتوقيع والتصديق الإلكترونيين". أما التوقيع الإلكتروني جاء بيانه في الفقرة الأولى من ذات المادة: "التوقيع الإلكتروني: بيانات في شكل إلكتروني، مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى، تستعمل كوسيلة توثيق". أما السلطة الوطنية للتصديق الإلكتروني، وحسب المادة 16 وما بعدها من ذات القانون، فهي سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي، تكلف بترقية استعمال التوقيع والتصديق الإلكترونيين وتطويرهما وضمان موثوقية استعمالهما، وحسب المادة 09 من المرسوم التنفيذي رقم 16-134، المـؤرخ في 17 رجب عام 1437 الموافق 25 أبريل 2016، الذي يحدد تنظيم المـصالح التقنية والإدارية للسلطة الوطنية للتصديق الإلكتروني وسيرها ومهامها، المـنشور بالج.ر عدد 26 مؤرخة في 28 أبريل 2016، الصـفحة 6، فـإنه من بين مصالح السلطة الوطنية للتصديق الإلكتروني، دائرة أمن البنى التحتية والتي تضم مصلحة الأمن المعلوماتي، التي من مهامها المشاركة في إعداد مشروع السياسة الأمنية للسلطة، والسهر على تنفيذ وتطبيق سياسة الأمن المعلوماتي لها، وإدارة تجهيزات وأنظمة الأمن التقنية والمادية، كما تضمن اليقظة المتعلقة بأمن الأنظمة والشبكات المعلوماتية.

2 حاول بعض الباحثين تصنيف نظم المعلومات في ضوء معايير محدد مثل تصنيفها في ضوء الدعم الذي تقدمه للمستوى الإداري أو في ضوء الأهداف الوظيفية والبنية التقنية لهذه النظم. **انظـــر**: عومار بوطبية، دراسة واقع نظم المعلومات بمديرية الشباب والرياضة لولاية قسنطينة، مذكرة مقدمة لنيل شهادة الماجستير في الإدارة والتسيير الرياضي، المركز الجامعي محمد الشريف مساعدية سوق أهراس، الجزائر، السـنة الجـامعية 2011-2012، ص 63.

وزارات ومصالح، وسلطات، وهيئات، كما يمكنها الاستعانة بأي شخص أو مؤسسة من شأنها أن تساعدها في أعمالها[1].

تكلف لجنة التوجيه بعدة مهام نصت عليها المادة 24 من المرسوم الرئاسي رقم 20-05 السالف الذكر، فبحسب هذه المادة تقوم لجنة التوجيه باقتراح عناصر الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية، ودراسة البرامج السنوية والمتعددة السنوات لتنفيذ تلك الإستراتيجية والمصادقة عليها، تقيم نتائج مجموع الأعمال التي قامت بها الوكالة، وتتداول في كل المسائل التي تتعلق بتنظيم وسير الوكالة، مثل حصائل الأنشطة، والتسيير المالي للسنة المالية المنصرمة والبيانات التقديرية للإيرادات والنفقات ومخطط توظيف وتكوين المستخدمين وكذا مرتبات مستخدمي الوكالة، وتُقدم لجنة التوجيه موافقتها على النظام الداخلي للوكالة، كما تقوم بتحديد وضبط الطرق والوسائل اللازمة لترقية البحث والتطوير في مجال أمن الأنظمة المعلوماتية، من أجل الاستجابة للحاجات الوطنية في هذا الخصوص.

يسهر المدير العام على تنفيذ المخططات والبرامج المسطرة من طرف لجنة التوجيه، ويمكنه أيضاً أن يستشير اللجنة العلمية في كل مسألة ذات طابع علمي، لأن اللجنة العلمية متكونة من عشرة (10) أعضاء من أساتذة وباحثين وخبراء في مجال أمن الأنظمة المعلوماتية[2]، فمن المهم أن يتم الاستعانة بأهل العلم والاختصاص والخبرة لرسم استراتيجية فعالة في وضع منظومة وطنية لحماية وأمن الأنظمة المعلوماتية، فهذه اللجنة يمكنها أن تبدي رأيها وأن تقدم توصياتها في عدة مسائل منها: كيفية تنفيذ برامج ومشاريع البحث والتطوير، ومدى تجانسها مع المقترحات المقدمة من المدير العام للوكالة، وتقوم باختيار واقتناء المراجع العلمية، وتنظم وتشارك في كل ما يتعلق بأمن

1 المادة 22 من المرسوم الرئاسي 20-05، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية السالف الذكر تنص: "تتكون لجنة التوجيه من ممثلي: – وزارة الدفاع الوطني، – الوزارة المكلفة بالشؤون الخارجية، – الوزارة المكلفة بالداخلية، – الوزارة المكلفة بالعدل، – الوزارة المكلفة بالمالية، – الوزارة المكلفة بالطاقة، – الوزارة المكلفة بالتعليم العالي، – الوزارة المكلفة بالصناعة، – الوزارة المكلفة بالاتصالات، – الوزارة المكلفة بالتجارة، – مصالح الأمن، – سلطة ضبط البريد والاتصالات الإلكترونية، – السلطة الوطنية للتصديق الإلكتروني،– الهيئة الوطنية لحماية البيانات ذات الطابع الشخصي، – السلطة الحكومية للتصديق الإلكتروني؛ وعلى سبيل الاستشارة ، المدير العام للوكالة. تتولى مصالح الوكالة لجنة التوجيه. يمكن أن تستعين لجنة التوجيه بأي شخص أو مؤسسة يمكنها تنويرها في أعمالها".

2 المادة 31 من المرسوم الرئاسي رقم 20-05، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، السالف الذكر.

الأنظمة المعلوماتية من أحداث وتظاهرات علمية، وكل المسائل ذات الطابع العلمي التي يَعرضها عليها المدير العام للوكالة، وتنشط عمليات التكوين العلمي والإتقان وإعادة التأهيل لفائدة مستخدمي الوكالة، وكذا المستخدمين في الإدارات والمؤسسات والهيئات العمومية المكلفين بأمن الأنظمة المعلوماتية، ويمكنها أيضاً الاستعانة بأي شخصية علمية أو خبير علمي له كـفاءة في مجال أمن الأنظمة المعلوماتية[1].

بالإضافة إلى كل تلك المهام التي تعنى بها لجنة التوجيه ولجنتـها العلمية، نصت المـادة 18 من المـرسوم 20-05 على مهـام كثيرة تكلف بها وكالة أمن الأنظمة المعلوماتية[2]، ومنها: تحضير عناصر الإستراتيجية الوطنية الخاصة بأمن الأنظمة المعلوماتية وعرضها وتنسيقها وتنفيذها مع المجلس، وأصبح للوكالة كمؤسسة عمومية دور في التدقيق في مجال أمن الأنظمة المعلوماتية، إذ بإمكانها تقديم اقتراح عن كيفيات اعتمـاد مزودي الخدمات لذلك التدقيق، خاصة وأنها هي من تقدم اعتماد إنشاء المنظومات المعلوماتية، والمنتجات ومقدمي الخدمات في مجال أمن الأنظمة المعلوماتية، لأن مقدمي الخدمات وكما رأينا من خلال هذه الدراسة لهم دور مهم في تسهيل

1 المادتين 32، و33 من نفس المرسوم الرئاسي.

2 المادة 18 من نفس المرسوم الرئاسي رقم 20-05 تنص: "...- تقديم المشورة والمساعدة للإدارات والمؤسسات والهيئات العمومية والخاصة من أجل وضع إستراتيجية أمن الأنظمة المعلوماتية، - ضمان اليقظة التكنولوجية في مجال أمن الأنظمة المعلوماتية، - مرافقة الإدارات والمؤسسات والهيئات، بالتشاور مع الهياكل المختصة في هذا المجال، في معالجة الحوادث المتصلة بأمن الأنظمة المعلوماتية، - رد الأنظمة المعلوماتية وعرضها على إلى المجلس للموافقـة على تصنيفها، - إعداد وتحيين خـارطة للأنـظمة المعلوماتية المصنفة، - اقتراح مشاريع نصـوص تشـريعية أو تنظيمية في مجال أمن الأنظمة المعلوماتية، بعد الرأي المطابق للمجلس، - إعداد وتحديث المرجعيات والإجراءات والأدلة العملية وتقديم توصيات في ميدان أمن الأنظمة المعلوماتية، - اعتماد منتجات أمن الأنظمة المعلوماتية والتصديق عليها، - اعتماد منظومات إنشاء وفحص الإمضاء الإلكتروني، - تحديد معايير وإجراءات منح علامة الجودة و/أو التصديق و/أو اعتماد المنتجات ومقدمي الخدمات في مجال أمن الأنظمة المعلوماتية، طبقا للتشريع والتنظيم المعمول بهما، - القيام بنشاطات التكوين والتوعية ذات الصلة بأمن الأنظمة المعلوماتية، - تقديم توجيهات تتعلق بتكوين أعوان المؤسسات العمومية في مجال أمن الأنظمة المعلوماتية، - اقتراح تدابير الترقية والبحث والتطوير في مجال أمن الأنظمة المعلوماتية، - تنشيط وتوجيه أنشطة البحث والتطوير في مجال أمن الأنظمة المعلوماتية، - اقتراح مشاريع اتفاقيات التعاون والاعتراف المتبادل مع الهيئات الدولية في مجال اختصاصها، - ابرام مشاريع شراكة في مجال أمن الأنظمة المعلوماتية بعد موافقة المجلس، - تعزيز ثقافة تأمين الأنظمة المعلوماتية، - إعداد تقارير دورية وحصيلة سنوية عن نشاطها، - إعداد وتحيين خارطة حالات هشاشة الأنظمة المعلوماتية على المستوى الوطني، - ضمان تبادل المعلومات مع الأمانة التقنية للجنة الوطنية لتصنيف النقاط الحساسة، - التنظيم والمشاركة في الأحداث والتظاهرات العلمية والتقنية المتعلقة بأمن الأنظمة المعلوماتية".

عملية الحصول على معلومات بخصوص الجرائم الإلكترونية الواقعة، وللتقليل من مخاطر تلك الجرائم، فالوكالة تعمد على فحص الإمضاء الإلكتروني، وتحدد معايير وإجراءات منح علامة الجودة و/أو التصديق، لأن القانون منحها الحق في إجراء تحقيقات رقمية في حالة حدوث هجمات أو جرائم إلكترونية تستهدف المؤسسات الوطنية، وألزمها بالسهر على جمع وتحليل وتقييم كل المعطيات واستخلاص المعلومات الملائمة، وإعداد وتحديث المرجعيات والإجراءات والأدلة العملية وتقديم التوصيات التي تسمح بتأمين منشآت المؤسسات الوطنية، وبناءً على كل تلك المعلومات التي تحصلت عليها بطُرقها الخاصة أو من خلال التعاون والتشاور مع الهياكل المختصة في هذا المجال، فالوكالة "مؤهلة لطلب أي وثيقة أو معلومة مفيدة للقيام بالمهام الموكلة لها بموجب هذا المرسوم، من الهيئات والمؤسسات والمتعاملين المزودين بنظام إعلام"[1].

وبذلك فإنه بإمكانها تقديم المشورة والمساعدة ومرافقة الإدارات والمؤسسات والهيئات العمومية والخاصة من أجل وضع إستراتيجية لأمن أنظمتها المعلوماتية، لتضمن بذل اليقظة التكنولوجية التي تساعدها على متابعة التطور التقني المرتبط بنشاط المؤسسات، كالطرق الجديدة للإنتاج، والإبداع والاختراع، والعمل على تطوير البحوث والتقنيات الجديدة؛ وبإمكان الوكالة اقتراح تدابير الترقية والبحث والتطوير والمشاركة في الأحداث والتظاهرات العلمية والتقنية المتعلقة بأمن الأنظمة المعلوماتية، والقيام بنشاطات التكوين والتوعية وتقديم توجيهات تتعلق بتكوين أعوان المؤسسات العمومية في نفس المجال، مستعينة في ذلك باليقظة القانونية التي تسمح لها بمتابعة القوانين الجديدة والنصوص التنظيمية، وكذا الاجتهادات القضائية، إذ بإمكانها اقتراح مشاريع اتفاقيات التعاون والاعتراف المتبادل مع الهيئات الدولية، واقتراح مشاريع نصوص تشريعية أو تنظيمية في مجال أمن الأنظمة المعلوماتية، بعد مطابقة رأيها برأي المجلس، كما يمكنها إبرام مشاريع شراكة لتعزيز ثقافة تأمين الأنظمة المعلوماتية وذلك بعد موافقة المجلس، فكل ذلك سيسمح لها بإعداد تقارير دورية وحصيلة سنوية عن نشاطها، وإعداد وتحيين خارطة حالات الخلل والنقص الموجود في الأنظمة المعلوماتية على المستوى الوطني.

ولتفادي المخاطر التي قد تتسبب فيها الجرائم الإلكترونية، ومواجهة لأولئك المجرمين قامت دول كثيرة بتأمين أنظمتها المعلوماتية من خلال الإطار التشريعي والإجرائي والعملياتي، فقد قام

1 المادة 19 من نفس المرسوم الرئاسي رقم 20-05.

المشرع المصري بإنشاء المجلس الأعلى للأمن السيبراني- مجلس أعلى للمجتمع الرقمي- والذي يختص بوضع منظومة متكاملة لبناء وإرساء قواعد إنشاء كيان قومي للمجتمع الرقمي ورسم السياسات والأولويات نفاذا لتلك المنظومة[1]، وحسب المادة الثالثة (03) من نفس القرار يمكن للمجلس أن يستعين بمن يرى لزوم الاستعانة بهم من الخبراء والأجهزة الأمنية، كما ألزم المشرع المصري كافة الجهات الحكومية بكافة مستوياتها وشركات قطاع الأعمال العام بتنفيذ قرارات وتوصيات المجلس الأعلى للأمن السيبراني، فيما يتعلق بتأمين البنية التحية الحرجة للاتصالات وتكنولوجيا المعلومات الخاصة بها، واتخاذ كافة الإجراءات الفنية والإدارية لمواجهة الأخطار والهجمات السيبرانية وتنفيذ الإستراتيجية الوطنية للأمن السيبراني[2].

أما بالنسبة لفرنسا فنجد أنها خصصت عدة جهات فاعلة في مكافحة الجريمة الإلكترونية منها: المديرية العامة للشرطة الوطنية (DGPN)، والمديرية العامة للدرك الوطني (DGGN)، والمديرية العامة للأمن الداخلي (DGSI)، ومحافظة الشرطة (PP)، ولكن بسبب التطور المثير للقلق الذي تعرفه الجرائم الإلكترونية، وكثرت هجمات الإلكترونية وسهولة إخفاء الهوية والانفتاح على شبكة الويب المظلمة (Dark Web) التي أصبحت سوق حقيقي للخدمات غير المشروعة عبر الإنترنت، مما سهل ارتكاب جرائم إلكترونية متنوعة، ونظراً لما قد ينجم عن تلك الجرائم من مخاطر وخسائر في كل مجالات الحياة، كان لابد من تأمين الأنظمة المعلوماتية بآليات تساعد في ذلك[3]، ومنها إنشاء الوكالة الوطنية لأمن الأنظمة المعلوماتية « Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) »، والتي تم إنشاؤها سنة 2009 بموجب المرسوم رقم 2009-834[4]، والذي نص في بعض مواده على المهام الموكلة للوكالة كتلك التي نصت عليها المادة الثالثة (03)[5]

1 المادة الثانية (02) من قرار رئيس مجلس الوزراء رقم 1453 لسنة 2015، بإنشاء مجلس أعلى للمجتمع الرقمي، الصادر في الج.ر.م العدد 24، بتاريخ 11 يونيو سنة 2015، ص 83.

2 المادة الأولى من: قرار رئيس مجلس الوزراء رقم 994 لسنة 2017، الصادر في الج.ر.م العدد 17 مكرر (ب)، بتاريخ 02 مايو سنة 2017، ص 02.

3 La cybersécurité, Revue de la Gendarmerie Nationale avec la collaboration du centre de recherche de l'École des officiers de la Gendarmerie nationale, 4etrimestre, Éditions esprit Du Livre, Paris, 2012, p :04.e

4 Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé «Agence nationale de la sécurité des systèmes d'information» , NOR: PRMD0914748D Version consolidée au 02 février 2020.

5 Article 3, Modifié par Décret n°2018-1136 du 13 décembre 2018 - art. 3 (VD), Ibid : « L'Agence nationale de la sécurité des systèmes d'information est l'autorité nationale en matière de sécurité des

وما بعدها، ومن بين تلك المهام أنها تقوم بجميع التدابير اللازمة لحماية الأنظمة المعلوماتية الفرنسية[1]، كما منحها المشرع الفرنسي سنة 2019 بموجب المادة الرابعة (04) من نفس المرسوم[2] صلاحية تقييم أمن المنتجات والأجهزة الخاصة بأنظمة تكنولوجيا المعلومات والخدمات المقدمة من مقدمي الخدمات الموثوق بهم، واعتماد مراكز التقييم وإصدار شهادات الأمان، كتلك المطلوبة في إنشاء التوقيع الإلكتروني، إصدار التراخيص وسحبها وإدارة الإعلانات المتعلقة بوسائل وخدمات التشفير.

وفي إطار التعاون الدول فإن الوكالة تقوم بالمشاركة في المفاوضات الدولية وتتواصل مع نظيراتها في الدول الأخرى، لذا دعت الوكالة الفرنسية لأمن الأنظمة المعلوماتية (ANSSI) إلى تعزيز قدرات الأمن السيبراني في الاتحاد الأوروبي، حيث قال مديرها العام: سيمثل عام 2020 بداية عهد جديد للدول الأوروبية يجب أن تكون فيها أوروبا قادرة على تأكيد سيادتها في مجال الإنترنت من أجل تعزيز قيم السلام والاستقرار في الفضاء الإلكتروني على المستوى الدولي[3].

systèmes d'information. A ce titre : - elle assure la fonction d'autorité nationale de défense des systèmes d'information. En cette qualité, elle propose au Premier ministre les mesures destinées à répondre aux crises affectant ou menaçant la sécurité des systèmes d'information des autorités publiques et des opérateurs d'importance vitale et elle coordonne, dans le cadre des orientations fixées par le Premier ministre, l'action gouvernementale en matière de défense des systèmes d'information ; - elle conçoit, fait réaliser et met en œuvre les moyens interministériels sécurisés de communications électroniques nécessaires au Président de la République et au Gouvernement ; - elle anime et coordonne les travaux interministériels en matière de sécurité des systèmes d'information ; - elle élabore les mesures de protection des systèmes d'information proposées au Premier ministre. Elle veille à l'application des mesures adoptées ; - elle mène des inspections des systèmes d'information des services de l'Etat et d'opérateurs publics ou privés ; - elle met en œuvre des dispositifs de détection des événements susceptibles d'affecter la sécurité des systèmes d'information de l'Etat, des autorités publiques et d'opérateurs publics et privés et coordonne la réaction à ces événements ; - elle recueille les informations techniques relatives aux incidents affectant les systèmes d'information des personnes mentionnées à l'alinéa précédent. Elle peut apporter son concours pour répondre à ces incidents ; - elle délivre des agréments aux dispositifs et aux mécanismes de sécurité destinés à protéger, dans les systèmes d'information, les informations couvertes par le secret de la défense nationale ; - elle participe aux négociations internationales et assure la liaison avec ses homologues étrangers ; - elle assure la formation des personnels qualifiés dans le domaine de la sécurité des systèmes d'information. »

1 Brigitte Pereira, *La lutte contre la cybercriminalité: de l'abondance de la norme à sa perfectibilité*, Distribution électronique Cairn.info pour De Boeck Supérieur., Article disponible en ligne à l'adresse, 2016/3 t. XXX | pages 387 à 409, p : 408.

2 Article 4, Modifié par Décret n°2019-1139 du 7 novembre 2019 - art. 1.

3 FIC 2020: ANSSI calls for European sovereignty in cybersecurity, in the web site : *https://www.ssi.gouv.fr /uploads/2020/01/anssi-press_release-fic_2020.pdf* : « The year 2020 marks the beginning of a new European cycle. Europe must be able to assert its sovereignty in the cyber field in

من جانب آخر، أسست المملكة المتحدة البريطانية هي الأخرى في الفاتح من أكتوبر سنة 2016 مركزاً لحماية منظومتها المعلوماتية، والمسمى بالمركز الوطني لأمن المعلوماتية (NCSC) والذي يستخدم قدرات دفاعية إلكترونية متطورة لحماية الفضاء الإلكتروني، وتعزيز الثقة في العالم الرقمي، بحيث سيعمل المركز على تحليل التهديدات الإلكترونية وكشفها وفهمها؛ ليتمكن من تقديم خبرته في مجال أمن المعلوماتية لدعم جهود الحكومة الرامية لرعاية الابتكار، وتحفيز ومساندة عملية تطوير مهارات أمن المعلوماتية، والتصدي للجرائم الإلكترونية التي قد تستهدف الأمن المعلوماتي البريطاني.

order to promote its values of peace and stability in cyberspace at the international level » said Guillaume Poupard, Director General of ANSSI.

المبحث الرابـــع:
وحدات الأمن الوطني المتخصصة في مكافحة الجريمة الإلكترونيـــة.

إن مكافحة الجريمة الإلكترونية أضحت من بين أولويات الدولة الجزائرية إذ لا بد من الاستجابة للانشغالات الأمنية المتزايدة، والمحافظة على الطمأنينة والأمن العمومي في الفضاء الإلكتروني – أو كما يسمى الفضاء الأزرق–، ولأجل ذلك فقد خصصت الدولة الجزائرية عدة وحدات متخصصة لمكافحة هذه الجريمة؛ فمنها المتواجدة في مؤسسة الشرطة (المطلب الأول)، وأخرى في مؤسسة الدرك الوطني (المطلب الثاني)، وتفصيلهما كما يلي:

المطلب الأول: الشرطة الجزائرية ودورها في مكافحة الجريمة الإلكترونية

إن من بين الأهداف الإستراتيجية التي تهدف مؤسسة الشرطة القيام بها هي كشف الجريمة والقبض على مرتكبيها والوقاية والحد منها، وحماية الحريات وصون الحقوق، والاستعداد لمواجهة الأزمات والكوارث بفعالية من أجل الضبط الجيد للأمن[1] وحفظ النظام العام، وأداء جميع المهام المسندة للأمن الوطني كما حددها التشريع والتنظيم المعمول بهما[2]، ففي سبيل المكافحة الفعالة للجريمة الإلكترونية خصص الأمن الوطني موارد بشرية متخصصة[3]، من خلال تعزيز صفوفه بضباط ذوي خلفيات جامعية عالية المستوى في ميادين العلوم الإنسانية والاجتماعية على الخصوص، تستفيد من تدريبات عالية المستوى في العلاقات العامة وإدارة عمل الفرق الشرطية

1 براردي نعيمة، الاتصال بين الشرطة والمواطن ودوره في مكافحة الجريمة في الجزائر (دراسة تحليلية استطلاعية بالجزائر العاصمة)، رسالة لنيل شهادة الدكتوراه في علوم الإعلام والاتصال، كلية العلوم السياسية والإعلام، جامعة الجزائر 03، السنة الجامعية 2012-2013، ص 117.

2 المادة 02 من المرسوم التنفيذي رقم 10-322، المؤرخ في 16 محرم عام 1432 الموافق 22 ديسمبر سنة 2010، المتضمن القانون الأساسي الخاص بالموظفين المنتمين للأسلاك الخاصة بالأمن الوطني، الصادر بالج.ر العدد 78، بتاريخ 26 ديسمبر سنة 2010، ص 04.

3 حسب المادة 109 من المرسوم التنفيذي رقم 10-322، المتضمن القانون الأساسي الخاص بالموظفين المنتمين للأسلاك الخاصة بالأمن الوطني، المرسوم نفسه، فإنه من بين المناصب العليا في الأسلاك الخاصة التابعة للأمن الوطني، الأشخاص التابعين للشرطة التقنية والعلمية والمكلفون بتقديم الخبرة في مجال الجرائم الإلكترونية، كما يوجد مدربين ومكونيين لضمان التكوين الجيد وتجديد المعلومات وتحسين المستوى التقني والبيداغوجي للمتدربين.

والتعامل مع الحالات الخاصة في صفوف المنحرفين والمجرمين[1]، كما خصص الأمن الوطني موارد هيكلية وتنظيمية لمحاربة الجريمة الإلكترونية كمديرية الشرطة القضائية[2]، والمصلحة المركزية لمكافحة الجريمة الإلكترونية التابعة لمديرية الأمن الوطني، والتي تم إنشاؤها بقرار من المدير العام للأمن الوطني سنة 2015، حيث كانت عبارة عن فصيلة شكلت النواة الأولى لتشكيل أمني على مستوى المديريـة العامة للأمن الـوطني تم إنشاؤها سنة 2011[3]، ولأن الجريمة الإلكترونية في تطور مستمر تم الانتقال إلى المرحلة الثانية، حيث تم توسيع التشكيل الأمني بتكوين فصائل على مستوى 48 ولاية تابعة للمصالح الولائية للشرطة القضائية بأمن الولايات[4]، فتم بذلك تقريب هذه المصالح من المواطنين.

ومن الأمثلة على ما قامت به هذه الفصائل لأجل مكافحة الجريمة الإلكترونية، القضية التي عالجتها فرقة مكافحة الجرائم الإلكترونية بالمصلحة الولائية للشرطة القضائية لأمن ولاية عين الدفلى، والمتعلقة بالغش في امتحانات شهادة التعليم المتوسط دورة جوان 2019 بواسطة الوسائط الاجتماعية، حيث أسفرت التحريات التقنية التي باشرتها عناصر الفرقة، وبالتنسيق مع المصلحة المركزية لمكافحة الجرائم الإلكترونية بمديرية الشرطة القضائية و بإشراف الهيئات القضائية على توقيف ثلاثة أشخاص وتقديمهم للعدالة[5].

ومن أجـل مواكبة التطور التكنولوجي والـرفع من المستوى المعرفي والمهاري والأدائي للمحققين، تم استحداث صنفين من التكوين المتخصص؛ الصنف الأول: محقق في الجريمة

1 عبد العزيز ديلمي، دور الشرطة المجتمعية في الوقاية من الجريمة والانحراف دراسة نظرية لبناء نموذج للشـرطة الجوارية في الجزائر، أطروحة مقدمة لنيل شهادة الدكتوراه في علوم اجتماع الجريمة والانحراف، قسم علم الاجتماع، كلية العلوم الإنسانية والاجتماعية، جامعة الجزائر 02، السنة الجامعية 2012-2013، ص. ص: 562-563.

2 تتمثل مهام مديرية الشرطة القضائية في: تنشيط، تنسيق وتوجيه المصالح المكلفة بمعاينة مخالفات قانون العقوبات وكذا جمع الأدلة والبحث عن المجرمين طالما لم يتم فتح تحقيق من قبل الجهات القضائية". معلومات متاحة على الموقع الإلكتروني لمديرية الأمن الوطني الجزائري الموالي: *https://www.algeriepolice.dz/*

3 بارة سمير، المرجع السابق، ص 437.

4 تقرير المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال حول تشكيل عملياتي لمحاربة الجريمة عبر الشبكة العنكبوتية، مجلة الشرطة، المؤسسة الوطنية للاتصال والنشر والإشهار وحدة الطبع رويبة، الجزائر، العدد 144، سبتمبر 2019، ص 69.

5 معلومات متاحة عبر الموقع الرسمي لمديرية الأمن الوطني: *https://www.algeriepolice.dz*

المعلوماتية "ICC"، خاص بإطارات ومفتشي المصالح المحققة في مجال الجريمة المعلوماتية. والصنف الثاني متدخل أول في الجريمة المعلوماتية "PICC"، خاص بأعوان الشرطة العاملين في مجال مكافحة الجريمة المعلوماتية[1]، كما يقوم الأمن الوطني بتأهيل وإعداد الكفاءات العلمية المؤهلة لمواجهة هذا النوع من الإجرام، وذلك بتطوير العملية التدريبية لرفع مستوى الأداء لتلبية الاحتياجات الأمنية الحالية والمستقبلية، لذا قامت المنظمات الحكومية ومنظمات الشرطة في بعض الدول بتدريب رجالها، وتكوينهم كما فعلت كل من الولايات المتحدة الأمريكية وكندا والمملكة العربية المتحدة، حيث قامت هذه الدول بدورات تكوينية من أجل تزويد محققي الشرطة والعاملين في إدارات العدالة الجنائية بمعارف وتقنيات الحوسبة ودراسة مجموعة من الحالات[2]، وإكسابهم المهارات التأسيسية للتحقيق في الجرائم الإلكترونية، وذلك بالتنسيق مع الشركات، والجهات الأكاديمية المتخصصة، في الداخل والخارج[3].

ولأن التدريب والتعليم هما أساس العملية التطويرية لأي مجتمع من المجتمعات، عمِل جهاز الأمن الوطني على تطوير قدرات ومهارات منتسبيه واستثمار طاقات العاملين في التعليم وخاصة العالي منها، من أجل عصرنة وتقديم الأفضل والحصول على قوة بشرية متخصصة، لذا تم إنشاء عدة مرافق خصصت لهذا الغرض ومنها المعهد الوطني للبحث في علم التحقيق الجنائي[4]، والذي

1 تقرير المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، حول تشكيل عملياتي لمحاربة الجريمة عبر الشبكة العنكبوتية، المرجع السابق، ص 70.

2 عادل عبد العال ابراهيم خراشي، جرائم الاستغلال الجنسي للأطفال عبر شبكة الانترنت وطرق مكافحتها في التشريعات الجنائية والفقه الجنائي الإسلامي، دار الجامعة الجديدة، الإسكندرية، مصر، 2015، ص 124 إلى 129، **نقلاً عن**: هشام محمد فريد رستم، الجريمة المعلوماتية، أصول التحقيق الجنائي الفني وآلية التدريب التخصصي للمحققين، مجلة الأمن والقانون، كلية الشرطة دبي، العدد الثاني، السنة السابعة 1999، ص 20 وما بعدها.

3 محمد بن نصير محمد سرحان، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والانترنت "دراسة مسحية على ضباط الشرطة بالمنطقة الشرقية"، رسالة ماجستير، قسم علوم الشرطة، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، 2004، 195؛ تاحي وحيد، المرجع السابق، ص 82.

4 مرسوم رئاسي رقم 04-432، المؤرخ في 17 ذي القعدة عام 1425 الموافق 29 ديسمبر سنة 2004، المتضمن إنشاء المعهد الوطني للبحث في علم التحقيق الجنائي، المنشور في الج.ر.ج العدد 84، بتاريخ 29 ديسمبر سنة 2004، وحسب المادة الثانية (02) والثالثة (03) منه فإن المعهد هو: "مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلال المالي، يوضع "تحت وصاية الوزير المكلف بالداخلية ويتبع المديرية العامة للأمن الوطني". وحسب المادة الخامسة (05) فإن المعهد يتولى المهام الآتية:"- تحليل المؤشرات المادية التي يتم جمعها بمناسبة معاينة المخالفات والتحريات التي تتطلب مشاركة مختلف التخصصات التقنية والعلمية، بناء على طلب من السلطات القضائية المختصة. – إعداد تقارير الخبرة بناء على طلب من السلطات المختصة المؤهلة

يضم خمسة (5) مخابر جهوية، موجودة في كل من: وهران وقسنطينة وورقلة وبشار وتامنغست، وهي بمثابة امتداد لنشاطات المعهد في مجال الخبرة والتكوين والبحث العلمي، حيث تقوم بإجراء التحاليل والخبرة العلمية الضرورية لسير التحقيقات القضائية المقدمة لها من قِبل المحققين والقضاة والسلطات المؤهلة، كما توفر تلك المخابر الدعم التقني الضروري والمتخصص والمجهز بالوسائل الملائمة لتسيير مواقع حدوث الجريمة، وتساعد في تكوين تقنيي السلسلة القضائية في مجالات البحث العلمي وعلم التحقيق الجنائي، وتساهم في أشغال المجلس العلمي للمعهد[1].

جدير بالذكر أن المخابر الجهوية تضم مصالح مقسمة إلى مكاتب ومخابر متخصصة، حيث يضم القسم التقني، مصلحة الخبرات الخاصة بالدلائل التكنولوجية، والتي تعمل على تحليل الدلائل المادية التي تم جمعها إثر معاينة المخالفات والتحريات في ميادين الدلائل الإلكترونية الناجمة عن الجرائم الإلكترونية والبصمات الصوتية، ومعالجة الصورة والإشارة واستغلال الهواتف المحمولة وإعداد تقارير الخبرة التي طلبتها منها السلطات القضائية المختصة، كما تعمل المصلحة على ضمان تسيير بنوك المعطيات في علم التحقيق الجنائي، بالأخص المحفوظات الآلية للبصمات الصوتية والمخالفات المرتبطة بتكنولوجيات الإعلام والاتصال[2].

وفي سنة 2017 تم استحداث معهد الدراسات العليا في الأمن الوطني بموجب المرسوم الرئاسي رقم 17-145[3]، والذي تم إلغاؤه سنة 2019 بموجب المرسوم الرئاسي 19-278[4]، حيث

قانوناً، – القيام بأعمال التكوين وتجديد المعارف وتحسين المستوى والتكوين ما بعد التدرج في ميداني علم التحقيق الجنائي والإجرام، ... – التحيين الدائم عن طريق متابعة: * النشاطات التقنية والعلمية، * الدراسات والمنشورات في هذا الميدان، * المستجدات في مجال البحث والتجهيزات التقنية والعلمية".

1 المادة 09 من القرار الوزاري المشترك، المؤرخ في 26 ربيع الأول عام 1428 الموافق 14 أبريل سنة 2007، المتعلق بتنظيم الأقسام والمصالح والمخابر الجهوية للمعهد الوطني للبحث في علم التحقيق الجنائي، المنشور بالج.ر العدد 36 بتاريخ 03 يونيو سنة 2007، ص 14.

2 المادة 05 من نفس القرار الوزاري المشترك.

3 من المرسوم الرئاسي رقم 17-145، المؤرخ في 22 رجب عام 1438 الموافق 19 أبريل سنة 2017، المتضمن إحداث معهد الدراسات العليا في الأمن الوطني ومهامه وتنظيمه وسيره، المنشور بالج.ر.ج العدد 26، بتاريخ 23 أبريل سنة 2017.

4 المرسوم الرئاسي رقم 19-278، المؤرخ في 21 صفر عام 1441 الموافق 20 اكتوبر سنة 2019، المتضمن مهام معهد الدراسات العليا في الأمن الوطني وتنظيمه وسيره، المنشور بالج.ر.ج، العدد 65، بتاريخ 24 أكتوبر سنة 2019، جاء في المادة 24 منه: "تلغى كل الأحكام المخالفة لهذا المرسوم، لاسيما المرسوم الرئاسي رقم 17-145 والمتضمن إحداث معهد الدراسات العليا في الأمن الوطني ومهامه وتنظيمه وسيره، باستثناء المادة الأولى منه".

نصت بعض مواده على المهام المسندة لهذا المعهد، ومنها أنه يضْمنُ تكوينات جامعية في الدرجتين الثانية والثالثة في الأمن الوطني وفي الدراسات الإستراتيجية والعلاقات الدولية، كما يمكنه أن يقدم تكوينات متواصلة مؤهلة، الأكاديمية منها والمتخصصة، والتي تخصص لفائدة المستخدمين العسكريين والمدنيين، والوطنيين والأجانب، ويعمل المعهد على القيام بدراسات وبحوث في اليقظة الاستراتيجية والاستشرافية في مجالات الأمن والدراسات الإستراتيجية والعلاقات الدولية، والتكنولوجيات العسكرية والأمن السيبراني ووسائل الإعلام والاتصال والتنمية الاقتصادية والاجتماعية الثقافية[1]، إضافة إلى تنظيمه دورات تكوين حسب الطلب وملتقيات ومحاضرات وأيام دراسية وطنية ودولية في مواضيع ذات علاقة بمجال اختصاصه، لفائدة إطارات وطنية وأجنبية[2]، حيث نجد مساهمة هذه المعاهد على أرض الواقع جلية، فالمعهد الوطني للشرطة الجنائية بسحاولة منذ سنة 2014 إلى يومنا هذا ساهم في تكوين (152) إطار شرطة من الدول الشقيقة، لاسيما تونس، فلسطين، ليبيا، أوغندا، السودان، النيجر، البنين وكينيا[3].

ولأن النتائج التي توصلت إليها الشرطة الجزائرية في مكافحة الجريمة الإلكترونية لا بأس بها، فقد كان ذلك محط إشادة من بعض الشخصيات، ومنها ما ورد في تصريح للسيد "مانغ هانغواي (Meng Hongwei)" رئيس منظمة الانتربول خلال زيارة العمل التي قام بها للجزائر في شهر ماي سنة 2018، حيث أشاد بالتقدم الذي أحرزه الجهاز الشرطي الجزائري، وما وصلت إليه الشرطة الجزائرية من تطور واحترافية، ودعا إلى تعزيز التعاون وتفعيل آليات تبادل الخبرات المعلوماتية من أجل ضمان فعالية أكثر في مواجهة جميع أشكال الجرائم المستحدثة وبالأخص الجريمة الإلكترونية.

ولأجل المواجهة الفعالة للجريمة الإلكترونية، فإن الشرطة تقوم بوضع قائمة اسمية لضباط مختصين يمكن الاستعانة بهم في مجال البحث والتحري في قضايا الجرائم الإلكترونية، وتُوفر للدول

1 المادة 08 من نفس المرسوم الرئاسي رقم 19-278.

2 المادة 09 من نفس المرسوم الرئاسي.

3 معلومات متاحة على الموقع الإلكتروني الرسمي للمديرية العامة للأمن الوطني الجزائري: *https://www.algeriepolice.dz* ، والذي تم الإطلاع عليه يوم: 2018/07/18.

الأطراف المعلومات العملية اللازمة، لخلق فرق عمل وورشات تكوين[1]، ولأن الكفاءات المتواجدة في جهاز الشرطة لها من الدراية ما يسمح بتقلدها مناصب قيادية تتمكن من خلالها المساهمة في عملية المواجهة والتحسيس بهذه الجريمة، الأمر الذي مكن من تعيين عميد من الشرطة الجزائرية، والذي كان رئيساً للمصلحة المركزية لمكافحة الجريمة الإلكترونية على رأس مجموعة خبراء الانتربول المختصة في مكافحة الجريمة الإلكترونية، فالمستوى الجيد الذي وصلت إليه الكفاءات العاملة في جهاز الشرطة في هذا الخصوص سوف يسمح بتعزيز برامج التعاون بين الجزائر ودول أخرى.

وتجسيداً لذلك، فالجزائر ممثلة في المديرية العامة للأمن الوطني والاتحاد الأوربي، قاما بتاريخ الحادي عشر (11) من شـــهر جوان سنـــة 2019، بالإطلاق الرسمي للتوأمة بعنوان "تعزيز الخبرة العلمية والتقنية الجزائرية" مما سيسمح بالرفع من مستوى خبرة الشرطة العلمية والتقنية الجزائرية بما يتماشى مع المعايير والممارسات الأوربية الحسنة[2]، حيث تمكنت الشرطة الجزائرية من حل لغز عديد القضايا من الجرائم الإلكترونية ذات البعد الدولي، ومنها قضية وقعت نهاية سنة 2009، والتي تم الإبلاغ عنها من طرف مكتب التحقيقات الفدرالية (FBI) كانت ضحيتها شركة أمريكية، تعرضت لعملية اختراق إلكتروني لبياناتها البنكية قامت بها منظمة إجرامية،كان أحد أفرادها يقطن بإحدى ولايات الشرق الجزائري، وبعد تحريات مكثفة حُدد مكانه وهويته وقُدم للعدالة، وبعد شهر من ذلك تلقت الشرطة الجزائرية بلاغاً آخر في قضية تعرض فيها بنك كندا إلى اختراق إلكتروني سَحب خلاله المجـــرمون مبلغ مالي قـدر بـ: 200 مليون دولار، وكان من بين المتورطين في ذلك مواطـن جـــزائري، وبفضل كفاءة الشرطة المتخصصة تم تحـديد هـوية ومكان إقامة المشتبه فيه وتم تقديمه إلى العدالة[3].

1 الشرطة الجزائرية في الجزائر المستقلة، ص ص 120-121، متاح على الموقع الإلكتروني لمديرية الأمن الوطني الجزائري الموالي: *https://www.algeriepolice.dz/IMG/pdf/histoire05.pdf* تاريخ الإطلاع: 2020/02/20.

2 الكادر البشري لنيابة مديرية الشرطة العلمية والتقنية والمقدر بحوالي 798 موظف شرطة، 58 إطار مكلف بالخبرة، 51 عون قياس بشري و2285 تقني مسرح الجريمة في تحقيق الشخصية. **نقلاً عـــن**: بسكري نعيمة، اتفاقية توأمة بين الشرطة الجزائرية ونظيرتها الفرنسية والإسبانية، مجلة الشرطة، المؤسسة الوطنية للاتصال والنشر والإشهار وحدة الطبع رويبة، الجزائر، العدد (144)، سبتمبر 2019، ص 20.

3 م.ش، المصلحة المركزية للجريمة الإلكترونية في مواجهة مجرمي العالم الإفتراضي، بواسطة جريدة السلام اليوم: 13/02/2016، على الموقع الإلكتروني الموالي: *http://www.essalamonline.com/ara/permalink/52564*، تاريخ الاطلاع: 2019/04/05.

مما سبق يتضح أن الشرطة الجزائرية تسعى لتكون لديها الجاهزية المادية المتقدمة والإمكانات البشرية المتخصصة لمكافحة الجريمة الإلكترونية، على غرار الدول الأخرى؛ العربية والغربية، فالمملكة المغربية استحدثت المديرية العامة للأمن الوطني، والتي بها وحدات متخصصة لمحاربة الجرائم الإلكترونية على الصعيد المركزي والجهوي، إذ تتوفر على مصلحة مركزية، ومكتب وطني على مستوى الفرقة الوطنية للشرطة القضائية، إلى جانب تسعة وعشرين (29) فرقة متخصصة على المستوى الجهوي، وأربعةُ (04) مختبرات لتحليل الآثار الرقمية على المستوى المغربي[1].

أما في جمهورية مصر العربية فهنالك إدارة مكافحة جرائم الحاسب الآلي وشبكة المعلومات التابعة للإدارة العامة للمعلومـات والتوثيق بوزارة الداخلية، والتي أُنشئت بالقرار الوزاري رقم 13507 سنة 2002[2]، كما تعمل وزارة الاتصالات المصرية بتطبيق العديد من الاستراتيجيات التي تمكن من حماية الأشخاص وتسعى لتحقيق الاستخدام الأمن على الإنترنت[3]، ومن الأمثلة على عـمل إدارة مكافـحة جرائم الحاسبات الآلية وشبكات المعلومات في مكافحة الجـرائم الإلكترونية، الفحص التقني الذي قامت به هذه الأخيرة إثر تَقدُم ربة منزل للإدارة العامة للمعلومات والتوثيق بوزارة الداخلية بمحضر، أكدت فيه تضررها من قيام زوجها السابق بالتشهير بها عن طريق الإنترنت، وقد بينت التحقيقات على وجود ثلاث مواقع على شبكة الإنترنت تحتوي على أفلام مخلة للمعنية وتعليقات وعبارات تشهير تضر بها وبزوجها[4]. كما تعمل الوزارة على التنسيق مع الهيئات الأخرى وخاصة الانتربول للقبض على مرتكبي جرائم غسيل الأموال عبر الإنترنت والجرائم الإلكترونية بصفة عامة.

1 ليلى الزوين، إستراتيجية المديرية العامة للأمن الوطني في محاربة الجرائم الإلكترونية، جريدة أنفاس بريس الإلكترونية، الأحد 10 نوفمبر 2019، متاح على الموقع الإلكتروني الموالي: *https://anfaspress.com/news/voir/57929-2019-11-10-04-48-49*، تاريخ الاطلاع: 2019/12/27.

2 عبد العالي الديربي، محمد صادق إسماعيل، المرجع السابق، ص 115؛ حسام محمد نبيل الشنراقي، الجريمة المعلوماتية دراسة تطبيقية مقارنة على جرائم الاعتداء على التوقيع الإلكتروني، دار الكتب القانونية، مصر، 2013، ص 759؛ نبيل محمد عثمان عرعارة، المرجع السابق، ص 136.

3 شيرين محمد إحسان عبد الحافظ، المرجع السابق، ص 114.

4 عبد العالي الديربي، محمد صادق إسماعيل، المرجع السابق، ص 117.

أما في الكويت فقد أَنشأت وزارة الداخلية الكويتية في الثاني من شهر يناير سنة 2009 شرطة مختصة في مكافحة الجرائم الإلكترونية، ولم تكتفِ بمجرد مصالح لمجابهة هذه الجريمة الخطيرة[1].

وبالعودة للدول الغربية نجد منها من خصصت وحدات متخصصة لهذه الجريمة، ومنها من أنشأت جهاز شرطة بأكمله، والبداية ستكون من بريطانيا التي أنشأت وحدة بوليسية تسمى الوحدة الوطنية لمكافحة جرائم التكنولوجيا المتطورة[2]، إضافة إلى مكافحتها لهذه الجريمة من خلال دائرة شرطة البريد والاتصالات، والتي انشئ بها المركز الوطني لجرائم تكنولوجيا المعلومات وحماية البنية التحتية الحيوية، ليكون المسؤول عن منع الجريمة الإلكترونية ومكافحتها خاصة منها تلك التي لها الطابع المنظم أو الإرهابي والمرتكبة ضد البنية التحتية الحيوية. كما يضم المركز نقطة اتصال لحالات الطوارئ التقنية والتشغيلية المتعلقة بالأحداث الإجرامية عبر الوطنية[3].

أما في الولايات المتحدة الأمريكية فقد أنشأت سنة 1978 شرطة الإنترنت لمحاربة الأنشطة غير المشروعة على شبكة الإنترنت، وخصصت عدة أقسام ووحدات شرطية لمواجهة الجرائم الإلكترونية، كمكتب رئيس التكنولوجيا، وهو مكتب مفوض مباشرة من مكتب التحقيقات الفيدرالية الأمريكي، وقسم مكافحة جرائم الحاسوب وجرائم حقوق الملكية الفكرية The Criminal Division's Computer Crime and Intellectual Property Section, (CCIPS) التابع لوزارة العدل الأمريكية والذي تم إنشاؤه سنة 1991، والمركز الوطني لحماية البنية التحتية تابع للمباحث الفيدرالية الأمريكية The FBI's National Infrastructeure Protection Center (NIPS) ، والذي أنشأ في الثامن والعشرين (28) من شهر فيفري سنة 1998، بالإضافة إلى مركز لتلقي شكاوى الاحتيال عبر الإنترنت، ووحدة متخصصة تابعة لقسم العدالة الأمريكي، مكلفة بمكافحة الإجرام

1 فهد عبد الله العبيد العازمي، المرجع السابق، ص 229.

2 عبد الفتاح بيومي حجازي، الجريمة في عصر العولمة " دراسة في الظاهرة الإجرامية المعلوماتية مع التطبيق على القانون الإماراتي، المرجع السابق، ص 25.

3 تقرير الأمين العام، الجمعية العامة، الأمم المتحدة، حول مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية (القرار رقم 73/187)، الدورة الرابعة والسبعون، البند 109 من جدول الأعمال المؤقت*(A/74/130)، 30 جويلية 2019، ص 47.

المعلوماتي، تتكون من خبراء تقنيين وقانونيين[1]، ولأن مثل هذه الوحدات والأجهزة مُهم للقيام بحماية أمن الشبكات ومواجهة الجرائم الإلكترونية لاسيما في الدول التي تعد الشبكات جزءاً من بنيتها الأمنية والتحتية، فقد أسست الصين قوة مكافحة قرصنة الإنترنت (The Internet Piracy Hitsquad) في ديسمبر سنة 1999، وقوة مضادة للقرصنة الإلكترونية أو ما يسمى الهكرة (The Anti-Hacking System) في الثاني والعشرين (22) من شهر أوت سنة 2000، والتي تختص بمرقابة المعلومات التي يُسمح لمواطنيها الدخول إليها عبر الإنترنت[2].

من المؤكد أن التقدم الذي شهده العالم في الميدان العلمي والتقني رافقه تطور الخدمات الشرطية، وبالأخص الشرطة القضائية في مجال الشرطة العلمية والتقنية، وذلك من خلال تحديث البنى التحتية واكتساب المهارات والمعدات والأنظمة التكنولوجية الحديثة لمواجهة أخطار الجرائم المستحدثة خاصة الجرائم الإلكترونية، فأصبحت بذلك الشرطة الجزائرية تصنف في مصف الدول المتقدمة[3]، إلا أن ذلك لا يعد كافياً لمكافحة الجريمة الإلكترونية، إذ لابد من تخصيص شرطة مستقلة؛ لها من التجهيزات والإمكانات البشرية والمادية ما يمكنها من مسايرة، أو بالأحرى استباق مخاطر الجرائم التي يقوم بها مرتكبو هذه الجريمة، كما يتعين إنشاء منصات إلكترونية تعمل على مدار الساعة وطوال أيام الأسبوع لتلقي البلاغات المقدمة من طرف الضحايا، مع توفير السرية اللازمة، والسرعة المطلوبة في القيام بعملية البحث والتحري قبل اندثار الأدلة الإلكترونية، ومن

1 المركز العالمي للشكاوي الخاص بجرائم الانترنت: يعد من أهم المؤسسات التي ظهرت في الولايات المتحدة الأمريكية سنة 1999، والتي تمت هيكلته بشكل رسمي سنة 2002 بولاية وست فرجينيا، ويتلقى هذا المركز شكاوي من الشاكين في إطار الجرائم الإلكترونية عبر العالم عن طريق الشبكة المعلوماتية، وموقعه هو: (htpp://www.ic3.gov)" زيبحة زيدان، المرجع السابق، ص 110؛ تلقى مركز شكاوى جرائم الإنترنت ("IC3") (The Internet Crime Complaint Center)، وحدة مكتب التحقيقات الفيدرالية (FBI) التي تتلقى وتتابع شكاوى الجرائم الإلكترونية من الضحايا، ما مجموعه 3785 شكوى نتيجة خرق بيانات الشركات في عام 2017، حيث تكبدت تلك الشركات خسائر تفوق 60 مليون دولار. **نقلاً عـــن**: ياسر محمد الكومي محمود أبو حطب، الحماية الجنائية والأمنية للتوقيع الإلكتروني في التشريع المصري والتشريعات المقارنـــة، أطروحة من أجل الحصول على درجة الدكتوراه في القانون الجنائي، كلية الحقـــوق، جامعة حلوان، مصر، سنة 2015، ص.ص: 346-347، **عن كلا مـــن**: محمود وهيب السيد، شبكة الانترنت ومزيد من التقدم التقني، مجلة مركز بحوث الشرطة، العدد رقم21، سنة 1999، ص 271؛ وعمر محمد ابو بكر يونس، الجرائم الناشئة عن استخدام الانترنت (الأحكام الموضوعية والجوانب الإجرائية)، دار النهضة، مصر، 2005، ص 231.

2 عمر محمد أبوبكر بن يونس، المرجع السابق، ص.ص: 812-813.

3 بن سعيد صبرينة، المرجع السابق، ص 268.

أجل التقريب بين الشرطة والمواطن لتجسيد الشرطة الجوارية باعتبارها شريكاً فاعلاً في الوقاية من الإنحراف والجنوح والإجرام[1].

المطلب الثاني: الدرك الوطني ودوره في مكافحة الجريمة الإلكترونية.

يعد الدرك الوطني من بين قوات الأمن الفاعلة في مكافحة الإجرام عموماً والجريمة الإلكترونية خصوصاً، وذلك من خلال ما له من إمكانات بشرية ومادية مخصصة لهذا الغرض[2]، فمكافحة الجريمة الإلكترونية أضحت من بين أولويات الدولة الجزائرية، وذلك في إطار الاستجابة للانشغالات الأمنية المتزايدة والمحافظة على الطمأنينة والأمن العمومي في الفضاء السيبراني الوطني[3]، فالبداية الفعلية لمحارب قيادة الدرك الوطني للجريمة الإلكترونية، كانت في سنة 2004[4]، ليتم بعدها إنشاء مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها والذي يعد اليوم العصب الذي يسير مهام المكافحة واليقظة وفرض احترام القوانين في الوقت الذي يبحر فيه

1 عبد العزيز ديلمي، المرجع السابق، ص 544.

2 المرسوم الرئاسي رقم 09-143، المؤرخ في 2 جمادى الأولى عام 1430 الموافق 27 أبريل سنة 2009، يتضمن مهام الدرك الوطني وتنظيمه، الصادر في الج.ر.ج العدد 26، بتاريخ 03 مايو سنة 2009، ص 17: جاء في المادة الثانية (02) منه أن: "الدرك الوطني قوة عسكرية منوطة بها مهام الأمن العمومي. وتحكمه القوانين والتنظيمات الجاري بها العمل في وزارة الدفاع الوطني، والقوانين والتنظيمات المتعلقة بمهمة الأمن العمومي وكذا أحكام هذا المرسوم"، ونصت المادة 08 من نفس المرسوم على أن: "يحارب الدرك الوطني، في مجال الشرطة القضائية، الإجرام والإجرام المنظم. ويستعمل لهذا الغرض وسائل تحريات الشرطة العلمية والتقنية وخبرة الأدلة الجنائية. ويمارس هذه المهمة طبقا لأحكام قانون الإجراءات الجزائية"، ونصت أيضاً المادة 13 على وحدات وهياكل الدرك الوطني: "-قيادة الدرك الوطني، - الوحدات الإقليمية، - الوحدات المشكلة، - الوحدات المتخصصة، وحدات الإسناد، - هياكل التكوين، - المعهد الوطني للأدلة الجنائية وعلم الإجرام، المصالح والمركز العملية والتقنية، المصلحة المركزية للتحريات الجنائية، المفرزة الخاصة للتدخل."؛ تتضمّن أركان الدرك الوطني مركز العمليات والمديريات السبع (7) الآتية: - مديرية الأمن العمومي والاستعمال، - مديرية الوحدات المشكّلة، - مديرية التلماتية، - مديرية المدارس، - مديرية الموارد البشرية، - مديرية التخطيط والماليّة، - مديرية الإمداد والمنشآت. تهيكل المديريات في أقسام ومصالح مركزية. تلحق قيادة وحدات حراس الحدود بقيادة الدرك الوطني، معلومات من الموقع الإلكتروني الرسمي للدرك الوطني : *http://www.mdn.dz/site_cgn/index.php?L=ar#undefined*، تاريخ الاطلاع: 2020/02/25.

3 **انظر في ذلك:** تصريح للسيد قائد الدرك الوطني اللواء مناد نوبة، يومية الجمهورية، العدد 6449 ليوم الاربعاء 28 مارس 2018، ص 02، الموضوع متاح على الموقع الإلكتروني الموالي: *https://www.eldjoumhouria.dz/Images/5abaa9b7.pdf 32418326691170*، تاريخ الاطلاع: 2019/12/05.

4 تم في سنة 2004 تعديل قانون العقوبات بموجب القانون 04-15، السالف الذكر، والذي أضيفت بموجبه المواد من 394 مكرر إلى 394 مكرر 07، والمتعلقة بمكافحة الجرائم الإلكترونية.

الملايين من المستخدمين عبر صفحات الإنترنت سواء من الخواص أو المؤسسات في الفضاء الإلكتروني[1].

لقد عمل المركز السالف الذكر منذ إنشائه سنة 2008 على تأمين منظومة المعلومات لخدمة الأمن العمومي، حيث يهدف ضباط وأعوان الشرطة القضائية المؤهلين في الدرك الوطني إلى تطبيق القوانين وجمع الأدلة وتحليل معطيات وبيانات الجرائم الإلكترونية المرتكبة والبحث عن مرتكبي الجرائم عموماً، وتحديد هوية أصحـابها سواءً أكانوا أشخاصاً فرادى أو عِصابات، ويعمل المركز على مساعدة باقي الأجهزة الأمنية الأخرى في أداء مهامها في هذا الخصوص، كما استطاع المركز معالجة أزيد من 100 جريمة إلكترونية سنة 2014، وما يفوق 500 قضـية رقمية خلال سنة 2015، منها 300 جريمة تتعلق بمواقع التواصل الاجتماعي "فايسبوك"، و20 جريمة رقمية تعلقت باختراق مواقع رسمية لمؤسسات خاصة وعامة، استهدف مجرموها أنظمة المعالجة الآلية للمعطيات[2]، وفي الخمسة أشهر الأولى من سنة 2019، تم معالجة 1188 قضية بنجاح من مجموع 1515 قضية مسجلة مع توقيف 1512 متورط[3]، ولأن الأطفال هم من أكثر الفئات العمرية تضرراً من الجريمة الإلكترونية فقد قامت قيادة الدرك الوطني بمجموعة من البرامج التوعوية بالتنسيق مع وزارة التربية الوطنية من خلال دروس التوعية في المدارس التي جُربت فيها تلك البرامج كخطوة أولى نحو زيادة وعي الطلاب بمخاطر الجريمة الإلكترونية وحمايتهم منها.[4]

ولأن عملية مواكبة التطورات والمستجدات الحاصلة في مجال التكنولوجيات الحديثة، أمر لابد من السعي لتحقيقه في سبيل تقديم خدمات أمنية ترقى إلى تطلعات المواطنين، عمل جهاز الدرك الوطني على تكوين الإطارات وأعوان الدرك الوطني بشكل متواصل، وذلك من خلال

1 Rachid JANKARI, *Les technologies de l'information au Maroc, en Algérie et en Tunisie, vers une filière euromaghrébine des TIC ?*, vers une filière euromaghrébine des TIC, Etudes & Analyse, l'Institut de Prospective économique du Monde Méditerranéen, France, Octobre 2014, p 19.

2 بارة سمير، المرجع السابق، ص 435.

3 تقرير المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، حول تشكيل عملياتي لمحاربة الجريمة عبر الشبكة العنكبوتية، السالف الذكر، ص 70.

4 Cybercriminalité: Un programme de sensibilisation bientôt lancé par la Gendarmerie nationale, dimanche 24 juin 2018 00:12:09, Voir : *http://www.elmoudjahid.com/fr/actualites/89227*.

إنشاء مدارس ومعاهد لهذا الغرض، كمدرسة الشرطة القضائية التابعة للدرك الوطني[1]، والمعهد الوطني للشرطة القضائية بالسحاولة، والذي تم إنشاؤه سنة 1999 ليقوم بتكوين متخصصين في الشرطة القضائية، وإجراء بحوث متعلقة بالظواهر الاجتماعية ذات الصلة بالجريمة[2].

ومن أجل التحكم الجيد في الجرائم يضم الدرك الوطني في هياكله المعهد الوطني للأدلة الجنائية وعلم الإجرام[3] ببوشاوي، والذي أُطلق عليه اسم الشهيد "بن شيشة أحمد" في الحادي عشر (11) من شهر ديسمبر 2019 بمناسبة الاحتفالات المخلدة للذكرى 59 لمظاهرات الحادي عشر (11) من شهر ديسمبر سنة 1960[4]، حيث يقوم المعهد الوطني للأدلة الجنائية وعلم الإجرام بإجراء الخبرات والفحوص العلمية في إطار التحريات الأولية والتحقيقات القضائية، باستخدام مناهج الشرطة العلمية والتقنية الرامية إلى تجميع وتحليل الأشياء والآثار والوثائق المأخوذة من مسرح الجريمة بغرض إقامة الأدلة التي تسمح بالتعرف على مرتكبي الجرائم، بناءً على طلب من القضاة والمحققين أو السلطات المؤهلة، ويقوم المعهد بالمشاركة في الدراسات والتحاليل المتعلقة بالوقاية والتقليل من كل أشكال الإجرام، كما يتم على مستوى المعهد تصميم بنوك المعلومات كالبصمات الجينية وغيرها لتكون في متناول المحققين والقضاة بغرض وضع المقاربات واستخلاص الروابط المحتملة بين المجرمين وأساليب النشاط الإجرامي.

ويعد المعهد مؤسسة فاعلة في تحديد السياسة الجنائية المثلى لمكافحة الإجرام بشتى أنواعه، من خلال البحوث المتعلقة بالجرائم والعمل على ترقية البحث التطبيقي وأساليب التحريات التي

1 مرسوم رئاسي رقم 08-151، المؤرخ في 20 جمادى الأولى علم 1429 الموافق 26 مايو سنة 2008، المتضمن إحداث مدرسة للشرطة القضائية تابعة للدرك الوطني، المنشور بالج.ر.ج العدد 27، الصادر بتاريخ 28 مايو سنة 2008، ص 4، حسب المادة الرابعة (04) منه فإن من بين المهام التي تضطلع بها هذه المدرسة: ضمان التكوين المتخصص لضباط الصف في الدرك الوطني أو التابعين للهياكل الأخرى التابعة لوزارة الدفاع الوطني، والمترشحين للحصول على صفة ضباط شرطة قضائية.

2 عبد العزيز ديلمي، المرجع السابق، ص 479.

3 مرسوم رئاسي رقم 04-183، المؤرخ في 08 جمادى الأولى عام 1425 الموافق 26 يونيو سنة 2004، المتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، المنشور في الج.ر.ج العدد 41، بتاريخ 27 يونيو سنة 2004، ص 18، جاء في المادة الثانية (02) منه بأن: "المعهد مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلال المالي. ويوضع تحت وصاية وزير الدفاع الوطني. ويمارس قائد الدرك الوطني سلطات الوصاية بتفويض منه. وبهذه الصفة، فإنه يخضع إلى جميع الأحكام التشريعية والتنظيمية المطبقة على المؤسسات العسكرية".

4 للمزيد من التفاصيل يمكن الرجوع لموقع المديرية العامة للدرك الوطني التالي: *www.mdn.dz/*

ثبتت فعاليتها في ميادين عِلمي الإجرام والأدلة الجنائية على الصعيدين الوطني والدولي، والتي يُستعان فيها بالتكنولوجيات الدقيقة، والاستفادة من النتائج المتوصل إليها في كل الملتقيات والمحاضرات أو الندوات التي يشارك فيها على الصعيدين الوطني والدولي، والتي يهدف من خلالها إلى تطوير مستوى مستخدمي المعهد، الذين يخضعون لدورات تحسين المستوى والتكوين ما بعد التدرج في تخصصات العلوم الجنائية التي تنظم من طرف المعهد، إضافة إلى مهام أخرى قد يضطلع بها[1].

وعلاوة على ذلك، يعد المعهد الوطني للأدلة الجنائية وعلم الإجرام من بين المؤسسات التي سيكون لها دور في مكافحة الجريمة الإلكترونية، حيث عملت دول كثيرة على تشكيل أجهزة متخصصة لإجراء الخبرة والقيام بعمليات البحث والتحري عن الإجرام المعلوماتي، ومن تلك الدول الولايات المتحدة الأمريكية، التي قامت بإنشاء المعمل الإقليمي الشرعي للحاسوب التابع للمباحث الفيدرالية الأمريكية (FBI)، والذي أنشئ في سنة 2002، والمسمى بمكتب البرنامج الوطني (RCFL) اختصارا لـ (The Regional Computer Forensices Laboratoy)، حيث يقوم هذا المعمل الإقليمي بإجراء فحص شامل للأدلة الإلكترونية، ويعمل كنقطة اتصال إقليمية لقضايا الأدلة الإلكترونية، ويقدم خدمات مهنية وتقنية في الطب الشرعي الرقمي في الوقت المناسب[2].

إن جميع الدول ملزمة على مواصلة جهودها الرامية إلى تطوير الهياكل المتخصصة في مكافحة الجريمة الإلكترونية داخل هيئات إنفاذ القانون وأجهزة النيابة العامة والجهاز القضائي، بحيث تحصل على الخبرات والمعدات اللازمة للتصدي للتحديات التي تفرضها الجريمة السيبرانية

1 المادة الرابعة (04) من المرسوم الرئاسي رقم 04-183، المتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، السالف الذكر.

2 طارق عفيفي صادق احمد، الجرائم الإلكترونية جرائم الهاتف المحمول دراسة مقارنة بين القانون المصري والإماراتي والنظام السعودي، الطبعة الأولى، المركز القومي للإصدارات القانونية، مصر، 2015، ص 264؛ **يُنظر أيضاً**:

- Office of the Inspector General, The Department of Justice, Audit of the Federal Bureau of Investigation's Philadelphia Regional Computer Forensic Laboratory Radnor, Pennsylvania, U.S, April 2015, p :02.

ولجمع الأدلة الإلكترونية في الإجراءات الجنائية وتبادل المعلومات عنها واستخدامها"[1] الاستخدام الأفضل حتى لا تفقد تلك الإجراءات مصداقيتها أمام الجهات القضائية المختصة.

1 تقرير عن اجتماع فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، الذي عُقد في فيينا في الفترة من 27 إلى 29 مارس 2019، ص 04.

الفصل الثانـــي:
آليات مؤسساتية خارجية لمكافحة الجريمة الإلكترونية

الفصل الثاني:
آليات مؤسساتية خارجية لمكافحة الجريمة الإلكترونية.

جرائـم اليوم معقـدة بشكل متزايـد، ومترابطة وعالمية وتحدث على المستويين المـادي والافتراضي، وهناك حاجة أكثر من ذي قبل لتعاون بين الجهات الأمنية المتعددة على المستوى العالمي والإقليمي من أجل التصدي للتحديات الأمنية التي تؤثر على المجتمعات، الأمر الذي دفع العديـد من الدول لإيجاد آليات مؤسساتـية تكون كفيلة بمحاربـة الجريمـة الإلكترونيـة، وعلى الرغم من أن بعـض الآلـيات العملياتـية لا تـرقى إلى أن تكـون مؤسسات أو هيئات قائمة بذاتها، إلا أن خطورة الوضع أرغمت بعض الدول على تخصيص مصالح داخل مؤسسـاتها الأمنية، أو الإدارية من أجل محاربة الجريمة الإلكترونية، ولم تكن تلك الآليات المؤسساتية مقتصرة على الحيز الوطني فقـط بل شملت أيضاً الجانب الإقليمي والدولي.

ولأجل الإحاطة بجميع جوانب المكافحة الفعالة للجريمة الإلكترونية، نتطرق في هذا الفصل للمكافحة المؤسساتية الدولية والإقليمية للجريمة الإلكترونية (المبحث الأول)، ثم نتطرق بعد ذلك للآليات المساعدة على مكافحة الجريمة الإلكترونية كالجمعيات ومعالجة الإدمان على الإنترنت (المبحث الثاني)، وتفصيل ذلك على النحو التالي:

المبحث الأول:

المكافحة المؤسساتية الدولية والإقليمية للجريمة الإلكترونية

المؤسسات الدولية والإقليمية لمكافحة الجريمة الإلكترونية، هي نماذج عملياتية وضعت من أجل المساعدة في عملية المكافحة بما لها من إمكانيات مادية وبشرية متخصصة في هذا النوع من الإجرام، الذي لابد فيه من توطيد العلاقات بين كل تلك المؤسسات للوصول إلى استغلال أمثل للمعلومة. فعلى المستوى الإقليمي نجد العديد من المؤسسات والهيئات، والمصالح التي خصصت لمكافحة الجريمة الإلكترونية، والتي سوف تقتصر الدراسة على أهمها، فعلى المستوى الدولي نجد المنظمة الدولية للشرطة الجنائية (الانتربول) كمؤسسة دولية شرطية بارزة في مكافحة الجريمة الإلكترونية، وكذا آليات التعاون الدولي وما لها من دور بارز ومُهم في مكافحة الجريمة الإلكترونية، ليأتي الدور في الحديث على كل من الافريبول واليوروبول والاوروجيست كمؤسسات إقليمية لمكافحة الجريمة الإلكترونية.

وعليه فإن هذا المبحث تم تقسيمه إلى شقين، يتم التطرق في الأول منه للمكافحة الدولية للجريمة الإلكترونية (المطلب الأول)، على نحو يمكن من التطرق للمؤسسات الإقليمية لمكافحة الجريمة الإلكترونية (المطلب الثاني).

المطلب الأول: المكافحة الدولية للجريمة الإلكترونيـــة.

إن من بين الخصائص التي تتميز بها الجريمة الإلكترونية؛ خاصية تعديها لحدود الدولة الواحدة مما فرض ضرورة إيجاد آليات دولية يُستطاع من خلالها مكافحة هاته الجريمة والقبض على مرتكبيها أينما وجدوا، ومن بين تلك الآليات المنظمة الدولية للشرطة الجنائية الانتربول (الفرع الأول)، والتعاون الدولي ومختلف ميكانيزماته التي تعد ضرورية جداً لمجابهة هذه الجريمة (الفرع الثاني).

الفرع الأول: المنظمة الدولية للشرطة الجنائية (الانتربول).

تعد المنظمة الدولية للشرطة الجنائية (الانتربول) من أقدم صور التعاون الشرطي في مكافحة الجريمة، ففي نهاية سنة 1923 نجح الدكتور "جوهانو سويرا" مدير شرطة فينا في عقد مؤتمر دولي يعد الثاني على المستوى الدولي للشرطة الجنائية، وذلك في الفترة من الثالث (03) إلى السابع (07) من شهر سبتمبر عام 1923، ضم مندوبي تسع عشرة (19) دولة، وتمخض عنه ولادة اللجنة الدولية للشرطة الجنائية (International Criminal Police Commission ICPO) حُدد مقرها بفينا، تعمل على التنسيق بين أجهزة الشرطة من أجل التعاون في مكافحة الجريمة[1]، والتي أطلق عليها اسم المنظمة الدولية للشرطة الجنائية (الانتربول) سنة 1956، وحدد مقرها في مدينة ليون الفرنسية[2]، حيث تنقسم شبكة اتصالات (الانتربول) إلى ثلاثة مستويات هرمية: المكاتب المركزية

---

1 يوسف حسن يوسف، الجرائم الدولية للانترنت، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، مصر، 2011، ص 146؛ أمير فرج يوسف، الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر، الطبعة الأولى، مكتبة الوفاء القانونية، الإسكندرية، مصر، 2011، ص427؛ بن عمر الحاج عيسى، الانتربول كآلية دولية شرطية لمكافحة الجريمة المنظمة العابرة للحدود، مجلة الدراسات القانونية والسياسية، جامعة عمار ثليجي بالأغواط، الجزائر، العدد الثالث (03)، جانفي 2016، ص 254، **نقلاً عن**: جهاد محمد البريزات، الجريمة المنظمة، دار الثقافة للنشر والتوزيع، عمان، الأردن، الطبعة الثانية، 2010، ص 160؛ رابحي عزيزة، المرجع السابق، ص 307؛ محمد فهاد الشلالدة، عبد الفتاح أمين ربعي، الجرائم الإلكترونية في دولة فلسطين المحتلة في ضوء التشريعات الوطنية والدولية، بحث مقدم إلى المؤتمر العلمي الحادي عشر حول الجرائم المعلوماتية، لكلية القانون، جامعة جرش، فلسطين، الأيام من 05 إلى 07 ماي 2015، ص 20، **نقلاً عن**: حمودة منتصر، المنظمة الدولية للشرطة الجنائية الانتربول، دار الفكر الجامعي، الاسكندرية، 2008، لم يشر للصفحة؛ مختار شبيلي، التعاون الدولي في مكافحة الجريمة المنظمة، رسالة لنيل شهادة دكتوراه في القانون العام، تخصص القانون الجنائي والعلوم الجنائية،كلية الحقوق، جامعة الجزائر 01، السنة الجامعة 2011-2012، ص 190؛ عائشة عبد الحميد، دور المنظمة الدولية للشرطة الجنائية (الأنتربول) في محاربة الإجرام الاقتصادي الدولي، مجلة جيل حقوق الإنسان، مركز البحث العلمي، طرابلس، لبنان، العام الخامس، العدد الرابع والثلاثين (34)، أكتوبر 2018، ص 70.

2 أهم المحطات التاريخية المميزة لمنظمة الأنتربول في سنة 1914 انعقاد المؤتمر الدولي الأول للشرطة الجنائية في موناكو (بحضور 23 بلد)، وفي سنة 1923 تم تأسيس اللجنة الدولية للشرطة الجنائية واتخاذ فينا مقرر لها، ثم في: 1946 تم إعادة تشكيل المنظمة بعد

الوطنية، والمحطات الإقليمية، والمحطة المركزية الموجودة في الأمانة العامة للانتربول[1]. وتضم المنظمة الدولية للشرطة الجنائية (الانتربول) حالياً حوالي 194 بلداً عضواً، تستضيف كل دولة مكتباً مركزياً وطنياً للانتربول (NCB)، يربط الشرطة الوطنية بشبكة الانتربول العالمية[2].

وعند البحث عن علاقة بعض الدول بالمنظمة الدولية للشرطة الجنائية، نجد أن الجزائر انخرطت في المنظمة مباشرة بعـد الاستقلال؛ أي في سنة 1963، وقد جسد المشرع الجزائري تلك العلاقة في العديد من النصوص القانونية؛ كقانون الإجراءات الجزائية من خلال مفهوم إجراءات التسليم وآثاره وحركة العبور، سواء طبقاً لاتفاقية أو بطريقة دبلومـاسية، وهذا بعد انجاز الطلبات الـواردة في شكل استمارات مـن الانـتربـول أو بضمانات دولية[3].

أما عن المملكة المغربية فقد عملت الأجهزة المغربية على إحداث المكتب المركزي الوطني بالرباط (National Rabat Bureau Centre) والذي يعد بمثابة همـزة وصل بيـن المغرب والانتربول[4]، وفي مصر تم إنشاء المكتب المركزي المصري للشرطة الجنائية الدولية بموجب قرار وزير الداخلية سنة 1948، ويعد المكتب أحد أجهزة مصلحة الأمن العام بوزارة الداخلية[5].

الحرب العالمية الثانية وجُعل مقرها بباريس كما تم إنشاء منظومة النشرات الحمراء الأولى، وفي 1956 اعتمدت تسمية المنظمة الدولية للشرطة الجنائية للانتربول، ليتم الاعتراف بها كمنظمة حكومية دولية من قبل الأمم المتحدة في 1971، أما في سنة 1989 تم نقل مقر الأمانة العامة من مدينة باريس إلى ليون بفرنسا. وفي سنة 2004 اعتماد ممثل الأنتربول الخاص لدى الأمم المتحدة بنيويورك. وفي سنة 2008 تم اعتماد ممثل الأنتربول الخاص لدى الاتحاد الأوروبي في بروكسل. للاستزادة يُنظر الموقع الرسمي للمديرية العامة للأمن الوطني الجزائري: *http://www.algeriepolice.dz/* ، تاريخ الاطلاع: 2019/12/28.

1LIANG Jiansheng, *Criminalité informatique*, Diplôme professionnel supérieur en Sciences de l'information et des Bibliothèques, Rapport de stage, Ecole Nationale Supérieure des Sciences de 1'information et des Bibliothèques, 1999. P 59.

2 للإطلاع على المزيد بالإمكان الرجوع لموقع الانتربول التالي: https://www.interpol.int/ar/3/10 , le 17/12/2019.

3 رابحي عزيزة، المرجع السابق، ص 309، **نقلاً عـن**: قادري أعمر، أطر التحقيق، دار هومة للنشر والتوزيع، الجزائر، 2013؛ ص ص 302-303؛ **وانظر كذلك**:

- Meriem ALI MARINA, Pour que le crime ne reste pas impuni, Police judicaire, Voir : *http://www.eldjazaircom.dz/index .php?id_rubrique=313&id_article=3745* , N° 114 - Juin 2018.

4 عبد السلام بنسليمان، المرجع السابق، ص 205.

5 عادل عبد العال إبراهيم خراشي، إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديدة، الازاريطة، الإسكندرية، مصر، 2015، ص 29، **نقلاً عـن كل من**: محمد نيازي حتاتة، حماية الأمن العام ومكافحة الجريمة على المستوى الوطني والإقليمي والدولي، الظواهر الإجرامية الوطنية والعالمية وصكوك المبادئ الإرشادية العالمية والاتفاقيات الدولية، الجزء

البند الأول: مهام المنظمة الدولية للشرطة الجنائية (الانتربول).

للمنظمة الدولية للشرطة الجنائية (الانتربول) عدة مهام كونها من أبرز المنظمات في مكافحة الجرائم الدولية العابرة للحدود في العالم، فقد وجدت الانتربول لتحقيق عدة أمور، منها: أولاً- التعاون الدولي لمواجهة الإجرام الدولي المتزايد باستمرار، وثانياً- تأمين الاتصال الرسمي بين رجال الشرطة في مختلف أرجاء العالم، بغية تبادل الخبرات والأفكار والمناهج وأساليب العمل في مجالات الأمن المختلفة منذ وجدت الدول القومية (الوطنية) التي تفصل بينها الحدود الجغرافية والصناعية، وارتباط الظاهرة الإجرامية برغبة المجرم للانتقال من مكان إلى آخر، ابتعاداً عن مسرح جريمته، واختفائه عن نظر السلطات الأمنية[1]، ولأجل تحقيق أهدافها تقوم الانتربول بتجميع البيانات والمعلومات المتعلقة بالجريمة والمجرم، من مختلف المكاتب المركزية الوطنية للشرطة الجنائية في الدول الأعضاء، حيث تقوم المنظمة بعد تجميعها للبيانات والمعلومات بتنظيمها لتُكون بها أرشيفاً متكاملاً يمكن الرجوع إليه عند الحاجة[2].

ومن المهام التي يقوم بها الانتربول فيما يخص الجريمة الإلكترونية تعقب مجرمي المعلوماتية عامة وشبكة الإنترنت خاصة، وتعقب الأدلة الرقمية وضبطها والقيام بعملية التفتيش العابر للحدود لمكونات الحاسب الآلي المنطقية والأنظمة المعلوماتية وشبكات الاتصال بحثا عن ما قد تحويه من أدلة وبراهين على ارتكاب الجريمة الإلكترونية[3]، إذ يتم تبادل المعلومات من خلال منصة الإتصالات الآمنة التي تعمل على مدار الساعة وطوال أيام الأسبوع من أجل تسهيل التحقيقات

الأول، مطبعة كلية الشرطة، القاهرة، 1994-1995، ص 299؛ عبد الفتاح محمد سراج، النظرية العامة لتسليم المجرمين، رسالة دكتوراه، حقوق الإسكندرية، 1999، ص 296.

1 مجاهدي خديجة، إستراتيجية المنظمة الدولية للشرطة الجنائية في مكافحة الجريمة المنظمة، مجلة الدراسات القانونية، مخبر السيادة والعولمة، جامعة يحي فارس، المدية الجزائر، المجلد الثاني، العدد الثاني، جوان 2015، ص 02؛ **نقلاً عن**: ماجد ابراهيم على، قانون العلاقات الدولية، دراسة في إطار القانون الدولي والتعاون الدولي الأمني، دار النهضة العربية، القاهرة، 1998، ص 371؛ وكذا مظهر جبران غالب المصري، التعاون الدولي في مكافحة الجريمة المنظمة، رسالة ماجيستير، كلية الحقوق، جامعة اسيوط، مصر، 2008، ص 228.

2 مجاهدي خديجة، نفس المرجع، ص 09.

3 حسين بن سعيد بن سيف الغافري، المرجع السابق، ص 507؛ بومامي العباس، المرجع السابق، ص 148، **نقلاً عن**: جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، 1998، ص 75.

المتعلقة بالجرائم الإلكترونية التي تجريها وكالات وزارة العدل ووزارة الأمن الوطني[1]، كما تعمل منظمة الانتربول على تغيير استراتيجية مكافحة الجريمة الإلكترونية تبعاً للبيئة المحيطة حتى تعطي تلك الإستراتيجية ثمارها، والتي تهدف أساساً إلى تحسين دور الانتربول في هيكل الأمن العالمي، وكذلك تعزيز العلاقة بين الانتربول ومنظمات الشرطة الإقليمية وغيرها من المنظمات الدولية، لسد الثغرات وزيادة التكامل بينها، وذلك بتقييم التهديدات وتحليلها، ورصد الاتجاهات للكشف عن جرائم الإنترنت والمجرمين الإلكترونيين ومجموعات الجريمة الإلكترونية، وتسهيل الوصول إلى البيانات المرتبطة بالهجمات الإلكترونية من خلال حسن استعمال الأدوات والأدلة الإلكترونية، وإشراك الشركاء ذوي الصلة لتوحيد عملية جمع البيانات وتعزيز استغلالها، والجمع القانوني للقرائن الرقمية، والحفاظ على الأدلة الإلكترونية، وجعلها واضحة ومقبولة للاستفادة منها في التحقيقات والملاحقات القضائية، وحتى تكون ذات أهمية عند عرضها أمام الجهات القضائية،كما تقوم منظمة الانتربول على تحسين إمكانية التشغيل البيني والتنسيق العالمي وتشجيع المواءمة التشريعية التي تعد من بين المشاكل العويصة التي تواجه عملية مكافحة الجرائم الإلكترونية[2].

ومن بين المهام المهمة جداً والتي تقوم بها المنظمة الدولية للشرطة الجنائية (الانتربول)، عملية ضبط المجرمين[3] أو توقيفهم مؤقتاً إلى حين تسليمهم[4]، هذا إلى جانب قيامها –منظمة الانتربول–

1 شعبان أبو عجيلة عصارة، أبو المعالي محمد عيسى أبو المعالي، الرصد المبكر لخطر الجريمة، مجلة العلوم القانونية والشرعية،كلية القانون، جامعة الزاوية، ليبيا، العدد السادس (06)، يونيو 2015، ص 321؛ **وكذلك**:

- Sujit Raman, Chair, John P. Cronan, and athers, OP.CIT, p :104.

2 INTERPOL**, Résolution No 5, GA-2018-87-RES-05**: « RAPPELANT ÉGALEMENT la résolution AG-2016-RES-03 qui a approuvé le cadre stratégique 2017 - 2020 d'INTERPOL, lequel visait notamment à optimiser le rôle d'INTERPOL au sein de l'architecture de sécurité mondiale, ainsi qu'à renforcer la relation entre INTERPOL, les organisations de police régionales et les autres organisations internationales, pour combler les lacunes et accroître la complémentarité, » ; INTERPOL General Secretariat, GLOBAL CYBERCRIME, STRATEGY, - 200, quai Charles de Gaulle - 69006 Lyon - France - www.interpol.int**,** February 2017, p : 03.

3 نادية دردار، الجهود الدولية لمكافحة الجريمة، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2017، ص.ص: 149–150.

4 يمكن الرجوع إلى الإتفاقيات التالية: لاتفاقية المتعلقة بتسليم المجرمين بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وحكومة الجمهورية الايطالية، المؤرخة في 04 محرم عام 1426 الموافق 13 فبراير 2005، الموقعة بالجزائر في 22 جويلية سنة 2003، المصادق عليها بالمرسوم الرئاسي رقم 05–74، الصادرة في الج.ر.ج رقم 13 المؤرخة في 16 فبراير سنة 2005؛ الاتفاقية المتعلقة بتسليم المجرمين بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وحكومة المملكة المتحدة لبريطانيا العظمى وإيرلندا الشمالية، المؤرخة

بتنظيم دورات تكوينية لتبادل الخبرات وتقديم الدعم الفني لأجهزة الشرطة، والمصالح الأمنية الدولية حتى يتسنى إعطاء بعد دولي لعملها[1]، وإقامة تبادل منظم للبيانات المتعلقة بالتهديدات الإلكترونية من أجل تعـزيز أنشطة الأمن السيبراني الذي يضطلـع به الانتـربول ودوله الأعضاء، حيـث قال: (وانغ بينغ) الباحث في معهد شارهار بشنغهاي في إطار اختتام أعمال اجتماع الجمعية العامة 86 للشرطة الجنائية الدولية" انتربول" التي تمت بمشاركة نحو ألف (1000) شخصية من كبار قادة الشرطة والسياسيين من 156 دولة في العاصمة الصينية بكين: "إن الجرائم السيبرانية ذات طبيعة عابرة للحدود، وذلك يحتم على كافة الدول التعاون مع منظمة الانتربول الدولية، لوضع حد لهذه الظاهرة، وهو ما تقوم به الصين الآن، حيث تمكنت في السنوات الأخيرة من استعادة أكثر من 2000 متهم في إطار الحملة التي أطلقها الرئيس الصيني عام 2013، وعرفت باسم "مطاردة النمور"، مُنوهاً بأن ذلك تم بفضل تعاون وتنسيق الصين مع الشرطة الجنائية الدولية[2].

البند الثاني: دور الانتربول في مكافحة الجريمة الإلكترونية.

تمثل المنظمة الدولية للشرطة الجنائية (الانتربول) همزة وصل بين مختلف أجهزة الشرطة عبر العالم، ومع المنظمات الإقليمية والدولية الأخرى من خلال موقعها الهام الذي يسمح لها بتعزيز قدرتها على منع الجريمة وتحديد هوية المجرمين واعتقالهم[3]. ولأن الجريمة الإلكترونية تعد إحدى أكبر التحديات التي تواجه مختلف دول العالم، فإن منظمة الانتربول قامت ومازالت تقوم ببذل مجهودات من أجل مكافحتها، والأمثلة على ذلك كثيرة، نذكر منها على سبيل المثال: ما حصل في الجمهورية اللبنانية، حين تلقت النيابة العامة اللبنانية برقية من الانتربول في ألمانيا، تم على إثرها

في 20 ذي القعدة عام 1427 الموافق 11 ديسمبر 2006، الموقع بلندن في 11 جويلية سنة 2006، المصادق عليها بالمرسوم الرئاسي رقم 06-464، الصادرة في الج.ر رقم 81 المؤرخة في 13 ديسمبر سنة 2006؛ اتفاقية تسليم المتهمين والمحكوم عليهم بين الجمهورية الجزائرية الديمقراطية الشعبية والمملكة العربية السعودية، المؤرخة في 04 شوال عام 1436 الموافق 20 جويلية سنة 2015، الموقعة بالرياض في 13 ابريل سنة 2013، المصادق عليها بالمرسوم الرئاسي رقم 15-192، الصادرة في الج.ر رقم 43 المؤرخة في 12 اوت سنة 2015.

1 بن عمر الحاج عيسى، المرجع السابق، ص 262.

2 علي أبو مريحيل، القرصنة الإلكترونية تتصدر أعمال الجمعية العامة للإنتربول، تقرير متاح على موقع الجزيرة نت: 29 سبتمبر 2017، على الموقع الإلكتروني: *https://www.aljazeera.net/news/reportsandinterviews/*، تاريخ الإطلاع: 2020/06/29.

3 INTERPOL General Secretariat, *GLOBAL CYBERCRIME, STRATEGY*, - 200, quai Charles de Gaulle - 69006 Lyon - France - www.interpol.int, February 2017, p : 04.

توقيف أحد الطلبة الجامعيين من قبل القضاء اللبناني بتهمة إرسال صور إباحية لقاصر دون العشرة أعوام من موقعه على شبكة الإنترنت[1]، وفي شهر مارس من العام 2008 قدم الانتربول مساعدة "لكولومبيا" -إثر طلبها ذلك-، بأن قام خبراء متخصصين في الأدلة الجنائية التابعين لمنظمة الانتربول بتحليل جنائي لحواسيب ومعدات حاسوبية تم ضبطها عند مداهمة أحد مخيمات القوات المسلحة الثورية الكولومبية في إطار عملية لمكافحة المخدرات والإرهاب والتي أصبحت الجريمة الإلكترونية محركها الأساسي، حيث استخدموا خلال عملية التحليل أحدث المعدات تطوراً مما مكنهم من تحليل كمية هائلة من البيانات المشفرة وغير المشفرة تحصلوا منها على أدلة إلكترونية مكنت من إثبات الوقائع الإجرامية[2].

وفي إطار عملية نسقها الإنتربول في منطقة آسيا والمحيط الهادي سميت بـ: First Light 2015 شاركت فيها 23 بلداً، تم خلالها اعتقال أكثر من 500 شخص وإغلاق 15 مركز للاتصال، استهدفت هذه العملية أشخاص قاموا بعمليات احتيال ارتكبت بواسطة الهاتف والبريد الإلكتروني، قدرت قيمتها بملايين الدولارات[3]. وفي سنة 2016 قام الانتربول والهيئة النيجيرية للجرائم الاقتصادية والمالية في إطار عملية مشتركة بالقبض على زعيم شبكة إجرام دولية، في نيجيريا اسمه "مايك" اشترك معه ما لا يقل عن أربعين (40) شخصاً من نيجيريا وماليزيا وجنوب إفريقيا، قاموا بآلاف عمليات الاحتيال عبر الإنترنت، والتي استهدفت مئات الضحايا في جميع أنحاء العالم مستعملين مختلف مخططات الاحتيال التجارية عبر البريد الإلكتروني. وفي السنة الموالية؛ أي سنة 2017 أطلقت منظمة الانتربول عملية سمتها (Blackwrist) -نسبة إلى ارتداء أحد الجناة لسوار- اكتشفت خلالها وحدة مكافحة الجرائم المرتكبة ضد الأطفال التابعة للمنظمة صور وفيديوهات لاعتداءات جنسية ارتكبت ضد أحد عشر (11) طفلاً جميعهم دون سن الثالثة عشرة

1 أمير فرج يوسف، الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر، المرجع السابق، ص 428؛ لورنس سعيد الحوامدة، المرجع السابق، ص 28؛ حسين بن سعيد بن سيف الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت"دراسة مقارنة"، دار النهضة العربية، القاهرة، مصر، سنة 2009، ص 238 وما بعدها.

2 الانتربول، مكافحة الجريمة في القرن الحادي والعشرين (2000-2010)، ليون، فرنسا، 2010، ص 15؛ عبد الحميد العبادي، الجرائم الإلكترونية، مجلة الدراسات المالية والمصرفية، السنة الثالثة والعشرون، العدد الأول، الأردن، مارس 2015، ص 05: من الأساليب المستعملة للقيام بالجرائم الإلكترونية: الهندسة الاجتماعية والتي تتم "من خلال الاتصال بالعملاء أو الموظفين في الأماكن المستهدفة للحصول على كلمات عبور ومعلومات أخرى مفيدة".

3 محمود مدين عبد الرحمان، المرجع السابق، ص 116.

(13) سنة، قام بها عدة أشخاص من بينهم شخص يدعى (Montri Salangam) يقيم في تايلند وصاحب الموقع الذي كانت تبث منه تلك الصور والفيديوهات، وهو الرجل الذي شوهد يعتدي على أولئك الأطفال الذين كان من بينهم أحد أقاربه. وفي شهر جوان سنة 2018، حكمت المحاكم التايلندية على ذلك المجرم بالسجن مدة 146 سنة لقيامه باغتصاب الأطفال وحيازته وترويجه لمواد الاعتداء الجنسي عليهم والاتجار بالبشر[1].

الفرع الثاني: التعاون الدولي ودوره في مكافحة الجريمة الإلكترونية.

إن الوقاية من الجريمة ووقف الزيادة غير الطبيعية لمعدلاتها في المجتمع، بالإضافة إلى التقليل من تكلفتها البشرية والمادية، والسعى بشكل مستمر للخفض من معدلاتها شيئا فشيئاً يعد ذلك عملاً إستباقياً لتقليل وقوع الفعل الإجرامي[2]، فبالاضافة إلى الآليات التي تم التعرض إليها توجد آليات أخرى لا تقل أهمية عن سابقاتها؛ ألا وهي الآليات الاستباقية لمكافحة الجريمة الإلكترونية والتي يعد التعاون الدولي إحداها؛ فهو: "تبادل العون والمساعدة وتضافر الجهود المشتركة بين دولتين أو أكثر لتحقيق نفع أو خدمة مشتركة سواء عالميا أو إقليميا"[3]، كما أنه كل ما تقدمه سلطات دولة لدولة أخرى من مساعدة وعون في سبيل ملاحقة الجناة بهدف معاقبتهم على جرائمهم، وذلك من خلال تدابير وقائية تستهدف الصيغة غير الوطنية للجريمة، وتستجمع الأدلة بمختلف الطرق، وهو ما يستغرق وقتاً، ويتطلب إمكانيات لا تملكها السلطات القانونية لدولة واحدة، ما لم تدعمها وتساندها جهود السلطات القانونية في الدولة الأخرى[4]، فهو يساعد في تنفيذ القرارات التعاونية التي من شأنها وضع حد للأنشطة غير القانونية خاصة المرتكبة عبر الإنترنت[5].

---

1 للإطلاع على المزيد بالإمكان الرجوع لموقع الانتربول التالي: https://www.interpol.int/ar/1/1/2019/50-9

2 محمد شنة، جرائم العنف الأسري وآليات مكافحتها في التشريع الجزائري، أطروحة مقدمة لنيل درجة دكتوراه العلوم في الحقوق، تخصص علم الإجرام وعلم العقاب، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر- باتنة 01، السنة الجامعية 2017-2018، ص 171.

3 محمد محمد الألفي، المرجع السابق، ص 16.

4 عادل عبد العال إبراهيم خراشي، المرجع السابق، ص 08، **نقلاً عن**: سالم محمد سليمان الأوجلي، أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوضعية، رسالة دكتوراه، حقوق عين شمس، القاهرة، 1997، ص 425.

5 Myriam Quéméner, *Le rapport sur la cybercriminalité et la protection des internautes*, La base de données juridique des Éditions Dalloz, France, AJ Pénal 2014, p:316.

البند الأول: صعوبات تعيق التعاون الدولي في مكافحة الجريمة الإلكترونية.

أثبت الواقع العملي أن الدولة لا تستطيع لوحدها وبمجهوداتها الخاص القضاء على الجرائم العابرة للحدود، وبالأخص الجريمة الإلكترونية، لذا يعد التوافق بين السياسة الجنائية الداخلية والسياسة الجنائية الدولية مقدمة طبيعية لتحقيق نتائج إيجابية في مكافحة الجريمة العابرة للحدود، والتي مثلت شبكة الإنترنت إحدى صورها المستحدثة، مما يوجب تعاونًا دوليًا في مكافحتها نظراً لطابعها المتخطي لحدود الدولة الواحدة والمتسمة بالبعد عبر الوطني[1]، وأحسن سبيل لذلك اللجوء لآليات التعاون الدولي في هذا الخصوص، بالاستعانة بالمعاهدات الدولية كأساس تعاوني في مكافحة الجرائم الإلكترونية، ومن بين تلك المعاهدات؛ نجد معاهدة بودابست لمكافحة الجرائم الإلكترونية[2]، والتي تعد المرجع القانوني لمكافحة هذه الجريمة، إذ ساهمت في التقليل من التحديات الكبيرة التي تقف في وجه التعاون الدولي الفعال، ومنها ما يتعلق بالأدلة الإلكترونية في المسائل الجنائية، والتباين الموجود في مختلف ضمانات التعاون الدولي[3]؛ لذا نجد أن دولاً كثيرةً صادقت على هذه الاتفاقية؛ كفرنسا والمملكة المغربية، والولايات المتحدة الأمريكية والتي دخلت حيز النفاذ لديها في الفاتح (01) من شهر يناير سنة 2007.[4]

لقد أدى اختلاف المفاهيم المتعلقة بتعريف الجرائم الإلكترونية بين تشريعات الدول إلى صعوبة وضع قانون موحد لمكافحتها، كما تواجه عملية مكافحة هاته الجريمة عدة صعوبات في التعاون الدولي[5]، نذكر منها على سبيل المثال لا الحصر ما يلي:

---

1 محمد أمين أحمد الشوابكة، المرجع السابق، ص 07.

2 سعيدي سليمة، حجاز بلال، المرجع السابق، ص 146.

3 فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، دراسة شاملة عن مشكلة الجريمة السيبرانية والتدابير التي تتَّخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدِّي لها، فيينا، 25-27 فبراير 2013. (UNODC/CCPCJ/EG.4/2013/2)، ص 16.

4 أحمد عبد اللاه المراغي، الجريمة الإلكترونية ودور القانون الجنائي في الحد منها دراسة تحليلية تأصيلية مقارنة، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، مصر،2017، ص 126.

5 عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكومبيوتر والانترنت، الطبعة الثالثة، دار الجامعة الجديدة، مصر، 1999، ص 102؛ شوقي يعيش تمام، عزيزة شبري، تفعيل مبدأ عالمية النص الجنائي في التصدي للجريمة المعلوماتية، مجلة الاجتهاد القضائي، مخبر أثر الاجتهاد القضائي على حركة التشريع، جامعة محمد خيضر بسكرة، الجزائر، العدد الخامس عشر(15)، سبتمبر 2017، ص 99.

1- **عدم وجود نموذج موحد للنشاط الإجرامي**: فالأنظمة القانونية التي وضعت من أجل مكافحة الجرائم الإلكترونية يختلف وصفها للأفعال الإجرامية التي تتم بها هذه الجرائم، نظراً لاختلاف العادات والتقاليد والديانات والثقافات وغيرها من مجتمع لآخر، مما أنتج اختلافاً في السياسات التشريعية وخاصة الجنائية منها، فقد نجد أنواعاً من الجرائم الإلكترونية مباحة في نظم قانونية معينة ومجرمة في أخرى[1]، فبغير التعاون الدولي في مجال التشريع العقابي سيزداد معدل ارتكاب الجرائم الإلكترونية، ويطمئن مرتكبوها من عدم إمكانية ملاحقتهم، إذ سيكون من السهل عليهم التنقل من دولة تجرم الفعل إلى أخرى تبيح قوانينها ذلك الفعل[2].

2- **تنوع واختلاف النظم القانونية الإجرائية**: والمتمثلة خاصة في طرق التحري والتحقيق والمحاكمة، كما هو الحال بالنسبة لطرق جمع الأدلة الإلكترونية، فهذه الإجراءات قد يكون لها قيمتها القانونية في دولة ما وعديمتها في دولة أخرى مما ينجر عنه عدم فائدة تلك الإجراءات التي قد تكلف الدولة القائمة بها مجهودات بشرية وتكاليف مادية كبيرة، ليحصل منها المجرم الإلكتروني في الأخير على فرصة للإفلات من العقاب[3] في حالة عدم جدواها والاعتداد بها أمام القضاء، وتعد قضية الدودة الحاسوبية (Love Bug) أحسن مثل على ذلك، حيث تم إعداد هذا الفيروس في الفلبين سنة 2000، وعند إطلاقه أصيب على إثره الملايين من الحواسيب في جميع أنحاء العالم، ولكن التحقيقات لم تجر حينها بسبب أن ذلك الفعل لم يكن مجرماً آنذاك في الفلبين.[4]

---

1 بدر عدنان الخبيزي، الجرائم الإلكترونية في المجتمع الكويتي (تحليل سوسيولوجي)، رسالة مقدمة لنيل درجة الدكتوراه في علم الاجتماع، قسم اجتماع، كلية الآداب، جامعة حلوان، مصر، سنة 2014، ص 178؛ يوسف حسن يوسف، المرجع السابق، ص 186؛ حليمة بن حفو، المرجع السابق، ص 208؛ فندوشي ربيعة، الصورة عبر الانترنت التجاوزات والحماية، مجلة البحوث والدراسات العلمية، المركز الجامعي الدكتور يحي فارس، المدية، الجزائر، العدد الخامس (05)، جويلية 2011، ص 329؛ محمد نصر محمد، المسئولية الجنائية لانتهاك الخصوصية المعلوماتية "دراسة مقارنة"، الطبعة الأولى، مركز الدراسات العربية للنشر والتوزيع، مصر، 2016، ص 111؛ حسام محمد نبيل الشنراقي، المرجع السابق، ص 733.

2 عادل عبد العال إبراهيم خراشي، المرجع السابق، ص76، **نقلاً عن**: محمد محمد عزت، الحماية الجنائية والإجرائية الاعتداء على المصنفات والحق في الخصوصية والكمبيوتر والانترنت في نطاق التشريعات الوطنية والتعاون الدولي، الطبعة الأولى، دار النهضة العربية، 2007، ص 344.

3 أيمن عبد الحفيظ، المرجع السابق، ص 451؛ محمود أحمد عبد القادر قشطة، التعاون الدولي في مكافحة الجريمة المعلوماتية، رسالة مقدمة لنيل درجة الدكتوراه في الدراسات القانونية، معهد البحوث والدراسات العربية، القاهرة، مصر، 2015، ص 283؛ درار نسيمة، المرجع السابق، ص 299.

4 صغير يوسف، المرجع السابق، ص 134، من مؤتمر الامم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية، ص 06.

3- **عدم وجود قنوات اتصال:** من أهم الأهداف المرجوة من التعاون الدولي الحصول على معلومات وبيانات متعلقة بالجريمة والمجرم الإلكتروني، ولتحقيق هذا الهدف كان لزاماً أن يكون هناك نظام إتصال يسمح للجهات القائمة على التحقيق بالإتصال بجهات أخرى خاصة الأجنبية منها لتسهيل عملية جمع الأدلة والمعلومات المهمة المطلوبة بخصوص الجرم المرتكب، ولكن غياب مثل هذا النظام يعني عدم القدرة على جمع الأدلة الإلكترونية والمعلومات التي ستساعد على مكافحة الجريمة الإلكترونية والمجرم الإلكتروني[1].

4- **مشكلة الإختصاص في الجرائم الإلكترونية:** من أكبر المشاكل التي تواجه مكافحة الجريمة الإلكترونية، إذ يتنج لنا ما يسمى بتنازع الاختصاص بين الدول، وإفلات المجرمين الإلكترونين بجـرائمهم الإلكترونية التي تتنـازعها مبـادئ الإختصاص التقليدية؛ كمبدأ الإقليمية ومبدأ الشخصية ومبدأ العينية[2].

5- **التجريم الـمزدوج:** يعتبر نظام تسليم المجرمين من الأنظمة التي تساهم بصورة ايجابية وفعالة في تحقيق الاستقرار العالمي، ودفاع دول العالم متضامنة ضد الجريمة في سبيل تحقيق مصالحها المشتركة[3]، إلا أن التجريم المزدوج الذي يفـرض في تسليم المجرمين[4] يعد عقبة كبيرة أمام

1 محمد أحمد سليمان عيسى، التعاون الدولي لمواجهة الجريمة الإلكترونية، المجلة الأكاديمية للبحث القانوني، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميره، بجاية، الجزائر، المجلد الرابع عشر (14)، العدد الثاني (02)، 2016، ص 60.

2 بدر عدنان الخبيزي، المرجع السابق، ص 179.

3 عـبد الرحمن فتحي عبد الرحمن سمحان، تسليم المجرمين في ظـل قواعد القانون الـدولي، الطبعة الأولى، دار النـهضة العربية، القاهرة، 2012، ص 10.

4 يقصد به أن يكون الفعل المطلوب التسليم بشأنه معاقبا عليه في قوانين كلتا الدولتين الطالبة التسليم والمطلوب إليها ذلك، وإذا لم يتحـقق هـــذا الشرط بالنسبة إلى الدول التي تتمسك به فإنه يرقض التسليم لعـدم توافر شرط من شروطه. **ينظر في ذلك:** زياد محمد جفال، تسليم المجرمين كأحد آليات جامعة الدول العربية لمكافحة الإرهاب وموقف المشرع الإماراتي، مجلة جامعة الشارقة للعلوم القانوني، جامعة الشارقة، الإمارات العربية المتحدة، العدد الأول (01)، المجلد السادس عشر (16)، يونيو 2019، ص 562، **نقلاً عن:** هشام صادق وحفيظة السيد الحداد، دروس في القانون الدولي الخاص والتحكيم، الطبعـة الثالثة، الاسكندرية، بدون سنة؛ عرفت المحكمة العليا الامريكية التجريم المزدوج على أنه "مبدأ يقضي بأنه في كل حالات تسليم المجرمين فإن الفعل الذي طلب من أجله التسليم يجب أن يكون جريمة في قوانين كلتا الدولتين". **ينظر في ذلك:** آلاء محمد صاحب، تبارك ناصر عزوز الزامليّ، ماهية التجريم المزدوج في نظام تـسليم المجرمين دراسة مقارنة، مجلة الكوفة للعلوم القانونية والسياسية، كلية القانون، جامعة الكوفة، العراق، المجلد الأول، العدد (44)، 2020، ص 354، **نقلاً عن:** خالد محمد القاضي، تأملات في القانون الدولي دراسات وابحاث ومقالات، الطبعة الأولى، دار النهضة العربية، القاهرة، 2013، ص 22.

التعاون الدولي في مجال تسليم المجرمين[1] بالنسبة للجريمة الإلكترونية وغيرها من الجرائم، فكما سبقت الإشارة إليه فإنه من بين عقبات التعاون الدولي عدم وجود إتفاق حول الوصف الإجرامي الذي تنعت به الجريمة الإلكترونية.

6- **الصعوبات الخاصة بالمساعدات القضائية الدولية:** تعرف المساعدة القضائية بأنها: "كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم"[2]. وتتخذ المساعدة القضائية عدة صور نذكر منها:

أ. **تبادل المعلومات:** والذي يشمل تقديم المعلومات والبيانات والوثائق والمواد الاستدلالية والسوابق القضائية للجناة وغيرها التي تطلبها سلطة قضائية أجنبية حين النظر في جريمة ما، وجهت فيها الاتهامات لشخص لا يتواجد تحت سلطتها، ومثالها ما نجده في البند (و)، والبند (ز) من الفقرة الثانية من المادة الأولى من معاهدة الأمم المتحدة النموذجية لتبادل المساعدة في المسائل الجنائية، والبند الأول من المادة الرابعة (04) من معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي. وكذلك المادة الأولى من اتفاقية الرياض العربية للتعاون القضائي[3].

ب. **نقل الإجراءات:** ويقصد به قيام دولة ما بناءً على اتفاقية أو معاهدة باتخاذ إجراءات جنائية بصدد جريمة ارتكبت في إقليم دولة أخرى ولمصلحة تلك الدولة متى توافرت

---

1 كانت حقبة الستينات هي بداية تاريخ ما يطلق عليهم المخترقون، حيث كان تصميم برنامج (UNIX) عاملا مساعد لهم، نظر للسرعة التي كان يتميز بها أنا ذاك، ومن أشهرهم (دينيس) و(ريتشي) و(كين تومسون). في تلك الحقبة أيضاً تم بنجاح إنتاج الكمبيوتر الشخصي، فتزامنت معه محاولة أولائك المخترقون في اكتشاف طريقة عمل ذلك الجهاز، وماهية البرامج المثبتة عليه وكيفية اختراقها، لذا اعتبرت الفترة الزمنية من عام 1979 وحتى عام 1989 هي العصر الذهبي لهؤلاء المخترقون. من خلال التواريخ السابق ذكرها ومتابعة الأحداث المتولية يلاحظ أن كثير من المجرمين افلتوا من العقاب نتيجة عدم وجود قوانين تنظم هذا النوع من الإجرام، أو لأن القانون لا يشمل فئة عمرية معينة، ومنها القانون الذي صدر في الولايات المتحدة الأمريكية عام 1986 لمعاقبة الهاكرز بالسجن، إلا أن ذلك القانون لا يعاقب الأحداث، ففي حادثة قام فيها طالب جامعي متخرج حديثا يدعى (روبرت موريس) بإطلاق دودة ذات نسخ ذاتي على نظام (UNIX) السالف الذكر، بغرض التجربة والاختبار، وكانت شبكة الحكومة الأمريكية (ARPA NET) هي المستهدفة، ولكن روبرت فقد السيطرة على الدودة، فانتقلت إلى حوالي (6000) كمبيوتر على نفس الشبكة، ليوضع بعدها تحت المراقبة لثلاث سنوات وغرامة قدرها (10) آلاف دولار. **انظر في ذلك:** منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، المرجع السابق، ص: 48.

2 وردة شرف الدين، المرجع السابق، ص89، **نقلاً عن:** سالم محمد سليمان الأوجلي، أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوضعية، دكتوراه الحقوق، جامعة عين شمس، 1997، ص 425؛ إيهاب السنباطي، المرجع السابق، ص 42.

3 يوسف حسن يوسف، المرجع السابق، ص 150.

شروط معينة من أهمها أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والدولة المطلوب منها نقل الإجراءات، بالإضافة إلى شرعية الإجراءات المطلوب اتخاذها؛ بمعنى أن تكون تلك الإجراءات مقررة في قانون الدولة المطلوب منها القيام بها عن ذات الجريمة، وقد أقرت العديد من الاتفاقيات الدولية والإقليمية، هذا النوع من المساعدة، كمعاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية في المادة 22 منها، واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لسنة 2000 في المادة 21 منها، وذات الشيء نجده في معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي لسنة 1999 في المادة التاسعة (09) منها، وأيضاً المادة 16 من النموذج الاسترشادي لاتفاقية التعاون القانوني والقضائي الصادر عن مجلس التعاون الخليجي[1].

ج. **الإنابة القضائية الدولية:** ويقصد بها ذلك الطلب الذي تقدمه الدولة الطالبة إلى دولة أخرى مطلوب منها إتخاذ إجراء قضائي من إجراءات الدعوى الجنائية، لما لذلك لإجراء من أهمية في تلك الدعوى القائمة، أو لتعذر القيام به نتيجة الاصطدام بالسيادة الدولية، ولأجل تسهيل تلك الإجراءات الجنائية بين الدول، جاءت الإنابة القضائية كحل يكفل إجراء التحقيقات اللازمة، كالتفتيش وسماع الشهود وغيرها، ولكن نظراً لتعقد إجراءات الإنابة القضائية[2] والفوارق الإجرائية فيها نتيجة نقص الموظفين المدربين،

1 تنص المادة (09) من معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي، اعتمدت من قبل مؤتمر وزراء الخارجية دول المنظمة المنعقد في أواغادوغو المنعقد خلال الفترة من 28 جوان إلى 01 جويلية 1999: "لكل دولة طرف أن تطلب إلى أية دولة أخرى متعاقدة القيام في إقليمها نيابة عنها بأي إجراء قضائي متعلق بدعوى ناشئة عن جريمة إرهابية وبصفة خاصة: 1- سماع شهادة الشهود والأقوال التي تؤخذ على سبيل الاستدلال. 2- تبليغ الوثائق القضائية. 3- تنفيذ عمليات التفتيش والحجز. 4- إجراء المعاينة وفحص الأشياء. 5- الحصول على المستندات أو الوثائق أو السجلات اللازمة أو نسخ مصدقة منها"، متاحة على الموقع الإلكتروني الموالي: *http://ww1.oic-oci.org/arabic/conventions /terrorism.htm*، والذي تم الاطلاع عليه في 2018/11/12. **للإستزادة يمكن الرجوع إلى:** خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص.ص: 407-408؛ سوزان نوري فقي محمد، المرجع السابق، ص 147.

2 خطوات المساعدة القضائية: لا تتحقق الا بواسطة ثلاث خطوات هي : 1- الطلب: تقدمه الدولة صاحبة الاختصاص الجنائي بالمحاكمة، عادة ما يتم تقديمه بالطرق الديبلوماسية كأصل عام، ولكسب الوقت أصبحت بعض الاتفاقات الدولية تسمح بان يتم الاتصال المباشر بين جهات العدل في الدولتين أو الدول المعنية. 2- فحص الطلب: يعود هذا الأمر للدولة التي ستقدم المساعدة، إذ تتحقق هذه الأخير من كون الواقعة المطلوب تحققها تعد جريمة وفقاً لقانون الدولة الطالبة، ووفقاً للاتفاق المبرم بين الدولتين. 3- تنفيذ المساعدة القضائية: ويتم ذلك وفقاً لقانون الدولة التي ستنفذها، ويستمد التنفيذ قوته من الاتفاقيات الدولية المبرم بين هته الدول، وأحياناً يكون ذلك وفقاً للمعاملة بالمثل"، **ينظر في ذلك:** عادل عبد العال إبراهيم خراشي، المرجع السابق، ص 31؛ علي

والصعوبات اللغوية التي يواجهونها[1]، أدى ذلك إلى تعقد الاستجابة وبطئها وهو ما لا يستجيب لطبيعة التعامل مع الجرائم الإلكترونية.

7- **الصعوبات الخاصة بالتعاون الدولي في مجال التدريب:** إن تدريب الجهات المختصة بالبحث والتحري ورجال العدالة هو شيء في غاية الأهمية، ففي كثير من الأحيان تكون بداية المكافحة من هذه النقطة، وإذ لم تكن البداية صحيحة فأكيد لن تكون النتيجة المتوصل اليها مرضية، فعملية التحري عن الجريمة الإلكترونية وضبط المجرم الإلكتروني والتحصل على الأدلة الإلكترونية ووضع الملف كاملاً أمام العدالة وقبوله من طرفها، هي سلسلة مترابطة إن فقدت حلقة منها فلن نستطيع إكمال دائرة مكافحة الجريمة الإلكترونية.

ولكن موضوع التدريب في هذا المجال تعتريه عدة صعوبات منها على سبيل المثال: النظرة السلبية لدى بعض القيادات الإدارية والمتدربين أنفسهم، والذين يرون أن هذه العملية التدريبية ما هي إلا مضيعة للوقت والمال، كما أن الفوارق الفردية التي نجدها في المتدربين، سيما في مجال تكنولوجيا المعلومات وشبكات الاتصال تعد عائقاً آخر أمام هذه العملية[2]، لذا يجب إعطاء هذه العملية مكانتها في المجال العملي ويجب إختيار المتدربين بناءً على كفاءاتهم التعليمية وطموحاتهم المهنية، دون المغالاة في الميزانية المالية المخصصة لهذه العملية.

البند الثاني: حلول للصعوبات التي تعيق التعاون الدولي في مكافحة الجريمة الإلكترونية.

تتعدد صور التعاون الدولي في المجال الجزائي؛ من تعاون تشريعي يهتم بتجريم الأفعال الإجرامية التي تمس بالنظام العام داخل الحدود الإقليمية للدولة وتهدد السلم والأمن الدوليين، إلى تعاون أمني يتم بين الأجهزة الأمنية لمختلف الدول بالتنسيق مع المنظمة الدولية في هذا المجال أحياناً أخرى، والتي يكون الهدف منها تبادل المعلومات وتحديد هوية الأشخاص المبحوث عنهم

شملال، المرجع السابق، ص 71. وبالإضافة إلى ذلك، توجد إنابة قضائية دولية، نصت عليها المادة 721 من ق.إ.ج.ج، ذلك أنه في حالات المتابعات الجزائية غير السياسية في بلد أجنبي تسلم الانابات القضائية الصادرة من السلطات الاجنبية بالطريق الدبلوماسي وترسل إلى وزارة العدل بالاوضاع المنصوص عليها في المادة 703 من ق.إ.ج.ج، وتنفذ وفقاً للقانون الجزائري ومبدأ المعاملة بالمثل. وفي هذا الإطار نص المشرع الجزائري في المادة 721 من قانون الإجراءات الجزائية على الإنابة القضائية في إطار العلاقات مع الدول الأجنبية على تنفيذ الإنابة القضائية إذا كان لها محل وفقا للقانون الجزائري، إلا انه يتم طلبها بالطريق الدبلوماسي الذي يُرسل إلى وزارة العدل.

1 عيسى سليم داود الزيدي، المرجع السابق، ص 125.

2 حسين بن سعيد بن سيف الغافري، المرجع السابق، ص 553.

ومتابعتهم للقبض عليهم وتسليمهم إلى الدول التي تُطالب بهم، ليمتد ذلك التعاون إلى تعاون قضائي يتخذ عدة أشكل كالإنابة القضائية، ونقل الإجراءات الجزائية، والمساعدة القضائية، والاعتراف بتنفيذ الأحكام الجزائية الأجنبية، وتسليم المجرمين أو نقل المحكوم عليهم[1].

ولأن التعاون الدولي في المجال الجزائي له أهمية كبيرة في مكافحة الجرائم فقد سعت الدول إلى توثيقه وتكثيفه من أجل مكافحة كل أشكال الإجرام وبالأخص الجرائم الإلكترونية التي تستلزم طبيعتها الخاصة إتخاذ الإجراءات المناسبة في الوقت الملائم كي لا تضيع الإدلة الإلكترونية وتندثر، لهذا تعد المعاهدات الدولية هي الأساس الذي يرتكز عليه التعاون الدولي في مجال مكافحة الجرائم الإلكترونية؛ وقد تم عقد العديد من المعاهدات التي تحث على التعاون الدولي في مجال مكافحة الجرائم الإلكترونية، ومنها معاهدة بودابست لمكافحة جرائم الإنترنت[2]، والإتفاقية العربية لمكافحة جرائم تقنية المعلومات من خلال مواد الفصل الرابع منها[3].

ولأجل القضاء على الصعوبات التي يواجهها التعاون الدولي، قامت مختلف الدول بتحديث تشريعاتها بما يسهل عملية مكافحة الجريمة الإلكترونية، كالقوانين الخاصة بحماية البيانات الشخصية، التوقيع الإلكتروني، حماية الملكية الفكرية، التجارة الإلكترونية، قانون الإجراءات الجزائية، الحماية من المضمون الضار[4]، وعلى إثر ذلك نص المشرع الجزائري في الفصل السادس من

1 بن زحاف فيصل، تسليم مرتكبي الجرائم الدولية، رسالة لنيل شهادة الدكتوراه في القانون الدولي والعلاقات السياسية الدولية، كلية الحقوق والعلوم السياسية، جامعة وهران، الجزائر، السنة الجامعة 2011-2012، ص 01.

2 سعيدي سليمة، حجاز بلال، المرجع السابق، ص 146.

3 المادة (32) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر سنة 2010، المصادق عليها بالمرسوم الرئاسي رقم 14-252، السالفة الذكر، والتي تنص على أن: "المساعدة المتبادلة :1- على جميع الدول الأطراف تبادل المساعدة فيما بينها بأقصى مدى ممكن لغايات التحقيقات أو الإجراءات المتعلقة بجرائم معلومات وتقنية المعلومات أو لجمع الأدلة الإلكترونية في الجرائم. 2- تلتزم كل دولة طرف بتبني الإجراءات الضرورية من أجل تطبيق الالتزامات الواردة في المواد من الرابعة والثلاثين إلى المادة الثانية والأربعين..."، وتنص المادة (42) من نفس الاتفاقية على التعاون والمساعدة الثنائية فيما يخص المعلومات المتعلقة بالمحتوى:" تلتزم الدول الأطراف بتوفير المساعدة الثنائية لبعضها فيما يتعلق بالجمع الفوري لمعلومات المحتوى لاتصالات معينة تبث بواسطة تقنية المعلومات الى الحد المسموح بحسب المعاهدات المطبقة والقوانين المحلية".

4 جاء في توصيات المجلس الاوربي (Eruopcounsil)، وبالأخص التوصية رقم 13/95 في الحادي عشر (11) من شهر سبتمبر سنة 1995 في شأن مشاكل الاجراءات الجنائية المتعلقة بتكنولوجيا المعلومات، حث الدول الاعضاء بمراجعة قوانين الاجراءات الجنائية الوطنية لتلائم والتطور في هذا المجال: لموسخ محمد، تنازع الاختصاص في الجريمة الإلكترونية، مجلة دفاتر السياسة والقانون، جامعة قاصدي مرباح بورقلة، الجزائر، العدد الثاني (02)، جوان 2009، ص 163.

القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، على التعاون والمساعدة القضائية الدولية، حيث سمح المشرع الجزائري بموجب مواد هذا الفصل القيام بالإجراءات القانونية التي تسهل التبادل الدولي لمكافحة الجرائم الإلكترونية وفقاً للأُطر المسموح بها قانوناً[1]. ومن أهم مظاهر المساعدة القانونية في مجال التعاون الدولي تبادل المعلومات[2]؛ والذي يشمل تبادل المعلومات والوثائق والبيانات التي تطلبها سلطة قضائية أجنبية حين النظر في جريمة إلكترونية[3].

ولأن الاستجابة السريعة لاتخاذ الاجراءات المطلوبة أمرُ ضروري في مكافحة الجرائم الإلكترونية، تم تجسيد ذلك في عدة اتفاقيات تراعي هذه الخاصية، ومنها: الاتفاقية الأمريكية الكندية التي تنص على إمكانية تبادل المعلومات شفوياً في حالة الاستعجال، ليتم تأكيد التبادل

1 كما جاء في المادة (16) من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، السالف الذكر، والمادة (18) من نفس القانون على:"يرفض تنفيذ طلبات المساعدة إذا كان من شأنها المساس بالسيادة الوطنية أو النظام العام. يمكن أن تكون الاستجابة لطلبات المساعدة مقيدة بشرط المحافظة على سرية المعلومات المبلغة أو بشرط عدم استعمالها في غير ما هو موضح في الطلب"، وجاء ايضاً في المادة (20) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، التي اعتمدت وعرضت للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة الدورة (25)، المؤرخ في (15) من شهر نوفمبر (تشرين الثاني) سنة 2000، وثيقة الأمم المتحدة A/RES/55/25 :" 1- تقوم كل دولة طرف، ضمن حدود إمكانياتها ووفقا للشروط المنصوص عليها في قانونها الداخلي، إذا كانت المبادئ الأساسية لنظامها القانوني الداخلي تسمح بذلك، باتخاذ ما يلزم من تدابير لإتاحة الاستخدام المناسب لأسلوب التسليم المراقب، وكذلك ما تراه مناسبا من استخدام أساليب تحر خاصة أخرى، مثل المراقبة الإلكترونية أو غيرها من أشكال المراقبة، والعمليات المستترة، من جانب سلطاتها المختصة داخل إقليمها لغرض مكافحة الجريمة المنظمة مكافحة فعالة...".

2 نظراً لأن تبادل المعلومات على درجة من الأهمية فقد نصت عليه عدة اتفاقية أبرمتها الجزائر مع مجموعة من الدول، من بينها: الاتفاقية المتعلقة بالتعاون القضائي في المجال الجزائي بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وحكومة الجمهورية الفرنسية، المصادق عليها بالمرسوم الرئاسي رقم 18-73،السالف الذكر؛ اتفاقية التعاون القانوني والقضائي في المجال الجزائي بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وحكومة دولة الكويت، المصادق عليها بالمرسوم الرئاسي رقم 15-255، السالف الذكر؛ اتفاقية تسليم المتهمين والمحكوم عليهم بين الجمهورية الجزائرية الديمقراطية الشعبية والمملكة العربية السعودية، المصادق عليها بالمرسوم الرئاسي رقم 15-192، السالف الذكر؛ اتفاقية التعاون القضائي والإعلانات والإنابات القضائية وتنفيذ الأحكام وتسليم المجرمين بين الجمهورية الجزائرية الديمقراطية الشعبية ودولة الإمارات العربية المتحدة، المؤرخة في 11 شوال عام 1428 الموافق 23 اكتوبر 2007، الموقعة بالجزائر في 12 اكتوبر سنة 1983، المصادق عليها بالمرسوم الرئاسي رقم 07-323، الصادرة في الج.ر رقم 67 المؤرخة في 24 اكتوبر سنة 2007.

3 إدريس النوازلي، جريمة النصب المعلوماتي –قانوناً واقعاً وقضاءً–، الطبعة الاولى، المطبعة والوراقة الوطنية، مراكش، المغرب، 2015، ص.ص: 195-196؛ نبيل محـمد عثمان عرعارة، المرجع السابق، ص 175.

بعد ذلك كتابة، ومن الأمثل أيضاً على ذلك تعاون ما قامت به المباحث الفيدرالية الأمريكية والبوليس الانجليزي في الكشف عن أول حادث إختراق للمعالجة الآلية للمعطيات للحكومة الفيدرالية الأمريكية، وكان المتهم يقيم في مقاطعة "ويلز" في بريطانيا وذلك في مارس 2000، وتم القبض على المسمى "Rafael Cray"[1].

ومن المواد الاتفاقية التي تنص على التبادل السريع للمعلومات المادة 53 من اتفاقية شنغين 1990 والخاصة باستخدام الاتصالات المباشرة بين السلطات القضائية في الدول الأطراف"[2]، والمادة 66 من قانون رومانيا رقم 2004/203 والتي تنص على حق السلطات الرومانية المختصة، في أن ترسل تلقائياً- إلى السلطات الأجنبية المختصة- المعلومات والبيانات الضرورية التي تسمح لهذه الأخيرة باكتشاف الجرائم المرتكبة بواسطة جهاز الحاسب الآلي، أو بحل القضايا المتعلقة بتلك الجرائم[3]، ومن الاتفاقيات أيضاً التي عالجت هذا الموضوع؛ اتفاقية بودابست من خلال المادة 35 منها والتي دعت الدول إلى إيجاد وسيلة تُسلم من خلالها طلبات الإنابة، كتعيين سلطة مركزية، أو السماح بالاتصال المباشر بين الجهات المختصة، وأوجبت على الأطراف تحديد نقاط إتصال مباشرة تعمل أربعة وعشرين (24) ساعة طوال السبعة أيام (7) لتؤمن المساعدة المباشرة للتحقيقات، المتعلقة بجرائم البيانات والشبكات، أو إستقبال الأدلة الإلكترونية[4].

ومن الاتفاقيات أيضاً الاتفاقية العربية لمكافحة جرائم تقنية المعلومات من خلال المادة 43 منها، والتي ألقت على عاتق الدول الأطراف التكفل بوضع جهاز متخصص ومتفرغ على مدار الساعة من أجل توفير المساعدة الفورية لغايات التحقيق أو الإجراءات المتعلقة بالجرائم الإلكترونية، وجمع الأدلة الإلكترونية، وتحديد مكان المشتبه فيهم، على أن يتم توفير العنصر البشري الكفء لتسهيل العملية، كما مكنت تلك الاتفاقيات والقوانين الداخلية السلطات المختصة من قبول طلبات المساعدة القضائية الدولية في حالة الاستعجال، إذا وردت عن طريق وسائل الاتصال

1 ياسر محمد الكومي محمود أبو حطب، المرجع السابق ص 333، **نقلاً عـــن**:

- Vergucht (p), *la repression des delait informatiques dans une prespective internationale*, these, Montpellie, 1996, p419.

2 يوسف حسن يوسف، المرجع السابق، ص 152.

3 ياسر محمد الكومي محمود أبو حطب، المرجع السابق، ص 331.

4 Conseil de l'Europe, Convention sur la cybercriminalité (STE n° 185) ; Budapest, 23.XI.2001, Sur le Site : *https://rm.coe.int/168008156d*.

السريعة كأجهزة الفاكس أو البريد الإلكتروني، على أن يتم التأكد من شروط أمنها وصحتها ومرجعيتها، طبعاً مع مراعاة الاتفاقيات الدولية ومبدأ المعاملة بالمثل، ومثالها ما جاء في المادة 32 من ذات الإتفاقية، والتي أجازت لكل دولة طرف في الحالات الطارئة أن تقدم طلب المساعدة القضائية بشكل عاجل عن طريق الفاكس أو البريد الإلكتروني.

ومن الأمثلة على المواد القانونية ما نصت عليه المادة 16 من القانون رقم 09-04 السالف الذكر، إذ يتعين على كل دولة تخصيص نقطة إتصال تكون متاحة طوال الأربع والعشرين (24) ساعة في اليوم وطيلة أيام الأسبوع، مراعاة لوصول المعلومات في الوقت المحدد، وقد جسد المشرع الجزائري ذلك في إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها والتي من مهامها كما رأينا تبادل المعلومات مع نظيراتها في الخارج في إطار التعاون والمساعدة القضائية الدولية[1]، والمادة الرابعة (04) من قانون تقنية المعلومات المصري لسنة 2018، والتي بينت أنه على السلطات المختصة تيسير التعاون مع نظيراتها بالبلدان الأجنبية بما يكفل تفادي الجرائم الإلكترونية، عن طريق مساعدتها على التحقيق فيها وتبادل المعلومات لتسهل تتبع مرتكبيها، على أن يتم ذلك في إطار الإتفاقيات الدولية والإقليمة والثنائية المصادق عليه، أو تطبيقاً لمبدأ المعاملة بالمثل، كما بينت أن المركز الوطني للاستعداد لطوارئ الحاسب والشبكات بالجهاز القومي لتنظيم الإتصالات هو النقطة الفنية المعتمدة لذلك التبادل.

ومواصلة للحلول المقترحة للصعوبات التي يواجهها التعاون الدولي، لا يمكننا أن نغفل عن موضوع تدريب رجال العدالة، والذي يعد مظهراً من مظاهر التعاون الدولي، حيث خصصت عدة برامج لهذا الموضوع، لأن عملية التدريب تفيد المتدرب في زيادة مهاراته ومعلوماته وقدراته على التعامل مع الأجهزة الدولية الأخرى، الأمر الذي ينعكس على الجهة التي ينتمي إليها بالفائدة[2]، ونذكر هنا تجربة الولايات المتحدة الأمريكية في هذا المجال كونها تعد من بين الدول المتقدمة في مجال مكافحة الجرائم الإلكترونية، كما أنها تعلم أن مواجهة هاته الجرائم لا يمكن أن تتم بشكل فعال دون أن يكون هنالك تعاون دولي في سبيل ذلك، لذا نجدها حَريصة على تقديم المساعدة التقنية والتدريب لرفع قدرات رجال العدالة الجنائية من مسؤولي الإدعاء العام، والقضاة، وأجهزة

1 محمودي سماح، المرجع السابق، ص 338.

2 أمير فرج يوسف، الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر، المرجع السابق، ص 430.

تطبيق القانون الأمريكية، وفي سبيل ذلك قامت بتنظيم دورات تدريبية لنظيراتها من الأجهزة في البلدان الأخرى، وأنشات معاهد خاصة لتدريب العاملين بتلك الأجهزة، يتم فيها اطلاعهم على أساليب مبتكرة للتحقيق والتحري، وتبادل الآراء والخبرات مع نظرائهم في مختلف الدول؛ ولتحقيق نتائج جيدة فقد أوكلت المهمة لعدة أجهزة، نذكر منها: مكتب المساعدة والتدريب الذي يعمل على تطوير أجهزة الادعاء العام في الخارج، التابع لوزارة العدل الأمريكية، والمكلف بتوفير المساعدة اللازمة لتعزيز مؤسسات العدالة الجزائية في دول أخرى، وتعزيز إدارة القضاء في الخارج.

وهناك كذلك البرنامج الدولي للمساعدة والتدريب على التحقيق الجزائي (ICITAP)، والذي يعمل على توفير مساعدات لأجهزة الشرطة في البلدان النامية في مختلف أنحاء العالم، لتعزيز القدرات التحقيقية لديها، كما تقوم الولايات المتحدة الأمريكية بتقديم المساعدة لتطوير القطاع القضائي في عدد من البلدان في إفريقيا، وآسيا، وأوربا الشرقية والوسطى، وأمريكا اللاتينية، وروسيا، والشرق الاوسط، ومنطقة حوض الكاريبتي[1].

ولأن معظم الدول أصبحت تَعي ما للعملية التدريبية من دور في تسهيـل عملية البحث عن الجرائم الإلكترونية والقبض على مرتكبيها وتقديمهم للعدالة، فقد عمدت إلى القيام بتـلك الدورات التـدريبية بصـفة دورية في عـدة قطاعات وأجهزة؛ الأمنية منها والقضائية، منتقية منها أهم العناصر الذين تتوفر فيهم القدرات العقلية والعلمية والتقنية، وكذا حب البحث والاطلاع، ولأن الجزائر تولي أهمية لعملية التكوين فقد قامت بعدة دورات تكوينة للعاملين بقطاع العدالة؛ وبالأخص القضاة[2]، لأجل تدعيم قدراتهم المهنية وتعميق معارفهم وتحيينها، ففي هذا الاطار تم

1 يقدم برنامج (ICITAP) المساعدة إلى قوات الدرك الوطني الجزائرية، المديرية العامة للأمن الوطني (DGSN) ومديرية الجمارك لتحسين قدرتها على التحقيق في مكافحة الجريمة المنظمة العابرة للحدود، المخدرات والإرهاب. ويتم توفير التدريب والتوجيه من طرف الخبراء في استخدام أساليب التحقيق المتطورة ضد المنظمات الإجرامية لتشمل ما يلي: إدارة مسرح الجريمة، تحليل الاستخبارات الجنائية، التحقيقات في الجرائم السيبرانية (جرائم الإنترنت)، الاستجابة لحوادث المتفجرات، التدخلات التكتيكية والعمليات السرية، تطوير مصدر إستخباراتي، التدخلات في حالات الاختطاف، مكافحة المخدرات، تمويل الجريمة / الإرهاب، المهارات التكتيكية وتقنيات التفاوض، تنمية المهارات القيادية والتغيير التنظيمي، وإدارة التحقيقات المعقدة العابرة للحدود. معلومات متاحة عبر موقع السفارة الأمريكية في الجزائر عبر الرابط الإلكتروني الموالي: https://dz.*usembassy.gov/ar/icitap-algeria*، والذي تم الاطلاع عليه في 2019/08/27.

2 التكوين التخصصي بالخارج: **في فرنسا**: استفـاد قـطاع العدالة بـ (12) منحة، انطلق التكوين شهر سبتمبر 2005، تكوين مجموعة مكونين لفائدة المدرسة العليا للقضاء (يختارون من سلك القضاء)، يجري فوج أول من 6 أفراد في أفريل 2005، تكويناً يدوم

عقد إجتماع حول موضوع مكافحة الجريمة السيبيرانية، وذلك خلال يومي 17 و18 فيفري 2020 بإقامة القضاة، في إطار البرنامج الأوروبي لمكافحة الجريمة السيبيرانية Cybersud ويشارك فيه تسعة (09) قضاة متخصصين في مجال الجريمة السيبيرانية مع خبراء المجلس الأوروبي. يهدف هذا الاجتماع إلى تقديم الدعم في مجال التكوين القاعدي والمستمر في المواضيع ذات الصلة بمكافحة الجريمة السيبرانية[1].

زيادة على ماسبق فإن البحث عن حلول للصعوبات التي يواجهها التعاون الدولي في مكافحة الجريمة الإلكترونية، تستدعي منا التطرق إلى موضوع في غاية الأهمية ألا وهو موضوع تسليم المجرمين[2]؛ فتسليم المجرمين هو عبارة عن "آلية قانونية للتعاون الدولي من أجل قمع الجريمة سواء كانت داخلية أو دولية، يتم بين دولتين تسمى الأولى الدولة الطالبة التي تسعى إلى استرداد المتهم لتحاكمه أو توقيع الجزاء الجنائي عليه، وتسمى الثانية بالدولة المطالبة وهي التي يكون الشخص المطلوب تسليمه موجوداً على أراضيها، فتقوم بإلقاء القبض عليه تحفظياً بمعرفة سلطاتها الأمنية والقضائية تمهيداً لتسليمه إلى الدولة الطالبة"[3].

---

(10) أيام ببوردو (Bordeaux)، يتبعه فوج آخر في الأشهر اللاحقة. تكوين بديجون (Dijon) (10) مكونين (من قضاة وكتاب الضبط) لفائدة المدرسة الوطنية لكتابة الضبط. **وفي بلجيكا:** "تحسبا لتنصيب الأقطاب القضائية المتخصصة، يتم تكوين خلال الثلاثي الثاني من هذه السنة، (10) قضاة في مجال تبييض الأموال والجرائم العابرة للحدود والمساس بأنظمة معالجة المعلوماتية – الجرائم الاقتصادية والمالية، ويدوم هذا التكوين ثلاثة أشـــهر، كما سيتابـــع فوج آخر من (12) قـــاض تكويناً مماثلاً، بداية من سبتمبر 2005. **ومع أمريكا:** تجسيداً لهذا التعاون، تم تنظم بالجزائر (6) دورات تكوينية لصالح (150) قاض من تنشيط قضاة أمريكيين في مجال الملكية الفكرية. مـــعلومات عن آفاق تكوين القضاة لسنة 2005، من الموقع الإلكتروني الخاص بوزارة العـــدل الجزائرية: *https://www.mjustice.dz/tableaux_dgrh_ar/tableau3.pdf*؛ تم الاطلاع عليه في 2019/12/19.

1 معلومات متاحة عبر الموقع الإلكتروني لوزارة العدل الجزائرية: *https://www.mjustice.dz*.

2 ولا تبدو تسمية "تسليم المجرمين" دقيقة من حيث كونها تتحدث عن "مجرم" وهو لفظ يفترض من ناحية أن الشخص المطلوب تسليمة قد تم سلفاً إدانته، مع أن التسليم قد ينصب على شخص لم تتم محاكمته بعد ومازال في طور الاتهام. كما أن لفظ "المجرم" يبدو من ناحية ثانية اليق بعلم الإجرام وعلوم الاجتماع بأكثر مما هو ذلك في إطار قانون العقوبات أو قانون الاجراءات الجنائية على وجه الخصوص، ورغم ذلك فمازالت تسمية تسليم أو استرداد المجرمين la restitution ou l'extradition des criminels هي الأكثر شيوعاً بالمقارنة مع تسليم الاشخاص la restitution des personnes. ويكشف التعريف السابق عن مجموعة من الخصائص؛ أولها أن التسليم هو بالأساس إجراء؛ أي أنه فكرة إجرائية تنتمي إلى أفكار قانون الإجراءات الجنائية، وذلك على الرغم مما يثيره من أفكار تتعلق بمفهوم الجرائم التي يجوز فيها التسليم"، **ينظر في ذلك:** سليمان عبد المنعم، الجوانب الاشكالية في النظام القانوني لتسليـــم المجرمين"دراسة مقارنة"، دار الجامعة الجديدة للنشر، الازاريطة، الإسكندرية، 2007، ص 07.

3 بن زحاف فيصل، المرجع السابق، ص 02، **نقلاً عـــن:**

وقد عرفه الفقه المصري على أنه:"إجراء تعاون دولي تقوم بمقتضاه دولة تسمى بالدولة الطالبة بتسليم شخص يوجد في إقليم دولة ثانية تسمى بالدولة المطلوب إليها أو جهة قضائية دولية بهدف ملاحقته عن جريمة اتهم بارتكابها أو لأجل تنفيذ حكم جنائي صدر ضده"[1]، لهذا يقال أن نظام تسليم المجرمين يساهم بصورة إيجابية وفعالة في تحقيق الاستقرار العالمي، ودفاع دول العالم متضامنة ضد الجريمة في سبيل تحقيق مصالحها المشتركة[2].

ويعد تسليم المجرمين في كثير من الأحيان عقبة كبيرة أمام معاقبة الجناة، لذا فقد عقدت الجزائر وغيرها من الدول معاهدات واتفاقيات عدة لتمكينها من تنفيذ هذا الإجراء في ظل إحترام القوانين والسيادة الوطنية لكل دولة، إذ تعد بلجيكا من بين أول الدول التي سنت قانوناً داخلياً في مجال تسـليم المجرمين، سنة 1833، لتتبعها الولايات المتحدة بعد خمس عشرة (15) سنة من ذلك التاريخ –أي سنة 1848–، لتقوم بعدها فرنسا بإصدار قانون في هذا المجال في سنة 1927، ليشكل هذا القانون المصدر الأساسي للقوانين الداخلية التي تبناها المغرب في مجال تسليم المجرمين، وذلك بمقتضى ظهير 21 فبراير 1941، وكذلك ظهير 08 نوفمبر 1958، والذي تم تضمينه فيما بعد في قانون المسطرة الجنائية المغربي[3]. ليتم في سنة 2011 الإشارة ولأول مرة في الدستور المغربي في الفقرة الخامسة من المادة 30 منه لتسليم الأشـخاص المتابعين أو المدانين [4]، كما نص المشرع

- Mikael Poutiers, *l'extradition des auteurs d'infractions internationales dans Hervé ASCENSIO*, Emmanuel DECAUX, Droit international pénal, Pédone, Paris, 2000, p 933.

1 أمل لطفي حسين جاب الله، نطاق السلطة التقديرية للإدارة في تسليم المجرمين (دراسة مقارنة)، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، 2013، ص 10، **نقلاً عـن**: هشام عبد العزيز مبارك، تسليم المجرمين بين الواقع والقانون، دار النهضة العربية، سنة 2006، ص 27.

2 عبد الرحمن فتحي عبد الرحمن سمحان، مرجع سابق، ص 21.

3 عبد الكافي الورياشي، المرجع السابق، ص 47.

4 **دستور المملكة المغربية**: الظهير الشريف رقم 1.11.91 الصادر في 27 من شعبان 1432، الموافق 29 يوليو 2011، الخاص بتنفيذ الدستور، المنشور بالج.ر، العدد 5964 مكرر، السنة المائة، الصادرة في 30 يوليو 2011، ص 3600؛ ظهير شريف رقم 1.02.255 صادر في 25 من رجب 1423، الموافق 03 أكتوبر 2002، الخاص بتنفيذ القانون رقم 22.01 المتعلق بالمسـطرة الجنائية المغربية، الصادر في الج.ر عدد 5078 بتاريخ 30 يناير2003، ص 315، مـعدل ومتمم بالقـانون رقم 32.18، الصادر بتنفيذه الظهير الشريف رقم 1.19.92 بتاريخ 5 ذي القعدة 1440، الموافق 8 يوليو 2019، الصادر في الج.ر عدد 6796 بتاريخ 18 يوليو 2019، ص 5036. نص المشرع المغربي على تسليم المجرمين في المواد من 718 إلى المادة 745 من الباب الرابع من القسم الثالث بشأن العلاقات القضائية مع السلطات الأجنبية من الكتاب السابع بشأن أحكام الاختصاص المتعلق ببعض الجرائم المرتكبة خارج المملكة والعلاقات مع السلطات القضائية الأجنبية من قانون المسطرة الجنائية، إلا أنه نص في المادة 713 منه

المغربي في ديباجة الدستور على جعل الاتفاقيات الدولية التي صادق عليها المغرب تسمو فور نشرها على التشريعات الوطنية، وعلى ضرورة ملاءمة تلك التشريعات مع ما تتطلبه الاتفاقيات، ولقد أعاد التأكيد على هذه المسالة –أولوية تطبيق ما جاء في بنود الاتفاقيات الدولية على ما تضمنته مواد القوانين الداخلية– في عدة مواد من قانون المسطرة الجنائية المغربي، ونذكر على سبيل المثال نص المادة 713 منه:"تكون الأولوية للاتفاقيات الدولية على القوانين الوطنية فيما يخص التعاون القضائي مع الدول الأجنبية. لا تطبق مقتضيات هذا الباب إلا في حالة عدم وجود اتفاقيات أو في حالة خلو تلك الاتفاقيات من الأحكام الواردة بها".

أما بالنسبة للمشرع الجزائري فقد تطرق لتسليم المجرمين في المادة 50 من التعديل الدستوري لسنة 2020[1]، وخصص له الباب الأول من الكتاب السابع من ق.إ.ج.ج المعنون بالعلاقات بين السلطات القضائية الأجنبية[2]، ولأن وجود معاهدات واتفاقيات يشكل فارقاً في تسليم المجرمين سعت الجزائر إلى الانضمام إلى العديد من الاتفاقيات الدولية والإقليمية وعقد مجموعة من الإتفاقيات، دعماً منها للعلاقة التي تربطها بمختلف الدول في ميدان التعاون القانوني والقضائي الساعي لمكافحة الإجرام بكل أشكاله، ورغبة منها في إقامة التعاون في ميدان تسليم المجرمين، ليتيسر لها جمع المعلومات[3] المطلوبة وكل شيء آخر للقيام بهذا الاجراء[4]، فأي دولة مهما كانت أجهزتها القضائية فعالة لا يمكنها لوحدها القبض على المجرمين الفارين خاصة[5] الإلكترونيين منهم،

على:"تكون الأولوية للاتفاقيات الدولية على القوانين الوطنية فيما يخص التعاون القضائي مع الدول الأجنبية. لا تطبق مقتضيات هذا الباب، إلا في حالة عدم وجود اتفاقيات أو في حالة خلو تلك الاتفاقيات من الأحكام الواردة به".

1 تنص الفقرة الثانية من المادة 50 من تعديل الدستور الجزائري لسنة 2020 على:"لا يمكن تسليم أحد إلا بمقتضى اتفاقية دولية مصادق عليها، أو بموجب قانون."

2 تنص المادة 694 من ق.إ.ج.ج على:" تحدد الأحكام الواردة في هذا الكتاب شروط تسليم المجرمين وإجراءاته وآثاره وذلك مالم تنص المعاهدات والاتفاقيات السياسية على خلاف ذلك".

3 المادة (17) من اتفاقية تسليم المجرمين بين الجمهورية الجزائرية الديمقراطية الشعبية ومملكة إسبانيا، المؤرخة في أول ربيع الأول عام 1429 الموافق 09 مارس 2008، الموقعة بالجزائر في 12 ديسمبر سنة 2006، المصادق عليها بالمرسوم الرئاسي رقم 08-85، الصادر في الج.ر.ج رقم 14 المؤرخة في 12 مارس سنة 2008؛ وغيرها.

4 المادة الأولى من الاتفاقية المتعلقة بالتعاون القضائي في المجال الجزائي بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وحكومة الجمهورية الايطالية، المؤرخة في 04 محرم عام 1426 الموافق 13 فبراير 2005، الموقعة بالجزائر في 22 جويلية سنة 2003، المصادق عليها بالمرسوم الرئاسي رقم 05-73، الصادر في الج.ر.ج رقم 13 المؤرخة في 16 فبراير سنة 2005.

5 رابحي عزيزة، المرجع السابق، ص 319.

فالإتفاقية العربية لمكافحة جرائم تقنية المعلومات تعتبر كأساس قانوني لتسليم[1] أولئك المتابعين أو الملاحقين بسبب ارتكابهم جرائم إلكترونية، فقد نصت المادة 31 منها على مجموعة من الاحكام في هذا الخصوص[2]، إلا أن تسليم المجرمين تواجهه عدة عقبات تشكل في بعض الأحيان موانعاً لتسليم مرتكبي الجريمة بصفة عامة سواء كانت جريمة داخلية أو دولية، تقوم هذه العقبات على عدة اعتبارات منها ما يتعلق بالشخص المطلوب، كأن يكون أحد رعايا الدولة المطلوب منها التسليم[3]، أو أن يكون لاجئاً سياسياً أو أن تسليمه يمس بحقوقه وحرياته، أو عرقه، أو ديانته، أو أن يكون حدثاً[1]، ومنها ما يرتبط بالجريمة والعقوبة المقررة لها[2].

1 توفيق مجاهد، طاهر عباسة، المرجع السابق، ص 93.

2 المادة (31) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر سنة 2010، والمصادق عليها بموجب المرسوم رئاسي رقم 14-252، السالفة الذكر؛ ونص الفصل الثاني من نفس الاتفاقية على تجريم مجموعة من الجرائم هي: جريمة الدخول غير المشروع المادة (06)، جريمة الاعتراض غير المشروع المادة (07)، الاعتداء على سلامة البيانات المادة (08)، جريمة إساءة استخدام وسائل تقنية المعلومات المادة (09)، جريمة التزوير المادة (10)، جريمة الإحتيال المادة (11)، جريمة الإباحية المادة (12)، الجرائم الأخرى المرتبطة بالإباحية المادة (13)، جريمة الاعتداء على حرمة الحياة الخاصة المادة (14)، الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات المادة (15)، الجرائم المتعلقة بالجرائم المنظمة والمرتكبة بواسطة تقنية المعلومات المادة (16)، الجرائم المتعلقة بانتهاك حق المؤلف والحقوق المجاورة المادة (17)، الاستخدام غير المشروع لأدوات الدفع الإلكترونية المادة (18)، الشروع والاشتراك في ارتكاب الجرائم المادة (19)، المسؤولية الجنائية للأشخاص الطبيعية والمعنوية المادة (20)، تشديد العقوبات على الجرائم التقليدية المرتكبة بواسطة تقنية المعلومات المادة (21).

3 "يسود المجتمع الدولي اتجاه عام بعدم جواز تسليم الرعايا أياً كان نوع الجريمة المرتكبة خارج دولتهم"، **انظر في ذلك:** باخويا دريس، جريمة غسل الأموال ومكافحتها في القانون الجزائري (دراسة مقارنة)، أطروحة مقدمة لنيل شهادة الدكتوراه في القانون الجنائي الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، السنة الجامعية 2011-2012، ص 361؛ "ويبقى استثناءان يمنع فيهما تسليم المجرمين، الأول متفق عليه وهو امتناع تسليم الدولة لرعاياها من المواطنين، والثاني مختلف حوله وهو إمكان رفض تسليم اللاجئين السياسيين المقيمين على إقليم الدولة المطلوب منها التسليم"، **ورد لدى:** علواش فريد، نظام تسليم المجرمين في الاتفاقيات الدولية، مجلة الدراسات القانونية والسياسية، جامعة عمار ثليجي بالأغواط، الجزائر، المجلد الثاني (02)، العدد الخامس (05)، جانفي 2017، ص 403، **نقلاً عن:** سليمان عبد المنعم، دروس في القانون الجنائي الدولي، دار الجامعة الجديدة، الاسكندرية، 2000، ص 98؛ وطبقا للفقرة الأولى من المادة الثالثة (3) من قانون تسليم المجرمين العماني يحظر نهائيا تسليم المواطنين العمانيين إلى أي دولة أجنبية، فإذا ما ارتكب احد مواطنيها جريمة ما في دولة أخرى وفر هاربا إلى السلطنة، ثم طالبة تلك الدولة بتسليمه، ففي هذه الحالة تحصنه الجنسية العمانية من عملية التسليم، لان السلطنة تعتبر نفسها الأحق بمحاكمته من دولة أخرى": عبد العزيز لطفي جاد الله، أمن المجتمع الإلكتروني بين سياسة السوق الإلكترونية والتعاون الدولي في إطار مواجهة الجرائم الإلكترونية، الطبعة الأولى، مكتبة الوفاء القانونية، الإسكندرية، مصر، 2017، ص 159. كما تنص المادة 696-4 من ق.إ.ج.ف بأنه:

Article 696-4 du **Code de procédure pénale ,** Créé par Loi n°2004-204 du 9 mars 2004 - art. 17 JORF 10 mars 2004: " L'extradition n'est pas accordée : 1° Lorsque la personne réclamée a la nationalité française, cette dernière étant appréciée à l'époque de l'infraction pour laquelle l'extradition est requise ; …"

وعملاً على تسهيل إجراءات[3] تسليم المجرمين عمدت بعض الدول إلى التخفيف من القيود المطبقة على تسليم المجرمين، ومنها أن تقبل الدول بتسليم رعاياها في حالة ارتكابهم لجرم ما خاصة إذا وجدت بين البلدين إتفاقية؛ رغم أنه أمر قليل الحدوث إلا أنه ممكن، ومثاله ما نصت عليه المادة 26 من الدستور الايطالي المعدل سنة 2012 بقولها:"يسمح بتسليم المواطنين فقط في الأحوال المنصوص عليها صراحة في المواثيق الدولية". وأمر مشابه نجده في الإتفاقية الثنائية المبرمة بين فرنسا ودولة سويسرا التي اكتفت بالحديث عن تسليم الأشخاص دون تمييز لجنسيتهم وما إذا كانوا رعايا الدولة المطلوب منها التسليم أم أجانب عنها[4]، وهو ذات الأمر نجده في بنود بعض الاتفاقيات التي أبرمتها الجزائر [5]، كما أيدت محكمة النقض الفرنسية حكم المحكمة بتسليم شخص فرنسي الجنسية، يدعى (M. X) صدرت بحقه مـذكرة توقيف من قبل السلطات القضائية الـبريطانية –محكمة سنارسبروك (Snaresbrook)– في (05) من شهر مارس سنة 2009، بتهمة

---

1 من بين الأفعال الجنائية التي يحظر فيها التسليم الجرائم السياسية والعسكرية والجمركية، فعدم التسليم في الجرائم السياسية هو مبدأ عالمي فرضه العرف الدولي، وتبنته جميع التشريعات في العالم؛ صراحة أو ضمناً، **ينظر في ذلك**: عبد الكافي الورياشي، المرجع السابق، ص 56؛ لذا فقد تضمنت الدساتير هذا المبدأ قبل الاتفاقيات الثنائية والتشريعات الداخلية؛ مثلاً الدستور الجزائري في المادة (83): "لا يمكن بأي حال من الأحوال أن يُسلم أو يُطرد لاجئ سياسي يتمتع قانوناً بحق اللجوء".

2 الشروط العامة للجريمة في نظام تسليم المجرمين: 1- جسامة الوقائع. 2- ازدواج التـجريم: ليس معناه وحدة التكييف القانوني للفعل المجرم، إذ يجوز اختلاف قوانين الدولتين الطالبة والمطالبة في بيان العناصر المكونة للجرم.، 3- عدم انقضاء الدعوى العمومية"، **انظر**: نادية دردار، المرجع السابق، ص 44. أما الشروط المتعلقة بالجريمة المطلوب التسليم لأجلها: 1- أسلوب الحصر أو ما يسمى بنهج القائمة قليل الاستعمال، 2- أسلوب جسامة الجريمة أو الحد الأدنى للعقوبة هو الأكثر شيوعا في تحديد الجرائم التي يجوز التسليم فيها، 3- النظام المختلط وهو من الأساليب الشائعة أيضاً، **انظر**: عيسى سليم داود الزيدي، المرجع السابق، ص 143. ويتوقف تسليم المجرمين المتهمين بقضايا القرصنة المعلوماتية بين الدول على توافر ثلاثة عناصر تتمثل في وجود معاهدة ثنائية بهذا الخصوص، واعتبار الحدث جريمة في كلتا الدولتين، وأن تكون الإساءة المزعومة على قائمة الأعمال التي تستوجب الملاحقة القضائية بين الدولتين، **انظر**: سالم بن محمد السالم، المرجع السابق، ص 31.

3 المادة 12 من الاتفاقية المتعلقة بتسليم المجرمين بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وحكومة الجمهورية الايطالية، المصادق عليها بالمرسوم الرئاسي رقم 05-74، السالفة الذكر؛ المادة (09) من الاتفاقية المتعلقة بتسليم المجرمين بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وحكومة المملكة المتحدة لبريطانيا العظمى وإيرلندا الشمالية، المصادق عليها بالمرسوم الرئاسي رقم 06-464، الاتفاقية السالفة الذكر، وغيرها من الاتفاقيات.

4 عبد السلام بنسليمان، المرجع السابق، ص 219.

5 من بينها: الاتفاقية المتعلقة بتسليم المجرمين بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وحكومة المملكة المتحدة لبريطانيا العظمى وإيرلندا الشمالية، المصادق عليها بالمرسوم الرئاسي رقم 06-464، السالفة الذكر: المادة (03): " 1- يمكن لأي طـرف أن يسلم مواطنيه للطرف الأخر، شريطة أن يسمح تشريعه بذلك...".

"التآمر من أجل السرقة"، فحكم عليه بالسجن لمدة أربع سنوات، كونه قام بالدخول إلى أنظمة الحاسب الآلي الخاصة بمؤسسة مصرفية بتواطؤ مع ضابط أمن بها، من أجل نقل مبلغ مائتين وتسعة وعشرين (229) مليون يورو إلكترونيًا إلى حسابات كان يتحكم بها، ولكن محاولته فشلت بسبب خطأ في كلمة المرور التي أدخلها في النظام[1].

ومهما كانت الاعتبارات التي تقوم عليها موانع التسليم التي تهدف لحماية الشخص المطلوب تسليمه، سواء بهدف محاكمته أو تنفيذ العقوبة الصادرة ضده فإنه يمكن تجاوزها وتذليل العقبات نظراً لخطورة هذه الجرائم وضمان عدم إفلات مرتكبيها من العقاب[2]؛ ومن تلك التذللات المعاملة بالمثل والتي دأبت العديد من الدول على مباشرة إجراءات التسليم إعتمادًا عليها في حالة عدم وجود معاهدة أو اتفاقية بخصوص تسليم المجرمين[3]، لأنه ولأجل حماية المجتمع الدولي، يتوجب على الدول أن تتعاون فيما بينها إما بمعاقبة المتهمين عن الجرائم المنسوبة إليهم، أو بتسليمهم إلى الدول المطلوبين فيها، وهذا حتى لا تتاح الفرصة للجناة أن يفلتوا من العقاب إذا ما خرجوا من حدود الإقليم الذي ارتكبوا فيه جرائمهم[4]، فالمعاملة بالمثل كما تعد سبب لتسلم المجرمين، قد تكون سبب لرفض ذلك التسليم، فقد سبق وأن رفضت السلطات الحكومية المغربية تسليم إيطالي مطلوب من طرف الدولة الايطالية رغم صدور حكم قضائي بتاريخ 1961/03/24 والقاضي بالموافقة على تسليمه، لأن السلطات الإيطالية رفضت الاستجابة لطلب تسليم تقدمت به السلطات المغربية لها[5]، لذا يجب حسن إستعمال هذا المبدأ لتقليل من عقبات تسليم المجرمين.

1 Cour de cassation, chambre criminelle, Audience publique du 23 avril 2013, N° de pourvoi: 13-82467, ECLI:FR:CCASS:2013:CR02491(Non publié au bulletin).

2 بن زحاف فيصل، المرجع السابق، ص ص 268-269.

3 Article 696 du **Code de procédure pénale**, Modifié par Loi n°2004-204 du 9 mars 2004 - art. 17 JORF 10 mars 2004: "En l'absence de convention internationale en stipulant autrement, les conditions, la procédure et les effets de l'extradition sont déterminés par les dispositions du présent chapitre. Ces dispositions s'appliquent également aux points qui n'auraient pas été réglementés par les conventions internationales."

4 آمال قارة، تفعيل آليات تسليم المجرمين في إطار المنظمة الدولية للشرطة الجنائية، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسيّة، جامعة الشهيد حمه لخضر بالوادي، المجلد التاسع (09)، العدد الثاني (02)، جوان 2018، ص 892، **نقلاً عن**: علي صادق أبو هيف، القانـون الدولي العام والمـبادئ العامة، مطبعة اطلس القاهرة، الطبعة الحادية عشرة، السنة، 1975، ص 301.

5 عبد الكافي الورياشي، المرجع السابق، ص 66.

ومن العقبات التي وقفت أمام تسليم المجرمين مبدأ التجريم المزدوج، والذي يعد شرطاً للمساعدة القضائية المتبادلة، لذا نادى فريق من الخبراء بوضع استراتيجية لمكافحة الجريمة يكون من مبادئها التخلي عن هذا المبـدأ وتوخي المرونة والسـرعة في تبادل كافة أشـكال المساعدة المتاحة، وتخفيف التطبيق الصارم له[1].

من المسائل كذلك التي سعت مختلف التشريعات والاتفاقيات الدولية إلى إيجاد حل لها موضوع الاختصاص في الجرائم الإلكترونية، لأن الإعتماد على الوسائل التقليدية للتـعاون الدولي الرسمي في مسائل الجرائم السيبرانية لا يكفي حالياً للاستجابة في الوقت المناسب لمقتضيات الحصول على أدلة إلكترونية سريعة الزوال والتغيُّر. وبما أنَّ عدداً متزايداً من الجرائم يشتمل على أدلة إلكترونية توجد في أماكن جغرافية متعددة، سيشكل ذلك مشكلة ليس فقط بشأن الجرائم السيبرانية، وإنما بشأن كل الجرائم عموماً، فالجـرائم الإلكترونية قد ترتكب في بلد وتقع نتائجها في بلد آخر أو عدة بلدان، كما قد ترتكب من شخص، أو عدة أشخاص في أماكن مختلفة، وقد يحدث أن ترتكب جريمة إلكترونية من شخص لا يحمل جنسية الدولة التي ارتكبت ضدها ولا الدولة التي ارتكبت فيها، فيثار التساؤل عن الدولة التي تختص قانوناً بمحاكمته[2].

لقد عالج المشرع الجزائري موضوع الاختصاص في الجرائم الإلكترونية من خلال المادة 15 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[3]، والذي بين أنه زيادة على قواعد الاختصاص المنصوص عليها في قانون الاجراءات الجزائية، تختص المحاكم الجزائرية بالنظر في الجرائم الإلكترونية المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبياً وتستهدف مؤسسات الدولة أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني، كأن يقوم الجاني أو الجناة بتدمير مواقع إلكترونية لمؤسسات حيوية

1 نقموش محمد، ميلودية أحمد، المرجع السابق، ص 271؛ محمد نصر محمد، المرجع السابق، ص 121، **نقلاً عن**: أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة العربية، القاهرة، 1988، ص85.

2 بلبالي ابراهيم، الجريمة الإلكترونية بين وضوح معالم وأهداف التجريم وصعوبة التصنيف والتطبيق، مجلة دراسات وأبحاث، جامعة زيان عاشور، الجلفة، الجزائر، العدد الأول، تاريخ النشر: 2009/09/15، ص 147.

3 يوسف قجاج، المرجع السابق، ص 36.

في الدولة أو بث فيروس إلكتروني يؤدي إلى إتلاف البرامج التي تعمل بها أجهزة الحواسيب الآلية في تلك المؤسسات أو التحريض على ارتكاب أعمال إرهابية في الدولة[1].

إن الاختصاص في الجريمة الإلكترونية مرتبط في أغلب الأحيان بالطابع العالمي الذي تتميز به، وهو ما جعل هذا الأخير –أي الاختصاص– يمتد إلى خارج الدولة[2]، وهو ما حث معظم الدول على النص في قوانينها الداخلية على ما يبيح ويسهل ذلك الامتداد في الإختصاص، إذ عملت على عقد عدة اتفاقيات؛ ومنها ما قامت به الدول العربية من خلال الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 من شهر ديسمبر سنة 2010، والتي تجسدت في القانون الجزائري من خلال المرسوم الرئاسي رقم 14-252، وبالذات من خلال المادة 03، والمادة 30 منها[3]، وهي ذات الأحكام بنفس ترقيم المواد نجدها مجسدة في التشريع المصري من خلال القرار الرئاسي رقم 276 لسنة 2014، بشأن الموافقة على انضمام جمهورية مصر العربية إلى الإتفاقية العربية لمكافحة جرائم تقنية المعلومات –الجرائم الإلكترونية–، ليتطرق بعدها المشرع المصري لموضوع الاختصاص في الجرائم الإلكترونية ضمن المادة 03 من القانون الصادر سنة 2018

1 محمد عبد الفتاح عبد المقصود على، القواعد الإجرائية للجرائم التي تقع عبر شبكة الانترنت، رسالة مقدمة للحصول على درجة الدكتوراه، قسم القانون الجنائي، كلية الحقوق، جامعة طنطا، مصر، 2015، ص 81.

2 شوقي يعيش تمام، عزيزة شبري، المرجع السابق، ص 101.

3 تنص المادة الثالثة 03 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر سنة 2010، المصادق عليها بالمرسوم الرئاسي رقم 14-252، السالفة الذكر، على:"تطبق هذه الاتفاقية ما لم ينص على خلاف ذلك، على جرائم تقنية المعلومات بهدف منعها والتحقيق فيها وملاحقة مرتكبيها، وذلك في الحالات الآتية: 1- ارتكبت في أكثر من دولة. 2- ارتكبت في دولة وتم الإعداد أو التخطيط لها أو توجيهها أو الإشراف عليها في دولة أو دول أخرى، 3- ارتكبت في دولة وضلعت في ارتكابها جماعة إجرامية منظمة تمارس أنشطة في أكثر من دولة، 4- ارتكبت في دولة وكانت لها آثار شديدة في دولة أو دول أخرى."، وتنص المادة 30 منه على: "1- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد اختصاصها على أي من الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية وذلك إذا ارتكبت الجريمة كليا أو جزئيا أو تحققت : أ – في إقليم الدولة الطرف، ب – على متن سفينة تحمل علم الدولة الطرف، ج – على متن طائرة مسجلة تحت قوانين الدولة الطرف، د – من قبل أحد مواطني الدولة الطرف إذا كانت الجريمة يعاقب عليها حسب القانون الداخلي في مكان ارتكبها أو إذ ارتكبت خارج منطقة الاختصاص القضائي لأية دولة، هـ – إذا كانت الجريمة تمس أحد المصالح العليا للدولة..."؛ **أشار إلى ذلك:** شرف الدين وردة، سليم بشير، حل مشكلة تنازع الاختصاص الجنائي الدولي في مجال مكافحة جرائم التجارة الإلكترونية، مجلة الحقوق والحريات، مخبر الحقوق والحريات في الأنظمة المقارنة، جامعة محمد خيضر، بسكرة، الجزائر، المجلد الخامس(05)، العدد الأول، 2019/04/30، ص 132.

والخاص بجرائم تقنية المعلومات[1]، فالمشرع المصري بموجب هذا القانون دعم ما جاء في الاتفاقية العربية لمكافحة الجرائم الإلكترونية، ومنح للمواطن المصري الحماية من خلال امتداد اختصاص الدولة المصرية للنظر في القضايا التي يكون ضحيتها مواطن مصري، أو كل مقيم على الاراضي المصرية تضرر من الجرائم الإلكترونية، وكل ذلك دون الإخلال بأحكام الباب الأول من الكتاب الأول من قانون العقوبات المصري[2]، والذي تنص مادته الأولى على مبدأ الإقليمية؛ الذي أخذ به المشرع المغربي في القضية المعروفة بقضية فيروس (ZOTOB) بعد أن ارتُكبت الجريمة انطلاقاً من المغرب، بينما تحققت نتيجتها بالولايات المتحدة الأمريكية بعد أن ألحقت الضرر بمواقع إلكترونية بهذه الأخيرة، ومن بينها تلك الخاصة بالكونغرس وبمطار سان فرانسيسكو[3].

أما القضاء الأمريكي فقد اعتبر أن الاختصاص المحلي قائم للقضاء الوطني حين مساس الجريمة الإلكترونية بالمصالح الأمريكية أو تعرض تلك المصالح للخطر بسببها حتى ولو ارتكبت الجريمة بالخارج، حيث تابعت ولاية بنسلفانيا مزود شبكة انترنت في ولاية كاليفورنيا بدعوى الاعتداء على علامة مسجلة في ولاية بنسلفانيا، كما تبنى القضاء الانجليزي مذهب القضاء الأمريكي في ذلك[4]، كما عمد المشرع الأمريكي في ولاية (Tennessee) إلى مد اختصاص محاكم الولاية بخصوص الجرائم الإلكترونية، بناءً على الفصل الخاص بالإختصاص من قانون جرائم الحاسوب والذي يعتبر أن الجريمة قد وقعت في كل مكان يقع فيه فعل من الأفعال المعاقب عليها،

1 قانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات، القانون السالف الذكر، جاء في المادة الثالثة (03) منه: نطاق تطبيق القانون من حيث المكان: "مع عدم الاخلال بأحكام الباب الاول من الكتاب الاول من قانون العقوبات، تسري أحكام هذا القانون على كل من ارتكب خارج جمهورية مصر العربية من غير المصريين جريمة من الجرائم المنصوص عليها من هذا القانون، متى كان الفعل معاقباً عليه في الدولة التي وقع فيها تحت أي وصف قانوني، وذلك في أي من الاحوال الاتية: 1- إذا ارتُكبت الجريمة علي متن أي وسيلة من وسائل النقل الجوي أو البري أو المائي وكانت مسجلة لدى جمهورية مصر العربية أو تحمل علمها. 2- إذا كان المجني عليهم أو أحدهم مصرياً. 3- إذا تم الإعداد للجريمة أو التخطيط أو التوجيه أو الإشراف عليها أو تمويلها في جمهورية مصر العربية. 4- إذا ارتكبت الجريمة بواسطة جماعة إجرامية منظمة، تمارس أنشطة إجرامية في أكثر من دولة من بينها جمهورية مصر العربية. 5- إذا كان من شأن الجريمة إلحاق ضرر بأي من موطني جمهورية مصر العربية أو المقيمين فيها أو بأمنها أو بأي من مصالحها في الداخل أو الخارج. 6- إذا وُجد مرتكب جريمة في جمهورية مصر العربية، بعد ارتكابها ولم يتم تسليمه".

2 الباب الأول من الكتاب الأول من قانون العقوبات المصري المعدل والمتمم.

3 نور الدين الواهلي، الاختصاص في الجريمة الإلكترونية، تأثير الجريمة الإلكترونية على الائتمان المالي، سلسلة ندوات محكمة الاستئناف بالرباط، العدد السابع، 2014، ص 138.

4 عمر بنيوني، الإجراءات الجنائية عبر الانترنت في القانون الأمريكي المرشد الفيدرالي الامريكي لتفتيش وضبط الحواسيب وصولا إلى الدليل الإلكتروني في التحقيقات الجنائية، الطبعة الأولى، 2004-2005، ص 201 وما يليها.

وفي كل مكان يسيطر فيه المتهم على مال متحصل عليه من جريمة من الجرائم الإلكترونية، أو محل حيازته لذلك المال.

كما تقع الجريمة وفقاً لذات القانون في كل مكان يحوز فيه المتهم أشياء مادية استخدمت في ارتكاب جريمة من الجرائم الإلكترونية، كالكتب أو التسجيلات أو الوثائق أو الأموال أو الأوراق المالية أو برامج الحاسوب أو أي شيء أخر، بل أن هذا القانون قد وسع من اختصاص محاكم الولاية لكي يمتد إلى الجرائم الإلكترونية المرتكبة خارج الدولة حين عبور تلك الأفعال بإقليمها، سواء تم هذا التداخل بأسلوب سلكي أو لاسلكي بطريق الموجات الكهرومغناطيسية أو الميكروفون، أو بأي أسلوب آخر من أساليب الاتصال. كما تعد قوة العقوبة المقررة للجرائم الإلكترونية من العوامل المهمة في تحديد أولوية دولة ما على أخرى في محاكمة الجاني في تلك الجرائم، فقوة العقوبة هي من بين المعايير التي يؤخذ بها عند تنازع الاختصاص بين أكثر من ولاية في الولايات الأمريكية.

أما المشرع الإنجليزي فإنه وبحسب الفصل الخامس من قانون إساءة استعمال الحاسوب (Computer Misuse Act) لسنة 1990 يمكن تطبيق الاختصاص في محاكمة المتهمين بالجرائم الإلكترونية إذا وجدت صلة بين الجريمة والإقليم البريطاني (significant link)، كأن تبدأ الجريمة في انجلترا أو يكون محلها حاسوب متواجد في الأراضي البريطانية[1]، وهو ذات الحكم نجده في القانون الفرنسي من خلال المادة 113-2-1 من قانون العقوبات الفرنسي، حيث تعتبر الجريمة أو الجنحة المرتكبة بواسطة شبكة اتصالات إلكترونية واقعة على الأراضي الفرنسية متى وقع أحد العناصر المكونة لها داخل الأراضي الفرنسية[2].

ومن مواقف القضاء الفرنسي قرار المحكمة الابتدائية في باريس باختصاص القاضي الجزائي الفرنسي بالنظر في الجرائم الإلكترونية، بمجرد وجود اتصال بمواقع الإنترنت داخل الأراضي الفرنسية، وكانت تلك المعلومات المنشورة على شبكة الإنترنت، والتي تم استلامها وعرضها

1 غانم محمد غانم، المرجع السابق، ص.ص: 222-223؛ محمد عبد الفتاح عبد المقصود على، المرجع السابق، ص 86.

2 Article 113-2-1 du **Code penal,** Créé par LOI n°2016-731 du 3 juin 2016 - art. 28: "Tout crime ou tout délit réalisé au moyen d'un réseau de communication électronique, lorsqu'il est tenté ou commis au préjudice d'une personne physique résidant sur le territoire de la République ou d'une personne morale dont le siège se situe sur le territoire de la République, est réputé commis sur le territoire de la République."

في فرنسا تشكل جريمة جنائية وفقاً للقانون الفرنسي، فإن المحاكم الفرنسية تكون مختصة بالنظر في تلك الجريمة بغض النظر عن جنسية كل من الجاني والمجني عليه، ومكان السلوك المجرم، فإمكانية استقبال وعرض نص نُشر في الخارج عبر شبكة الإنترنت داخل فرنسا، يكفي لاختصاص القاضي الفرنسي بنظر الجريمة المترتبة عن الفعل المقترف عبر شبكة الإنترنت، لذا قال الأستاذ " Etienne wery" أن سلطة واختصاص القاضي الجنائي الفرنسي في الجرائم المرتكبة عبر شبكة الإنترنت بلا حدود أو عالمية[1]، وذهب الاستاذ "Guillaume Gardet" إلى أنه لا يوجد فراغ قانوني في المسائل الجنائية المتعلقة بالإنترنت[2] بما فيها مشكلة الاختصاص القضائي في الجرائم الإلكترونية، لأنه يرى أن المشرع الفرنسي وضع ضوابط تحكم الاختصاص القضائي الفرنسي، فيما يخص الجرائم المرتكبة في الخارج، وذلك وفقاً للمادة (113-2) من ق.ع.ف، والتي تعتبر الجريمة واقعة على الأراضي الفرنسية متى وقعت أحد عناصرها المكونة لها داخل الأراضي الفرنسية.

ومن الأمثلة عن الجرائم الإلكترونية التي تضرر منها أكثر من إقليم، جريمة قام بها المدعو غاري ماكينون (Gary McKinnon)، الذي كان يعمل مسؤول نظم في المملكة المتحدة في عامي 2001 و2002، حين اخترق من حاسوبه المنزلي (97) حاسوبًا عسكريًا خاصاً بوكالة ناسا التابعة للولايات المتحدة الأمريكية، حيث قام بحذف بيانات وملفات نظام التشغيل مما أدى إلى إغلاق الشبكة العسكرية لواشنطن لمدة أربع وعشرين ساعة (24)، كما تمكن من الوصول إلى سجلات في أجهزة الحواسيب الخاصة بمحطة الأسلحة البحرية الأمريكية "إيرل" والتي كانت تستخدم لرصد الهوية والموقع والحالة المادية، والاستعداد للقتال واستعداد السفن البحرية، كما قام المدعى عليه بنسخ بيانات وملفات تحتوي على حسابات وكلمات المرور من بينها ملفات كانت موجودة في أجهزة حواسيب تابعة للجيش الأمريكي، وأخرى تابعة للبحرية الأمريكية ووكالة ناسا (NASA).

وبعد التحقيقات التي أجرتها وحدة الجرائم التقنية الوطنية في المملكة المتحدة تبين أن غاري ماكينون كان مسؤولاً عن تلك الاختراقات، ورغم اعتقاله إلا أنه لم يتم توجيه أي اتهام له من المملكة المتحدة، وفي شهر سبتمبر من سنة 2004 وجهت له تهم من مقاطعتي فرجينيا ونيوجيرسي

1 معتز سيد محمد أحمد عفيفي، قواعد الاختصاص القضائي بالمسؤولية الإلكترونية عبر شبكة الانترنت، الطبعة الأولى، دار الجامعة الجديدة، الازاريطة، الإسكندرية، القاهرة، 2013، ص47.

2 معتز سيد محمد أحمد عفيفي، المرجع نفسه، ص 45.

اللتين أصدرتا فيما بعد مذكرة توقيف ضده، وفي شهر ماي سنة 2006 قرر قاضي من محكمة الصلح في بوستريت أنه يجب تسليم ماكينون؛ بعدها وقع وزير الداخلية أمراً يسمح بتسليم ماكينون إلى الولايات المتحدة الامريكية بناءً على الأمر القضائي الصادر ضده، وكذلك تنفيذاً لبنود المعاهدة الجديدة لتسليم المجرمين التي تمت بين الولايات المتحدة والمملكة المتحدة[1].

لقد كان للتعاون دور كبير في حل عدة قضايا إلكترونية والقبض على مرتكبيها، ولولا التعاون الدولي لبقي مرتكبوها أحراراً، فأول قضية سجلت على أنها دولية كانت من نصيب ألمانيا الغربية عام 1989 بعد اتهام أربعة من الهاكرز الألمان –انتحر أحدهم قبل القبض عليه– باختراق أجهزة حكومية أمريكية وسرقة المصدر البرمجي لنظام تشغيل وبيعه للاتحاد السوفيتي[2]، كما كانت القضية المعروفة باسم نقص المناعة المكتسبة (الايدز) من القضايا التي لفتت النظر إلى البعد الدولي للجريمة الإلكترونية[3].

وفي قضية أخرى قضت إحدى المحاكم الألمانية في جريمة إلكترونية ارتكبت على أراضيها بأن الحصول على البيانات الخاصة بهذه الجريمة والمخزنة بشبكات اتصال موجودة في سويسرا لا يتحقق إلا بطلب المساعدة من الحكومة السويسرية، وهو ذات الأمر حدث حين تم نشر فيروس (Love Bug) عام 2000 الذي تسبب في إتلاف المعلومات الموجودة في العديد من أجهزة الحاسب الآلي، إذ عند اكتشاف الخبراء الأمريكيون المكان الذي أُرسل منه الفيروس، استدعى منهم الأمر تفتيش

1 Adel Azzam Saqf Al- Hait, op.cit, p: 80-81.

2 منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، المرجع السابق، ص 49.

3 وتتلخص وقائع هذه القضية التي حدثت عام 1989، في قيام أحد الاشخاص بتوزيع عدد كبير من النسخ الخاصة باحد البرامج الذي هدَف في ظاهره إلى اعطاء بعض النصائح الخاصة بمرض نقص المناعة المكتسبة، الا ان هذا البرنامج في حقيقته كان يحتوي على فيروس (حصان طروادة) اذ كان يترتب على تشغيله تعطيل جهاز الحاسوب عن العمل، ثم تظهر بعد ذلك عبارة على الشاشة يقوم الفاعل من خلالها بطلب مبلغ مالي يرسل على عنوان معين حتى يتمكن المجني عليه من الحصول على مضاد للفيروس وفي الثالث من فبراير من عام 1990، تم القاء القبض على المتهم جوزيف بوب في أوهايو بالولايات المتحدة الامريكية وتقدمت المملكة المتحدة بطلب تسليمه لها لمحاكمته أمام القضاء الانجليزي، حيث أن إرسال هذا البرنامج قد تم من داخل المملكة المتحدة وبالفعل وافق القضاء الامريكي على تسليم المتهم وتم توجيه أحدى عشرة (11) تهمة ابتزاز اليه وقعت معظمها في دول مختلفة، إلا أن إجراءات محاكمة المتهم لم تستمر بسبب حالته العقلية ومهما كان الامر، فانه لهذه القضية أهميتها من ناحيتين: الأولى: أنها المرة الاولى التي يتم فيها تسليم متهم في جريمة معلوماتية، والثانية: أنها المرة الأولى التي يقدم فيها شخص للمحاكمة بتهمة اعداد برنامج خبيث (فيروس)"،**انظر في ذلك:** تركي بن عبد الرحمن المويشير، المرجع السابق، ص.ص: 28–29، نائلة عادل محمد فريد قورة، مرجع سابق، ص 48.

منزل المشتبه فيه المتواجد بالفيليبين، والذي لم يكن ممكننا إلا بالتعاون مع السلطات الفيليبينية، والحصول على إذن من قاضي التحقيق بالفيليبين[1].

ومن الأمثلة أيضاً على دور التعاون الدولي في مكافحة الجرائم الإلكترونية عملية (Falcon)، والتي تمت في شهر أبريل سنة 2005، بمشاركة الشرطة الفيدرالية الأمريكية (FBI) والانتربول والشرطة الفرنسية، مما سمح بتفكيك شبكة تنشط في العديد من الدول الاوربية، وعملية محطم الجليد (IceBreaker) التي قامت بها يوروبول (EUROPOL) في 14 من شهر جوان سنة 2005، والتي تمت خلالها مداهمة وتفتيش أماكن في ثلاثة عشر دولة أوربية هي: النمسا، وبلجيكا، وفرنسا، وألمانيا، والمجر، وايسلندا، وايطاليا، وهولندا، وبولونيا، والبرتغال، وسلوفاكيا، والسويد، وبريطانيا العظمى، كما تم توقيف أشخاصاً في كل من فرنسا، وبلجيكا، والمجر، وايسلندا والسويد، وعملية أوديسيوس (Odysseus) والتي تمت في 26 من شهر فبراير سنة 2004 بمبادرة من يوروبول، وقوات الشرطة تمت خلالها عمليات شملت عشرة (10) دول هي: استراليا، وبلجيكا، وكندا، والمانيا، والنرويج، وبيرو، واسبانيا، والسويد وبريطانيا[2].

ومن الأمثلة أيضاً على القضايا الدولية التي شاركت فيها السلطات المتخصصة المعنية بالجرائم السيبرانية في صربيا، ونجحت القضايا بسبب تنفيذ اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية وأحكامها المتعلقة بالتعاون الدولي المنفذة في القانون الصربي[3].

---

1 حنان ريحان مبارك المضحي، المرجع السابق، ص 365، **نقلا عن**: مفتاح بوبكر المطردي، الجريمة الإلكترونية والتغلب على تحدياتها، ورقة مقدمة إلي المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية، المنعقد بجمهورية السودان، من 23 إلى 25 سبتمبر 2012، ص 23.

2 درار نسيمة، المرجع السابق، ص.ص: 307-308، **نقلاً عن**: جان فرنسوا هنروت، أهمية التعاون الدولي والتجربة البلجيكية في تبادل المعلومات بين عناصر الشرطة والتعاون القضائي، مداخلة في الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، 16-20 يونيو 2007، المملكة المغربية، ص 108.

3 (أ) عملية "Shadow Web" في فبراير 2018 تمت السيطرة على أحد أكبر المنتديات الإجرامية، المسمى " In Fraud" والذي يتعامل في معلومات بطاقات الائتمان المسروقة. وقد قُبض على مواطن صربي ووُجهت إليه تُهم جنائية؛ (ب) عملية "Power Off" في أبريل 2018 تمت السيطرة على أكبر خدمة إجرامية للهجمات الموزَّعة الخاصة بحجب الخدمة في العالم، وهي "Webstresser" وقُبض على مواطنَين صربيَين اثنين ووُجهت إليهما تُهم جنائية. وشاركت في العملية السلطات المختصة في إسبانيا وألمانيا وإيطاليا وصربيا وكرواتيا وكندا والمملكة المتحدة والنمسا وهولندا والولايات المتحدة، بالإضافة إلى هونغ كونغ، الصين. وبدأ المدعي الخاص المعني بجرائم التكنولوجيا العالية التحقيقات مع شخصين مشتبه بهما، وضُبطت للمرة الأولى عملة مشفرة لدى أحد المشتبه بهما؛

وعلى الرغم من كل المجهودات التي تقوم بها مختلف الدول للتقليل من الصعوبات التي تواجه مكافحة الجرائم الإلكترونية، وخاصة تلك التي تواجهها آليات التعاون الدولي، الذي يهدف إلى مكافحة الجريمة، وإلى تحقيق غاية سامية تتمثل في تحقيق الأمن الجماعي لأعضاء الجماعة الدولية، وكفالة العيش الآمن للشعوب، من خلال تبني سياسة محكمة في مجال مكافحة الإجرام، لاسيما الإجرام المعلوماتي، وذلك بالبحث عن المجرمين وملاحقتهم والقبض عليهم، وتنفيذ العقوبات المحكوم عليهم بها، والاعتداد بالأحكام الصادرة ضدهم عند محاكمتهم عن الجرائم الأخرى التي يرتكبونها في غير دولة الإدانة[1]، إلا أن تلك المجهودات تبقى غير كافية، وتصادفها عدة عقبات كسيادة الدول، وحقوق الانسان، وقواعد الاختصاص في القانون الجنائي التي في كثير من الاحيان تحول دون تنفيذ العقوبة على المتهم في حالة إثبات الجريمة من حيث القانون الواجب التطبيق[2]، كما أن مسالة التعاون الدولي على الرغم من أهميتها نجد أن بعض الدول لم تنص عليها، كما هو الحال لدى المشرع الكويتي[3].

لذا يجب البحث عن طرق أخرى لمكافحة الجريمة الإلكترونية، تكون بالموازاة مع الآليات السابقة حتى نصل إلى إيجاد آليات تكون قادرة على مواجهة هذا النمط من الجرائم.

البند الثالث: الدعوة لإنشاء محكمة جنائية دولية للجرائم الإلكترونية.

من خلال ما تم استعراضه في البندين السابقين، يتبين لنا أن البعد الدولي للجرائم الإلكترونية يستدعي تنظيم تعاون دولي في سبيل مكافحتها، كالمساعدة الدولية بين أجهزة الشرطة الدولية "الانتربول" لمتابعة المجرمين والقبض عليهم، إضافة إلى تنظيم تعاون على مستوى أجهزة التحقيق (النيابة العامة) وأجهزة المحاكمة، بحيث يتم الإعتداد بأعمال التحقيق والمحاكمة التي تجري في دولة

(ج) عملية "The Dark Overlord" في ماي 2018 وتتعلق بجماعة إجرامية سرقت بيانات شخصية وابتزت أصحابها"، **ينظر**: تقرير الأمين العام، الجمعية العامة، الأمم المتحدة، مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية (القرار رقم 73/187)، الدورة الرابعة والسبعون، البند 109 من جدول الأعمال المؤقت*(A/74/130)، 30 جويلية 2019، ص 09.

1 عادل يحيي، المرجع السابق، ص.ص: 115-116.

2 أحمد عبد اللاه المراغي، المرجع السابق، ص 126.

3 بوقرين عبد الحليم، المرجع السابق، ص 321.

معينة من الدول الأخرى في مجال هذا النوع من الجرائم[1]، عملاً بمبدأ عالمية النص الجنائي[2]، وتفادياً لكل العراقيل التي تواجه آليات التعاون الدولي. ولأجل مكافحة أفضل ومحاكمة أسرع وأوسع نطاقاً واختصاصاً، وتخفيفاً من الفوارق الموجودة بين الأنظمة العقابية الداخلية، دعا معظم رجال القانون إلى إنشاء محكمة إلكترونية لسد الفجوة القانونية التي أحدثها التطور التكنولوجي الهائل في السنوات الأخيرة، كون التعاون الدولي أصبح حتمية يفرضها الواقع وخطورة هذه الجريمة[3].

فالتقاضي الإلكتروني هو تلك السلطة الممنوحة لمجموعة متخصصة من القضاة النظاميين بنظر الدعوى ومباشرة الإجراءات القضائية بوسائل إلكترونية مستحدثة، ضمن نظام أو أنظمة قضائية معلوماتية متكاملة الأطراف والوسائل، تعتمد منهج تقنية شبكة الربط الدولية (الإنترنت) وبرامج الملفات الحاسوبية الإلكترونية بنظر الدعاوى والفصل بها وتنفيذ الأحكام بغية الوصول لفصل سريع بالدعاوى والتسهيل على المتقاضين[4]، فإنشاء محكمة رقمية (Digital Court) – المحكمة التي تختص بالجرائم الرقمية Digital crime-[5] هو أمر يجب أن تسعى فيه كل الدول بمساعدة الأمم المتحدة وتحت رعايتها، حتى يتم إنشاء محكمة جنائية دولية للجرائم الإلكترونية تنظر في الجرائم الخطيرة؛ كالإرهاب الإلكتروني، والحروب الإلكترونية، جرائم الفساد وغسيل الأموال المرتكبة عبر الوسائط الإلكترونية، الجرائم المرتكبة ضد الأطفال بصفتهم فئة ضعيفة تجب حمايتها وغيرها من الجرائم الخطيرة التي يجب ملاحقة مرتكبيها والعمل على عدم إفلاتهم من العقاب.

1 غانم محمد غانم، المرجع السابق، ص 218.

2 مبدأ العالمية: ويقصد به تطبيق النص الجنائي للدولة التي يتواجد فيها الجاني، دون النظر إلى جنسيته أو جنسية المجني عليه أو مكان ارتكاب الجريمة"، **انظر**: نديم محمد حسن الترزي، المرجع السابق، ص 309.

3 عبد العال الديربي، محمد صادق اسماعيل، الجرائم الإلكترونية دراسة قانونية قضائية مقارنة مع احدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والإنترنت، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2012، ص 122؛ شيرين محمد إحسان عبد الحافظ، المرجع السابق، ص 193.

4 عرفت المحاكم – ولاية نيويورك- مصطلح الوسائل الإلكترونية بأنه: أية طريق لإرسال المعلومات بين الحواسيب المرتبطة بشبكات وأجهزة أخرى من غير أجهزة البث الإذاعي، وتصميم هذه الآلية لاستقبال وإرسال البيانات والمعلومات بحيث تسمح هذه العملية للمستقبل باستخدام نسخ على شيء ملموس مادي تعبر عن ما تضمنته هذه البيانات. **أشار إلى ذلك**: حازم محمد الشرعة، التقاضي الإلكتروني والمحاكم الإلكترونية (كنظام قضائي معلوماتي عالي التقنية وكفرع من فروع القانون بين النظرية والتطبيق)، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2010، ص 57،

5 محمد رضوان هلال، المرجع السابق، ص 13.

فالسعي إلى إنشاء محكمة افتراضية (Virtual Tribunal)، هي فكرة تم إرساء دعائمها في شهر مارس سنة 1996، بهدف إعطاء حلول سريعة للمنازعات المتعلقة بالإنترنت عن طريق وسيط معتمد من المركز تكون له الخبرة القانونية في الفصل في المنازعات الإلكترونية، ودراية بالقوانين الناظمة للتجارة الإلكترونية وعقودها، وقانون الإنترنت ومنازعات العلامات التجارية والملكية الفكرية، وغيرها من المواضيع المتصلة بالتجارة، حيث تفصل المحكمة الافتراضية في النزاع خلال 72 ساعة، ويكون حكمها نهائياً غير قابل للاستئناف[1]؛ لأن موافقة الأطراف عليه هي التي تعطيه القوة القانونية، كما تم إنشاء محكمة فضائية (Cyber Tribunal) في كلية الحقوق بجامعة مونتريال بكندا في شهر سبتمبر سنة 1996 من قبل باحثين بقسم القانون العام الكندي، والتي كانت تهدف إلى تطوير قواعد التنظيم الذاتي الخاص بالإنترنت، ومراقبة التطبيق الفعلي لهذه القواعد، وحل المنازعات التي تنشأ عن طريق شبكة الإنترنت، حيث تختص في المنازعات الناشئة عن التجارة الإلكترونية، المنافسة، حق المؤلف، حرية التعبير، الحياة الخاصة[2].

ومن المؤكد أن مثل هذه المحاكم سوف يذلل العديد من الصِعاب التي كانت تواجه المتقاضين ومنها مشكلة المحكمة المختصة[3]، وطول الإجراءات، ولكن المحكمة التي نتمنى أن يتم إنشاؤها هي محكمة جنائية دولية متخصصة إلكترونية تكون من ضمن هياكل الأمم المتحدة وتحت إشرافها تشارك في إنشائها كل الدول المنضمة لهذه الهيئة، يخصص لها طاقم من القضاة المتخصصين في مثل هذه القضايا، خاصة وأننا نعلم أنه من بين الصعوبات التي تواجه مكافحة هذه الجريمة الخطيرة قلة القضاة المتخصصين، وكذا المحامين[4]؛ لأن هناك اتجاه قوي بين المتخصصين ورجال القانون ينادي بضرورة عقد دورات تدريبية لرجال القانون لدراسة قانون الحاسبات وتقنيته في المعاهد المتخصصة على أن تكون هذه الدراسات نصف سنوية أو سنوية على أقصى حد، حتى يستطيع

1 معتز سيد محمد أحمد عفيفي، المرجع السابق، ص ص 111-112.

2 معتز سيد محمد أحمد عفيفي، نفس المرجع، ص ص 112-113.

3 معتز عفيفي، المحكمة المختصة بدعوى التعويض عن الجريمة المعلوماتية (بين منصة القضاء ومنصة التحكيم)، مجلة الفكر القانوني والاقتصادي، كلية الحقوق، جامعة بنها، مصر، العدد (04)، يونيو 2011، ص 536.

4 أحمد خليفة الملط، المرجع السابق، 2006، ص 164-165، **نقلاً عن**:

- Germinant michael, *viruses and the law communication of the ACM*, vol 32 june1989,p 660. Where he said « Even if computer crims tried in cout, few lawyer. Judge of jaurors are very knowledgeable regarding computers with the growith in computer viruses lawyer repesenting suppliers and users need to understand he basic technology involved and the legal implication.»

رجال القانون الذين يرغبون في التخصص في مجال المعلوماتية أن يلحقوا بركب التقنية المعلوماتية السريعة التطور[1]، فقد أصبح ذلك ممكناً من خلال عـدة عـوامل ستسهل تلك العملية، ومنها أن الدول أصبحت تبرم اتفاقيات تحتوي على عدة بنود تمكنها من إجراء مختلف الإجراءات المطلوبة للتحقيق في الجرائم وجمع الأدلة عنها[2]، والقيام بسماع الشهود عن طريق المحادثة المرئية عن بعد[3]، مثلما نص على ذلك المشـرع الجـزائري من خـلال عـدة نصوص قانونية، كقانون الإجراءات الجزائية الجزائري، والقانون رقم 15-03 الخاص بعصرنة قطاع العدالة[4].

وبالإضافة إلى ما نص عليه المشرع الجزائري في هذا الإطار، قام القضاء الجزائري بطبيق المحادثة المرئية عن بعد في قضايا عرضت عليه؛ مثل: القضية التي استجوب فيها المتهم المحبوس بمؤسسة إعادة التربية والتأهيل بمدينة القليعة عن طريق الشاشة الإلكترونية، وبعد اعترافه بالوقائع المنسوبة إليه، وتقديم النيابة طلباتها، والدفاع الذي التمس ظروف التخفيف، أصدرت المحكمة حكماً علنياً ابتدائياً حضورياً وجاهياً بإدانة المتهم "د/ج"[5].

---

1 أحمد خليفة الملط، نفس المرجع، ص 165، **نقلاً عن**:

- Diane Crawford, *why is the law always behind?* Published in computer under attack, P.R article 28, p 451.

2 يمكن الرجوع إلى الفقرة الأولى من المادة الأولى (1) من الاتفاقية المتعلقة بالتعاون القضائي في المجال الجزائي بين الجمهورية الجزائرية الديمقراطية الشعبية والبوسنة والهرسك، المؤرخة في 16 شوال عام 1441 الموافق 08 يونيو سنة 2020، الموقعة بالجزائر في 20 سبتمبر سنة 2011، الصادرة في الج.ر.ج، رقم 36، المؤرخة في 17 يونيو سنة 2020، المصادق عليها بالمرسوم الرئاسي رقم 20-148.

3 المحادثة المرئية عن بعد هي وسيلة اتصال مرئي ومسموع متعدد الأطراف يستطيع بمقتضاها شـخصان أو عدة أشخاص المشاركة في مناقشة أو حوار بصور ايجابية وفعالة، رغم اختـلاف الأمـاكن التي يتواجدون فيها داخل الدولة الواحدة أو تفرقهم بين عدة دول. **انظر في ذلك:** محي الدين حسيبة، سماع الشهود عن طريق المحادثة المرئية عن بعد بين الحق في الحماية وحقوق الدفاع، مجلة البحوث والدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة لونيسي علي، البليدة 02، الجزائر، العدد العاشر (10)، جانفي 2017، ص 283، **نقلاً عن:** خالد موسي توني، الحماية الجنائية الإجرائية للشهود"دراسة مقارنة"، دار النهضة العربية، القاهرة، الطبعة الأولى، 2010، ص 119.

4 المـادة (65 مكرر 27) من الأمر رقم 15-02 يعدل ويتمم الأمر رقم 66-156 المؤرخ في 8 يونيو 1966 والمتـضمن ق.إ.ج.ج، المؤرخ في 23 يوليو 2015، المنشور في الج.ر العدد 40 بتاريخ 23 يوليو 2015؛ القانون رقم 15-03، المؤرخ في 11 ربيع الثاني عام 1436 الموافق أول فبراير سنة 2015، المتعلق بعصرنة العدالة، المنشور بالج.ر.ج العدد 06، بتاريخ 10 فبراير سنة 2015: المادة (09):" فضلاً عن الطرق المنصوص عليها في قانون الإجراءات المدنية والإدارية وقانون الإجراءات الجزائية في هذا المجال، يمكن أن يتم تبليغ وإرسال الوثائق والمحررات القضائية بالطريق الإلكتروني وفقا للشروط والكيفيات المحددة في هذا القانون...".

5 حكم عن محكمة القليعة، قسم الجنح، قضية رقم 17982بتاريخ 07 أكتوبر 2015.

إن أداء الشهادة بواسطة إحدى برامج المحادثة أو مؤتمر الفيديو عبر شبكة الإنترنت، هو أمر جائز إذا تم الاتصال المرئي مباشرة بين القاضي والشاهد أثناء النظر في الدعوى، وهو إجراء قد يلجأ إليه في حالة عدم تمكن الشاهد من الإدلاء بشهادته نظراً لمرض أو لسفر أو لبعد المسافة[1]، ومن القوانين التي تجيز سماع الشهادة المسجلة في شريط فيديو قانون الإجراءات النمساوي في المادة 247/أ وقانون الإجراءات الايطالي، الذي أدخل نظام المشاركة عن بعد بواسطة التسجيل التليفزيوني في الدعوى الجنائية بموجب قانون صدر سنة 1992، وفي سنة 1998 وسع المشرع الإيطالي من نطاق هذه الوسيلة، بحيث يمكن استعمالها في كافة مراحل الدعوى الجنائية[2].

أما في القضاء الأمريكي فيوجد نظامين للشهادة المرئية؛ الأول وهو نظام الشهادة المرئية ذات الاتجاه الواحد، والذي تكون الرؤية من جانب واحد، وهو هيئة المحلفين والمحكمة، أما الشاهد فلا يرى إلا الكاميرا التي أمامه، أما النظام الثاني فهو أن تتم الشهادة المرئية في اتجاهين، إذ يرى الشاهد المحكمة ويراه من في المحكمة من قاضي ومحلفين، ويكون كل ما يدور في الجلسة مرئياً له بالمقابل، بما يحقق قاعدة الوجاهية المطلوبة في إجراءات المحاكمات[3]، فلمحكمة الموضوع كامل الحرية في تكوين عقيدتها مما ترتاح اليه من أقوال الشهود ومتى أخذت بشهادة شاهد، فإن ذلك يفيد أنها أطرحت جميع الاعتبارات التي ساقها الدفاع لحملها على عدم الأخذ بها[4]، وهو ما سيضمن عدالة المحاكمة، ونزاهة الإجراءات القضائية ويُسرها[5]، فاستعمال المحكمة الإلكترونية للوسائل التقنية الحديثة سوف يعمل على تخطي عدة تعقيدات كانت موجودة في الإجراءات التقليدية كتسليم المجرمين وسماع الشهود[6]، والحصول على الأدلة الإلكترونية في وقتها.

1 المتولي عطيه عبد الباقي إبراهيم، أداء الشهادة بوسائل الاتصال الحديثة في منظور الفقه الإسلامي، مجلة كلية الشريعة والقانون بطنطا، العدد الثلاثون، الجزء الرابع، مصر، ديسمبر 2015، ص 1434.

2 فهد عبد الله العبيد العازمي، المرجع السابق، ص.ص: 432 إلى 436.

3 فهد عبد الله العبيد العازمي، المرجع نفسه، ص.ص: 433-434.

4 حكم محكمة النقض المصرية، الدائرة الجنائية، في الطعن المقيد بجدول المحكمة رقم 8426 لسنة 87 القضائية، السالف الذكر.

5 محمد عبد الفتاح عبد المقصود على، المرجع السابق، ص 93.

6 يحصر قانون الدليل بولاية كاليفورنيا شهود الجريمة الإلكترونية في قائمة هي كالتالي: محلل النظم الذي صمم وحدد برنامج الكمبيوتر الذي أنتج الدليل، المبرمج الذي قام بتحرير البرنامج واختباره، المشغل الذي يقوم بتشغيل البرامج، طاقم عمليات البيانات الذي يعد البيانات بالصورة التي يستطيع الكمبيوتر قراءتها (شريط أو اسطوانة)، أمناء مكتبة الأشرطة الذين يتحملون مسؤولية توفير الأشرطة أو الأسطوانات التي تشتمل على البيانات، مهندس الصيانة الإلكترونية الذي يقوم على صيانة الجهاز الأصلي والتأكد من عمله بصورة

المطلب الثاني: المؤسسات الإقليمية لمكافحة الجريمة الإلكترونية.

وُضعت عدة مؤسسات إقليمية لمكافحة الجريمة، كانت نتاج توحيد مجهودات دول جمع بينها في كثير من الأحيان الموقع الجغرافي والحدود السياسية، والتهديد المشترك الذي تفرضه الجرائم العابرة للحدود كما هو الحال في الجرائم الإلكترونية، ومنها على سبيل المثال الأسيابول (Asianopol) الخاصة بدول آسيا والأميروبول (Ameropol) الخاصة بدول أمريكا، واليوروبول (Europol)، والأورجست (Eueojust) الخاصين بدول أوروبا، والاتحاد الإفريقي للتعاون الشرطي (Afripol)، الخاص بدول إفريقيا، والموجود مقره في الجزائر العاصمة.

فهي كلها آليات مؤسساتية قوية جُعِلت لمكافحة هذه الظاهرة الإجرامية وتسهل القبض على مرتكبيها، ولكن نظراً لكثرة تلك المؤسسات ستقتصر الدراسة على ثلاثة منها، وهي: الاتحاد الإفريقي للتعاون الشرطي (Afripol) (الفرع الأول)، ومكتب الشرطة الأوروبية اليوروبول (Europol) والوكالة الأوروبية للتعاون في مجال العدالة الجنائية الأورجست (Eueojust) (الفرع الثاني).

الفرع الأول: الآفريبول كمؤسسة إقليمية لمكافحة الجريمة الإلكترونية.

الإتحاد الإفريقي للتعاون الشرطي"آفريبول"، هو آلية أنشئت من أجل مضاعفة رصيد التعاون الشرطي في الدول الإفريقية على المستويات الإستراتيجية والعملياتية والتكتيكية بين مؤسسات الشرطة في إفريقيا[1]، ولمنع الجريمة العابرة للحدود الوطنية والكشف عنها والتحقيق فيها بالتعاون مع المؤسسات الشرطة الوطنية والإقليمية والدولية.

ولقد شكلت الندوة الجهوية الإفريقية الثانية والعشرون (22) للانتربول المنعقدة أيام 10، و11، و12 من شهر سبتمبر سنة 2013 بمدينة وهران بالجزائر، الانطلاقة الأساسية لإنشاء الآفريبول، حيث تبنى المدراء والمفتشون العامون للشرطة من الدول الأعضاء للإتحاد الإفريقي فكرة إنشاء آلية للتعاون الشرطي الإفريقي، ثم تلا ذلك اللقاء عدة لقاءات، أُعلن في اللقاء المنعقد بالجزائر بتاريخ الحادي عشر (11) من شهر فبراير سنة 2014، على إنشاء الآلية الإفريقية للتعاون الشرطي

صحيحة، موظفو المدخلات والمخرجات المسئولون عن معالجة المدخلات المستخدم في تنفيذ البرامج، المستخدم النهائي الذي يمد بالمعلومات المدخلة ويصرح بتنفيذ برامج الكمبيوتر ويستخدم نواتجها"، **انظر**: علاء محمود يسن حراز، المرجع السابق، ص 402.

1 براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل شهادة الدكتوراه في العلوم، تخصص القانون، قسم الحقوق، كلية الحقوق والعلوم الإنسانية، جامعة مولود معمري، تيزي وزو، الجزائر، نوقشت في 2018/06/27، ص 308.

"آفريبول"[1]، ويعد انعقاد الجمعية العامة الأولى لآلية الإتحاد الأفريقي للتعاون في مجال الشرطة "الآفريبول" بمثابة التأسيس الفعلي للآفريبول، والذي تم بفندق الأوراسي بالجزائر العاصمة أيام 14، و15، و16 من شهر ماي سنة 2017، بعد أن كانت قد تمت المصادقة على القوانين المُنظِمة للآفريبول من قبل قادة الدول والحكومات الإفريقية خلال القمة العادية 28 للإتحاد الإفريقي التي انعقدت بالعاصمة الإثيوبية "أديس أبابا" شهر جانفي 2017.[2]

وحسب المادة الثانية (02) من النظام الأساسي لآلية الإتحاد الإفريقي للتعاون الشرطي "آفريبول"، فإن هذه الأخيرة تعتبر مؤسسة تقنية، باعتبارها آلية التعاون الشرطي بين الدول الأعضاء في الاتحاد الإفريقي، وتستمد شخصيتها القانونية منه، حيث تقوم الآفريبول على عدة مبادئ كما جاء في المادة الخامسة (05) من نفس النظام، والتي تضمنت بعض المبادئ المنصوص عليها في المادة الرابعة (04) من القانون التأسيسي للإتحاد الإفريقي، ومن هذه المبادئ: "احترام مبادئ الديمقراطية وحقوق الإنسان، وسيادة القانون والحكم الراشد"[3]، وفقاً لما جاء في الميثاق الإفريقي لحقوق الإنسان والشعوب، والإعلان العالمي لحقوق الإنسان وغيرها من الصكوك والمواثيق ذات الصلة، مع عدم تدخل أي دولة عضو في الشؤون الداخلية لدولة أخرى، ضماناً لاحترام السيادة والقوانين الوطنية للدول الأعضاء في الإتحاد الإفريقي للتعاون الشرطي"آفريبول"، واحتراماً لأخلاقيات المهنة الشرطية.

كما يسعى الاتحاد الإفريقي للتعاون الشرطي"آفريبول" في ظل كل تلك المبادئ لتحقيق عدة أهداف ومهام نصت عليها المادتين: الثالثة (03)، والرابعة (04) من النظام الأساسي لآلية الاتحاد الإفريقي للتعاون الشرطي "آفريبول" منها: مساعدة مؤسسات الشرطة في الدول الأعضاء على وضع إطار للتعاون بين مؤسسات الشرطة على المستويات الوطنية والإقليمية والقارية والدولية، والعمل على تطوير قدرات أجهزة الشرطة في الدول الأعضاء، بواسطة برامج متطورة لتدريب

1 Déclaration d' Alger relative a la création du mécanisme africain de coopération policière AFRIPOL, Conférence africaine des directeurs et inspecteurs généraux de police sur AFRIPOL, Alger, les 10 et 11 fevrier 2014, p :01 , sur le site : *http://www.peaceau.org/ uploads /algiers -declaration-afripol-french.pdf*

2 جوزي صليحة، الجزائر تحتضن الجمعية العامة الأولى لآلية الإتحاد الإفريقي للتعاون في مجال الشرطة "الأفريبول"، مجلة الشرطة، وحدة الطباعة الرويبة، الجزائر، العدد مائة وستة وثلاثين (136)، جوان 2017، ص 09.

3 الفقرة (و) من المادة الرابعة (04) من القانون التأسيسي للاتحاد الإفريقي، على الموقع الإلكتروني الموالي: *https://au.int/sites /default/files/pages/34873-file-au_constitutive_act_ar.pdf* ، تاريخ الاطلاع: 2018/08/02.

الشرطة من خلال إنشاء مراكز امتياز إفريقية، وكذا تعزيز التنسيق مع هياكل مماثلة في منع ومكافحة الجريمة، وتشجيع المساعدة الفنية المتبادلة ذات الخبرة العالية والممارسات الجيدة بين مؤسسات الشرطة، لتحسين كفاءتها وفاعليتها وتسهيل المساعدة القانونية المتبادلة، وبالأخص تسليم المجرمين، من خلال تيسير تبادل أو تقاسم المعلومات والاستخبارات لمنع الجريمة والكشف عنها وتسهيل التحقيق فيها بالتعاون والتنسيق مع الآليات العملياتية الأخرى، سواء إقليمية أو دولية لدعم استراتيجية التنسيق والتعاون بين مختلف تلك الآليات المؤسساتية، وتطوير الأدوات القارية لمنع الجريمة، وإعداد إستراتيجية إفريقية منسقة لمكافحة مختلف أنواع الجرائم الخطيرة كالجريمة الإلكترونية[1]، مما يستدعي منها تطوير أنظمة الاتصال المناسبة وقواعد البيانات الضرورية مثلما تم الإشارة إليه في توصية من توصيات أشغال الجمعية العامة الثانية للآفريبول، المنعقدة في الجزائر العاصمة يومي 15 و16 من شهر أكتوبر سنة 2018، والتي دعت فيها منظمة الآفريبول إلى دعم وتسريع وتفعيل نظام الاتصالات (AFSYCOM) لجميع قوات الشرطة في البلدان الأعضاء لتبادل المعلومات والوثائق[2]، من أجل أداء مهامه على أحسن وجه مع إمكانية قيامها بأي مهام أخرى قد تحددها أجهزة صنع السياسة للاتحاد الإفريقي.

لذلك، تعتبر هذه المنظمة أداة فعالة وفاعلة لا يمكن الاستغناء عنها في مجال التعاون الشرطي الذي سيضمن رداً مشتركاً ومناسباً على كل التهديدات المستحدثة التي تواجهها بلدان إفريقيا وتمس بالأمن والسلم العالميين، كما تعد منظمة الاتحاد الإفريقي للتعاون الشرطي"آفريبول" إضافة نوعية بالنسبة للجزائر التي لها عدة مقومات تساعدها في أن يكون لها دور بارز في أمننة القارة الإفريقية، خاصة وأنها احتضنت مقر "الآفريبول"، وتم اختيارها لرئاسة هذه المنظمة مرتين متتاليتين.

الفرع الثاني: اليوروبول والأوروجيست آليتين إقليميتين لمكافحة الجريمة الإلكترونية

اليوروبول والأوروجيست وكالتين مهمتين على المستوى الأوربي في مكافحة الجريمة الخطيرة بصفة عامة، والجريمة الإلكترونية بصفة خاصة، هذه الجريمة التي فرضت نفسها على جميع

1 المادة الثالثة (03)، والرابعة (04) من النظام الأساسي لآلية الاتحاد الإفريقي للتعاون الشرطي" آفريبول"، السالف الذكر.

2 Déclaration de l'Algérie, *Segment Ministériel de la 62ème session de la Commission des Stupéfiants Vienne*, 14 et 15 mars 2019, sur le site : *https://www.unodc.org/documents/commissions/CND/2019/2019_MINISTERIAL_SEGMENT/19March/ALGERIA.pdf.*

المستويات الدولية والإقليمية والوطنية، مما استوجب وضع آليات كفيلة للتصدي لخطورتها، ويعد جهاز الشرطة الأوربية المسمى "اليوروبول (Europol)" إحدى تلك الآليات العملياتية التي لها دور مهم في مكافحة الجريمة الإلكترونية.

البند الأول: اليوروبول وكالة إقليمية لمكافحة الجريمة الإلكترونية.

تم اقتراح إنشاء مكتب مركزي للشرطة الجنائية لدول الإتحاد الأوربي، والمسمى حالياً "اليوروبول" في قمة لكسمبورج سنة 1991، ليتم إنشاؤه بشكل ملموس بموجب اتفاقية ماستريخت التي وقعت في السابع من شهر فبراير سنة 1992 في مدينة ماستريخت الهولندية، والتي دخلت حيز التنفيذ في الأول من نوفمبر سنة 1993 [1]، ولأن الإتفاقية كانت تهدف لإقامة وحدة أوروبية شاملة وإلى تحسين التعاون، وتيسير الاتصال، وضمان تبادل المعلومات بشكل فعال بين الدول الأعضاء في مجالات مختلفة خاصة مكافحة الجريمة، تم تحديد مقر اليوروبول في مدينة لاهاي سنة 1994، ليحصل على الشخصية القانونية في الفاتح من شهر أكتوبر سنة 1998، ليبدأ عمله بصفة فعلية في الأول من شهر جويلية سنة 1999[2].

إن مكتب الشرطة الأوروبية "يوروبول" (Europol) هو وكالة لإنفاذ القانون تابع للاتحاد الأوروبي، يحتل موقعًا مركزيًا في بنية الأمن الأوروبي، يوظف أفضل محللي الجريمة المدربين في أوروبا والذين يستخدمون أدوات فنية متطورة من أجل مساعدة الوكالات الوطنية في تحقيقاتها اليومية[3].

1 جون بيندر، سايمون أشروود، الاتحاد الأوربي مقدمة قصيرة جداً، **ترجمة**: خالد غريب على، الطبعة الأولى، مؤسسة هنداوي للتعليم والثقافة، القاهرة، مصر، 2015، ص 34.

2 نقموش محمد، ميلودية أحمد، الجريمة المعلوماتية: المفهوم – حتمية تطوير آليات التعاون الدولي في مجال مكافحتها، مجلة الدراسات القانونية والسياسية، جامعة عمار ثليجي بالأغواط، الجزائر، المجلد الرابع (04)، العدد الثاني (02)، جوان 2018، ص 277، **نقلاً عن**: اسكندر غطاس، الندوة العربية حول التعاون القضائي الدولي في المجال الجنائي في العالم العربية، دار القلم، بدون سنة نشر، ص 21؛ صالح شنين، الحماية الجنائية للتجارة الإلكترونية "دراسة مقارنة"، المرجع السابق، ص 225، حليمة بن حفو، محاربة الجرائم الإلكترونية على الصعيد الدولي "الواقع والأفاق"، مجلة العلوم الجنائية، العدد الأول، الرباط، 2014، ص 206؛ **وانظر أيضاً**:

- Michel Richardot, *Interpol, Europol*, Distribution électronique Cairn.info pour Le Seuil, France, 2002,p :82, Article disponible en ligne à l'adresse :*https: //www .cairn.info/revue-pouvoirs-2002-3-page-77.htm.*

3 وللاطلاع على المزيد بخصوص مكتب الشرطة الأوروبية "يوروبول" (Europol)، يرجى الرجوع للرابط التالي: https://europa.eu */european-union/about-eu/agencies/europol_fr.*

ولأجل المكافحة الفعالة للجريمة الإلكترونية قام "اليوروبول (Europol)" بإنشاء مراكز ووحدات تابعة له، على غرار الفريق العامل المعني بالجريمة الإلكترونية –السيبرانية– (European Union Cybercrime Task Force (EUCTF) التابع للإتحاد الأوروبي، والذي تم إنشاؤه سنة 2010 داخل "اليوروبول (Europol)" بهدف توفير منصة لمديري التحقيقات والملاحقات القضائية في مجال الجريمة الإلكترونية، وتطوير وتعزيز نهج منسق داخل الاتحاد الأوروبي لمكافحة الجريمة الإلكترونية، لجعل الفضاء الإلكتروني مكانًا آمنًا لمواطني الإتحاد الأوروبي ومؤسساته وحكوماته.

ويتألف (EUCTF) من رؤساء الوحدات الوطنية لمكافحة الجرائم الإلكترونية لمختلف الدول الأعضاء بالإضافة إلى ممثلين عن المفوضية الأوروبية، وممثلين عن "اليوروبول (Europol)" و"الاوروجيست (Eurojust)"[1]، كما تم إنشاء المركز الأوربي للجريمة الإلكترونية (EC3) سنة 2013، والذي قدم مساهمة كبيرة في الجهود التي تبذلها الدول الأعضاء في الإتحاد الأوربي من أجل حماية المواطنين والشركات والحكومات الأوروبية من هذه الجريمة، هذا المركز الذي ساهم كثيراً في مكافحة الجريمة الإلكترونية من خلال عمليات الدعم العملياتي الفوري، مما سهل في اعتقال المجرمين، إضافة إلى قيامه بتحليل مئات الآلاف من الملفات، والتي في غالبيتها تكون خبيثة أو تحتوي فيروسات إلكترونية[2]، كما يهتم المركز (EC3) بدراسة التهديدات التي قد يشكلها الإجرام الإلكتروني المنظم وبالأخص الإرهاب الإلكتروني، وكل الجرائم الإلكترونية التي تؤثر على البنية التحتية الحيوية والمعلوماتية للاتحاد الأوروبي، والجرائم الإلكترونية التي تتسبب في أضرار جسيمة لضحاياهم، مثل الاستغلال الجنسي للأطفال عبر الإنترنت[3].

كما تم إنشاء وحدة إحالة الإنترنت في الاتحاد الأوروبي (EU Internet Referral Unit (EU IRU والتابعة "لليوروبول (Europol)" سنة 2015، والتي تعمل على اكتشاف المحتوى الضار خاصة المحتوى ذو الطابع الإرهابي والتحقق منه على الإنترنت وفي وسائل التواصل الاجتماعي، والإبلاغ

1 للمزيد حول (EUCTF)، يمكن الرجوع للرابط التالي: *https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/euctf.*

2 تقرير الأمين العام، الجمعية العامة، الأمم المتحدة، حول مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية (القرار رقم 73/187)، الدورة الرابعة والسبعون، البند 109 من جدول الأعمال المؤقت*(A/74/130)، 30 جويلية 2019، ص 09.

3 Europol Public Information, Europol Programming Document 2017 - 2019, The Hague, 17 January 2017, p :34.

عن المحتوى الإرهابي والمتطرف العنيف عبر الإنترنت ومشاركته مع الشركاء المعنيين، واكتشاف وطلب إزالة محتوى الإنترنت الذي تستخدمه شبكات المنظمات الإرهابية في أعمالها الدعائية؛ ومنصات الهجرة غير الشرعية التي وضعت من أجل جذب المهاجرين واللاجئين، وتنفيذ ودعم عملية الإحالة بسرعة.

ولذلك، فقد شارك فيسبوك في يناير 2018 في محادثات رئيسية مع أجهزة الشرطة الأوروبية حول كيفية وقف واستئصال منشورات المتطرفين على الإنترنت والمرتبطة بالإرهاب والعنف، وقال"فنسنت سيمستر" رئيس وحدة الإنترنت في اليوروبول إن وكالة الشرطة الأوروبية تتعاون مع فيسبوك منذ عامين من أجل الحد من الوصول للدعاية على الإنترنت، كما تعمل وحدة إحالة الإنترنت في الاتحاد الأوروبي على دعم سلطات الاتحاد الأوروبي المختصة من خلال توفير التحليل الإستراتيجي والتشغيلي لها بما يكفل تجنبها مخاطر الجرائم الإلكترونية.

وتعمل وكالة الشرطة الأوروبية "اليوروبول" (Europol) على مكافحة الجريمة الإلكترونية من خلال عدة وسائل وأدوات، وبرامج[1]، وعمليات[2]،كالتي قامت بها في إطار مكافحة جريمة

1 من بين تلك البرامج؛ برنامج (EMPACT) للفترة بين 2018 و2021، والذي يهدف إلى مكافحة الجرائم الإلكترونية، من خلال: 1- تعطيل الأنشطة الإجرامية المتعلقة بالهجمات ضد أنظمة المعلومات، لاسيما تلك التي تتبع نموذج أعمال (Crime-on-Service)، 2- مكافحة الاعتداء الجنسي على الأطفال والاستغلال الجنسي لهم، بما في ذلك إنتاج ونشر مواد إساءة معاملة الأطفال، 3- ومن خلال استهداف المجرمين المتورطين في الاحتيال وتزوير وسائل الدفع غير النقدية، بما في ذلك الاحتيال على نطاق واسع ببطاقة الدفع (لاسيما الاحتيال في البطاقات غير الموجودة) والتهديدات الناشئة لوسائل الدفع غير النقدية الأخرى وتمكين الأنشطة الإجرامية. المصدر: *https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime*

2 شاركت البلدان التالية: قبرص وإيطاليا وهولندا والنرويج والمملكة المتحدة، في عملية قام بها ضباط الشرطة، من الخامس (5) إلى التاسع (9) من شهر جوان 2017 فتشوا على إثرها عشرين (20) منزلاً وقبضوا على ستة (6) أشخاص مشتبه بهم، وتمت مقابلة ستة وثلاثين (36) مشتبه بهم آخرين، كما تم الاستيلاء على عدد كبير من الأجهزة، وفي عام 2018 قامت الإنتربول بعملية (Raven) لمعرفة ملابسات جريمة احتيال بالبريد الإلكتروني المهني وقعت ضحيتها إحدى الشركات النرويجية، واتضح أن هذه القضية لها صلة مع العديد من القضايا الأخرى في أوروبا. وفي شهر أكتوبر سنة 2018 نظمت وحدة الإنتربول لمكافحة الجرائم المالية بحضور ممثلين عن البلدان المتضررة اجتماعا لتنسيق القضايا شارك فيه محققون ومدعون عامون من سبعة بلدان ومن "اليوروبول (Europol)" الذي اضطلع بدور رئيسي في عمليات التحليل، واستنادا إلى المعلومات الاستخباراتية المتبادلة، تم في شهر مارس 2019 اعتقال الشخص المسؤول عن تلك الجرائم والذي كشفت التحقيقات عن وجوده في نيجيريا، وتعتقد السلطات المختصة أن هذا الشخص وشركاءه قد فتحوا حسابات مصرفية متعددة لتلقي وغسل عائدات جريمة الاحتيال المذكورة.

-المصدر: الموقع الرسمي للإنتربول عبر الابط الإلكتروني التالي: *https://www.interpol.int/ar/1/1/2019/52*

استغلال الأطفال في إنتاج المواد الإباحية والمسماة عملية تحطيم الجليد (Icebreaker)، والمنفذة في الرابع عشر (14) من شهر جوان سنة 2005، والتي تم خلالها مداهمة وتفتيش عدة دول أوربية، منها النمسا، بلجيكا، فرنسا، ايطاليا وغيرها تم خِلالَها توقيف أشخاص من تلك الدول[1].

البند الثاني: الأوروجيست كوكالة إقليمية لمكافحة الجريمة الإلكترونية.

بدأت مناقشة إنشاء وحدة تعاون قضائي لأول مرة في اجتماع المجلس الأوروبي في تامبيري بفنلندا يومي الخامس عشر (15) والسادس عشر (16) من شهر اكتوبر سنة 1999، بحضور رؤساء الدول والحكومات، وفي الرابع عشر (14) من شهر ديسمبر سنة 2000، وبمبادرة من البرتغال وفرنسا والسويد وبلجيكا، تم تشكيل وحدة تعاون قضائي مؤقتة تحت اسم (Pro-Eurojust)، بدأت عملها رسمياً في الفاتح من شهر مارس سنة 2001، وبعد هجمات الحادي عشر (11) من شهر سبتمبر 2001 التي شهدتها الولايات المتحدة الأمريكية، ازداد التركيز على مكافحة الإرهاب، ولم يعد الأمر ينصب على المجال الوطني والإقليمي، فقط بل تعداه ليشمل البعد الدولي، مما دفع المجلس الأوربي إلى إصدار قرار في الثامن والعشرين (28) من شهر فبراير سنة 2002 تم من خلاله إنشاء الاوروجيست "Eurojust" كوحدة تنسيق قضائي[2]، مهمتها كما جاء في المادة 85 من معاهدة لشبونة "دعم وتعزيز التنسيق والتعاون بين السلطات الوطنية المسؤولة عن التحقيق في الجرائم الخطيرة التي تمس دولتين أو أكثر من الدول الأعضاء أو مقاضاتها على

1 درار نسيمة، المرجع السابق، ص 308، **نقلاً عن:** جان فرنسوا هنروت، أهمية التعاون الدولي والتجربة البلجيكية في تبادل المعلومات بين عناصر الشرطة والتعاون القضائي، مداخلة في الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، 16-20 يونيو 2007، المملكة المغربية، ص 108.

2 صايش عبد المالك، الأجهزة الأوربية المكلفة بمكافحة الهجرة السرية مهمة مستحيلة بمعدات عسكرية، المجلة الأكاديمية للبحث القانوني، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرة، بجاية، الجزائر، المجلد الحادي عشر (11)، العدد الأول (01)، 2015، ص 20؛ حسام محمد نبيل الشنراقي، المرجع السابق، ص 740؛ ياسر محمد الكومي محمود أبو حطب، المرجع السابق، ص 345؛ آمال حجيج، نحو قوة أورو –متوسطية للشرطة وتسيير الحدود، مجلة دفاتر السياسة والقانون، جامعة قاصدي مرباح بورقلة، الجزائر، العدد الثاني عشر (12)، جانفي 2015، ص 258؛ نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات "دراسة مقارنة"، المرجع السابق، ص 251؛ وأيضاً:

- David Bénichou, *Cybercriminalité: jouer d'un nouvel espace sans frontière*, La base de données juridique des Éditions Dalloz, France, AJ Pénal 2005, p :224.

أساس مشترك، على أساس العمليات المنفذة والمعلومات المقدمة من سلطات الدول الأعضاء واليوروبول"[1].

وفي شهر جوان من سنة 2013، قدمت المفوضية الأوروبية اقتراحًا إلى البرلمان والمجلس الأوروبيين بشأن لائحة جديدة توفر إطار قانوني جديد للأوروجيست "Eurojust" خليفة للقانون الذي كان سنة 2002، والذي عدل عدة مرات[2]، وبعد مفاوضات مكثفة اعتمد البرلمان والمجلس الأوروبيين لائـــحة الاوروجيست "Eurojust" الجـديدة في شهر نوفمبر 2018، والتي بدأ تطبيقها في الثاني عشر (12) من شهر ديسمبر سنة 2019 [3]، وأصبح بإمكان الأوروجيست "Eurojust" مكافحة مستويات متزايدة من الجرائم الخطيرة العابرة للحدود والتي تعد الجريمة الإلكترونية إحداها[4].

وبعدما كانت الاوروجيست "Eurojust" عبارة عن وحدة فقط في سنة 2002، أصبحت بموجب اللائحة الجديدة وكالة الاتحاد الأوروبي للتعاون في مجال العدالة الجنائية (European Union Agency for Criminal Justice Cooperation) لها شخصيتها القانونية[5]، تضطلع بعدة مهام نصت

1 VERSION CONSOLIDÉE DU TRAITÉ SUR LE FONCTIONNEMENT DE L'UNION EUROPÉENNE, Article 85 : (ex-article 31 TUE).

2 Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime (OJ L 63, 6.3.2002, p. 1). 2Council Decision 2003/659/JHA of 18 June 2003 amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime (OJ L 245, 29.9.2003, p. 44). 3Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime (OJ L 138, 4.6.2009, p. 14).

3 REGULATION (EU) 2018/1727 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA, Official Journal of the European Union, L 295/138, 21.11.2018.

4 نصت الفقرة التاسعة من المادة (9/21) من اللائحة (2018/1727 (EU))، الخاصة بالبرلمان والمجلس الأوروبيين المؤرخ في الرابع عشر (14) من شهر نوفمبر سنة 2018 بشأن وكالة الاتحاد الأوروبي للتعاون في مجال العدالة الجنائية (Eurojust)، السالفة الذكر: على أن الجريمة الإلكترونية تعتبر جريمة خطيرة تدخل ضمن اختصاص (Eurojust)، ونصت على ذلك أيضاً الفقرة الثانية والعشرين (22) من الملحق الأول التابع لنفس اللائحة، والذي تضمن قائمة للأشكال الخطيرة للجريمة التي تدخل في اختصاص (Eurojust) والجرائم هي: – ...، – **جريمة الكمبيوتر**، – ...

5 Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime (OJ L 63, 6.3.2002, p. 1), Article premier : « Création et personnalité juridiqueLa présente décision institue une unité dénommée «Eurojust» entant qu'organe de l'Union.Eurojust est dotée de la personnalité juridique. » ; REGULATION (EU) 2018/1727 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision

عليها المادة الثانية (02)، والمادة الرابعة (04) من اللائحة الجـديدة، وفقاً للاختصاص المنوط بها كما جاء في المادة الثالثة (03) من نفس اللائحة؛ ومن مهامها: أنها تدعم وتعزز التنسيق والتعاون بين السلطات الوطنية المسؤولة عن التحقيقات والملاحقات القضائية المتعلقة بالجرائم الخطيرة على أساس العمليات التي نفذت والمعلومات التي قدمتها سلطات الدول الأعضاء، واليوروبول والانتربول، ومكتب المدعي العام الأوروبي، ومؤسسات وهيئات ومكاتب ووكالات الاتحاد المسؤولة والمتخصصة، خاصة إذ كانت الجريمة لها تأثير على دولتين أو أكثر من الدول الأعضاء أو يتطلب الأمر محاكمة على أُسس مشتركة، كما تقوم الاوروجيست "Eurojust" بتسهيل تنفيذ طلبات التعـاون القضـائي والقـرارات في هـذا المجـال، كما يجوز لها أن تطلب على أسـاس مسبب إلى السلطات المختصة في الدول الأعضاء المعنية: اتخاذ تدابير تحقيق خاصة، أو أي إجراء آخر يبرره التحقيـق أو الادعاء، وتشـكيل فـريق تحـقيق مشـترك وفـقًا لأدوات التعـاون ذات الصـلة، وتزويدها بجميع المعلومات اللازمة لممارسة مهامها.

وتقوم الاوروجيست "Eurojust" أيضاً بتقديم آراء في حدود صلاحياتها إلى اليـوروبول بعد دراسـة التـحليلات التي أجراها بمبادرة منها أو بناءً على طلب مكتب المدعي العام الأوروبي، كما تقوم أيضاً بعقد اجتماعات، كالذي قامت به في 14 و15 من شهر سبتمبر من عام 2011 حول سفر مرتكبي الجرائم الجنسية ضد الأطـفال، والذي كان الغرض منه دراسـة المشاكل الرئيسية التي تواجـهها السـلطات القضائية في مواجهة جرائم السفر إلى الخارج بغرض الاعـتداء الجنسي على الأطفال، حيث حَضَر الاجتماع ممثلو الادعاء العـام في الاتحـاد الأوروبي، ومتخصصون قضائيون في مجال استغلال الأطفال وضباط الشرطة، والمنظمات غير الحكومية من كمبوديا والهند –الدولتين الأكثر شيوعًا لاستغلال الأطفال– والـولايات المتحدة الأمريكية واليـوروبول والمفوضية الأوروبية[1]، لأن الأوروجيست "Eurojust" منذ تأسيسها لعبت دورًا مهماً

2002/187/JHA, Official Journal of the European Union, L 295/138, 21.11.2018, Article 1 : Establishment of the European Union Agency for Criminal Justice Cooperation : « 1. The European Union Agency for Criminal Justice Cooperation (Eurojust) is hereby established. 2. Eurojust as established by this Regulation shall replace and succeed Eurojust as established by Decision 2002/187/JHA. 3. Eurojust shall have legal personality »

1 للمزيد بخصوص هذه المسألة يمكن الرجوع للموقع الإلكتروني للأوروجيست من خلال الرابط التالي:

http://www.eurojust.europa.eu/doclibrary/corporate/newsletter/Eurojust

تاريخ الإطلاع: 2020/04/05

في مكافحة الإجرام المرتبط بالأطفال، لذا تم تقديم اقتراح في سنة 2007 أن تُخصص الأوروجيست نقطة اتصال لحماية الأطفال في مسائل معينة مثل اختطاف الأطفال والإيذاء الجنسي لهم والمواد الإباحية ضدهم والاتجار بهم، وحمايتهم عندما يكونوا شهوداً في قضايا معينة[1].

لقد سمح التنسيق والتعاون الدوليين بين مختلف الدول الأعضاء في الاتحاد الأوروبي، واليوربول والاوروجيست وكذا جمع المعلومات والأدلة الإلكترونية من اعتقال ستة (06) أفراد؛ خمسة رجال وامرأة إثر قيامهم بعملية احتيالية استهدفت رموز مستخدمي النقود الإلكترونية "Bitcoin"، والتي كان ضحيتها أكثر من أربعة آلاف (4000) ضحية في اثنتي عشرة دولة[2].

وعليه فإنه وبالنظر إلى كل تلك المهام التي تقوم بها الأوروجيست يمكن الوقوف على الدور المهم الذي تلعبه هذه الوكالة في مكافحتها للجريمة الإلكترونية على الصعيد الأوروبي، كونها ساعدت على تذليل العديد من الصعوبات خاصة منها الإجرائية التي تواجهها الدول الأوربية.

1 في عام 2008 سجلت الأوروجيست قضية بناءً على طلب من المدعي العام للاتصال في النرويج اسمها "لوست بوي Lost "Boy"، لدعم التحقيق في الاعتداء الجنسي على الأطفال وإنتاج وتوزيع وتبادل صورهم عن طريق الانترنت، وكشفت التحقيقات عن وجود مشتبه فيهم في (12) دولة منها: إيطاليا والولايات المتحدة وفرنسا وألمانيا، ساعد التنسيق وتبادل المعلومات عبر الأوروجيست في تسهيل بدء التحقيقات، وتم حل المشكلات المتعلقة بالاختصاص القضائي، وكذا تخطيط وتنفيذ عمليات مشتركة من قِبل السلطات النرويجية والإيطالية والرومانية والأمريكية، وتفتيش منازل المشتبه فيهم، واعتقال (30) شخص، والتعرف على (70) ضحية. كما أدى التنسيق والتعاون الدوليين بين الاوروجيست، واليوروبول، والانتربول، ووزارة العدل الأمريكية وإنفاذ قوانين الهجرة والجمارك الأمريكية (ICE)، وسلطات إنفاذ القانون في جميع أنحاء العالم إلى اعتقال (71) متهماً من أعضاء شبكة إجرامية تسمى لوحة الاحلام "Dreamboard" في (13) دولة، كما بينت التحقيقات أن هناك أكثر من (500) فرد إضافي في جميع أنحاء العالم ينتمي لتلك الشبكة الاجرامية، ادين ستة مذنبين بأحكام تتراوح بين (20) إلى (35) عامًا، مع بقائهم تحت المراقبة مدى الحياة بعد الإفراج عنهم، كما تم إنقاذ ما لا يقل عن (16) طفلاً، والتحقيقات مازالت مستمرة. **انظر في ذلك**:

- Aled Williams, *EUROJUST News*, Issue No. 5 -, Eurojust News is produced by Eurojust's Press & PR Service., Catalogue no: QP-AB-11-002-EN-C, ISSN: 1831-5623, EUROJUST, Maanweg 174, NL - 2516 AB The Hague December 2011, p :09.

2 للمزيد حول هذه العملية الاحتيالية يمكن الرجوع إلى االموقع الإلكتروني لليوروبول الموالي:

- *https://www.europol.europa.eu/newsroom/news/6-arrested-in-uk-and-netherlands-in-%E2%82%AC24-million-cryptocurrency-theft*

- تاريخ الاطلاع: 2020/01/01

المبحث الثاني:
الآليات المُساعدة على مكافحة الجريمة الإلكترونية.

نظراً لارتفاع الجرائم الإلكترونية وتضاعف أعدادها وأنواعها، وتطور أساليبها، وانطوائها على مخاطر جمة تُلحِق بالأفراد والمؤسسات خسائر كبيرة، باعتبارها تستهدف الإعتداء على المعطيات بدلالاتها التقنية الواسعة (البيانات والمعلومات والبرامج بكافة أنواعها) وتطال المعطيات المخزنـة والمعلومات المنقولة عبر نظم وشبكات المعلومات، فهي تطال الحق في المعلومات والحقوق المالية، وحقوق الملكية الفكرية، والحق المعنوي كما أنها تمس الحقوق والحريات الشخصية، وتهدد الأمن القومي، والسيادة الوطنية، وتشيع فقدان الثقة بالتقنية، وتهدد إبداع وابتكار العقل البشري[1].

فعلى الرغم من تخصيص آليات إجرائية ومؤسساتية عملياتية من أجل مكافحة الجريمة الإلكترونية، إلا أن دائرة آليات المكافحة لن تكتمل من دون الآليات المساعدة التي تمثل في كثير من الأحيان عامل تعزيز لوسائل المكافحة، كما هو الشأن في حالة الإستعانة بما تؤديه الجمعيات والمجتمع المدني من دور في عملية التوعية بمخاطر الجرائم الإلكترونية (المطلب الأول)، وما يمكن أن يستفاد منه من معالجة الإدمان على الإنترنت (المطلب الثاني).

1 محمد احمد السويحلي، المرجع السابق، ص 06.

المطلب الأول: الجمعيات كآلية مساعدة على مكافحة الجريمة الإلكترونية

الإنترنت سلاح ذو حدين، يمكن أن يكون مفيداً جداً إذا عرفنا كيف نستعمله ونستغله، كما يمكن أن يكون أداة تخريب للنفوس والأرواح عن طريق المواقع التي تنشر الرذيلة[1]، وتحث على ارتكاب الجرائم تارة، وتقدم لمرتكبيها الإغراء والتمويل تارة أخرى، فالموعظة الحسنة ثم التوعية المستمرة بالجريمة وأخطارها من كافة الجهات المعيشية، وأيضاً سد الأبواب والمنافذ التي تؤدي إلى اقتراف الجريمة[2]، كل ذلك يدخل ضمن ما تقوم به جمعيات الوقاية من الجريمة، وتنميتها للحس الأمني لدى المواطنين، والتوعية القانونية لمختلف فئات المجتمع[3]، فالأفراد لهم دور مهم في تحقيق الأمن، إذ بإمكانهم الإبلاغ عن الجريمة حال عِلمهم بوقوعها والإبلاغ عن مرتكبيها، وإعطاء أوصافه وأماكن تواجده، وتحديد هويته إن أمكن ذلك، والتعاون مع رجال الأمن بكل ما قد يفيد في التحقيق وكشف لغز الجريمة، وتسهيل القبض على مرتكبها، وكذا التعاون مع أجهزة العدالة الجنائية بتقديم الشهادة مثلاً، ويمكن للإفراد أيضاً أن يشاركوا في وضع البرامج والأنشطة المجتمعية وتنفيذها من أجل إعادة تأهيل وإصلاح الجناة والعمل على إدماجهم مجدداً في مجتمعاتهم[4].

إن للجمعيات دوراً فاعلاً في توعية أفراد المجتمع من المخاطر التي قد تسببها الوسائط الإلكترونية الحديثة، وبالأخص على الأطفال؛ إذ يجب إتباع الإجراءات والتدابير اللازمة لضمان سلامتهم ووضع قيود لقبول دخولهم إلى المواقع الإلكترونية، وبالذات مواقع التواصل الاجتماعي، فمن الواجب على كل الفاعلين في المجتمع الإكثار من البرامج التوعوية وبث المعرفة وتثقيف الشباب لتحصينه ضد هذه الآفة، وإقامة نشاطات جمعوية بديلة تمتص قدراته وطاقاته وتوجيهها إلى منحى يخدم الأمة[5]، مستعينين في ذلك بتلك الوسائط حتى لا نتركها مصدراً لتخريب عقول

1 سمير سعدون مصطفى، محمود خضر سلمان، حسن كريم عبد الرحمن، الجريمة الإلكترونية عبر الانترنيت أثرها وسبل مواجهتها، مجلة التقني، تصدر عن هيئة التعليم التقني، وزارة التعليم العالي والبحث العلمي، العراق، المجلد 24، العدد 09، 2011، ص 08.

2 براهيم رمضان إبراهيم عطايا، المرجع السابق، ص 385.

3 ناصري سميرة، بسمة ترغيني، دور المجتمع المدني في مكافحة الجريمة المنظمة، مجلة الحقوق والعلوم السياسية، جامعة عباس لغرور خنشلة، المجلد الأول، العدد الثاني، جويلية 2014، ص 168.

4 شيرين محمد إحسان عبد الحافظ، المرجع السابق، ص 190.

5 دنيا عبد العزيز فهمي، المرجع السابق، ص 112؛ جبيري ياسين، المخدرات الرقمية، مجلة الشريعة والاقتصاد، كلية الشريعة والاقتصاد، جامعة الأمير عبد القادر للعلوم الإسلامية قسنطينة، الجزائر، المجلد الرابع (04)، العدد الثامن(08)، 2015/12/01، ص 612.

الشباب فقط، فالشبكات الاجتماعية على سبيل المثال تعتبر من أهم الوسائل الاتصالية الحديثة، والتي بإمكان الجمعيات وكافة مؤسسات المجتمع المدني[1] الاستفادة منها بشكل كبير، لذا على الجمعيات الاهتمام باستخدامها لأنها تشكل البديل عن وسائل الإعلام التقليدية، والتي لا يمكن للجمعيات الشبابية الجديدة الوصول إليها[2].

ولمعرفة المزيد بخصوص دور الجمعيات كآلية مساعدة على مكافحة الجريمة الإلكترونية، نتطرق لبعض النماذج عن جمعيات مكافحة الجريمة الإلكترونية (الفرع الأول)، ثم لدورها في مكافحة الجريمة الإلكترونية والحد منها (الفرع الثاني).

الفرع الأول: نماذج عن جمعيات مكافحة الجريمة الإلكترونية

إن الحقبة التي نحياها هي بكل تأكيد حقبة الإنترنت والتكنولوجيات الحديثة، والتي تفرض على القائمين على أمر المجتمع وأصحاب القرار فيه استيعاب ذلك[3]، والعمل على التأقلم مع الوضع لإيجاد وسائل كفيلة بمحاربة الجرائم الإلكترونية التي قد تنتج عن ذلك، فالمجتمع ككل ينبغي أن يتحمل مسؤولية علاج المجرمين وتأهيلهم، وتقديم الوسائل التي تؤدي إلى خفض الجريمة، فالمجتمع عند انحراف فرد منه وارتكابه الجريمة يكون قد خسر فرداً ايجابياً[4]، لذا فإن تشجيع ودعم تأسيس جمعيات الوقاية من الإجرام والانحراف، ورعاية المبتلين، وتأهيل وإعادة إدماج المفرج

1 عرفت منظمات المجتمع المدني بأنها: مجموعة من المؤسسات السياسية والاقتصادية والاجتماعية والثقافية التي تعمل في ميادينها المختلفة في استقلال عن سلطة الدولة لتحقق أغراض متعددة، منها أغراض سياسية، مثل المشاركة في صنع القرار على المستوى القومي، ومثال ذلك الأحزاب السياسية، ومنها أغراض نقابية مثل الدفاع عن المصالح الاقتصادية لأعضاء النقابة، ومنها أغراض مهنية كالنقابات للارتفاع بمستوى المهنة والدفاع عن مصالح أعضائها، ومنها أغراض ثقافية مثل اتحاد الكتاب والمثقفين والجمعيات الثقافية التي تهدف إلى نشر الوعي وفقا لاتجاهات أعضاء كل جمعية، ومنها أغراض اجتماعية للإسهام في تحقيق التنمية"، **أشار إلى ذلك:** ناصري سميرة، بسمة ترغيني، المرجع السابق، ص 161، **نقلاً عن:** مدحت ابو النصر، إدارة منظمات المجتمع المدني مصر، ايتراك للنشر والتوزيع، الطبعة الاولى، 2007، ص 69.

2 أمال عزري، جمال بن زروق، استخدام جمعيات المجتمع المدني في الجزائر للشبكات الاجتماعية الإلكترونية (دراسة ميدانية على جمعيات المجتمع المدني في ولاية سكيكدة)، مجلة آفاق للعلوم، جامعة الجلفة، الجزائر، العدد السابع، مارس 2017، ص 235؛

3 قامت جامعة "إكسفورد" في بريطانيا بافتتاح معهد إكسفورد للانترنت خصصته كليا لدراسة تأثيرات الانترنت على المجتمع، يوجد بهذا المعهد مركز أبحاث متعدد التخصصات والتوجهات في العالم، يقدم توصيات واستشارات حول السياسات الحكومية في المجالات التي يتوصل فيها إلى نتائج يعتمد عليها في ذات المجال: عبد الفتاح حجازي، الإثبات الجنائي في جرائم الكمبيوتر والانترنت، المرجع السابق، ص 218؛ المرجع نفسه، ص 206.

4 عبد الرحمن العيسوي، المرجع السابق، ص 134؛ محمد شنة، المرجع السابق، ص 171.

عنهم، وإصلاح المحكوم عليهم بعقوبات موقوفة التنفيذ، وحماية الأحداث، وتحصين أفراد المجتمع من الآفات الاجتماعية سيساهم في الوقاية من الإجرام والانحراف[1]، وتعد جمعيات مكافحة الجرائم الإلكترونية عينة من تلك الجمعيات التي تسعى إلى خفض نسبة ارتكاب الجرائم الإلكترونية، والتي لم تبق فئة من فئات المجتمع إلا وطالتها.

وعلى الرغم من أن الجزائر بها ما يقارب مائة وتسعة آلاف جمعية – أي 108940 جمعية- في مختلف المجالات[2]، إلا أننا لم نجد أي جمعية تنشط في مجال محاربة الجرائم الإلكترونية، بخلاف الدول العربية الأخرى؛ كتونس ومصر والأردن التي بها جمعيات تعنى بهذا النوع من الجرائم، ففي تونس مثلاً هناك الجمعية التونسية لمقاومة الجريمة الإلكترونية، والجمعية التونسية للانترنت[3]، وفي الأردن هناك الجمعية الأردنية المتخصصة في الجرائم الإلكترونية والحد منها، والتي تم توقيع نظامها الأساسي عام 2006، ومركز عملها عمان ولها مجموعة من الأهداف يلاحظ عليها أنها جميعها تهدف إلى إنتاج التوعية ونشر الأفكار للحد من جرائم الحاسوب والإنترنت[4]، وفي مصر بعد انعقاد المؤتمر التأسيسي الأول لجمعيات قانون الإنترنت بالقاهرة في شهر سبتمبر سنة 2004، وكذا المؤتمر الدولي الأول لقانون الإنترنت بمدينة الغردقة في شهر أوت سنة 2005، بدأ الاهتمام بمكافحة الجريمة الإلكترونية؛ وتأسست على إثر ذلك الجمعية المصرية لمكافحة الجرائم المعلوماتية والإنترنت سنة 2005، والمشهرة تحت رقم (2176) لسنة 2005 بتاريخ 2005/08/05[5]، وفي نفس السنة وبمناسبة نفس المؤتمر تم تأسيس الجمعية العربية لقانون الإنترنت[6]، وهناك أيضاً الجمعية الدولية لمكافحة الجريمة الإلكترونية بفرنسا (Association Internationale de Lutte Contre La

1 عبد العزيز ديلمي، المرجع السابق، ص 546.

2 المصدر: الموقع الرسمي لوزارة الداخلية والجماعات المحلية: *http://www.interieur.gov.dz/images/pdf/listeassossaciation-ar.pdf* تاريخ الاطلاع: 2020/04/25.

3 محمد محمد الألفي، المرجع السابق، ص 32.

4 محمد نافع فالح رشدان العدواني، المرجع السابق، ص 72.

5 معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة مكملة لنيل شهادة الماجستير في العلوم القانونية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة العقيد لخضر، باتنة، السنة الجامعية 2011-2012، ص97؛ عبد الله عبد الكريم عبد الله، المرجع السابق، ص 103.

6 المنظمة العربية للتنمية الإدارية، جامعة الدول العربية، المؤتمر الدولي الأول، لقانون الإنترنت (Cyberlaw)، "نحو علاقات قانونية وإدارية واقتصادية وسياسية واجتماعية جديدة"، 21-2005/8/25، الغردقة – جمهورية مصر العربية.

(Cybercriminalité (A.I.L.C.C.)، والتي هي عبارة عن منظمة دولية غير حكومية وغير هادفة للربح منشاة طبقا للقانون الفرنسي رقم 1901 حيث تم إيداع نظامها الأساسي في الجهة الإدارية الفرنسية بتاريخ 13فبراير 2006 ونشر نظامها الأساسي بالجريدة الرسمية الفرنسية بتاريخ 18 مارس 2006، والجمعية معنية بمكافحة الجريمة الإلكترونية بكافة صورها وأشكالها وتقليص حجم ارتكاب الجرائم المعلوماتية عبر شبكة الإنترنت.

الفرع الثاني: دور جمعيات مكافحة الجريمة الإلكترونية في الحد منها.

إن السياسة الزجرية لا تكفي لوحدها لصد الجرائم الإلكترونية، لذا قامت عدة دول في السنوات الأخيرة بوضع سياسية وقائية أطلق عليه تسمية الثقة الرقمية[1]، وقامت بسن قوانين بمحفزات معينة لتشجيع تأسيس جمعيات يتعلق نشاطها بالإنترنت والحاسوب، هدفها نشر ثقافة الإنترنت والاستخدام الواعي للحاسوب، وإشراك القطاع الخاص في مكافحة جرائم الإنترنت؛ لأنها ضرورية لمساعدة السلطات العامة من خلال تحسين الحماية الذاتية كخط دفاع أول لهذا القطاع[2]، لأن للبيئة الاجتماعية تأثير قوي على بعض الأشخاص، فهم يتلقون فيها العديد من القيم والعادات ويأخذون منها نظرة على الحياة والمجتمع[3]، كما أن مشاركة القطاع المدني والعمل الأهلي التطوعي في التصدي لهذه المشكلات، التي تواجه المجتمع أصبحت عاملاً حاسماً لضمان النجاح في التصدي لهذه المشكلات، من خلال تنمية الوعي المجتمعي وإيجاد ثقافة عامة على صعيد المجتمع بكامله تفض السلبيات وتعمل على تنمية الايجابيات[4]، وهنا يظهر بشكل جلي الدور الذي تلعبه جمعيات مكافحة الجرائم الإلكترونية في تسليط الضوء على السلبيات والأخطار التي قد تتسبب فيها الوسائل الإلكترونية الحديثة؛ وبالذات الإنترنت، ففي سبيل ذلك فإن الجمعيات تقوم بعدة أشياء منها على سبيل المثال:

1- قيامها بعقد بروتوكولات تعاون مع المؤسسات التعليمية من أجل تثقيف وتدريب الطلبة وخريجي الكليات في مختلف التخصصات، وكذا السادة القضاة وأعضاء النيابة العامة والسادة

1 خالد عثماني، المرجع السابق، ص 48.

2 بومامي العباس، المرجع السابق، ص 167.

3 محمد الازهر، مبادئ في علم الإجرام، الطبعة التاسعة، مطبعة دار النشر المغربية، الدار البيضاء، المغرب، 2015، ص 228.

4 عبد الله عبد الكريم عبد الله، المرجع السابق، ص 94.

المحاميين والعاملين في القطاعات القانونية في المؤسسات وتأهيل وإكساب المتدربين المهارات القانونية والعلمية والعملية والفنية الخاصة بارتباط المعلوماتية والاتصالات بتخصصاتهم، وتبين الإشكاليات القانونية التي قد يتلقونها في حقل المعاملات الإلكترونية[1].

2- تتعاون الجمعيات فيما بينها لتخطي الصعوبات التي تواجه عملية مكافحة الجرائم الإلكترونية، ومن ذلك المبادرة التي تبنتها الجمعية الدولية لمكافحة الجرائم الإلكترونية بفرنسا، والجمعية المصرية لمكافحة جرائم الإنترنت، في محاولة لسن قوانين رادعة تحمي رواد شبكة الإنترنت من التجاوزات غير اللائقة التي تحدث على الشبكة، بداية من الإرهاب الإلكتروني ومروراً بالسطو على الحقوق الفكرية، وانتهاء بتجريم تجارة الرقيق الأبيض على الشبكة العنكبوتية وماهية التنظيم القانوني للعالم الافتراضي بأقسامه من المعاملات القانونية الرقمية وعقود التجارة الإلكترونية وحماية الملكية الفكرية عبر الإنترنت والتعريف بأنماط وأشكال الجرائم عبر الإنترنت وماهية الدليل الرقمي وحجيته في الإثبات وعرض أحدث التقنيات الفنية العالمية للتعامل مع مثل هذه النظم[2].

3- إعداد الدراسات والبحوث حول العلاقة الرقمية بالقاعدة الموضوعية والإجرائية في القانون الجنائي والحث على تطويره، وتشجيع البحث العلمي للوقاية من الجرائم الإلكترونية[3].

4- تنظيم ورشات عمل وملتقيات في مختلف المواضيع التي تمسها الجرائم الإلكترونية لإيجاد حلول تتناسب مع خطورة هذه الجرائم، والاستفادة من خبرة ذوي الاختصاص.

---

1 قامت الجمعية الأوربية للمعلومات بتعزيز التواصل والحوار بين الأطراف المعنية والعمل على تأهيل وتعليم العاملين في أجهزة العدالة الجنائية والمتعاملين معها بصفة خاصة والمجتمع بصفة عامة: عبد الصبور عبد القوي علي، الجريمة الإلكترونية والجهود الدولية للحد منها، مجلة الدراسات المالية والمصرفية، السنة الثالثة والعشرون، العدد الأول، الأردن، مارس 2015، ص 16؛ **وكذلك عن:** محمد الأمين البشري، المرجع السابق: ص 18.

2 عبد العال الديربي، محمد صادق اسماعيل، المرجع السابق، ص 120.

3 المنظمة العربية للتنمية الإدارية السالفة الذكر، المادة الثالثة (3): أهداف وأنشطة الجمعية: "تهدف الجمعية وتستهدف تحقيق ما يلي: 1. إعداد الخطوط الإستراتيجية الكبرى لقانون للانترنت. 2. تحقيق نمو في الوعي الأكاديمي بقانون الإنترنت على مستوى العالم العربي. 3. المساهمة في رسم سياسات صحيحة وفي تصحيح مسار الموجود من سياسات قانون الانترنت. 4. تشجيع وتنمية وتطوير تفاعل العمل الأهلي غير الحكومي مع قانون الانترنت. 5. المساهمة في وضع التصور الإقليمي لقانون الانترنت والتعاون مع الجهات الحكومية المحلية الإقليمية والدولية في هذا الإطار. 6. إصدار الوثيقة العربية لقانون الانترنت ومتابعة تنفيذها وتطويرها وتنميتها بما يحقق مصلحة المجتمع العربي والإنساني عالميا. عبد الله دغش العجمي، المشكلات العلمية والقانونية للجرائم الإلكترونية –دراسة مقارنة–، قدمت هذه الرسالة استكمالا للحصول على درجة الماجستير في القانون العام، جامعة الشرق الأوسط، الأردن، 2014، ص.ص: 103-104.

إن مكافحة الجريمة الإلكترونية ليست حكراً على جهة معينة بل هي مسؤولية الجميع؛ بداية من الأسـرة ثم المـدرسة والمسجد والجمعيات وكل الفاعلين في المجتمع، إذ يجب تحذير أبنائنا من إعطاء معلومات شخصية عن أنفسهم للأشخاص الذين يتم التعارف بهم عن طريق الإنترنت، سيما عن طريق غرف الدردشة، وتنبيههم إلى خطورة تنظيم لقاءات مباشرة مع أولئك الأشخاص دون استشارة الوالدين أولاً[1]، فالضحية في الجريمة الإلكترونية في كثير من الأحيان هو من يمد المجرم بالمعلومات التي يحتاجها من أجل تنفيذ جريمته؛ ومن تلك العينة قيام العديد من الأشخاص بنقل تفاصيل دقيقة عن حياتهم من أجل الحصول على أكبر قدر من الجيمات واللايكات كما يسمونها، فيصورون كل زاوية من البيت، ومكان كل غرفة فيه، وأوقات النوم والاستيقاظ، ومنهم من يصور الاستعداد للسفر والذهاب إليه، ومواعيد العودة بالثواني والدقائق، رغم علمهم بوجود أشخاص عملهم الوحيد هو إيذاء الآخرين –سواء كانوا أشخاص طبيعيين أو معنويين– عبر وسائل الاتصال الحديثة كالهاتف، والإنترنت ونحوها[2]، لذا فإن التوعية المستمرة تعد من بين الآليات الاستيباقية المهمة التي يجب العمل على إيصالها إلى أكبر قدر من فئات المجتمع، وخاصة فئة الأطفال.

1 عبد الفتاح بيومي حجازي، الأحداث والانترنت دراسة متعمقة عـن اثر الانترنت في انحـراف الأحـداث، المرجع السابق، ص 291.

2 عرف القضاء المغربي نماذج من هذه الجرائم، كالقضية الجنحية المسجلة لدى المحكمة الابتدائية بخريبكة تحت عدد 04/385 (حكم جنحي تلبسي عدد 04/408 صدر بتاريخ 2004/02/18 عن ابتدائية خريبكة في الملف الجنحي عدد 04/358): حيث أدانت أحد التقنيين من أجل جنحة الدخول إلى نظام المعالجة الآلية للمعطيات، ونتج عنه حذف واضطراب في سيره، ذلك أن هذا الجانب أحدث موقعا له بالانترنت وبدا يراسل أشخاص ذاتية ومعنوية بواسطة الانترنت وتسلم على ضوء ذلك بريدا إلكترونيا حقق له منفعة مالية بدون وجه حق كما الحق ضررا بمواقع إحدى الشركات، ولم تختلف قضيته عن قضية (ملف تحقيق عدد 2005/25 بمحكمة الاستئناف بالرباط) المغربي (ف.ص) الملقب "بديابلو Diablo" والتركي (ب.ا) المتهمين بتكوين عصابة إجرامية والسرقة الموصوفة واستعمال بطاقة ائتمان مزورة والولوج إلى أنظمة المعالجة الآلية للمعطيات عن طريق الاحتيال وإدخال تزوير على وثائق المعلوميات مما الحق ضررا ببعض الشركات الأمريكية: صليحة حاجي، الآليات القانونية لتكريس الأمن المعلوماتي، مجلة العلوم الجنائية، العدد الثاني، مطبعة الأمنية وتوزيع مكتبة الرشاد، المغرب، 2015، ص ص: 09-10. **كما أشار إلى ذلك**: ابراهيم بن لعيد، المجني عليه" في خدمة" الجاني: الفايسبوك نموذجاً، المجلة المغربية للقانون الجنائي والعلوم الجنائية، العدد المزدوج الرابع والخامس (4-5)، ديسمبر 2017، ص 309؛ إبراهيم محمد قاسم الميمن، العقوبات البديلة الفقه الإسلامي، ورقة بحثية مقدمة للمشاركة في ندوة بعنوان: بدائل العقوبات السالبة للحرية، المنعقدة بالتعاون بين مركز الدراسات والبحوث بجامعة نايف العـربية للعلوم الأمنية وإدارة السجون الجزائرية بوزارة العدل، الجزائر، الفترة ما بين 10 و12 ديـسمبر 2012.

المطلب الثاني: معالجة الإدمان على الإنترنت كآلية مساعدة على مكافحة الجريمة الإلكترونية

أصبحت الشبكة العالمية اليوم تضم مجموعة من الأنشطة والخدمات المختلفة التي لا غنى عنها، فهي البنية التحتية للاتصالات[1]، والشعور بالحاجة الملحة إلى الإبحار فيها يحصل عند الكثير من المستخدمين؛ هذه الحاجة التي عند تعديها الحدود المعهودة وتحولها إلى تَعَوُّدٍ تعتبر إحدى ظواهر الإدمان على الشبكة[2].

وتعتبر الأخصائية النفسانية (Kimberly Young) أول من أطلقت مفهوم الإدمان على استخدام الإنترنت (Internet Addiction) سنة 1996 بعدما أجرت أول دراسة أمبريقية على عينة مكونة من 600 شخص، واعتبرت (Young) أن الإدمان على استخدام الإنترنت لا يختلف عن مشكلات الإدمان الأخرى[3]، كما أن أغلب الدراسات كشفت أن الإدمان على الإنترنت؛

---

1 أهم خدمات الشبكة العنكبوتية" البريد الإلكتروني E-Mail والمنتديات News Group والناقل Transforse protocol FTB لنقل الملفات بين أرجاء الشبكة ووسيلة المتصل Telnet وهو البرنامج الذي يتيح لأي شخص استخدام برامج ومميزات حاسوبية موجودة في جهاز أخر بعيد ولا توجد في جهاز المستخدم، أما شبكة المعلومات www فهي إحدى خدمات الشبكة من صفحات مصححة بلغة Html التي تتيح إمكانية ربط الصفحات بالوسائط LINKS وهو سر تسميتها بالشبكة العنكبوتية. **انظر:** محمد نصر محمد، المرجع السابق، ص 77، **نقلاً عن:** فهد بن عبد الله اللحيدان، الانترنت شبكة المعلومات العالمية، الطبعة الأولى، الناشر غير معروف، 1996، ص 51 وما بعدها.

2 رصاع فتيحة، الحماية الجنائية للمعلومات على شبكة الانترنت، مذكرة لنيل شهادة ماجستير في القانون العام، كلية الحقوق والعلوم السياسية، جامعة ابي بكر بلقايد، تلمسان، السنة الجامعية 2011-2012، ص 21.

3 إسماعيل بن دبيلي، الإدمان على استخدام الانترنت وعلقته بالاكتئاب والعزلة الاجتماعية – دراسة على عينة من الطلبة الجامعيين بالجزائر العاصمة-، أطروحة مقدمة لنيل شهادة دكتوراه الطور الثالث في علوم الإعلام والاتصال، قسم علوم الاتصال، كلية علوم الإعلام والاتصال، جامعة الجزائر 03، 2015-2016، ص 02: **نقلاً عـــن:**

- K. Siomos:, *Evolution of Internet addiction in Greek adolescent students,over a two-year period: the impact of parental bonding*, Euro Child Adolescent Psychiatry, Springer, 2012 , p:212.

جدير بالذكر أن مصطلح إدمان الانترنت يقابله العديد من التسميات مثل: الإدمان التكنولوجي، الاعتماد على الانترنت، إساءة استخدام الانترنت، الاعتماد على الكمبيوتر، إدمان الكمبيوتر، الاستخدام المفرط للانترنت. **انظر في ذلك:** سامية ابريعم، العلاقة بين إدمان الانترنت والشعور بالاغتراب النفسي (دراسة ميدانية لدى عينة من طلاب وطالبات جامعة أم البواقي)، مجلة علوم الإنسان والمجتمع، كلية العلوم الإنسانية والاجتماعية، جامعة محمد خيضر، بسكرة، الجزائر، العدد الخامس عشر (15)، جوان 2015، ص 222، **نقلاً عـــن:** عصام محمد زيدان، إدمان الانترنت وعلاقته بالقلق والاكتئاب والوحدة النفسية والثقة بالنفس، مجلة دراسات عربية في علم النفس، القاهرة، مجلد 07، العدد 02، ابريل 2008، ص 311؛ خالد العمار، إدمان الشابكة المعلوماتية (الانترنت) وعلاقته ببعض المتغيرات لدى طلبة جامعة دمشق – فرع درعا، مجلة جامعة دمشق، سوريا، المجلد الثلاثون (30)، العدد الأول، 2014، ص 401.

وبالأخص مواقع التواصل الاجتماعي من شأنه أن يقود الشباب إلى العزلة الإجتماعية سواء داخل الأسرة أو المدرسة، ويقلل من فرص التفاعل الاجتماعي الواقعي، ليعيش المراهق في عالم افتراضي يشبع فيه حاجاته التي لم تتحقق ولم تشبع في العالم الحقيقي الذي يعيشه، الأمر الذي يصرف نظره شيئا فشيئا عن دراسته، مما يحول دون توافقه الدراسي[1]، فأكبر عدد من مدمني الإنترنت هم من الذين تقل أعمارهم عن عشرين عاماً بنسبة 53 % من عينة المدمنين[2]، ولأن الإبحار في الفضاء الأزرق هو إمكانية متاحة لمختلف الفئات العمرية في المجتمع، فقد تنوعت وتعددت الآثار السلبية التي قد يخلفها الإدمان على الإنترنت.

وسنحاول من خلال هذا المطلب التطرق لسلبيات الإدمان على الإنترنت (الفرع الأول)، على نحو يمكننا من التطرق لآليات الحد من الإدمان على الإنترنت (الفرع الثاني).

الفرع الأول: سلبيات الإدمان على الإنترنت.

تعد شبكة المعلومات الدولية، أو ما يطلق عليه الإنترنت من الوسائط القوية، لأنها تنشر الأفكار والمعلومات والتصريحات والأحكام بين الأطراف المشتركين فيها على امتداد العالم كله وهي مفتوحة على مصراعيها للانضمام المطرد إليها يوما بعد يوم، وهي تضم –علاوة على ذلك – كل شئ بدءاً من الكتب التراثية وانتهاء بالأفلام المحظورة[3]، فقد أدت الشبكة عبر العديد من المواقع إلى خوض الشباب في الكثير من الممارسات التي تتنافى والقيم الثقافية والاجتماعية لهم[4]، وكثيراً ما يقعون في ممارسات تنتهي في أغلب الأحيان بارتكاب جرائم خطيرة[5]، لذا كان الإدمان على

1 حياة لموشي، الإدمان على الفيسبوك وعلاقته بالتوافق الدراسي لدى المراهقين، مجلة آفاق للعلوم، جامعة زيان عاشور، الجلفة، العدد التاسع (09)، سبتمبر 2017، ص 65.

2 حمودة سليمة، الإدمان على الانترنت: اضطراب العصر، مجلة العلوم الإنسانية والاجتماعية، جامعة قاصدي مرباح، ورقلة، الجزائر، العدد الواحد و العشرون (21)، ديسمبر 2015.

3 أحمان لبني، جنوح الأحداث بين العوامل النفسية والتنشئة الاجتماعية، الملتقى الوطني: جنوح الأحداث "قراءة في الواقع وآفاق الظاهرة وعلاجها، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة باتنة 01، يومي 04 و05 ماي 2016، ص 60.

4 بوعزة رضا، النشاط الجنسي للشباب في الفضاء السيبيراني– دراسة ميدانية على عينة من الشباب المتردد على مقاهي الانترنت–، مجلة آفاق للعلوم، جامعة زيان عاشور بالجلفة، العدد الثاني (02)، 2016، ص 236.

5 هناك عدة جرائم إلكترونية يمكن أن يقع ضحيتها مدمن الانترنت، ذُكر بعضها في المرسوم رئاسي رقم 14-252، المتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر سنة 2010، ومنها: المادة (15): الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات : 1- نشر أفكار ومبادئ جماعات إرهابية والدعوة لها. 2- تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الإرهابية. 3- نشر طرق صناعة المتفجرات والتي تستخدم

الإنترنت موضوع حوار تناولته عدة دراسات، فقد نظم سنة 1996 منتدى حول الإنترنت حضره عدد من الأطباء الأمريكيين المتخصصين في الأمراض العقلية والنفسية، والذين اقترح بعضهم تكوين فوج لمساعدة الأشخاص الذين يعانون من الإدمان على الإنترنت[1]؛ والذي يمكن إثباته من خلال وجود ثلاثة أو أكثر من بين الأعراض السبعة التي وضعوها[2].

إن سلبيات الإدمان على الإنترنت كثيرة جداً، تتفاوت درجة خطورتها حسب الضرر الذي ينتج عنها، فكثيراً ما يؤدي الادمان على الإنترنت إلى اقتراف جرائم تضع صاحبها في مسائلة قانونية توجب معاقبته، بأقصى العقوبات أحياناً[3]، وبالأخص حينما أصبح الإرهابيون من خلال المواقع الإلكترونية التي ينشؤونها يستخدمون ما يسمى بالمخدرات الرقمية[4] يؤثرون بها على عقول

خاصة في عمليات إرهابية.4- نشر النعرات والفتن والاعتداء على الأديان والمعتقدات"؛ المادة (16): غسيل الأموال، ترويج المخدرات، الاتجار بالأشخاص، بالأعضاء، الأسلحة، المادة (17): حقوق المؤلف، المادة (18): الاستخدام غير المشروع لأدوات الدفع الإلكترونية، المادة (19): الشروع والاشتراك في ارتكاب الجرائم.

1 يقصد بإدمان الانترنت: 1- قضاء وقتا طويلا في التعامل مع الانترنت (اكثر من 03 ساعات يوميا)، 2- عدم الاستطاعة على مقاومة الرغبة في استخدام الانترنت، 3- تزايد الرغبة في قضاء اكبر وقت في التعامل مع الانترنت، 4- استخدام الانترنت بدون هدف مقصود. **انظـــر**: نور على سعد درويش، قيم وخصائص مدمني الانترنت، الطبعة الأولى، دار الوفاء لدنيا الطباعة والنشر، الإسكندرية، مصر، 2016، ص 46.

2 الأعراض السبعة هي: 1- قدرة الاحتمال، 2- حالة الفقد (الانسحاب)، 3- استعمال الانترنت لمدة طويلة أكثر مما حُضِر له، 4- ضعف الإرادة لضبط مدة الاستخدام والفشل في التقليل أو التوقف منه، 5- استغراق وقت كبير في نشاطات لها علاقة بالانترنت (البحث عن إصدارات جديدة لكتب أو برامج عن طريق الانترنت، التسوق، 6- إهمال الحياة الخاصة سواء الاجتماعية أو التعليمية أو المهنية، 7- استخدام مستمر رغم معرفته بالأضرار الاجتماعية والنفسية والصحية التي نتجت عن هذا الاستخدام. **انـــظر**: حمودة سليمة، المرجع السابق، ص 218.

3 حكم محكمة النقض المصرية، الدائرة الجنائية، الخميس (ج)، في الطعن المقيد بجدول المحكمة رقم 29953 لسنة 86 القضائية، في الجلسة العلنية المنعقدة بدار القضـاء العالي بمدينة الـقاهرة، في يوم الخـميس الأول من شعبان سنة 1438هـ الموافق 27 أبريل 2017، ص 03.

4 المخدرات الرقمية هي ملفات صوتية تترافق مع مواد بصرية أحياناً وأشكال وألوان تتحرك وفق مجال مدروس، تمت هندستها لتخدع الدماغ عن طريق بث أمواج صوتية مختلفة، التردد لكل أذن، ولان هذه الموجات الصوتية غير مألوفة، يعمل الدماغ على توحيد الترددات الآتية من الأذنين للوصول إلى مستوى واحد، وحينها يصبح الدماغ غير مستقر كهربائياً مما ينتج عنه الإحساس بصوت ثالث يدعى "Binaural beats"إضافة إلى النغمتين وهذا ما يدعى بالخداع السمعي. **انظر في ذلك**: عبد الله عويدات، الآثار النفسية والاجتماعية للمخدرات الرقمية ودور مؤسسات الضبط الاجتماعي في الحد من آثارها، الندوة العلمية "المخدرات الرقمية وتأثيرها على الشباب العربي"، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، الفترة من 16 إلى 18 فيفري 2016، ص.ص: 03-04، **نقلاً عـــن**: حسن زينب عبد الكاظم، المخدرات الرقمية، ورقة مقدمة إلى ندوة المخدرات الرقمية، جامعة ميسان العراق، 2014، ص 20.

الشباب[1]، بنقل الأفكار المدمرة فكرياً وسلوكياً، ويعملون كذلك على نشر بعض المواقع المنحرفة التي تبين الخبرات الناجحة لبعض متعاطي المخدرات العادية والرقمية[2]، إذ أصبحت اليوم الشبكة العاليمة من أفضل الأماكن –إن صح التعبير– التي تروج فيها المخدرات والمهلوسات والمؤثرات العقلية، ومواقع أخرى تقدم فيها مختلف الشُروحات عن كيفية صنع المخدرات والمؤثرات العقلية[3].

وعن جانب آخر من الجوانب السلبية التي نتجت عن الإدمان على الإنترنت ممارسة الألعاب الإلكترونية[4]، والتي شكلت في الآونة الأخيرة موضوع حديث العدد من الصحف والمواقع الإلكترونية، لأن ممارسة اللعب الإلكتروني من شأنه أن يفتح أمام المستخدمين الشباب أطراً اجتماعية واسعة للاندماج النفسي والاجتماعي في عوالم غير محدودة للصراع والعنف والمواجهة الخيالية، وهي عوالم كثيرا ما تكون لها تأثيرات نفسية سلبية تؤثر على نمو الشخصية العامة للفرد المستخدم[5]، هذا التأثير الخطير هو ما لفت انتباه المجتمع الوطني والدولي إلى تجنيد الجميع بما فيها الوزارات والقطاعات المعنية من أجل التحسيس بأخطار مثل هذه الألعاب الإلكترونية، فبالإضافة إلى هدر الوقت، وضياع المال وتفاقم حالات العزلة والانزواء، وتأثر أخلاق اللاعبين وسلوكاتهم

1 حكم محكمة تمييز دبي رقم: 289/2005، جزائي، بتاريخ 2005/11/19. **أشار إلى هذا الحكم:** عمر عبد المجيد مصبح، الإشكالات الجزائية في تكييف "المخدرات الرقمية"، مجلة القانون والمجتمع، مخبر القانون والمجتمع، جامعة أحمد دراية أدرار، الجزائر، العدد التاسع، جوان 2017، ص.ص:233-234.

2 محمد مرسي محمد مرسي، إدمان المخدرات الرقمية عبر الانترنت وتأثيرها علي الشباب العربي"دراسة ميدانية مطبقة على الشباب العربي بجامعة الأزهر بالقاهرة"، الندوة العلمية" المخدرات الرقمية وتأثيرها على الشباب العربي"، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، الفترة من 16 إلى 18 فيفري 2016، ص 21.

3 من الممارسات الكثيرة التي توجد عبر الإنترنت، الصيدليات الافتراضية غير القانونية، والمواقع الإلكترونية التي تتم عبرها تجارة المواد الكيمياوية التي يكثر استخدامها في صنع العقاقير المخدرة والمؤثرات العقلية على نحو غير مشروع: تقرير الهيئة الدولية لمراقبة المخدرات لسنة 2017، ص.ص: 22-23، متاح على الموقع الإلكتروني الموالي: *https://www.incb.org/documents/AR2017/Press_Kit/PressKit_A.pdf Publications/AnnualReports/*، تاريخ الاطلاع: 2019/12/21.

4 أمل كاظم حمد، إدمان الأطفال والمراهقين على الانترنت وعلاقته بالانحراف، مجلة العلوم النفسية، مركز الدراسات التربوية والبحوث النفسية، جامعة بغداد، العراق، العدد تسعة عشر (19)، ديسمبر 2011، ص 116.

5 فريد الصغيري، اللعبة الإلكترونية، الممارسة الشبابية وعلاقتها بالعنف، مجلة دراسات وأبحاث، جامعة زيان عاشور، الجلفة، الجزائر، المجلد الخامس (05)، العدد الحادي عشر(11)، جوان 2013، ص 302؛ **وانظر أيضاً:**

– Roberts, Kevin J, **Cyber junkie**, Printed in the United States of America, Published 2010, p: 14 : « I believe video games represent for me, as for many an attempt to escape from the dullness of everyday reality. »

بتلك الألعاب، مما أدى إلى تهديد القيم الاجتماعية وتشويه العقائد الدينية[1]، بل أكثر من ذلك؛ إذ أصبحت مخاطر الألعاب الإلكترونية تحصد الأرواح، الشيء الذي دفع المنظمة العالمية للصحة إلى تصنيف الألعاب الإلكترونية على أنها اضطراب في الصحة النفسية الموجب للعلاج.

جدير بالذكر أن اللعب عبر الإنترنت يشمل طائفة واسعة من السلوكيات[2]، ومن بينها القمار والذي أصبح يلعب عبر الكازينوهات الافتراضية (Virtual Casino)، والتي هي عبارة عن مواقع ويب تم تصميمها على طراز كازينوهات"لاس فيغاس"[3]، ولقد شجعت الخصائص المغرية لهذا النوع من أنواع الإدمان، على وجود جيل جديد من المدمنين على الإنترنت، من مختلف الفئات الاجتماعية من شباب ومراهقين وطلبة؛ وهو ما ساهم في جعل لعب القمار على الخط Online Gambling الأكثر شعبية في الوقت الراهن.

كما تعتبر شركات المقامرة أن فضاءات المقامرة على الخط هي الرهان لكسب الملايير من الدولارات، خصوصاً وأنها تعتمد على مبدأ مجانية الاشتراك وتنوع أشكال المقامرة عكس المقامرة التقليدية[4]، كما أصبح القمار عبر الإنترنت وسيلة هامة في عملية غسيل الأموال، حيث يتم تبادل هذه الأموال عبر هذه النوادي بكل سهولة[5]، لذا نجد أن عدة دول نصت في قوانينها على حظر ممارسة القمار عبر الشبكة، ومنها الولايات المتحدة الأمريكية[6]، والتي قدمت مواطناً أمريكياً للمحاكمة الجنائية نتيجة قيامه بتقديم خدمة المقامرة عن طريق الإنترنت، وإنشاء هذا الموقع في دولة انتيغوا وبربودا، وبيعه هذه الخدمة لمواطني الولايات المتحدة الأمريكية بالمخالفة لقانون الإتصالات السلكية لسنة 1961 (Wire Communication Act of 1961)، وهنا قضت المحكمة

1 فاطمة همال، الألعاب الإلكترونية عبر الوسائط الإعلامية الجديدة وتأثيرها في الطفل الجزائري (دراسة ميدانية على عينة من أطفال ابتدئيات مدينة باتنة)، مذكرة مكملة لنيل شهادة الماجستير، تخصص: الإعلام وتكنولوجيا الاتصال الحديثة، قسم العلوم الإنسانية، كلية العلوم الإنسانية والاجتماعية والعلوم الإسلامية، جامعة الحاج لخضر، باتنة، السنة الجامعية 2011-2012، ص 150.

2 نور على سعد درويش، المرجع السابق، ص48.

3 ياسمينة بونعارة، المرجع السابق، ص 23؛ على جبار الحسيناوي، المرجع السابق، ص 84؛ خالد العمار، المرجع السابق، ص 414.

4 Griffiths, M. D., Wood, R. T. A., & Parke, J Social responsibility tools in online gambling: A survey of attitudes and behaviour among Internet gamblers. CyberPsychology & Behavior, 12, 2009, P .418

5 عبد الفتاح بيومي حجازي، الأحداث والانترنت دراسة متعمقة عن اثر الانترنت في انحراف الأحداث، المرجع السابق، ص 254.

6 عادل عبد العال ابراهيم خراشي، المرجع السابق، ص 116.

بحبسه 21 شهراً، ومنعت الموقع من الاستمرار[1]، كما منع المشرع الجزائري كل المعاملات التي تتم عن طريق الاتصالات الإلكترونية والمتعلقة بلعب القمار والرهان واليانصيب[2].

نأتي الآن للحديث عن أخطر أنواع الإدمان باستخدام الإنترنت، والذي يتعلق بنشر الإباحية وممارسة السلوك الجنسي على الخط من دون أية قيود أو معايير اجتماعية وأخلاقية[3]، حيث هناك عدة أشكال لهذا النوع من الإدمان، ومنها إدمان الجنس في السيبر (Cyber Sexual Addiction)؛ أي البحث عن المواقع الجنسية في الشبكة المعلوماتية، وإدمان علاقات السيبر (Cyber-Relationship Addiction)؛ أي الإفراط في العلاقات على الشبكة[4]، والمشكلة تصبح أكثر خطورة عندما يتعلق هذا النوع من الإدمان بالأطفال، فتلك طائفة من الجرائم الجنسية Sexual Crimes تشمل حض وتحريض القاصرين على أنشطة جنسية غير مشروعة، وإفساد القاصرين بأنشطة جنسية عبر الوسائل الإلكترونية، وإغواء أو محاولة إغواء القاصرين لارتكاب أنشطة جنسية غير مشروعة[5]، حيث يستغل الجناة غرف الدردشة لمقابلة الأطفال، كما حدث حين قيام رجل أمريكي تجاوز الأربعين (40) من عمره، باصطياد ضحاياه من البنات دون الرابعة عشر (14) عن طريق غرف الدردشة ثم الإيقاع بهن، ولحسن الحظ تمكنت أم إحداهن من الإيقاع به، ليحاكم ويسجن بعدها[6].

1 عبد العالي الديربي، محمد صادق إسماعيل، المرجع السابق، ص 175.

2 القانون رقم 18-05، المتعلق بالتجارة الإلكترونية، السالف الذكر: المادة الثالثة (03): تمارس التجارة الإلكترونية في إطار التشريع والتنظيم المعمول بهما. غير أنه، تمنع كل معاملة عن طريق الاتصالات الإلكترونية تتعلق بما يلي: – لعب القمار والرهان واليانصيب، – المشروبات الكحولية والتبغ، – المنتجات الصيدلانية، –المنتجات التي تمس بحقوق الملكية الفكرية أو الصناعية أو التجارية، كل سلعة أو خدمة محظورة بموجب التشريع المعمول به، كل سلعة أو خدمة تستوجب إعداد عقد رسمي".

3 نور على سعد درويش، المرجع السابق، ص 53.

4 خالد العمار، المرجع السابق، ص 413.

5 أيمن عبد الله فكري حسين، المرجع السابق، ص 153؛ أيمن عبد الحفيظ، المرجع السابق، ص 140؛ محمد أمين الرومي، المرجع السابق، ص 130.

6 نجد صدى ذلك في القضية التي عرضت على القضاء الأمريكي والمعروفة باسم USAV ROOTS، والتي تتلخص وقائعها، في أن المدعو ROOTS قام عبر غرفة الدردشة بواسطة الانترنت بالتحدث مع فتاة لم تتجاوز الرابعة عشر من عمرها في موضوعات جنسية، وتناول الكلام عرضه لها بممارسة الأفعال الجنسية معها وتم تحديد موعد للقاء بينها، وعندما حان الموعد تم القبض عليه، وتبين أثناء التحقيق أن الفتاة الصغيرة لم تكن سوى عضو فريق مكافحة جرائم الانترنت، متنكرة في هيئة فتاة صغيرة، وبتكليف من الإدارة التي تعمل بها، وعندما دفع ROOTS بعدم وجود للمجني عليه في الدعوى أمام محكمة الموضوع، رفضت المحكمة الدفع مستندة إلى ما

ومن الأمثلة أيضاً أنه؛ في شهر فبراير من سنة 1998 أنشأ شخص إسباني يبلغ من العمر ثلاثين (30) سنة موقعاً خاصاً بصور جنسية يشارك فيها الأطفال القصر، وما أن فتح ذلك الموقع حتى تلقى طلبات مشاركة من مختلف أنحاء العالم. وفي يوم الاربعاء 1999/08/07 ألقت عليه الشرطة الاسبانية القبض، وعند تفتيشه عثرت في حيازته على 5000 صورة لأطفال عراة مع تعليق جنسي على كل صورة، و200 شريط فيديو والعديد من الالمبومات والمطبوعات التي يشارك فيها الأطفال بأوضاع جنسية[1].

في بعض الأحيان يتم تجسيد وتصوير صور قريبة من الواقع أو من الطبيعة بطريقة احترافية حتى يتم الإيقاع بالضحايا وبالباحثين عن هكذا صور ولقطات، وهو موضوع حكم عدد 06/4/395 بتاريخ 2006/03/04 صادر عن المحكمة الابتدائية بمراكش: حيث أنه بعد نجاح عمليات التصوير التي قام بها الظنين غادر المغرب رفقة شريكه الفرنسي من أجل المونطاج وتركيب ما تم تصويره لاستغلاله في الموقع الخاص بشركته وبيعه للزبائن عبر شبكة الإنترنت[2]، كما أُدين شخص فرنسي بالسجن لمدة أربع سنوات (04) بعدما ضبط بالجرم المشهود وهو يأخذ صور إباحية لأطفال قصر، كما ضبطت لديه صور إباحية —حوالي 117000 صورة – في آلة التصوير[3].

إن خطورة هذا النوع من الإدمان على الإنترنت؛ والذي غالباً ما يتحول إلى جرائم إلكترونية جعل مختلف التشريعات تقوم برصد عقوبات لمرتكبيه[4]، فاستغلال الأطفال في المواد

هو مقرر في القسم USC.2422(618) من تقرير لجريمة المحاولة، وفي الاستئناف قررت الدائرة الحادي عشر الاستئنافية أنه لا داعي للوجود المادي للمجني عليه في إطار المادة المذكورة، إذ يكفي أن يكون هناك احتمال ارتكاب هذه الجريمة. **انظر**: عبد الفتاح بيومي حجازي، الأحداث والانترنت دراسة متعمقة عن اثر الانترنت في انحراف الأحداث، المرجع السابق، ص 296؛ أحمد عبد اللاه المراغي، المرجع السابق، ص 33، **نقلاً عن**: عمر محمد ابو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، دار النهضة العربية، القاهرة، 2004، ص 276.

1 مصطفى محمد موسى، المرجع السابق، ص 185.

2 إدريس النوازلي، موقف القضاء من الجريمة الإلكترونية، من كتاب جماعي بعنوان التجارة الإلكترونية أية حماية؟، الطبعة الأولى، المطبعة والوراقة الوطنية، مراكش، المغرب، 2010، ص 102.

3 Ali ElAZZOUZI, OP.CIT, p 83.

4 الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر سنة 2010، المصادق عليها بالمرسوم الرئاسي رقم 14-252، السالفة الذكر: المادة (12): جريمة الإباحية: " 1- إنتاج أو عرض أو توزيع أو توفير أو نشر أو شراء أو بيع أو استيراد مواد إباحية أو مخلة بالحياء بواسطة تقنية المعلومات. 2- تشدد العقوبة على الجرائم المتعلقة بإباحية الأطفال والقصر. 3- يشمل التشديد الوارد في الفقرة (2) من هذه المادة، حيازة مواد إباحية الأطفال والقصر أو مواد مخلة بالحياء للأطفال والقصر على

الإباحية، بأشكاله المختلفة، يعد جريمة فيدرالية[1]، ففي القانون الأمريكي وتحت عنوان Child Pornography Prevention Act (CPPA) نص القانون على معاقبة أولئك الذين يقومون بتوزيع أو استقبال مواد إباحية سواء كانت كتابات أو صور أو أية وسيلة أخرى للأطفال بصورة غير مشروعة[2].

إن الإدمان على الإنترنت يساهم في قيام بعض الأشخاص بأفعال تُخلف لأصحابها أشياءً تثبت تورطهم في ارتكاب جرائم، وهو ما أثبته الواقع العملي، فقد مكنت عمليات البحث -بعد الموافقة الخطية للمعني- من حجز جهاز الحاسب الآلي الخاص به، وبعد الفحص التقني له تبين زيارة المعني لمواقع إباحية، كان يُحَمل منها صور خلعية لأطفال، كما تم حجز تسعة عشر (19) قرص (DVD) يحتوي على ملفات إباحية للأطفال؛ منفردين تارة، ومع بالغين تارة أخرى، بالإضافة إلى أشرطة فيديو بها مشاهد إباحية لأطفال، وعلى إثرها أصدرت ضده محكمة باريس، حكما بالسجن لمدة ستة أشهر مع وقف التنفيذ، وغرامة قدرها (5000) يورو[3]، كما قام شاب مصري باستخدام حاسوب مزود بكارت فيديو وطابعة وجهاز ماسح ضوئي ووحدات للقراءة والكتابة على الأقراص المدمجة من نسخ عدد كبير من الأفلام سواء من خلال قنوات فضائية أو من أشرطة فيديو أخرى، وسجل منها أفلاماً فاضحة وأعاد نسخها وبيعها[4].

تقنية المعلومات أو وسيط تخزين تلك التقنيات."؛ القانون 03-24 المتعلق بتعزيز الحماية الجنائية للطفل والمرأة (الفصل 1-503 والفصل 2-503 من مجموعة القانون الجنائي المغربي. الفصل 1-503 عاقب على جريمة التحرش الجنسي، والفصل 2-503 جرم كل صور التحريض أو التشجيع أو تسهيل استغلال أطفال تقل أعمارهم عن ثمانية عشر (18) سنة في مواد إباحية"؛ ولمزيد من التفاصيل بخصوص خطورة الإدمان على الإنترنت يمكن الرجوع إلى: نعيم مغبغب، مخاطر المعلوماتية والانترنت (المخاطر على الحياة الخاصة وحمايتها دراسة في القانون المقارن)، المرجع السابق، ص 226؛ شنتير خضرة، الجريمة الإلكترونية تستهدف الأطفال"جريمة الاستغلال الجنسي للأطفال عبر الانترنت (نموذجاً)"، مجلة دفاتر السياسة والقانون، جامعة قاصدي مرباح بورقلة، الجزائر، العدد الخاص، جوان 2018، ص. ص: 309-310.

1 Sizwe Snail , *Cyber Crime in South Africa – Hacking, cracking, and other unlawful online activities*, Journal of Information, Law & Technology (JILT), 28/05/2009, p : 10.

2 أيمن عبد الحفيظ، المرجع السابق، ص 144.

3 Cour de cassation, chambre criminelle, Audience publique du 28 mars 2012, N° de pourvoi: 11-83012 (Non publié au bulletin).

4 أيمن عبد الحفيظ، المرجع السابق، ص 456.

كثيراً ما يستغل مرتكبو جرائم الجنس صعوبة تحديد هويتهم لافتراس الأطفال، لكن الشرطة تمكنت من تعقب بعضهم والحصول على أجهزة الحواسيب الشخصية الخاصة بهم[1]، ولأجل تسهيل تلك المهمة يتعاون الأنتربول بشكل وثيق مع مزودي خدمة الإنترنت لمنع الوصول إلى مواد إساءة معاملة الأطفال عبر الإنترنت، وكذلك يفعل المركز الوطني التابع لدائرة شرطة البريد والاتصالات الإيطالية، والخاص بمكافحة استغلال الأطفال في المواد الإباحية على الإنترنت، الذي يقوم بتحديث قائمة سوداء لإرسالها إلى مقدِمي خدمة الإنترنت، لكي يتمكنوا من منع مستخدمي الإنترنت في إيطاليا من الوصول إلى الفضاءات الافتراضية المحتوية على مواد الاعتداء الجنسي على الأطفال الصادرة من بلدان أخرى[2].

وفي هذا الإطار، نجح المركز الاسترالي لمكافحة جرائم الإنترنت في توقيف 40 متهماً بجرائم الاغتصاب والاستغلال الجنسي وتنظيم السياحة الجنسية وتوزيع أفلام إباحية باستخدام شبكة الإنترنت[3]، وقامت مصر في إطار مجهوداتها الوطنية لمكافحة جرائم الاستغلال الجنسي للأطفال، بإنشاء اللجنة الوطنية التنسيقية لمكافحة ومنع الاتجار بالبشر، والتي أنشأت بموجب قرار من رئيس مجلس الوزراء رقم 1584 لسنة 2007 بموجب المادة (27) من القانون الوطني الجديد رقم 64 لسنة 2001 بشأن مكافحة الاتجار بالبشر[4]، وفي استراليا تحركت مجموعة من البرلمانيين لوضع حد للألعاب التي تحوي في طياتها عنفاً وجنساً، فلعبة Nite Trap، صودرت ومنعت من الأسواق بأمر من المحكمة حتى صدور تصنيف لتلك الألعاب، كما في الأفلام[5].

الفرع الثاني: آليات الحد من الإدمان على الإنترنت.

بينت الإحصائيات التي أجريت عن استخدام الإنترنت في مختلف الدول أن نسبة استخدامه في ارتفاع مستمر، ففي الجزائر وصلت النسبة إلى ما يزيد عن أربعة وثلاثين (34) مليون مشترك

1 على جبار الحسيناوي، المرجع السابق، ص 83.

2 تقرير الأمين العام، الجمعية العامة، الأمم المتحدة، مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية (القرار رقم 73/187)، الدورة الرابعة والسبعون، البند 109 من جدول الأعمال المؤقت (A/74/130)، 30 جويلية 2019، ص 48.

3 عبد العالي الديربي، محمد صادق إسماعيل، المرجع السابق، ص 178.

4 عادل عبد العال ابراهيم خراشي، المرجع السابق، ص 122-123.

5 عنو عزيزة، آثار الألعاب الإلكترونية على الخصائص النفسية السلوكية لدى الطفل، حوليات جامعة قالمة للعلوم الاجتماعية والإنسانية، جامعة 08 ماي 1945 قالمة، المجلد الثامن (08)، العدد الحادي عشر (11)، جوان 2015، ص 234.

سنة 2017، وفي مصر ما يقارب واحد وأربعين (41) مليون مشترك خلال سنتي 2018، و2019[1]، وهو الأمر الذي ساعد في انتشار الإدمان على الإنترنت بمختلف أنواعه، إذ أكدت بعض المراكز المتخصصة من خلال الدراسات والبحوث التي قامت بها أن الإدمان على الإنترنت أصبح واقعاً وحمى مرضية[2]، الشيء الذي يستدعي البحث عن آليات لمعالجته والتقليل منه؛ ومن تلك الآليات مراكز معالجة الإدمان على الإنترنت، وحجب المواقع الإلكترونية، والسوار الإلكتروني كعقوبة بديلة.

البند الأول: مراكز معالجة الإدمان على الإنترنت

إن من بين التدابير الاحترازية بحق مرتكبي الأفعال والسلوكيات المجرمة بالقانون: الإشراف، الرقابة، الحرمان، الوضع في مأوى علاجي أو مركز تأهيل، بخلاف العقوبات الأصلية للجريمة والعقوبات التبعية أو التكميلية لها[3]، فإنشاء مراكز متخصصة لمعالجة الإدمان على الإنترنت هي بمثابة تدبير من بين تلك التدابير الاحترازية، وذلك بالحرمان من استعمال أو استخدام الشبكة المعلوماتية، هذا الحرمان الذي حدده المشرع الجزائري لمدة أقصاها ثلاث (3) سنوات تسري ابتداء من يوم انقضاء العقوبة الأصلية أو الإفراج عن المحكوم عليه، أو من تاريخ صيرورة الحكم نهائيا بالنسبة للمحكوم عليه غير المحبوس[4].

---

1 **عن الجزائر**: محمد.ل، بانتقال مشتركين نحو شبكات الجيل الثالث والرابع قرابة 34 مليون مشترك في الانترنت بالجزائر، جريدة الشروق، العدد 5502، الجمعة 30 جوان 2017، متاح على الرابط الإلكتروني التالي:

https://www.echoroukonline.com/%D9%82%D8%B1% ، تاريخ الإطلاع: 2020/07/05.

وعن مصر: هبة السيد، لأول مرة تقرير لـ"الاتصالات" يكشف: 40.9 مليون مستخدم للإنترنت في مصر، اليوم السابع، الثلاثاء، 30 أبريل 2019، متاح على الرابط الإلكتروني الموالي:

https://www. youm7.com/story/2020/7/5/%D9%81%D9 تاريخ الإطلاع: 2020/07/05.

2 حمودة سليمة، المرجع السابق، ص 216.

3 عبيد صالح حسين، سياسة المشرع الإماراتي لموجهة الجرائم الإلكترونية، مجلة الفكر الشرطي، مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، الإمارات، المجلد الرابع والعشرون (24)، العدد الخامس والتسعون (95)، اكتوبر 2015، ص 47.

4 تنص المادة 149 مكرر 8 من الأمر رقم 20-01، الذي يعدل ويتمم الأمر رقم 66-156 والمتضمن قانون العقوبات، السالف الذكر على:"...، يمكن حرمان المحكوم عليه بسبب ارتكابه جريمة من الجرائم المنصوص عليها في هذا القسم، من استخدام أي شبكة إلكترونية أو منظومة معلوماتية أو أية وسيلة من وسائل تكنولوجيات الإعلام والاتصال، لمدة أقصاها ثلاث (3) سنوات تسري ابتداء من يوم انقضاء العقوبة الأصلية أو الإفراج عن المحكوم عليه، أو من تاريخ صيرورة الحكم نهائيا بالنسبة للمحكوم عليه غير المحبوس".

وعلى اعتبار أن إدمان الإنترنت هو مرض العصر فقد أنشئت له عدة مصحات متخصصة وعيادات نفسية لعلاجه[1]، حيث أنشأ أول مستشفى في الولايات المتحدة لعلاج إدمان الإنترنت في سنة 1995 في مركز برادفورد الطبي الإقليمي في بنسلفانيا[2]، ثم بعدها أقيمت عشرات العيادات لإعادة التأهيل الرقمي في وادي السيليكون، والذي يعتبر مركز تواجد أكبر شركات التكنولوجيا في العالم، كشركة آبل، وفيسبوك، وتويتر، وجوجل.

وفي سابقة تعد الأولى من نوعها عربيا، أنشأت مجموعة من المختصين النفسانيين الجزائريين مركز لمكافحة وعلاج الإدمان على الإنترنت ومواقع التواصل الاجتماعي بولاية قسنطينة، ليكون هذا المركز هو الثالث من نوعه في العالم إلى جانب آخرين أحدهما بجمهورية الصين والثاني بكوريا، والتي أعلنت –كوريا الجنوبية– أن إدمان الإنترنت هو "قضية صحية عامة"، توجب تقدم العلاج اللازم لها في المستشفيات الحكومية.

إن معالجة مدمني الإنترنت هي مسألة في غاية الأهمية في وقتنا هذا، نظراً لانتشار استخدام الإنترنت بين مختلف فئات المجتمع، وهو ما سيوسع من دائرة مدمنيه، ويُكثر من احتمال ارتكاب جرائم إلكترونية، وعودة بعض المجرمين الإلكترونيين لارتكاب تلك الجرائم[3]، فمعالجة مدمني الإنترنت قد تبعدهم عن كل ذلك؛ وتوجههم نحو استغلال مواهبهم في مجالات أكثر فائدة.

البند الثاني: حجب المواقع الإلكترونية

يعد حجب المواقع الإلكترونية من بين الأساليب المتبعة في مواجهة الجرائم الإلكترونية خاصة تلك المرتكبة عبر الإنترنت، وقد أولتها بعض التشريعات اهتماماً خاصاً، إذ نصت عليها

1 يوسف أبو الحجاج، المرجع السابق، ص 170.

2 حمودة سليمة، المرجع السابق، ص 222.

3 كان المدعو "كافين متنك" من مدينة لوس انجلوس الأمريكية، يقضي معظم وقته في ممارسة هواية الاعتداء على نظم الهاتف، وفي عام 1981 القي عليه القبض لأول مرة بسبب إتلافه بيانات شبكة حاسوب وسرقة دليل العمليات من إحدى شركات الهاتف، ومن حينها اعتاد "متنك" ارتكاب العديد من الجرائم الإلكترونية كالسطو على نظم الحاسوب، وسرقة البرامج والمعلومات وأرقام بطاقات الائتمان، إلى أن القي عليه القبض في عام 1989 بعد أن سرق برامج تقدر قيمتها بملايين الدولارات من شركة المعدات الرقمية (DEC)، فتمت إدانته بموجب قانون التزوير وسوء استخدام الحاسوب، وحكم عليه بالسجن لمدة عام، ثم أفرج عنه لصغر سنه، ليختفي بعدها "متنك" مواصلا نشاطه الإجرامي، الشيء الذي أدى إلى القبض عليه مرة أخرى عام 1995 وهو يحاول السطو على شبكة معلومات مكتب التحقيقات الاتحادي (FBI). **انظر**: أحمد يوسف أحمد حسين الطحطاوي، المرجع السابق، ص 333.

في قوانينها للحد من قيام الأشخاص بتصرفات معينة عبر المواقع والوسائط الإلكترونية[1]، وعلى الرغم من أن بعض التشريعات لم تتضمن فيما سبق قوانين تبين المجالات التي يمكن فيها إجراء عملية حجب المواقع الإلكترونية، إلا أن القضاء كان يأمر بذلك عندما يستدعي الموقف ذلك[2].

لقد خُصص لموضوع حجب المواقع الإلكترونية عدة برامج؛ ومن تلك البرامج برنامج يعمل "بالويندوز" حيث يقوم هذا البرنامج بالبحث عن الصور الجنسية الموجودة بالحاسوب ويبلغ الهيئات الحكومية عنها لتطهير الشبكة من المواقع الإباحية والجنسية، إذ تصلها رسائل إلكترونية بعنوان "ساعدونا لإنهاء المواقع الإباحية"[3]، ومنها أيضاً ما قامت به وزارة الأمن العام الصينية حين طرحت برنامجاً مصمماً لإبعاد المعتقدات والجنس والعنف عن الإنترنت، سمته "شرطة الإنترنت 110" لمنع المستخدمين من تلقي معلومات ضارة من مواقع أجنبية ومحلية، وهذا البرنامج به ثلاثة نسخ للمنازل ومقاهي الإنترنت والمدارس، ويمكنه منع الرسائل التي تصل من مواقع مشينة[4]. ولكن على الرغم من كثرة البرامج وخاصة تلك التي حاولت وضع حد لولوج الأطفال لمواقع إباحية، إلا أنه لا يوجد برنامج متكامل يتسم بالإتقان الكامل لمراقبة شبكة الإنترنت حتى الآن[5].

1 المواد 05، و37، و38 من القانون رقم 18-05، المتعلق بالتجارة الإلكترونية، السالف الذكر؛ المادة 7 من القانون رقم 175 لسنة 2018، والخاص بمكافحة جرائم تقنية المعلومات المصري، السالف الذكر.

2 لقد جاء في حكم لمحكمة القضاء الإداري، الدائرة الأولى:"...، كما لم تتضمن هذه التشريعات ثمة نصوص تجيز للأجهزة الحكومية تقرير حظر أو حجب المواقع الإلكترونية من الظهور على شبكة الانترنت بصفة عامة أو من الظهور لمستخدمي الشبكة داخل مصر بصفة خاصة غير أن هذا الفراغ التشريعي لا يخل بحق الأجهزة الحكومية من إلزام مزودي الخدمة بحجب أي من المواقع المسجلة لديها حيثما تمس الأمن القومي أو المصالح العليا للدولة، وذلك بما لتلك الأجهزة من سلطة في مجال الضبط الإداري لحماية النظام العام بمفهومه المثلث الأمن العام والصحة العامة والسكينة العامة للمواطنين". **نقلاً عن:** وجدي شفيق، الجديد في الإثبات الإلكتروني (ومدى حجية المستخرجات الإلكترونية في الإثبات ودورها في حجب المواقع الإلكترونية والاختصاص الجنائي بجرائم التوقيع الإلكتروني وفق القانون رقم 15 لسنة 2004 ولائحته التنفيذية)، الطبعة الأولى، شركة آل طلال للنشر والتوزيع، القاهرة، 2015، ص 98.

3 مرنيز فاطمة، المرجع السابق، ص.ص: 236-237، **نقلاً عن:** مصطفى محمد مرسي، المراقبة الإلكترونية عبر شبكة الانترنت دراسة مقارنة بين المراقبة الأمنية والإلكترونية، الكتاب الخامس، الطبعة الأولى، دار الكتب والوثائق القومية المصرية، 2003، ص 217.

4 مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 326.

5 جعفر حسن جاسم الطائي، المرجع السابق، ص 255.

إن حجب المواقع الإلكترونية الإباحية يعد من بين الأساليب المجدية والفعالة في خفض نسبة الجرائم وبالأخص جريمة الاغتصاب[1]، لذا تم تشكيل لجنة أمنية دائمة للانترنت في المملكة العربية السعودية، والتي من بين مهامها حجب المواقع الإباحية والمواقع التي توفر وسائل لتجاوز الترشح[2]، كما قامت مدينة الملك عبد العزيز للعلوم والتقنية بإغلاق مجموعة من المواقع الإباحية، ومنها موقع (Yahoo)، وموقع (Globelist)، وموقع (Topica)[3].

وقد لا تقتصر عملية حجب المواقع الإلكترونية على المواقع الإباحية فقط، بل تشمل أيضاً مواقع أخرى كتلك التي تنتهك العلامات التجارية والملكية الفكرية[4]، والتي تمس بنزاهة الامتحانات والمسابقات[5]، وكذا المواقع الإلكترونية المتطرفة، كتلك التي تدعو للتمييز والحض على الكراهية[6]، أو تلك التي تهين وتتعدى على المؤسسات الصحية ومستخدميها[7]، وكذا المواقع الإلكترونية التي

1 عادل عبد العال ابراهيم خراشي، المرجع السابق، ص.ص: 131-132.

2 عبد الصبور عبد القوي علي مصري، المحكمة الرقمية والجريمة المعلوماتية دراسة مقارنة، المرجع السابق، ص 99.

3 عبد الصبور عبد القوي علي مصري، المرجع نفسه، ص 70.

4 في نوفمبر 2014 طالبت شركة Cartier International AG & Ors في قضيتها ضد شركة British EWHC 3354 (Ch) 2014 Sky Broadcasting Ltd & Ors، بإصدار أمر قضائي يلزم مزودي خدمات الانترنت بحجب الوصول إلى مواقع شبكية تبيع سلعاً تنتهك العلامات التجارية لشركة كارتييه. وتكتسي تلك القضية أهمية خاصة في المملكة المتحدة نظرًا لعدم وجود أي تشريع ينص صراحة على ذلك النوع من أوامر حجب المواقع الشبكية التي تُنتهك فيها العلامات التجارية. وتعد تلك الأوامر أداة قيمة من حيث التدابير المتاحة لأصحاب الحقوق من أجل حماية حقوقهم المتعلقة بالملكية الفكرية وإنفاذها في المملكة المتحدة، ولكن يقتضي استصدارها جهدًا كبيرًا وتكلفة عالية، فلا يُلجأ إليها إلا ضد المواقع الشبكية التي ترتكب أشد الانتهاكات ضرراً. **نقلاً عن**: تقرير للمنظمة العالمية للملكية الفكرية WIPO، اللجنة الاستشارية المعنية بالانفاذ، الدورة الثانية عشر، الترتيبات المؤسسية لمعالجة التعديات على الملكية الفكرية على الانترنت في الدول الأعضاء في الويبو، جنيف، من 04 إلى 06 سبتمبر 2017، متاح عبر الرابط الإلكتروني الموالي: *http://www.wipo.int/edocs/mdocs/enforcement%20/ar/wipo_ace_12/wipo_ace_12_10.pdf* والذي تم الاطلاع عليه يوم 2018/10/03.

5 تنص المادة 253 مكرر 11 من الفصل التاسع، الذي يحمل عنوان: المساس بنزاهة الامتحانات والمسابقات، من القانون 20-06، والمتضمن تعديل وتتميم قانون العقوبات، السالف الذكر على أنه: "دون الإخلال بحقوق الغير حسن النية، يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة في ارتكاب الجرائم المنصوص عليها في هذا الفصل والأموال المتحصلة منها، وإغلاق الموقع الإلكتروني أو الحساب الإلكتروني الذي ارتكبت بواسطته الجريمة، أو جعل الدخول إليه غير ممكن، وإغلاق محل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكه".

6 المادة 37 من القانون رقم 20-05، المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما، السالف الذكر.

7 المادة 149 مكرر 9 من الأمر رقم 20-01، الذي يعدل ويتمم الأمر رقم 66-156 والمتضمن قانون العقوبات، السالف الذكر .

تسعى إلى تجنيد الشباب في صفوف الإرهابيين عن طريق شبكة الإنترنت[1]، فكل تلك الممارسات التي تتم عبر المواقع الإلكترونية دفعت بالحكومات إلى اتخاذ مجموعة من الإجراءات؛ كمراقبة نشاطات تلك الجماعات على شبكات التواصل الاجتماعي لقطع التواصل بين عناصرها، وسد منافذ تمويلها، والضغط على مقدمي الخدمات والشركات الإعلامية خاصة منها الاجتماعية لضبط المحتويات غير المرغوبة على مواقعها[2].

كما عمدت عدة شركات تقنية كبرى أو ما يسمى بشبكات التواصل الاجتماعي، كالفيس بوك، ويوتيوب، ومايكروسوفت، وتويتر، إلى تشكيل تعاون فيما بينها من أجل حذف المحتوى المتطرف من منصاتها، وفي هذا الصدد أعلنت تويتر أنها تستخدم الذكاء الاصطناعي للقضاء على المحتوى الإرهابي على صفحاتها، وتقول الشركة أن ما يقرب من (377.000) حساب تمت إزالتها بين شهري يوليو وديسمبر من عام 2016.[3]

1 توفيق مجاهد، طاهر عباسة، المرجع السابق، ص 97؛ أحمد عبد اللاه المراغي، المرجع السابق، ص 148.

2 القانون رقم 16-02، يعدل ويتمم قانون العقوبات، المادة الثانية تتمم قانون العقوبات بثلاث مواد منها المادة 394 مكرر 08 التي تنص: "دون الإخلال بالعقوبات الإدارية المنصوص عليها في التشريع والتنظيم الساري المفعول، يعاقب بالحبس من سنة إلى ثلاث(3) سنوات وبغرامة من 2.000.000 دج إلى 10.000.000 دج، أو بإحدى هاتين العقوبتين فقط، مقدم خدمات "الانترنت" بمفهوم المادة 2 من القانون رقم 09-04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام الاتصال ومكافحتها، الذي لا يقوم رغم إعذاره من الهيئة الوطنية المنصوص عليها في القانون المذكور أو صدور أمر أو حكم قضائي يلزمه بذلك: أ- بالتدخل الفوري لسحب أو تخزين المحتويات التي يتيح الاطلاع عليها أو جعل الدخول إليها غير ممكن عندما تتضمن محتويات تشكل جرائم منصوص عليها قانونا، ب- بوضع ترتيبات تقنية تسمح بسحب أو تخزين المحتويات التي تتعلق بالجرائم المنصوص عليها في الفقرة (أ) من هذه المادة أو لجعل الدخول إليها غير ممكن"؛ تنص المطة الثالثة من الفقرة الثانية من المادة (23) – تدابير حماية الأطفال والأشخاص الضعفاء- من الفصل الرابع: شروط استغلال الخدمات من المرسوم التنفيذي رقم 20-61، المتضمن الموافقة على رخصة لإقامة واستغلال شبكة مفتوحة للجمهور للاتصالات الشخصية النقالة العالمية، عبر السواتل من نوع GMPCS، ولتوفير خدمات الاتصالات الإلكترونية للجمهور، الممنوحة على سبيل التنازل لشركة "اتصالات الجزائر الفضائية، شركة ذات أسهم"، وتحديدها، مؤرخ في 20 رجب عام 1441 الموافق 15 مارس سنة 2020، الصادر في الج.ر.ج العدد 17 المؤرخة في 28 مارس سنة 2020، على أنه: "يلتزم صاحب الرخصة بوضع حلول، تكنولوجية وتنظيمية على الخصوص، لغرضها على زبائنه ولترقية الخدمة لديهم، تسمح لهم بحماية أطفالهم أو الأشخاص الضعفاء الموجودين تحت وصايتهم وذلك عبر تقييد النفاذ إلى وجهات أو محتويات غير مرغوب فيها".

3 حنان خرباشي، المرجع السابق، ص 144؛ **وانظر أيضاً:**

- Danny Vena, «*How Social Media Is Using AI to Fight Terrorism*», The Motley Fool, 26 June 2017.

البند الثالث: السوار الإلكتروني كآلية لمراقبة مدمني الإنترنت.

من خلال ما سبق يتبين أن إدمان الإنترنت لا يختلف تماماً عن إدمان الكحوليات، والمواد المخدرة، والعقاقير وذلك لما يحمله من أضرار نفسية كالاكتئاب والقلق والشعور بالوحدة النفسية وفقدان الثقة بالنفس، إضافة إلى أضرار صحية واجتماعية، وأسرية، وأكاديمية[1]، لذا يمكن جداً مستقبلاً أن يتم النص على معاقبة تعاطي المخدرات الرقمية والإدمان على الإنترنت؛ إذ يمكن أن يكون السوار الإلكتروني[2] كوسيلة لمراقبة مدمني الإنترنت، أو كعقوبة بديلة لتنفيذ العقوبة السالبة للحرية قصيرة المدة خارج أسوار السجن، فالسوار الإلكتروني يعد من العقوبات البديلة التي تتلاءم مع التطور التكنولوجي الحاصل في العالم ككل، والتي جسدها المشرع الجزائري من خلال القانون 18-01، الذي تمم القانون رقم 05-04 الخاص بقانون تنظيم السجون وإعادة الإدماج الاجتماعي للمحبوسين[3]، وذلك من خلال المواد: 150 مكرر إلى المادة 150 مكرر 16.

---

1 في دراسة أجريت هدفت إلى معرفة تأثير الإدمان على الانترنت والأنشطة عبر الإنترنت على نوعية الحياة ذات الصلة بالصحة (HRQOL)لدى الشباب الفيتنامي، شملت 566 شابًا فيتناميًا (56.7٪ إناث ، 43.3٪ ذكر) تتراوح أعمارهم بين 15 إلى 25 عامًا، وأظهرت نتائج هذه الدراسة أن 21.2٪ من المشاركين يعانون من الإدمان على الانترنت (IA)، حيث أن ذلك أثر بشكل كبير على سلـوكياتهم وأنماط حياتهم اليومية، حيث أصـبح لديهم صـعوبة في القيام بالأعمال المعتادة، والتي يطلق عليها البعض الأعمال اليومية الروتينية، كما أنهم يعانون من الألم وعدم الراحة والقلق والاكتئاب، **نقلاً عـن**:

- Bach Xuan Tran, *A study on the influence of internet addiction and online interpersonal influences on health-related quality of life in young Vietnamese*, BMC Public Health, Published online 2017 Jan 31.

وقد أشار إلى ذلك أيضاً: محمد بن سالم محمد القرني، إدمان الانترنت وعلاقته ببعض الاضطرابات النفسية لدى عينة من طلاب جامعة الملك عبد العزيز، مجلة كلية التربية، جامعة المنصورة، مصر، الجزء الثالث، العدد الخامس والسبعون (75)، يناير 2011، ص 133.

2 المراقبة الإلكترونية هي أحد الأساليب المبتكرة لتنفيذ العقوبة السالبة للحرية قصيرة المدة خارج أسوار السجن – في الـوسط الحر – أو ما يسمى "السجن في البيت"، وسمي كذلك لأن المحكوم عليه يسمح له البقاء في منزله، وتكون تحركاته محدودة ومراقبة بواسطة جهاز يشبه الساعة أو السوار مثبت في معصمه أو أسفل قدمه. **انظـر**: صفاء أوتاني، الوضع تحت المراقبة الإكترونية "السوار الإلكتروني" في السياسة العقابية الفرنسية، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، سوريا، المجلد 25، العدد الاول، 2009، ص 131؛ سلطان سالم فاضل البقي، العقوبات البديلة لذوي الاحتياجات الخاصة: دراسة تأصيلية مقارنة، رسالة مقدمة استكمالاً لمتطلبات الحصول على درجة الماجستير في العدالة الجنائية تخصص السياسية الجنائية، قسم العدالة الجنائية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2012، ص 52.

3 القانون رقم 18-01، المؤرخ في 12 جمادى الأولى عام 1439 الموافق 30 يناير سنة 2018، والمتضمن قانون تنظيم السجون وإعادة الإدماج الاجتماعي للمحبوسين، المنشور بالج.ر.ج العدد 05، الصادر في 30 يناير سنة 2018، يتمم القانون رقم 05-04 المؤرخ في 27 ذي الحجة عام 1425 هـ الموافق 06 فبراير سنة 2005.

خـــــاتمـــــة

خاتــمــة:

لقد أدى التطور الكبير والمتسارع للوسائل التكنولوجية الحديثة؛ والتحول إلى العالم الرقمي لخلق مجموعة من أخطر الجرائم التي يشهدها العالم اليوم؛ ألا وهي الجرائم الإلكترونية التي باتت تهدد مختلف فئات المجتمع دون استثناء، الأمر الذي دفع أغلب الدول إلى تخصيص قوانين واستحداث آليات للحد منها، إلا أن ذلك لم يحد من انتشارها واستفحالها واستمرارها في المجتمعات، الشيء الذي جعل من عملية البحث عن آليات قانونية لمكافحتها ذا أهمية بالغة يسعى لها جل الباحثين القانونيين، لسد ذلك النقص الذي يواجه عملية المكافحة؛ وما هذه الدراسة إلا عينة من تلك الدراسات.

فلقد حاولنا من خلال هذه الدراسة تتبع القوانين وإيجاد الملغى منها والساري المفعول، لأن الجريمة الإلكترونية في عدة دول ساهمت في تحريك عجلة التشريع، الذي حاول اللحاق بطبيعتها المتسارعة، التي سبقت في أحيان عدة تفكير رجال القانون الذين حاولوا خلق إطار قانوني كفيل بحصر الأفعال الإجرامية التي يقوم بها مرتكبوها، أولئك المجرمون الـذين لهـم من الصفات ما مكنهم من القـيام بجرائمهم بكل احترافية ودقة في التنفيذ وسرعة في إخفاء الدليل مما استلزم إيجاد آليات مكافحة خاصة، واعتماد جهات بحث وتحري مدربة ومتمكنة من تقنية المعلومات وكذا جهات محاكمة متخصصة.

ولأن الجريمة الإلكترونية هي جريمة ذات طابع عابر للحدود لم تكن الآليات المخصصة لها على المستوى الداخلي لوحدها قادرة على مجابهتها؛ بل استلزم الأمر إيجاد آليات مكافحة بتنسيقٍ وتعاونٍ إقليمي ودولي تتكاثف فيه كل الجهود وتتوحد من أجله كل القوى لإيجاد آليات مكافحة فعالة وفاعلة لهذه الظاهرة الإجرامية التي أصبحت تتم بها أخطر الجرائم التي يشهدها عصرنا هذا الذي أضحت فيه التكنولوجيا المتقدمة عصب الحياة ومحركها، فكما استغلها ويستغِلها مجرمو المعلوماتية، يجب أن تكون تلك الوسائل التقنية وسيلة لمحاربتهم والتبليغ عنهم، وكشف جرائمهم الإلكترونية، وإلقاء القبض عليهم، وذلك من خلال عدة أمور كاستغلال وسائل التواصل الاجتماعي والبريد الإلكتروني، والرسائل عبر الهواتف من أجل التوعية بخطورة هذه الجريمة،

وتخصيص مواقع رسمية للإبلاغ عن الجرائم الإلكترونية بمختلف أنواعها، واللجوء إلى تفعيل التعاون الدولي الذي يعد من أهم سبل مكافحتها وملاحقة مرتكبيها، دون أن ننسى الدور الذي تلعبه الجمعيات في هذا الإطار، فكثير من الضحايا يفضلون التعامل مع الجمعيات بدل الجهات الأمنية، إذ يمكن لهذه الجمعيات أن تكون همزة وصل بين الضحايا والجهات الأمنية المتخصصة في مكافحة الإجرام الإلكتروني.

هذا بالإضافة إلى الجانب التوعوي الذي يمكن أن تساهم فيه هذه الأخيرة مع الجهات الأمنية المختصة والجامعات والمساجد والأسر لتوضيح الصورة عن مدى خطورة هذه الجريمة لدى مختلف الفئات؛ خاصة المتمدرسة منها، لأننا في بلدنا على مشارف مـرحلة ستلعب فيها الوسائل الإلكترونية الأداة الرئيسية في المنهج التعليمي والتكويني في مختلف المؤسسات على المستوى الوطني، هاته الوسائل التي ستكون المحرك الرئيسي في الإدارات الجزائرية التي تسعى لأن تكون في مصف الإدارات الإلكترونية المتطورة، وهو سبب من الأسباب التي ستزيد من نسبة المدمنين على الإنترنت والوسائل الإلكترونية عامة، هذا النوع من الإدمان الذي لا يقتنع الكثيرون بأنه مرض من أمراض التـكنولوجيا الحـديثة، التي تستوجب الخضوع للعلاج؛ هذا النوع من العلاج الذي سيكون مستقبلاً كنوع من أنواع العقاب تلجأ إليه الجهات القضائية في معاقبة الجرائم الإلكترونية البسيطة، وبالأخص التي يكون مرتكبوها صغار السن، كما قد يكون السـوار الإلكتروني كنوع من أنـواع المراقبة وكسبيل للـعقوبة البديلة التي يُعنى بها مجرمو المـعلوماتية، خاصة إذا كانت جرائمهم ليست على درجة كبيرة من الخطورة، وكانوا صغار السن.

لقد خلصت هذه الدراسة إلى عدة نتائج وتوصيات، والتي قد يكون بعضها بداية لدراسات جديدة، نوردها كالأتـي:

أولاً– النتائـج:

1- أول ما يمكن استنتاجه هو عدم وجود تعريف جامع مانع للجريمة الإلكترونية، مما نتج عنه الإختلاف المتباين في الأفعال التي تعد من قبيل الجرائم الإلكترونية، وقد يكون سبب ذلك الطبيعة المتسارعة والتطور الكبير الذي تشهده هذه الجريمة الخطيرة وعدم قدرة التشريع على مجاراتها، نظراً لما يتميز به هذا الأخير من جمود وبطء في إجراءات صدوره.

2- أن الجريمة الإلكترونية لها ميزات خاصة تختلف بها عن الجرائم التقليدية الأخرى، ومرد ذلك يعود للبيئة الرقمية الإلكترونية التي ترتكب فيها، مما أكسبها وأكسب مرتكبها المجرم الإلكتروني سمات معينة، صعبت معها عملية المكافحة الإجرائية والمؤسساتية والاستباقية المتخذة بشأنها.

3- لم يضع المشرع الجزائري نصاً قانونياً خاصاً بالجرائم الإلكترونية رغم ما تسببه هذه الجرائم من أضرار على المجتمع والدولة معاً، خاصة وأن الجزائر تتجه نحو رقمنة الإدارة الجزائرية بما يتماشى والعصرنة الحاصلة في العالم.

4- الدليل الإلكتروني له طبيعة خاصة تستدعي التعامل معها بحذر، خاصة حين القيام بعملية التفتيش والضبط، لأن المجرم الإلكتروني لديه خبرة جيدة في إخفاء ما ينتج عنه من أدلة.

5- آليات المكافحة الحالية غير كافية لمجابهة الجريمة الإلكترونية، فلا يمكن لأي دولة مهما بلغ تطورها التكنولوجي والمعلوماتي أن تتصدي لهذه الجريمة العالمية بمفردها، فالمجرم الإلكتروني قد يكون في دولة ما وينفذ جريمته الإلكترونية في دولة ثانية، وبالإمكان أن تتحقق نتيجتها في دولة ثالثة، أو حتى في عدة دول، مما يُصَعِب عملية متابعته خاصة في حالة عدم وجود اتفاقية بين الـدولة التي يتواجد على أرضــها والدولـة المطــالبة بـه، وعليه فإن آليات المكافحة المخصصة من طرف بعض الدول تعد غير كافية للتصدي للجريمة الإلكترونية.

6- شكلت الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها محور اهتمام العديد من السلطات، مما أدى إلى تعاقب السلطات على ترأسها؛ بداية من وزارة العدل سنة 2015، ثم وزارة الدفاع الوطني سنة 2019، لتوضع تحت سلطة رئيس الجمهورية سنة 2020.

7- الإدمان على الإنترنت، والمخدرات الرقمية هما حقيقة موجودة رغم إنكارها من قبل الكثيرين، فانشغال الشباب بالساعات بالألعاب الإلكترونية، وسقوط بعضهم في مصيدة مصممي الألعاب الإلكترونية الخطيرة خير دليل على ذلك، إضافة إلى التقارير التي أصدرتها عدة هيئات في هذا الاطار، مثل تقرير الهيئة الدولية لمراقبة المخدرات.

8- تعد مراكز معالجة الإدمان على الإنترنت آلية استباقية مهمة للحد من الاستعمال المفرط للإنترنت، والذي قد يوقع صاحبه في مخاطر الجرائم الإلكترونية، سواءً كضحية، أو كمرتكب للجريمة الإلكترونية.

9- سيكون السوار الإلكتروني في المستقبل بمثابة وسيلة لمراقبة مدمني الإنترنت، وكذا عقوبة بديلة عن الحبس قصير المدة لمجرمي المعلوماتية؛ خاصة صغار السن، والاقل خطورة لتجنيبهم الإختلاط مع المساجين المتواجدين في المؤسسات العقابية.

ومما سبق يمكن أن نخرج بمجموعة من التوصيات نذكرها فيما يلـــي:

1- نناشد المشرع الجزائري بإصدار قانون خاص بمكافحة الجرائم الإلكترونية، وإرفاقه بالآليات الإجرائية والمؤسساتية الكفيلة التي تسهل تلك المكافحة.

2- يجب توفير الجو الملائم حتى تتعزز ثقة المواطن بالمعاملات الإلكترونية، خاصة بطاقات الدفع الإلكتروني وما يحتاجه ميدان التجارة الإلكترونية من تعاملات بهذا الخصوص.

3- لا بد من تفعيل آليات التعاون الدولي التي تتسم بسرعة التنفيذ حتى لا يترك للمجرم الإلكتروني ملاذاً آمناً يلتجئ إليه، وتوسيع الاتفاقيات الدولية الثنائية والجماعية لمكافحة الجرائم الإلكترونية.

4- يتعين على الدولة حجب المواقع المخالفة للقوانين والأخلاق، وخاصة تلك التي تستهدف الأطفال، لأنه ورغم كثرة البرامج المخصصة لهذا الشأن إلا أنها لم تُجْدِ نفعاً، ذلك أن تلك البرامج قد تصعب عملية التحميل العادية، وتبطئ من سرعة الانترنت، إضافة إلى قيام أصحاب تلك المواقع بتغيير عنوان الويب الخاص بها بشكل مستمر، مما يحول دون ملاحقة تلك المواقع وحجبها.

5- ضرورة تكثيف الحملات التوعوية للشباب والأطفال، من أجل وقايتهم من خطورة الإدمان على الإنترنت، لأن هذا النوع من الإدمان يقتل فيهم روح الإبداع، ويجعلهم في عـــزلة عن العالم الحقيقي، كما قد يوقعهم في جـرائم إلكترونية مختلفة، والتي تصـــل نتائجها في بعض الاحيان إلى حصد الأرواح، كما حصل لمن كانوا ضحايا للألعاب الإلكترونية الخطيرة؛ كلعبة الحوت الازرق.

6- خلق فضاءات تنافسية للمواهب التي لديها إمكانات تقنية، كتخصيص جائزة لأحسن برنامج حماية لنظام معلوماتي ما، والذي تم اختراقه رغم وسائل الحماية التي كانت مخصصة له. كل ذلك من أجل استغلال هذه المواهب في الأمور المشروعة بدل تركها عرضة للإجرام.

7- يتعين على القائمين على الشؤون القانونية والقضائية الإهتمام بتكوين رجال البحث والتحري في الجرائم الإلكترونية تكويناً قانونياً، وتكوين رجال العدالة تكويناً تقنياً حتى يكون هناك تكامل وتنسيق فيما بينهم للوصول إلى أدلة إلكترونية صحيحة ومقبولة أمام الجهات المعنية.

8- نظراً لكثرة الجرائم الإلكترونية وتنوعها، يستحسن إنشاء شرطة متخصصة بهذه الجرائم، تكون مهمتها الوحيدة متابعة مثل هذا النوع من الجرائم.

9- إنشاء محكمة جنائية دولية تحت مظلة الأمم المتحدة يكون لها صلاحية النظر في القضايا التي تعنى بالجرائم الإلكترونية الخطيرة ذات الطابع الدولي.

10- تشجيع البحث العلمي في المجال الجنائي وبالأخص ما يتعلق بالجريمة الإلكترونية والعمل بنتائجه في السياسة الجنائية.

11- يتعين على وزارة العدل الجزائرية إصلاح وتطوير المواقع الإلكترونية التابعة لها –كموقع المحكمة العليا الجزائرية– حتى يتمكن الباحثون وخاصة القانونيين منهم أن يعززوا دراساتهم بأحكام قضائية متخصصة، كي لا تبقى دراساتنا فارغة من اجتهادات الجهات القضائية الجزائرية.

قائمـــــة المراجـــــع

قائمـــة المراجـــع:

أولاً- المراجع العربيـــة:

أ)- المراجـــع العامـــــة:

1- أبـــو عامر محمد زكى، الإثبات في المواد الجنائية، الفنية للطباعة والنشر، الإسكندرية، مصر، 1985.

2- أحمد عوض بلال، النظرية العامة للجزاء الجنائي، دار النهضة العربية، القاهرة، مصر، 1995.

3- أمل لطفي حسين جاب الله، نطاق السلطة التقديرية للإدارة في تسليم المجرمين (دراسة مقارنة)، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، 2013.

4- أوشن حنان، وادي عماد الدين، الإثبات الجنائي والوسائل العلمية الحديثة، دار الخلدونية للنشر و التوزيع، الجزائر، 2015.

5- جابر جاد نصار، أصول وفنون البحث العلمي، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 2002.

6- جون بيندر، سايمون أشروود، الاتحاد الأوربي مقدمة قصيرة جداً، ترجمة خالد غريب على، الطبعة الأولى، مؤسسة هنداوي للتعليم والثقافة، القاهرة، مصر، 2015.

7- عبد الله جعفر كوفلي، مراقبـة الاتصالات في التنظيم الدولي والـداخلي، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، مصر،2017.

8- عبد الوهاب عمر البطراوي، مخاطر الهاتف المـحمول (مجالها وأسبابها وعلاجها)، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 2003.

9- علي شملال، المسـتجدات في قـانون الإجراءات الجزائية الجزائري (الكتاب الثاني: التحقيق والمحاكمة- نسخة معدلة ومنقحة 2017-)، الطبعة الثانية، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2017.

10- مجيد خضر السبعاوي، مولان قادر احمد، الضرورة الإجرائية في مرحلة التحقيق الابتدائي (تحليلية—مقارنة)، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، مصر، 2017.

11- محمد أمين الخرشة، مشـروعية الصوت والـصورة في الإثبات الجـنائي دراسة مقارنة، الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2015.

12- محمد الأمين البشري، العـدالة الـجنائية ومـنع الجريمة "دراسـة مقارنة"، الطبعة الأولى، أكاديمية نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، 1997.

13- محمد الازهر، مبادئ في علم الإجـرام، الطبعة التاسعة، مطبعة دار النشر المغربية، الدار البيضاء، المغرب، 2015.

14- مونة جنيح، احمد الزعري، تدبير مسرح الجـريمة وتـحويل الآثار إلى أدلة جنائية، الطبعة الأولى، مطبعة الأمنية، الرباط، المغرب، 2015.

15- نادية دردار، الجهود الدولية لمكافحة الجريمة، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2017.

16- نبيل صقر، الوسيط في جرائم الأموال، دار الهدى، عين مليلة، الجزائر، 2012.

17- نجيمي جمال، إثبات الجريمة على ضوء الاجتهاد القضائي دراسة مقارنة، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2011.

ب)- المراجع المتخصصـــة:

18- إبراهيم عبد الخالق، الشامل في جرائم الإنترنت (جرائم الحاسوب والإنترنت وفقا لنصوص قانون العقوبات ومعلقا عليها بالشرح والأيضاًح بأحدث أحكام النقض – التعويض عن الضرر الناتج عن جرائم الإنترنت)، الطبعة الثانية، دار شادي للموسوعات القانونية، القلعة، القاهرة، 2018.

19- أحمد خليفة الملط، الجرائم المعلوماتية دراسة مقارنة، الطبعة الثانية، دار الفكر الجامعي، الازاريطة، الإسكندرية، مصر، 2006.

20- أحمد عبد اللاه المراغي، الجريمة الإلكترونية ودور القانون الجنائي في الحد منها دراسة تحليلية تأصيلية مقارنة، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، مصر،2017.

21- أحمد محمد عبد الباقي، التحقيق الجنائي الرقمي، دار النهضة العربية، القاهرة، مصر، 2015.

22- أحمد يوسف الطحطاوي، الأدلة الإلكتروني ودورها في الإثبات الجنائي (دراسة مقارنة)، دار النهضة العربية، القاهرة، مصر، 2015.

23- إدريس النوازلي، موقف القضاء من الجريمة الإلكترونية، من كتاب جماعي بعنوان التجارة الإلكترونية أية حماية؟، الطبعة الأولى، المطبعة والوراقة الوطنية، مراكش، المغرب، 2010.

24- إدريس النوازلي، جريمة النصب المعلوماتي –قانونا واقعا وقضاء–، الطبعة الأولى، المطبعة والوراقة الوطنية، مراكش، المغرب، 2015.

25- أسامة أحمد المناعسة وآخرون، جرائم الحاسب الآلي والإنترنت –دراسة تحليلية مقارنة–، الطبعة الأولى، دار وائل للنشر، عمان، الأردن، 2000.

26- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، الطبعة الأولى، دار هومة، الجزائر، 2006.

27- أمير فرج يوسف، الإثبات الجنائي للجريمة الإلكترونية والاختصاص القضائي بها (دراسة مقارنة للتشريعات العربية والأجنبية)، الطبعة الأولى، مكتبة الوفاء القانونية، الإسكندرية، مصر، 2016.

28- أمير فرج يوسف، الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر، الطبعة الأولى، مكتبة الوفاء القانونية، الإسكندرية، مصر، 2011.

29- أيمن عبد الحفيظ، إستراتيجية مكافحة جرائم استخدام الحاسب الآلي، دار النهضة العربية، القاهرة، مصر، 2003.

30- أيمن عبد الله فكري حسن، الجرائم المعلوماتية دراسة مقارنة في التشريعات العربية والأجنبية، الطبعة الأولى، مكتبة القانون والاقتصاد، الرياض، السعودية، 2014.

31- إيهاب السنباطي، الترجمة الجديدة والكاملة للاتفاقية المتعلقة بالجريمة الإلكترونية (بودابست 2001) والبروتوكول الملحق بها، دار النهضة العربية، القاهرة، مصر، 2009.

32- تركي بن عبد الرحمن المويشير، بناء أمني لمكافحة الجـرائم المعلوماتية وقياس فاعليته، الطبعة الأولى، جامعة نايف العربية للعلوم الأمنية فهرسة مكتبة الملك فهد الوطنية أثناء النشر، الرياض، السعودية، 2012.

33- جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات- رؤية جديدة للجريمة الحديثة- الطبعة الأولى، دار البداية، عمان، الأردن، 2007.

34- جلال محمد الزغبي، أسامة احمد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية دراسة مقارنة، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2010.

35- حازم محمد حنفي، الدليل الإلكتروني ودوره في المجال الجنائي، الطبع الأولى، دار النهضة العربية، القاهرة، مصر، 2017.

36- حازم محمد الشرعة، التقاضي الإلكتروني والمحاكم الإلكترونية (كنظام قضائي معلوماتي عالي التقنية وكفرع من فروع القانون بين النظرية والتطبيق)، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2010.

37- حسام محمد نبيل الشنراقي، الجريمة المعلوماتية دراسة تطبيقية مقارنة على جرائم الاعتداء على التوقيع الإلكتروني، دار الكتب القانونية، مصر، 2013.

38- حسين بن سعيد بن سيف الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت"دراسة مقارنة"، دار النهضة العربية، القاهرة، مصر، سنة 2009.

39- حسين محمد الغول، جرائم شبكة الإنترنت والمسؤولية الجزائية الناشئة عنها (دراسة مقارنة في التشريع اللبناني والمصري والفرنسي والأمريكي)، الطبعة الأولى، مكتبة بدران الحقوقية، صيدا، لبنان، 2017.

40- حنان ريحان مبارك المضحي، الجـرائم المعلوماتية، دراسـة مقارنة، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2014.

41- خالد سليمان عبد الله الغثبر، مهندس محمد عبد الله على القحطاني، أمن المعلومات بلغة ميسرة، مكتبة الملك فهد الوطنية، الطبعة الأولى، الرياض، السعودية، 2009.

42- خالد حربي السعدي، جريـمة إتلاف بـرامج ومـعلومات الـحاسب الآلي في التشريعيين الكويتي والمقارن، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 2012.

43- خالد عياد الجلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2011.

44- خالد مصطفى فهمي، الحماية القانونية لبرامج الحاسب الآلي في ضوء قانون الملكية الفكرية المصري 82 لسنة 2002 (دراسة مقارنة)، دار الجامعة الجديدة، الازاريطة، الإسكندرية، مصر، 2005.

45- خالد ممدوح ابراهيم، أمن الجريمة الإلكترونية، الدار الجامعية، الإسكندرية، مصر، 2008.

46- خالد ممدوح إبراهيم، الجرائم المعلوماتية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، 2009.

47- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجريمة الإلكترونية (دراسة مقارنة)، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، 2018.

48- دنيا عبد العزيز فهمي، الحماية الجنائية من إساءة استخدام مواقع التواصل الاجتماعي "دراسة مقارنة"، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 2018.

49- ذيب بن عايض القحطاني، أمن المعلومات، إصدارات مدينة الملك عبد العزيز للعلوم والتقنية (KACST)، الرياض، المملكة العربية السعودية، 2015.

50- زيبحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة، الجزائر، 2011.

51- سامر سليمان الجبوري، جريمة الاحتيال الإلكتروني دراسة مقارنة، الطبعة الأولى، مكتبة زين الحقوقية والادبية، لبنان، 2018.

52- سعيدي سليمة، حجاز بلال، جرائم المعلومات والشبكات في العصر الرقمي، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، 2016.

53- سليمان عبد المنعم، الجوانب الإشكالية في النظام القانوني لتسليم المجرمين"دراسة مقارنة"، دار الجامعة الجديدة للنشر، الازاريطة، الإسكندرية، 2007.

54- سيد أحمد محمود، إلكترونية القضاء والقضاء الإلكتروني وإلكترونية التحكيم والتحكيم الإلكتروني "دراسة مقارنة"، دار التتفكر والقانون للنشر والتوزيع، المنصورة، مصر، 2015.

55- طارق عفيفي صادق احمد، الجرائم الإلكترونية جرائم الهاتف المحمول دراسة مقارنة بين الـقانون المصري والإمـاراتي والنظام السعودي، الطبعة الأولى، المركز القومي للإصدارات القانونية، مصر، 2015.

56- عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي الجزائري والقانون المقارن، دار الجامعة الجديدة، الازاريطة، الإسكندرية، مصر، 2010.

57- عبد الحكيم زروق، تنظيـم التبـادل الإلكتروني للمعطيات القانونية عبـر الإنترنت، الطبعة الاولى، دار الامان، الرباط، المغرب، 2016.

58- عبد الحليم موسى يعقوب، الإعلام الجديد والجريمة الإلكترونية، الطبعة الأولى، الدار العالمية للنشر والتوزيع، مصر، 2014.

59- عبد الرحمن بن عبد الله السند، الأحكام الفقهية للتعاملات الإلكترونية (الحاسب الآلي وشبكة المعلومات الإنترنت)، الطبعة الأولى، دار الوراف للبطاعـة والنشـر والتـوزيع، بيروت، لبنان، 2004.

60- عبد الصبور عبد القوى على مصري، المحكمة الرقمية والجريمة المعلوماتية (دراسة مقارنة)، الطبعة الأولى، مكتبة القانون والاقتصاد، الرياض، المملكة العربية السعودية، 2012.

61- عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكومبيـوتر والإنترنت، الطبعة الثالثة، دار الجامعة الجديدة، مصر، 1999.

62- عبد الفتاح بيومي حجازي، النظام القانوني للحكومة الإلكترونية، الكتاب الثاني الحماية الجنائية والمعلوماتية للحكومة الإلكترونية، دار الكتب القانونية، القاهرة، مصر، 2007.

63- عبد الفتاح حجازي، الإثبات الجنائي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة، مصر، 2007.

64- عبد الفتاح بيومي حجازي، الأحداث والإنترنت دراسة متعمقة عن اثر الإنترنت في انحراف الأحداث، دار الكتب القانونية، مصر، 2007.

65- عبد الفتاح بيومي حجازي، الجريمة في عصر العولمة "دراسة في الظاهرة الإجرامية المعـلوماتية مع التطبيق على الـقانون الإماراتي"، دار الفـكر الجـامعي، الازاريطة، الإسكندرية، مصر، 2008.

66- عبد الفتاح بيومي حجازي، دراسة متعمقة عن جريمة غسيل الأموال عبر الوسائط الإلكترونية في التشريعات المقارنة، الطبعة الأولى، المركز القومي للإصدارات القانونية، مصر 2009.

67- عبد الله حسين على محمود، سـرقة المعلومات المخزنـة في الحاسب الآلي، الطبعة الأول، دار النهضة العربية، القاهرة، مصر، 2001.

68- عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والإنترنت (الجرائم الإلكترونية دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والإنترنت مع الإشارة إلى جهود مكافحتها محليا وعربيا ودوليا)، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2007.

69- عبد الرحمن فتحي عبد الرحمن سمحان، تسليم المجرمين في ظل قواعد القانون الدولي، الطبعة الأولى، دار النهضة العربية، القاهرة، 2012.

70- عبد السلام بنسليمان، الإجرام المعلوماتي في التشريع المغربي دراسة نقدية مقارنة في ضوء آراء الفقه وأحكام القضاء، الطبعة الأولى، دار الأمان، الرباط، 2017.

71- عبد العزيز لطفي جاد الله، أمن المجتمع الإلكتروني بين سياسة السوق الإلكترونية والتعاون الدولي في إطار مـــواجهة الجرائم الإلكترونية، الطبعة الأولى، مكتبة الوفاء القانونية، الإسكندرية، مصر، 2017.

72- عبد العال الديربي، محمد صادق اسماعيل، الجرائم الإلكترونية دراسة قانونية قضائية مـــقارنة مـع احـدث التشريعات العربية في مجال مكافحة جـرائم المـعلوماتية والإنترنت، الطبعة الأولى، المركـز القــومي للإصـدارات القانونية، القاهرة، 2012.

73- عبد الله الكرجي، صليحة حاجي، الإثبات الـرقمي، الطـبعة الأولى، مـطبعة الأمنية، الرباط، 2015.

74- عادل عبد العال إبراهيم خراشي، إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديدة، الازاريطة، الإسكندرية، مصر، 2015.

75- عادل عبد العال ابراهيم خراشي، جرائم الاستغلال الجنسي للأطفال عبر شبكة الإنترنت وطرق مكافحتها في التشريعات الجنائية والفقه الجنائي الإسلامي، دار الجامعة الجديدة، الإسكندرية، مصر، 2015.

76- عادل يحيي، السياسة الجنائية في مواجهة الجريمة المعلوماتية، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 2014.

77- عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون (دراسة مقارنة)، دار الكتب القانونية، الإسكندرية، 2002.

78- على جبار الحسيناوي، جرائم الحاسوب والإنترنت، دار اليازوري العلمية للنشر والتوزيع، عمان، الأردن، 2009.

79- على عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب، دار الجامعة الجديدة للنشر، الازاريطة، الإسكندرية، مصر، 1997.

80- علي عبود جعفر، جـرائم تـكنولوجيا الـمعلومات الحـديثة الـواقـعة على الأشخاص والحكومة، الطبعة الأولى، منشورات زين الحقوقية، لبنان، 2013.

81- عمر محمد بن يونس، التحكيم في جرائم الحاسوب وردعها (المراقبة الدولية للسياسة الجنائية)، دار النهضة العربية، مصر، 2008.

82- عمر الفاروق الحسيني، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية، الطبعة الثانية، دار النهضة العربية، القاهرة، 1995.

83- غانم محمد غانم، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والإنترنت وجرائم الاحتيال المنظم باستعمال شبكة الإنترنت، الطبعة الأولى، دار الفكـــر والقـــانون، المنصورة، مصر، 2017.

84- فائزة يونس الباشا، السياسة الجنائية لجرائم الكمبيوتر التشريع الليبي (أنموذجاً ومقارناً)، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 2013.

85- فتوح الشاذلي، عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون (دراسة مقارنة)، منشورات الحلبي الحقوقية، بيروت، لبنان، 2003.

86- فهد عبد الله العبيد العازمي، الإجراءات الجنائيـة المعلوماتيـة، دار الجـامعة الجديدة، الإسكندرية، مصر، 2016.

87- فؤاد أمين السيد محمد، جـرائم مراقبة المراسلات الإلكترونية "دراسة مقارنة"، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 2016.

88- لؤي عبد الله نوح، مدى مشروعية المراقبة الإلكترونية في الإثبات الجنائي وحجية مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي وعوامل حجية الصورة والصوت في الإثبات الجنائي "دراسة مقارنة"، الطبعة الأولى، مركز الدراسات العربية للنشر والتوزيع، الجيزة، مصر، 2018.

89- محمد أبو العلا عقيدة، مراقبة المحادثات التليفونية دراسة مقارنة في تشريعات الولايات المتحدة الأمريكية وانجلترا وايطاليا وفرنسا ومصر، دار الفكر العربي، مصر، 1994.

90- محمد أمين احمد الشوابكة، جرائم الحاسوب والإنترنت (الجريمة المعلوماتية)، الطبعة الأولى، الإصدار الأول، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2004.

91- محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية، مصر، 2004.

92- أمين الشوابكة، جرائم الحاسوب والإنترنت: الجريمة المعلوماتية، الطبعة الرابعة، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2011.

93- محمد بن نصير محمد سرحان، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت، قسم علوم الشرطة، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004.

94- محمد حماد مرهج الهيتي، التكنولوجيا الحديثة والقانون الجنائي، الطبعة الأولى، الإصدار الأول، دار الثقافة للنشر والتوزيع، الأردن، 2004.

95- محمد حماد مرهج الهيتي، أصول البحث والتحقيق الجنائي (موضوعه أشخاصه والقواعد التي تحكمه)، دار الكتب القانونية، مصر 2008.

96- محمد رضوان هلال، المحكمة الرقمية مفهومها- مقوماتها، دار العلوم للنشر والتوزيع، القاهرة، مصر، 2006.

97- محمد عبد الكريم حسين، المسؤولية الجنائية لمورد خدمة الإنترنت، منشورات الحلبي الحقوقية، بيروت، 2017.

98- محمد على العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، الازاريطة، الإسكندرية، 2004.

99- محمد على قطب، الجرائم المستحدثة وطرق مواجهتها (قراءة في المشهد القانوني والأمني وعلاقته بالشريعة الإسلامية)، الطبعة الأولى، دار الفجر للنشر والتوزيع، القاهرة، مصر، 2009.

100- محمد كمال شاهين، الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، مصر، 2018.

101- محمد نصر محمد، المسئولية الجنائية لانتهاك الخصوصية المعلوماتية "دراسة مقارنة"، الطبعة الأولى، مركز الدراسات العربية للنشر والتوزيع، مصر، 2016.

102- محمود مدين عبد الرحمان، الجريمة الإلكترونية وتحديات الأمن القومي، دار المصرية للنشر والتوزيع، القاهرة، مصر، 2017.

103- مختار الاخضري، الإطار القانوني لمواجهة جرائم المعلوماتية وجرائم الفضاء الافتراضي، مجلة نشرة القضاة، المديرية العامة للشؤون القضائية والقانونية، مديرية الدراسات القانونية والوثائق، وزارة العدل، الجزائر، العدد 66، 2011.

104- مصطفى على خلف، الضوابط الإجرائية لجرائم التقنية الحديثة (دراسة مقارنة)، نادي القضاة، مصر، 2017.

105- مصطفى محمد موسى، أساليب إجرامية بالتقنية الرقمية ماهيتها...مكافحتها دراسة مقارنة، دار الكتب القانونية، مصر، 2005.

106- مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، مطابع الشرطة، القاهرة، مصر، 2008.

107- معتز سيد محمد أحمد عفيفي، قواعد الاختصاص القضائي بالمسؤولية الإلكترونية عبر شبكة الإنترنت، الطبعة الأولى، دار الجامعة الجديدة، الازاريطة، الإسكندرية، القاهرة، 2013.

108- منير محمد الجنبيهي، ممدوح محمد الجنبيهي، بروتوكولات وقوانين الإنترنت، دار الفكر الجامعي، الازاريطة، الإسكندرية، القاهرة، 2005.

109- منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الازاريطة، الإسكندرية، مصر، 2005.

110- منير محمد الجنبيهي، ممدوح محمد الجنبيهي، أمن المعلومات الإلكترونية، دار الفكر الجامعي، الازاريطة، الإسكندرية، مصر، 2005.

111- مونة جنيح، أحمد الزعري، تدبير مسرح الجريمة وتحويل الآثار إلى أدلة جنائية، الطبعة الأولى، مطبعة الأمنية، الرباط، المغرب، 2015.

112- نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية دراسة نظرية وتطبيقية، الطبعة الأولى ، منشورات الحلبي الحقوقية، لبنان، 2005.

113- نبيل صقر، جرائم الكومبيوتر والإنترنت في التشريع الجزائري، دار الهلال للخدمات الإعلامية، الجزائر، 2005.

114- نبيل محمد عثمان عرعارة، الحماية الجنائية للحق في حرمة المراسلات عبر البريد الإلكتروني، الطبعة الأولى، المصرية للنشر والتوزيع، القاهرة، مصر، 2018.

115- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات "دراسة مقارنة"، دار الفكر الجامعي، الإسكندرية، مصر، 2013.

116- نعيم مغبغب، حماية برامج الكمبيوتر (الأساليب والثغرات دراسة في القانون المقارن)، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2006.

117- نعيم مغبغب، مخاطر المعلوماتية والإنترنت (المخاطر على الحياة الخاصة وحمايتها دراسة في القانون المقارن)، الطبعة الثانية، منشورات الحلبي الحقوقية، لبنان، 2008.

118- نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الأولى، الإصدار الأول، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2008.

119- نور على سعد درويش، قيم وخصائص مدمني الإنترنت، الطبعة الأولى، دار الوفاء لدنيا الطباعة والنشر، الإسكندرية، مصر، 2016.

120- هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، مصر، إصدار 1992.

121- هشام زوين، التجسس والتنصت (مراقبة التيلفون والموبايل وتسجيل المكالمات والتصوير وتتبع الرسائل الإلكترونية عبر شبكة الإنترنت ونشر الأفلام المخلة بالآداب وتداولها بالموبايل)، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، مصر، 2014.

122- هشام ملاطي، خصوصية القواعد الإجرائية للجريمة المعلوماتية – محاولة لمقاربة مدى ملائمة القانون الوطني مع المعايير الدولية –، مطبعة الأمنية بالرباط، المغرب، 2014.

123- هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 2003.

124- هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 2007.

125- هلالي عبد اللاه أحمد، التزام الشاهد بالإعلام في الجرائم المعلوماتية دراسة مقارنة، الطبعة الثانية، دار النهضة العربية، القاهرة، مصر، 2008.

126- هلالي عبد اللاه أحمد، كيفية المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء اتفاقية بودابست، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 2011.

127- هلالي عبد اللاه احمد، جرائم الحاسب والإنترنت بين التجريم الجنائي وآليات المواجهة (مجموعة محاضرات أُلقيت على طلاب كلية الحاسبات والمعلومات)، دار النهضة العربية، القاهرة، مصر، 2015.

128- وجدي شفيق، الجديد في الإثبات الإلكتروني (ومدى حجية المستخرجات الإلكترونية في الإثبات ودورها في حجب المواقع الإلكترونية والاختصاص الجنائي بجرائم التوقيع الإلكتروني وفق القانون رقم 15 لسنة 2004 ولائحته التنفيذية)، الطبعة الأولى، شركة آل طلال للنشر والتوزيع، القاهرة، مصر، 2015.

129- ياسر حسين بهنس، الإثبات بالوسائل العلمية الحديثة وسلطة القاضي الجنائي في تقديرها، دار النهضة العربية، القاهرة، مصر، 2017.

130- يوسف أبو الحجاج، أشهر جرائم الكمبيوتر والإنترنت، الطبعة الأولى، دار الكتاب العربي، القاهرة، مصر، 2010.

131- يوسف بن سعيد بن محمد الكلباني، الحماية الجزائية للبيانات الإلكترونية في التشريعين العماني والمصري (دراسة مقارنة)، الطبعة الأولى، دار النهضة العربية، القاهرة، 2017.

132- يوسف حسن يوسف، الجرائم الدولية للانترنت، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، مصر، 2011.

133- يوسف قجاج، خصوصية القواعد الإجرائية في مجال البحث عن الجريمة الإلكترونية – دراسة مقارنة –، دار السلام للطباعة والنشر والتوزيع، الرباط، المغرب، 2016.

134- الشحات إبراهيم محمد منصور، الجرائم الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، 2011.

ج)- الرسائـل العلميـــة:

1). اطروحات الدكتوراه:

135- إبراهيم محمد إبراهيم محمد، النظرية العامة لتفتيش المساكن في قانون الإجراءات الجنائية "دراسة مقارنة"، رسالة مقدمة لنيل درجة الدكتوراه في الحقوق، قسم القانون الجنائي، كلية الحقوق، جامعة القاهرة، مصر، سنة 2005.

136- إحسان طبال، النظام القانوني للتحقيق الدولي في جرائم الكمبيوتر، أطروحة دكتوراه في الحقوق، كلية الحقوق، جامعة الجزائر 01، الجزائر، السنة الجامعية 2013-2014.

137- أحمد يوسف احمد حسين الطحطاوي، الأدلة الإلكترونية ودورها في الإثبات الجنائي"دراسة مقارنة"، رسالة مقدمة لنيل درجة الدكتوراه في القانون الجنائي، قسم القانون الجنائي، كلية الحقوق، جامعة حلوان، مصر، سنة 2015.

138- إسماعيل بن دبيلي، الإدمان على استخدام الإنترنت وعلقته بالاكتئاب والعزلة الاجتماعية –دراسة على عينة من الطلبة الجامعيين بالجزائر العاصمة –، أطروحة مقدمة لنيل شهادة دكتوراه الطور الثالث في علوم الإعلام والاتصال، قسم علوم الاتصال، كلية علوم الإعلام والاتصال، جامعة الجزائر 03، 2015-2016.

139- أكسوم عيلام رشيدة، المركز القانوني للمستهلك الإلكتروني، أطروحة لنيل درجة الدكتوراه الطور الثالث (ل.م.د) في القانون تخصص: قانون خاص داخلي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة مولود معمري بتيزي وزو، الجزائر، 12 جوان 2018.

140- إلهام بن خليفة، الحماية الجنائية للمحررات الإلكترونية من التزوير، أطروحة مقدمة لنيل درجة دكتـوراه علوم في العـلوم القـانونية والإدارية تخصص قـانون جنائي، قـسم الحـقوق،كلية الحقوق والعـلوم السياسية، جامعة الحاج لخـضر باتـنة، الموسم الجامعي 2015-2016.

141- باخويا دريس، جريمة غسل الأموال ومكافحتـها في القانـون الجزائري (دراسـة مقارنة)، أطروحة مقدمة لنيل شهادة الدكتوراه في القانون الجنائي الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، السنة الجامعية 2011-2012.

142- بدر عدنان الخبيزي، الجرائم الإلكترونيـة في المجتمـع الكويـتي (تحليل سوسيولوجي)، رسالة مقدمة لنيل درجـة الدكتوراه في عـلم الاجـتماع، قسم اجتماع، كلية الآداب، جامعة حلوان، مصر، سنة 2014.

143- براردي نعيمة، الاتصـال بين الشرطة والمواطن ودوره في مكافحة الجريمة في الجزائر (دراسة تحليلية استطلاعية بالجزائر العاصمة)، رسالة لنيل شهادة الدكتوراه في علوم الإعلام والاتصال، كلية العلوم السياسية والإعلام، جامعة الجزائر 03، السنة الجامعية 2012-2013.

144- براهمي حنان، جـريمة تزوير الوثيقة الرسمـية الإدارية ذات الطبيعة المعلوماتية، أطروحة مقدمة لنيل شهادة دكتوراه علوم تخصص قانون جنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر، السنة الجامعية 2014-2015.

145- براهيمي جمال، التحـقيق الجنائي في الجـرائم الإلكترونية، أطروحة لنيل شهادة الدكتوراه في العلوم، تخصـص القانون، قسم الحقوق، كـلية الحـقوق والعلوم الإنسانية، جامعـة مولـود معمري، تيزي وزو، الجزائر، نوقشت في 2018/06/27.

146- بن دريس حـليمة، حماية حقوق الملكيـة الفـكرية في التـشريع الجـزائري، أطروحة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق، جامعة ابي بكر بلقايد، تلمسان، الجزائر، السنة الجامعية 2013-2014.

147- بن زحاف فيصل، تسليم مرتكبي الجرائم الدولية، رسالة لنيل شهادة الدكتوراه في القانون الدولي والعلاقات السياسية الدولية، كلية الحقوق والعلوم السياسية، جامعة وهران، الجزائر، السنة الجامعة 2011-2012.

148- بن سعيد صبرينة، حماية الحق في حرمة الحياة الخاصة في عهد التكنولوجيا "الإعـلام والاتصال"، أطروحة مقدمة لنيل شهادة الدكتوراه العلوم في العلوم القانونية، قـسم الحـقوق،كلية الحـقوق والعـلوم السياسية، جـامعة الحاج لخضر باتنة، الجزائر، السنة الجامعية 2014-2015.

149- بن طالب ليندا، الدليل الإلكتروني ودوره في الإثبات الجنائي (دراسة مقارنة)، أطروحة لنيل شهادة دكتوراه علوم تخصص قانون، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة مولود معمري بتيزي وزو، الجزائر، تاريخ المناقشة 2019/01/23.

150- بوكر رشيدة، الحماية الجزائية للتعاملات الإلكترونية، أطروحة مقدمة لنيل شهادة دكتوراه علوم، تخصص قانون جزائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الجيلالي اليابس، سيدي بلعباس،2017.

151- تومي يحي، جرائم الاعتـداء ضـد الأفراد باستخـدام تكنولوجيـا الإعـلام والاتصال، أطروحة من أجـل نيل شهادة الدكتوراه علوم تخصص قانون، كلية الحقوق، جامعة الجزائر 01، الجزائر، السنة الجامعية 2017-2018.

152- درار نسيمة، الأمن المعلوماتي وسبل مواجهته مخاطره في التعامل الإلكتروني – دراسة مقارنة–، رسالة لنيل شهادة الدكتوراه في القانون الخاص،كلية الحقوق والعلوم السياسية، جامعة ابوبكر بلقايد، تلمسان، الجزائر، السنة الجامعية 2015–2016.

153- رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة مقدمة لنيل شهادة الدكتوراه علوم في القانون الخاص، قسم القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، الجزائر، السنة الجامعية 2017-2018.

154- ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة دكتوراه العلوم في الحقوق تخصص قانون العقوبات والعلوم الجنائية، قسم الحقوق،كلية الحقوق والعلوم السياسية، جامعة باتنة01، الموسم الجامعي 2015-2016.

155- روابح فريد، الأساليب الإجـرائية الخاصة للـتحري والتـحقيق في الجريمة المنظمة، أطروحة لنيل شهادة الدكتوراه في القانون العام، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة بن يوسف بن خدة، الجزائر 01، 18 فبراير 2016.

156- زروق يوسف، حجية وسائل الإثبات الحديثة، رسالة مقدمة لنيل شهادة دكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، السنة الجامعية 2012-2013.

157- شيخ ناجية، خصوصيات جريمة الصرف في القانون الجزائري، رسالة لنيل شهادة الدكتوراه في العلوم تخصـص قانون،كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، الجزائر، 2012.

158- شيرين محمد إحسان عبد الحافظ، العلاقة بين جهود منظمات مكافحة الجريمة الإلكترونية وتحـقيق الأمـن الاجتماعي، أطروحـة ضمن مـقتضيات الحصول على درجة دكتوراه الفلسفة في الخدمة الاجتماعية، قسم تنظيم المجتمع، كلية الخدمة الاجتماعية، جامعة حلوان، مصر، سنة 2016.

159- صالح شنين، الحماية الجنائية للتجارة الإلكترونية "دراسة مقارنة "، رسالة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق، جامعة أبو بكر بلقايد، تلمسان، الجزائر، السنة الجامعية 2012-2013.

160- صفية بشاتن، الحماية القانونية للحياة الخاصة (دراسة مقارنة)، رسالة لنيل شهادة الدكتوراه في العلوم تخصص قانون، جامعة مولود معمري، تيزي وزو، الجزائر، السنة الجامعية 2011-2012.

161- عاقلي فضيلة، الحمايـة القانونيـة للحـق في حرمة الحياة الخاصة (دراسـة مقارنة)، بحث مقدم لنيل شهادة الدكتـوراه علوم في القانون الخاص، جـامعة الإخـوة مـنتوري، قسنطينة، الجزائر، 2011-2012.

162- عبد الرحمن بن عبد الله السند، أحكام تقنية المعلومات "الحاسب الآلي وشبكة المعلومات(الإنترنت)"، رسالة مقدمة لنيل درجة الدكتوراه في الفقه المقارن، المعهد العالي

للقضاء، قسم الفقه المقارن، جامعة الإمام محمد بن سعود الإسلامية، المملكة العربية السعودية، 1424-1425 هـ.

163- عبد العزيز ديلمي، دور الشرطة المجتمعية في الوقاية من الجريمة والانحراف دراسة نظرية لبناء نموذج للشرطة الجوارية في الجزائر، أطروحة مقدمة لنيل شهادة الدكتوراه في علوم اجتماع الجريمة والانحراف، قسم علم الاجتماع، كلية العلوم الإنسانية والاجتماعية، جامعة الجزائر 02، السنة الجامعية 2012-2013.

164- علاء محمود يسن حراز، الحماية الجنائية للمعلومات المعالجة آلياً "دراسة مقارنة بين القانون الوضعي والشريعة الإسلامية"، رسالة مقدمة لنيل درجة الدكتوراه في الحقوق، قسم القانون الجنائي، كلية الحقوق، جامعة عين شمس، مصر، سنة 2015.

165- عمار غالي عبد الكاظم العيساوي، المسئولية الجنائية عن جرائم انتهاك الحق في سرية المراسلات "دراسة في القوانين المقارنة"، رسالة مقدمة لنيل درجة الدكتوراه في الحقوق، قسم الدراسات العليا، كلية الحقوق، جامعة عين شمس، مصر، سنة 2016.

166- عمر محمد ابوبكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، رسالة مقدمة لنيل درجة الدكتوراه في القانون الجنائي، كلية الحقوق، جامعة عين شمس، مصر، سنة 2004.

167- مجرب الدوادي، الأساليب الخاصة للبحث والتحري في الجريمة المنظمة، أطروحة لنيل شهادة دكتوراه علوم في القانون العام، كلية الحقوق، جامعة الجزائر 01 يوسف بن خدة، السنة الجامعية 2015-2016.

168- مختار شبيلي، التعاون الدولي في مكافحة الجريمة المنظمة، رسالة لنيل شهادة دكتوراه في القانون العام، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر 01، السنة الجامعة 2011-2012.

169- مرنيز فاطمة، الاعتداء على الحق في الحياة الخاصة عبر شبكة الإنترنت، أطروحة مقدمة لنيل شهادة الدكتوراه في القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، الجزائر، السنة الجامعية 2012-2013.

170- فايز محمد راجع غلاب، الجـريمة المـعلوماتية في الـقانون الجزائري واليمني، أطروحة من أجل الحصول على شهادة الدكتوراه في الحقوق فرع القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر 01، السنة الجامعة 2009-2010.

171- فريجه محمد هاشم، دور القـضاء الـدولي الجنائي في مكافحة الجريمة الدولية، أطروحة مقدمة لنيل شهادة الدكتوراه علوم في الحقوق تخصص قانون دولي جنائي، قسـم الحقوق،كليـة الحقوق والـعلوم السياسية، جامعة محمد خيضر ببسكرة، الجزائر، السنة الجامعية 2013-2014.

172- كاظم عبد الله نزال المياحي، حجية المراقبـة الإلكترونية للـصوت والصورة في الإثبات الجنائي "دراسة في القانون العراقي والمقارن"، رسالة مقدمة لنيل درجـة الدكتوراه في الحـقوق، قـسم القانون الجنائي، كلية الحقوق، جـامعة عين شمس، مصر، سنة 2016.

173- مجرب الدوادي، الأساليب الخاصة للبحث والتحري في الجريمة المنظمة، أطروحة لنيل شهادة دكتوراه علوم في القانون العام،كلية الحقوق، جامعة الجزائر 01 يوسف بن خدة، السنة الجامعية 2015-2016.

174- محمود احمد عبد القادر قشطة، التعاون الدولي في مكافحة الجريمة المعلوماتية، رسالة مقدمة لنيل درجة الدكتوراه في الدراسات القانونية، معهد البحوث والدراسات العربية، القاهرة، مصر، 2015.

175- محمد عبد الفتاح عبد المقصود على، القواعد الإجرائية للجرائم التي تقع عبر شبكة الإنترنت، رسالة مقدمة من اجل الحصول على درجة الدكتوراه، قسم القانون الجنائي، كلية الحقوق، جامعة طنطا، مصر، سنة 2015.

176- محمد الصالح روان، الجريمة الدولية في القانون الدولي الجنائي، رسالة مقدمة لنيل شهادة الدكتوراه في العلوم، كلية الحقوق، جامعة منتوري، قسنطينة، الجزائر، السنة الجامعية 2008-2009.

177- محمد شنة، جـرائم العنف الأسـري وآليات مكافحتها في التشريع الجزائري، أطروحة مقدمة لنيل درجة دكتوراه العلوم في الحقوق، تخصص علم الإجرام وعلم العقاب، قسـم

الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر- باتنة 01، السنة الجامعية 2017-2018.

178- محمد كمال عبد السميع شاهين، الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي (دراسة مقارنة)، أطروحة من أجل الحصول على شهادة الدكتوراه في الحقوق، كلية الحقوق، جامعة حلوان، مصر، سنة 2015.

179- مستاري عادل، المنطق القضائي ودوره في ضمان سلامة الحكم الجزائي، رسالة مقدمة لنيل شهادة دكتوراه العلوم في الحقوق، فرع القانون الجنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر، السنة الجامعية 2010-2011.

180- نويري عبد العزيز، الحماية الجزائية للحياة الخاصة – دراسة مقارنة-، أطروحة لنيل شهادة دكتوراه العلوم، شعبة القانون الجنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، السنة الجامعة 2010-2011.

181- هروال هبة نبيلة، جرائم الإنترنت دراسة مقارنة، أطروحة مقدمة لنيل شهادة الدكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، الجزائر، السنة الجامعية 2013-2014.

182- ياسر محمد الكومي محمود أبو حطب، الحماية الجنائية والأمنية للتوقيع الإلكتروني في التشريع المصري والتشريعات المقارنة، أطروحة من اجل الحصول على درجة الدكتوراه في القانون الجنائي، كلية الحقوق، جامعة حلوان، مصر، سنة 2015.

183- العربي جنان، الأنظمة المعلوماتية والإنترنت بين التنظيم وأحكام المسؤولية –النظرية والتأصيل-، أطروحة لنيل الدكتوراه في الحقوق، كلية العلوم القانونية والاقتصادية والاجتماعية، جامعة القاضي عياض، مراكش، المغرب، 2010.

2). رسائل الماجستير:

184- أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال في ضوء القانون رقم 09-04، مذكرة مقدمة لنيل شهادة الماجستير، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح بورقلة، الجزائر، 2013.

185- آمنة بن عبدربه، الجزائر في مجتمع المعلومات سنة 2003: حصيلة وآفاق، مذكرة لنيل شهادة الماجستير في علوم الاعلام والاتصال، قسم علوم الإعلام والاتصال، كلية العلوم السياسية والإعلام، جامعة الجزائر، السنة الجامعية: 2005-2006.

186- بومامي العباس، الجريمة الإلكترونية بين التحصين التقني والتحصين الجنائي، مذكرة مكملة لنيل شـهادة الماجستير في علوم الإعلام والاتصال، قسم علوم الإعلام والاتصال، كلية علوم الإعلام والاتصـال، جـامعة الجـزائـر 3، العام الجامعي 2014-2015.

187- تركي بن حمد هلال النصر، التحقيق في جريمتي التحرش والابتزاز عبر الشبكات الإلكترونية دراسة تطبيقية على هيئة التحقيق والادعاء العام بالمنطقة الشرقية، رسالة مقدمة لاستكمال متطلبات نيل درجة الماجستير في الدراسات الأمنية، تخصص القيادة الأمنية، قسم الدراسات الأمنية، كلية الـعدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2017.

188- ثنيان ناصر آل ثنيان، إثبات الجريمة الإلكترونية، دراسة تأصيلية تطبيقية، رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير، تخصص السياسة الجنائية، قسم العدالة الجنائية،كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، 2012.

189- رصاع فتيحة، الحماية الجنائية للمعلومات على شبكة الإنترنت، مذكرة لنيل شـهادة ماجسـتير في الـقانون الـعام، كلية الحـقوق والعـلوم السـياسية، جامعة ابي بكر بلقايد، تلمسان، السنة الجامعية 2011-2012.

190- سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهادة الماجستير في العلوم القانونية، جامعة الحاج لخضر، باتنة، الجزائر، السنة الجامعية 2012-2013.

191- سلامة محمد المنصور، تطبيق مبدأ الاقتناع القضائي على الدليل الإلكتروني، أطروحة مقدمة لاستكمال متـطلبات الحصول على درجـة الماجستير في القانون، قسم القانون العام، كلية القانون، جامعة الإمارات العربية المتحدة، نوفمبر 2018.

192- سلطان سالم فاضل البقي، العقوبات البديلة لذوي الاحتياجات الخاصة دراسة تأصيلية مقارنة، رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير في العدالة الجنائية تخصص السياسية الجنائية، قسم العدالة الجنائية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2012.

193- سوزان نوري فقي محمد، الإثبات في جرائم الإنترنت في القانون العراقي والقانون المقارن، رسالة مقدمة لنيل درجة الماجستير في الحقوق، قسم الدراسات العليا، كلية الحقوق، جامعة المنصورة، مصر، السنة الجامعية 2014- 2015.

194- عبد الرحمان جميل حسين، الحماية القانونية لبرامج الحاسب الآلي"دراسة مقارنة"، قدمت هذه الأطروحة استكمالا لمتطلبات درجة الماجستير في القانون الخاص بكلية الدراسات العليا، جامعة النجاح الوطنية في نابلس، فلسطين، 2008.

195- عبد الله دغش العجمي، المشكلات العلمية والقانونية للجرائم الإلكترونية –دراسة مقارنة–، قدمت هذه الرسالة استكمالا للحصول على درجة الماجستير في القانون العام، جامعة الشرق الأوسط، الأردن، 2014.

196- عومار بوطبية، دراسة واقع نظم المعلومات بمديرية الشباب والرياضة لولاية قسنطينة، مذكرة مقدمة لنيل شهادة الماجستير في الإدارة والتسيير الرياضي، المركز الجامعي محمد الشريف مساعدية سوق أهراس، الجزائر، السنة الجامعية 2011-2012.

197- عيسى سليم داود الزيدي، جرائم القرصنة الإلكترونية (دراسة مقارنة)، رسالة لنيل درجة الماجستير في الحقوق، قسم القانون الجنائي، كلية الحقوق، جامعة الإسكندرية، مصر، سنة 2018.

198- محمد نافع فالح رشدان العدواني، حجية الدليل الإلكتروني كوسيلة من وسائل الإثبات في المسائل الجزائية "دراسة مقارنة بين القانونين الكويتي والأردني"، قدمت هذه الرسالة استكمالاً لمتطلبات الحصول على درجة الماجستير في القانون العام، قسم القانون العام، كلية الحقوق، جامعة الشرق الأوسط، الأردن، تشرين الثاني 2015.

199- معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشـريع المقارن، مذكرة مكملة لنيل شهادة المـاجستير في العلوم القانونية، قسم

الحقوق، كلية الحقوق والعلوم السياسية، جامعة العقيد لخضر، باتنة، السنة الجامعية 2011-2012.

200- صغير يوسف، الجريمة المرتكبة عبر الإنترنت، مذكرة لنيل شهادة الماجستير في القانون تخصص القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2013/03/06.

201- فاطمة همال، الألعاب الإلكترونية عبر الوسائط الإعلامية الجديدة وتأثيرها في الطفل الجزائري (دراسة ميدانية على عينة من أطفال ابتدئيات مدينة باتنة)، مذكرة مكملة لنيل شهادة الماجستير، تخصص: الإعلام وتكنولوجيا الاتصال الحديثة، قسم العلوم الإنسانية، كلية العلوم الإنسانية والاجتماعية والعلوم الإسلامية، جامعة الحاج لخضر، باتنة، السنة الجامعية 2011-2012.

202- فؤاد احمد حسين السايس، الجريمة المعلوماتية، بحث مقدم للحصول على درجة الماجستير في القانون، قسم البحوث والدراسات القانونية، معهد البحوث والدراسات العربية، القاهرة، مصر، 2015.

203- نبيل محمد عثمان عرعارة، الحماية الجنائية للحق في حرمة المراسلات عبر البريد الإلكتروني، رسالة مقدمة لنيل درجة الماجستير في الحقوق، كلية الحقوق، جامعة القاهرة، مصر، 2016.

204- نواف بن نايف بن دبيان الحربي، الضبط والتفتيش في الجريمة المعلوماتية في النظام السعودي (دراسة تحليلية تطبيقية)، رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير في العدالة الجنائية تخصص التشريع الجنائي الإسلامي، قسم العدالة الجنائية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، 2011.

د)- المقالات العلمية:

205- ابراهيم بن لعليد، المجني عليه"في خدمة" الجاني: الفايسبوك نموذجا، المجلة المغربية للقانون الجنائي والعلوم الجنائية، العدد المزدوج الرابع والخامس (4-5)، ديسمبر 2017.

206- براهيم رمضان ابراهيم عطايا، الجريمة الإلكترونية وسبل مواجهتها في الشريعة الإسلامية والأنظمة الدولية- دراسة تحليلية تطبيقية، مجلة كلية الشريعة والقانون بطنطا، مصر، العدد (30)، الجزء الثاني، ابريل 2015.

207- أحمد علي، مفهوم المعلومات وإدارة المعرفة، مجلة جامعة دمشق، سوريا، المجلد 28، العدد الأول، 2012.

208- أحمد عبد الحكيم عبد الرحمن شهاب، نور عزم الميل بن مارني، شروط قبول الأدلة الإلكترونية أمام القاضي الجنائي الفلسطيني، مجلة العلوم السياسية والقانون، المركز العربي الديمقراطي للدراسات الإستراتيجية والسـياسية والاقتصادية، ألمانيا، برلين، المجلد الثاني (02)، العدد السابع (07)، فبراير 2018.

209- أحمد قاسم فرح، النظام القانوني لمقدمي خدمات الإنترنت —دراسة مقارنة-، مجلة المنارة للبحوث والدراسات، عمادة البحث العلمي، جامعة آل البيت، المملكة الأردنية الهاشمية، المجلد الثالث عشر (13)، العدد التاسع (09)، 2007.

210- أروى محمد تقوى، التزامات مزودي خدمات الإنترنت في مجال حماية الأطفال من المواد الضارة على الشبكة في النظام القانوني السوري" دراسة مقارنة"، مجلة جامعة الخليل للبحوث، فلسطين، المجلد الثامن (08)، العدد الثاني (02)، 2013.

211- أروى محمد تقوى، مدى مسؤولية مشغلي الهاتف النقال عن إساءة استخدامه في الاتصال بالإنترنت دراسة مقارنة، مجلة الحقوق، جامعة البحرين، البحرين، المجلد الحادي عشر (11)، العدد الثاني (02)، 2014.

212- أسعيداني سلامي، طارق طراد، التجربة الجزائرية لمواجهة الجريمة الإلكترونية في ظل البيئة التفاعلية الجديدة (عرض تشريعي قانوني)، مجلة الحقوق والعلوم السياسية، جامعة عباس لغرور، خنشلة، الجزائر، العدد الثاني عشر (12)، جوان 2019.

213- آلاء محمد صاحب، تبارك ناصر عزوز الزامليّ، ماهية التجريم المزدوج في نظام تـسليم المجرمين دراسة مقارنة، مجلة الكوفة للعلوم القانونية والسياسية، كلية القانون، جامعة الكوفة، العراق، المجلد الأول، العدد (44)، 2020.

214- أمحمدي بوزينة امينة، الحماية الجنائية للمعطيات الإلكترونية في إطار القانون الجزائري (دراسة تحليلية لقانوني العقوبات وحقوق المؤلف)، مجلة القانون والمجتمع، دورية محكمة في الدراسات القانونية تصدر عن مخبر القانون والمجتمع، جامعة ادرار، الجزائر، العدد السادس، ديسمبر2015.

215- إلهام شهرزاد روابح، الدليل الرقمي بين مشروعية الإثبات وانتهاك الخصوصية المعلوماتية، مجلة البحوث والدراسات القانونية والسياسية، كلية الحقوق والـعلوم السياسية، جامعة لونيسي علي، البليدة 02، الجزائر، العدد العاشر (10)، جانفي 2017.

216- آمال حجيج، نحو قوة أورو –متوسطية للشرطة وتسيير الحدود، مجلة دفاتر السياسة والـقانون، جامـعة قاصدي مرباح بورقلة، الجزائر، العدد الثاني عشر (12)، جانفي 2015.

217- أمال عزري، جمال بن زروق، استخدام جمعيات المجتمع الـمدني في الجزائر للشبكات الاجتماعية الإلكترونية (دراسة ميدانية على جمعيات المجتمع المدني في ولاية سكيكدة)، مجلة آفاق للعلوم، جامعة الجلفة، الجزائر، العدد السابع، مارس 2017.

218- آمال قارة، تفعيل آلـيات تسليم المجرمين في إطار المنظمة الـدولية للشرطة الجنائية، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر بالوادي، الجزائر، المجلد التاسع(09)، العدد الثاني (02)، جوان 2018.

219- أمل كاظم حمد، إدمان الأطفال والمراهقين على الإنترنت وعلاقته بالانحراف، مجلة العلوم النفسية، مركز الدراسات التربوية والبحوث النفسية، جامعة بغداد، العراق، العدد تسعة عشر(19)، ديسمبر 2011.

220- أمين اعزان، مواجـهة الجريمة الإلكترونية في ضوء القانون الجنائي المغربي، مجلة الحقوق المغربية،كلية العلوم القانونية والاقتصادية والاجتماعية، جـامعة محمـد الأول بوجـدة، العدد الثاني عشر (12)، السنة السادسة (06)، المغرب، 2011.

221- باخويا دريس، شنتير خضرة، أثر تطبيق مبدأ السرية المصرفية في محاربة جريمة غسيل الأموال، مجلة القانون والمجتمع، مخبر القانون والمجتمع، جامعة احمد دراية ادرار، الجزائر، العدد العاشر، ديسمبر 2017.

222- باسم السيد، النظام القانوني لمزود خدمة الإنترنت في سورية، مجلة جامعة البعث، سورية، المجلد التاسع والثلاثون (39)، العدد الخمسون (50)، 2017.

223- بدرة عمارة، الحماية الجنائية للمعلومات الإلكترونية دراسة في القانون (04-15)، مجلة البحوث القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الدكتور الطاهر مولاي، سعيدة، الجزائر، العدد الثاني، 2014.

224- براهيمي جمال، مكافحة الجرائم الإلكترونية في التشريع الجزائري، المجلة النقدية للقانون والعلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، العدد الأول، 2017.

225- بردال سمير، الجريمة المعلوماتية في التشريع الجزائري، مجلة القانون، معهد العلوم القانونية والإدارية بالمركز الجامعي أحمد زبانة، غليزان، الجزائر، العدد الثاني (02)، 2010.

226- بسكري نعيمة، اتفاقية توأمة بين الشرطة الجزائرية ونظيرتها الفرنسية والإسبانية، مجلة الشرطة، المؤسسة الوطنية للاتصال والنشر والإشهار وحدة الطبع رويبة، الجزائر، العدد مائة وأربعة وأربعون (144)، سبتمبر 2019.

227- بلبالي ابراهيم، الجريمة الإلكترونية بين وضوح معالم وأهداف التجريم وصعوبة التصنيف والتطبيق، مجلة دراسات وأبحاث، جامعة زيان عاشور، الجلفة، الجزائر، العدد الأول، تاريخ النشر: 2009/09/15.

228- بن حيدة محمد، النظام القانوني لحق الإنسان في صورته، مجلة القانون والمجتمع (جامعة أحمد دراية أدرار)، العدد الخامس، 2015.

229- بن زيطة عبد الهادي، إنشاء ضرورة سلطة إدارية مستقلة كآلية للحماية القانونية للبيانات الشخصية في مواجهة استخدامات المعلوماتية، مجلة الحقيقة، جامعة احمد دراية ادرار، العدد 39، سنة 2016.

230- بن عمر الحاج عيسى، الانتربول كآلية دولية شرطية لمكافحة الجريمة المنظمة العابرة للحدود، مجلة الدراسات القانونية والسياسية، جامعة عمار ثليجي بالأغواط، الجزائر، العدد الثالث (03)، جانفي 2016.

231- بن قارة مصطفى عائشة، الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية القانونية، مجلة الفقه والقانون (مجلة الكترونية شهرية تعنى بنشر الدراسات الشرعية والقانونية)، العدد الثاني والأربعون (42)، المملكة المغربية، ابريل 2016.

232- بوحليط يزيد، تفتيش المنظومة المعلوماتية وحجز المعطيات في التشريع الجزائري، مجلة التواصل في الاقتصاد والإدارة والقانون، تصدر عن جامعة باجي مختار، عنابة، الجزائر، العدد الثامن والأربعون (48)، ديسمبر 2016.

233- بوعزة رضا، النشاط الجنسي للشباب في الفضاء السيبيراني- دراسة ميدانية على عينة من الشباب المتردد على مقاهي الإنترنت-، مجلة آفاق للعلوم، جامعة زيان عاشور بالجلفة، العدد الثاني (02)، 2016.

234- بوعناد فاطمة الزهرة، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة الندوة للدراسات القانونية، كلية الحـقوق والعلوم السياسية، جـامعة الجيلالي ليابس بسيدي بلعباس، الجزائر، العدد الأول، 2013.

235- بوقرين عبد الحليم، قـانون مكافحة جـرائم تقنية المعلومات الكويتي: دراسة مقارنة، مجلة كلية القانون الكـويتية العالمية، السـنة الخامسة، العدد 04، العدد التسلسلي 20، الكويت، ديسمبر 2017.

236- تاحي وحيد، المديرية العامة لأمن الوطني تنظم سلسلة محاضرات حول الجريمة المستحدثة، مجلة الشرطة، باب الواد، الجزائر، العدد 140، مارس 2018.

237- توفيق مجاهد، طاهر عباسة، جريمة الإرهاب الإلكتروني في ضوء أحكام الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010، مجلة العلوم القانونية والسياسية، كلية الحقوق والـعلوم السياسية، جامعة الشهيد حمه لخضر بالـــوادي، الجزائر، المجـلد التاسع (09)، العدد الثالث (03)، ديسمبر 2018.

238- ثابت دنيازاد، مـراقبة الاتـصالات الإلكترونية والـحق في حرمة الحياة الخاصة في القانون الجزائري، مجلة العلوم الاجتماعية والإنسانية، جامعة العربي التبسي، تبسة، الجزائر، المجلد الثالث (03)، العدد السادس (06)، ديسمبر 2012.

239- ج. اسماعيل، مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها، مجلة الجيش، مجلة شهرية تصدر عن مؤسسة المنشورات العسكرية، العدد 599، الجزائر، جوان 2013.

240- جبيري ياسين، المخـدرات الرقمية، مجلة الشريعة والاقتصاد، كلية الشـريعة والاقتصاد، جامعة الأمير عبد القادر للعلوم الإسلامية قسنطينة، الجزائر، المجلد الرابع (04)، العدد الثامن(08)، 2015/12/01.

241- جميلة محلق، اعتراض المراسلات، تسجيل الأصوات والتقاط الصور في قانون الإجراءات الجزائية الجزائري، مجلة التواصل في الاقتصاد والإدارة والقانون، كلية الحقوق والعلوم السياسية، جامعة باجي مختار عنابة، الجزائر، العدد الاثنان والأربعون (42)، جوان 2015.

242- جوزي صليحة، الجزائر تحتضن الجمعية العامة الأولى لآلية الاتحاد الإفريقي للتعاون في مجال الشرطة "الأفريبول"، مجلة الشرطة، وحدة الطباعة الرويبة، الجزائر، العدد مائة وستة وثلاثين (136)، جوان 2017.

243- حاحة عبد العالي، قلات سمية، المكافحة الإجرائية للجرائم الإلكترونية دراسة حالة الجزائر، مجلة المفكر،كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، العدد السادس عشر(16)، ديسمبر 2017.

244- حزام فتيحة، الضمانات القانونية لمعالجة المعطيات ذات الطابع الشخصي دراسة على ضوء القانون رقم 18-07، مجلة الاجتهاد للدراسات القانونية والاقتصادية، كلية الحقوق والعلوم السياسية، المركز جامعي تمنراست، الجزائر، المجلد الثامن (08)، العدد الرابع (04)، 2019.

245- حدة بوخالفة، النظام القانوني لمتعهد الإيواء عبر الإنترنت، مجلة المفكر، كلية الحقوق والعلوم السياسية بجامعة محمد خيضر – بسكرة ، الجزائر، 2017/01/19.

246- حسيني مراد، إجراءات التحقيق المستحدثة في قانون الإجراءات الجزائية الجزائري (عملية التسرب)، قراءات في المادة الجنائية، الجزء الأول، الإصدار السادس عشر، الطبعة الأولى، مجلة الحقوق (R.D) سلسلة المعارف القانونية والقضائية، دار نشر المعرفة، الرباط، المغرب، 2013.

247- حصة راشد محمد الحسن السليطي، جرائم القذف والسب العلني عبر الإنترنت (دراسة مقارنة)، المجلة القانونية والقضائية، مركز الدراسات القانونية والقضائية، وزارة العدل، قطر، العدد الأول، السنة التاسعة، يونيو 2015.

248- حكيم سياب، السمات المميزة للجرائم المعلوماتية عن الجرائم التقليدية، مجلة دراسات وأبحاث، جامعة زيان عاشور، الجلفة، الجزائر، العدد الأول، تاريخ النشر: 2009/09/15.

249- حكيم غريب، الجريمة الإلكترونية والجهود الدولية لمكافحتها، المجلة الجزائـرية للـدراسات السياسية، المدرسة الوطنية العليا للعلوم السيـاسية، المجـلد الثاني، العدد الأول، الجزائر، 2015/09/03.

250- حليمة بن حفو، محـاربة الجـرائم الإلكترونية على الصعيد الدولي "الواقع والأفاق"، مجلة العلوم الجنائية، مطبعة الأمنية، العدد الأول، الرباط، 2014.

251- حمودة سليمة، الإدمان على الإنترنت: اضطراب العصر، مجلة العلوم الإنسانية والاجتماعية، جـامعة قاصدي مرباح، ورقلة، الجزائر، العـدد الواحد والعشرون (21)، ديسمبر 2015.

252- حنان خرباشي، دور شبكات التواصل الاجتماعي في تشكيل الوعي بالظاهرة الإرهابية، مجلة اتجاهات سياسية، الـمركز الديمقراطي العربي، برلين، ألمانيا، العدد الثالث (03)، يناير 2018.

253- حياة لموشي، الإدمان على الفيسبوك وعلاقته بالتوافق الدراسي لدى المراهقين، محلة آفاق للعلوم، جامعة زيان عاشور، الجلفة، الجزائر، العدد التاسع (09)، سبتمبر 2017.

254- خالد حمد، الـقناعة القضائية في مـجال تقدير الأدلة، مجلة البـحثية، العدد الثالث، الرباط، المغرب، ربيع 2015.

255- خالد عثماني، مكافحة الجريمة الالكترونية في ضوء التشريع المغربي، مجلة العلوم الجنائية، مطبعة الأمنية، العدد الأول، الرباط، 2014.

256- خالد العمار، إدمان الشابكة المعلوماتية (الإنترنت) وعلاقته ببعض المتغيرات لدى طلبة جامعة دمشق – فرع درعا، مجلة جامعة دمشق، سوريا، المجلد الثلاثون (30)، العدد الأول، 2014.

257- خذيري عفاف، الجريمة الإلكترونية والأمن الوطني، المجلة الجزائرية للدراسات السياسية، المدرسة الوطنية العليا للعوم السياسية، بن عكنون، الجزائر، العدد الثامن (08)، ديسمبر 2017.

258- خليلي سهام، خصوصية المجـرم الإلكتروني، مجلة المفكر، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، العدد الخامس عشر (15)، جوان 2017.

259- خليل يوسف جندي، المواجهة التشريعية للجريدة المعلوماتية على المستويين الدولي والوطني (دراسة مـقارنة)، مجـلة كليـة القـانون للـعلوم الـقانونية والسياسية، جامعة كرموك، العراق، المجلد السابع (07)، العدد السادس والعشرون(26)، 2018.

260- دليلة العـوفي، إشكالية مواكبة الـجزائر لمجتمع المعلومات من الفجوة الرقمية إلى الجريمة المعلوماتية، مجلة الحـكمة للدراسات الإعـلامية والاتصالية، تصدر عن مؤسسة كنوز الحكمة للنشر والتوزيع، المجلد 04، العدد 08، الجزائر، 2016.

261- ربيعي حسين، المجرم المعلوماتي – شخصيته وأصنافه، مجلة العلوم الإنسانية، جامعة محمد خيضر ببسكرة، الجزائر، العدد الأربعون (40)، جوان 2015.

262- رحموني محمد، خصائص الجريمة الإلكترونية ومجالات استخدامها، مجـلة الحقيقة، جامعة أحمد دراية أدرار، العدد 41، جوان 2017.

263- رضا هميسي، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسيّة، جامعة الشهيد حمّه لخضر بالوادي، الجزائر، العدد الخامس (05)، جوان 2012.

264- رويس عبد القادر، أساليب البـحث والتحري الخاصة وحجيتها في الإثبات الجنائي، المجلة الجزائرية للـحقوق والعـلوم السياسية، مـعهد العلوم القانونية والإدارية، المركز الجامعي احمد بن يحي الونشريسي، تيسمسيلت، الجزائر، العدد الثالث (03)، جوان 2017.

265- زغنوف عبد الغني، عظيمي احمد، المـعلومة وأهميتها في الـمجتمع الـمعلوماتي، مجلة البحوث والدراسات الإنسانية، جامعة 20 اوت، سكيكدة، الجزائر، العدد 09، ديسمبر 2014.

266- زوزو زوليخة، مشروعية أساليب التحري الحديثة، مجلة الحقوق والعلوم السياسية، جامعة عباس لغرور خنشلة، الجزائر، العدد الثامن (08)، الجزء الثاني (02)، جوان 2017.

267- زياد محمد جفال، تسليم المجرمين كأحد آليات جامعة الدول العربية لمكافحة الإرهاب وموقف المشرع الإمـاراتي، مجلة جامعة الشارقة للعلوم القانوني، جامعة الشارقة، الإمارات العربية المتحدة، العدد الأول (01)، المجلد السادس عشر (16)، يونيو 2019.

268- زينة حازم خلف الجبوري، القانـون الواجب التطبيق على مسؤولية مزود خدمة الإنترنت، مجلة جامعة تكريت للحقوق، العراق، السنة الأولى (01)، المجـلد الأول (01)، العـدد الرابع (04)، الجـزء الثاني (02)، جـوان 2017.

269- سامية ابريعم، العلاقة بين إدمان الإنترنت والشعور بالاغتراب النفسي (دراسة ميدانية لدى عينة من طلاب وطالبات جامعة ام البواقي)، مجلة علوم الإنسان والمجتمع، كلية العلوم الإنسـانية والاجـتماعية، جامعة محمد خيضر، بسـكرة، الجزائر، الـعدد الخـامس عشر (15)، جوان 2015.

270- سامية بولافة، مبروك ساسي، الأسـاليب المستحدثة في التحريات الجزائية، مجلة الباحث للدراسات الأكاديمية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر (جامعة باتنة 1)، الجزائر، العدد الحادي عشر (11)، جوان 2017.

271- سميرة معاشي، ماهية الجريمة المعلوماتية، مجلة المنتدى القانوني، قسم الكفاءة المهنية للمحاماة، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجـزائر، العـدد السابع، افريل 2010.

272- سمير سعدون مصطفى، محمود خضر سلمان، حسن كريم عبد الرحمن، الجريمة الإلكترونية عبر الانترنيت أثرها وسبل مواجهتها، مجلة التقني، تصدر عن هيئة التعليم التقني، وزارة التعليم العالي والبحث العلمي، العراق، المجلد 24، العدد التاسع (09)، 2011.

273- سمير شعبان، الجريمة الإلكترونية، مقاربة تحليلية لتحديد مفهوم الجريمة والمجرم، مجلة دراسات وأبحاث، جامعة زيان عاشور، الجلفة، الجزائر، العدد الأول، تاريخ النشر: 2009/09/15.

274- سوزان عدنان الأستاذ، انتهاك حرمة الحياة الخاصة عبر الإنترنت (دراسة مقارنة)، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، سوريا، المجلد 29، العدد 03، 2013.

275- شرف الدين وردة، مشروعية أساليب التحري الخاصة المتبعة في مكافحة الجريمة المعلوماتية– في التشريع الجزائري–، مجلة المفكر، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، العدد الخامس عشر (15)، جوان 2017.

276- شرف الدين وردة، سليم بشير، حل مشكلة تـنازع الاخـتصاص الجـنائي الدولي في مجال مكافحة جرائم التجارة الإلكترونية، مجلة الحقوق والحريات، مخبر الحقوق والحريات في الأنظمة المقارنة، جامعة محمد خيضر، بسكرة، الجزائر، المجلد الخامس (05)، العدد الأول، 2019/04/30.

277- شريفي الشريف، مدى احترام الحق في الخصوصية في الحسابات الإلكترونية على الإنترنت، مجلة القانون والمجتمع، مخبر القانون والمجتمع، جامعة احمد دراية، ادرار، الجزائر، العدد السابع، جوان 2016.

278- شعبان ابو عجيلة عصارة، أبو المعالي محمد عيسى أبو المعالي، الرصد المبكر لخطر الجريمة، مجلة العلوم القانونية والشرعية،كلية القانون، جامعة الزاوية، ليبيا، العدد السادس (06)، يونيو 2015.

279- شنتير خضرة، الجريمة الإلكترونية تستهدف الأطفال جريمة الاستغلال الجنسي للأطفال عبر الإنترنت (نموذجاً)، مجلة دفاتر السياسة والقانون، جامعة قاصدي مرباح بورقلة، الجزائر، العدد الخاص، جوان 2018.

280- شوقي يعيش تمام، عزيزة شبري، تـفعيل مـبدأ عـالمية النص الجنائي في التصدي للجريمة المعلوماتية، مجلة الاجتهاد القضائي تصدر عن مخبر أثر الاجتهاد القضائي على حركة التشريع، جامعة محمد خيضر ببسكرة، الجزائر، العدد الخامس عشر (15)، سبتمبر 2017.

281- شوقي يعيش تمام، فريد علوش، العوائق التي تواجه مكافحة الجريمة الإلكترونية (دراسـة مقارنة)، مجلة العلوم السياسية والقانون، المركز الديمقراطي العربي، ألمانيا، المجلد الثلاثون (30)، العدد الثالث عشر (13)، يناير 2019.

282- شيخي عائشة، عياشي بوزيان، الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وأشكالها الاقتصادية وآليات مكافحتها، مجلة الدراسات الحقوقية، مخبر حماية حقوق الإنسان بين النصوص الدولية والنصوص الوطنية وواقعها في الجزائر، كلية الحقوق والعلوم السياسية، جامعة الدكتور الطاهر مولاي، سعيدة، العدد الرابع، ديسمبر 2015.

283- صباح مصباح محمود الحمداني، نادية عبد اللطيف أحمد، ماهية السياسة الوقائية الجزائية، مجلة جامعة تكريت للحقوق، كلية الحقوق، جامعة تكريت، العراق، السنة (02)، المجلد (02)، العدد (01)، الجزء (01)، ايلول 2017.

284- صالح شنين، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور في قانون الإجراءات الجزائية الجزائري، المجلة الاكادمية للبحث القانوني، مجلة سداسية، جامعة عبد الرحمان ميرة – بجاية–، عدد 02، 2010.

285- صايش عبد المالك، الأجهزة الأوربية المكلفة بمكافحة الهجرة السرية مهمة مستحيلة بمعدات عسكرية، المجلة الأكاديمية للبحث القانوني، كلية الحقوق والعلوم السياسية، جامعة عـبد الرحمان ميرة، بجاية، الجزائر، المجلد الحادي عشر (11)، العدد الاول (01)، 2015.

286- صفاء أوتاني، الوضع تحت المراقبة الاكترونية "السوار الالكتروني" في السياسة العقابية الفرنسية، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، سوريا، المجلد 25، العدد الاول، 2009.

287- صليحة حاجي، الآليات القانونية لتكريس الأمن المعلوماتي، مجلة العلوم الجنائية، العدد الثاني، مطبعة الأمنية وتوزيع مكتبة الرشاد، المغرب، 2015.

288- طباش عز الدين، الحماية الجزائية للمعطيات الشخصية في التشريع الجزائري دراسة في ظل قانون 18-07 بالمتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، المجلة الأكاديمية للبحث القانوني، جامعة عبد الرحمان ميرة، بجاية، الجزائر، العدد الثاني (02)، ديسمبر 2018.

289- طه عيساني، القرصنة الإلكترونية؛ الضرر الاقتصادي والفكري، مجلة جيل الأبحاث القانونية المعمقة، مركز جيل البحث العلمي، العدد الخامس (05)، يوليو 2016.

290- عادل جارش، الإرهاب الجديد: دراسة في المفهوم، الطبيعة، الأنواع وإجراءات المواجهة، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر بالوادي، الجزائر، المجلد التاسع (09)، العدد الثالث (03)، ديسمبر 2018.

291- عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية وأزمة الشرعية الجـزائية، مركز دراسات الكوفة، كلية القانون، جامعة الكوفة، العراق، العدد السابع، 2008.

292- عائشة عبد الحميد، دور المنظمة الدولية للشرطة الجنائية (الأنتربول) في محاربة الإجرام الاقتصادي الدولي، مجلة جيل حقوق الإنسان، مـركز البحث العلمي، طرابلس، لبنان، العـام الخـامس، العدد الرابع والثلاثين (34)، أكتوبر 2018.

293- عبد الحكيم الحكماوي، الإثبات في الجريمة الإلكترونية، تأثير الجريمة الإلكترونية على الائتمان المالي، سلسلة ندوات محكمة الاستئناف بالرباط، العدد السابع، 2014.

294- عبد الصبور عبد القوي علي، الجريمة الإلكترونية والجهود الدولية للحد منها، مجلة الدراسات المالية والمصرفية، مركز البحوث المالية والمصرفية، الأكاديمية العربية للعلوم المالية والمصرفية، السنة الثالثة والعشرون، المجلد الثالث والعشرون، العدد الأول، اذار (مارس) 2015.

295- عبد الكريم غالي، الجريمة الإلكترونية في حقل الائتمان بين مواقف القضاء ومستجدات التشريع، تأثير الجريمة الإلكترونية على الائتمان المالي، سلسلة ندوات محكمة الاستئناف بالرباط، العدد السابع، 2014.

296- عبد الكافي الورياشي، نظام تسليم الـمجرمين، قـراءات في المـادة الجنائية، الجـزء الأول، الإصدار السادس عشر، الطبعة الأولى، مجلة الحقوق (R.D) سلسلة المعارف القانونية والقضائية، دار نشر المعرفة، الرباط، المغرب، 2013.

297- عبد المنعم ابقال، الإطـار القانوني لمكافحة الجريمة الإلكترونية دراسة مقارنة، مجلة المنارة للدراسات القانونية والإدارية، عدد خاص، مركز المنارة للدراسات والأبحاث بالرباط، المغرب، 2017.

298- عبد الوهاب ملياني، إشكالية التوازن بين حرية تداول المعلومات الإلكترونية والحماية القانونية من الاعتداء عليها، مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور بالجلفة، الجزائر، المجلد الثاني (02)، العدد (22)، تاريخ النشر: 2015/03/15.

299- عبيد صالح حسين، سـياسة المـشرع الإماراتي لموجهة الجرائم الإلكترونية، مجلة الفكر الشرطي، مـركز بحوث الشرطة، القيادة العامة لشرطة الشـارقة، الإمارات، المجلد الرابع والعشرون (24)، الـعدد الخامس والتسعون (95)، اكتوبر 2015.

300- عبير بعقيقي، فيصل نسيغة، الإثبات في الجرائم المعلوماتية على ضوء القانون 09-04، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر بالوادي، الجزائر، المجلد التاسع (09)، العدد الثاني (02)، جوان 2018.

301- عطوي مليكة، الجريمة المعلوماتية، مجلة حوليات جامعة الجزائر، جامعة الجزائر 01 بن يوسف بن خدة، الجزائر، العدد 21، الجزء الأول، جوان 2012.

302- معتز عفيفي، المحكمة المختصة بدعوى التعويض عن الجريمة المعلوماتية (بين منصة القضاء ومنصة التحكيم)، مجلة الفكر القانوني والاقتصادي، كلية الحقوق، جامعة بنها، مصر، العدد (04)، يونيو 2011.

303- علواش فريد، نظام تسليم المجرمين في الاتفاقيات الدولية، مجلة الدراسات القانـونية والـسياسية، جـامعة عـمار ثليجي بالأغـواط، الجـزائر، المجلد الثاني (02)، العدد الخامس (05)، جانفي 2017.

304- عمر عبد المجيد مصبح، الإشكالات الجزائية في تكييف "المخدرات الـرقمية"، مجلة الـقانون والمجتـمع، مخبر الـقانون والمجتمع، جامـعة احمد دراية ادرار، الجزائر، العدد التاسع، جوان 2017.

305- علاوة هوام، التسرب كآلية للكشف عن الجرائم في قانون الإجراءات الجزائية الجزائري، مجلة الفقه والقانون، جامعة الحاج لخضر- باتنة -، ديسمبر 2012.

306- عنو عزيزة، آثار الألـعاب الإلكترونية على الخصائص النفسية السلوكية لدى الطفل، حوليات جامـعة قالمة للعلوم الاجتماعية والإنسانية، جامعة 08 ماي 1945 قـالمة، الجزائر، المجلد الثامن (08)،العدد الحادي عشر (11)، جوان 2015.

307- فاديا سليمان، الجـرائم المعلوماتية وأثـرها على العمليات المالية والمصرفية، مجـلة الدراسات المالية والمصرفية، السنة الثالثة والعشرون، الـعدد الأول، الأردن، مارس 2015.

308- فريجة محمد هشام، النظام القانوني للجريمة المعلوماتية وصعوبات تحقيق الأمن الإلكتروني، حوليات جامعة قالمة للعلوم الاجتماعية والإنسانية، الجزائر، العدد الرابع والعشرون (24)، جوان 2018.

309- فريد الصغيري، اللعبة الإلكترونية، الممارسة الشبابية وعلاقتها بالعنف، مجلة دراسات وأبحاث، جامعة زيان عاشور، الجلفة، الجزائر، المجلد الخامس (05)، العدد الحادي عشر (11)، جوان 2013.

310- فندوشي ربيعة، الصورة عبر الإنترنت التجاوزات والحماية، مجلة البحوث والدراسات العلمية، المركز الجامعي الدكتور يحي فارس، المدية، الجزائر، العدد الخامس (05)، جويلية 2011.

311- فوزي عمارة، اعتراض المراسلات والتسجيلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراء تحقيق قضائي في المواد الجزائية، مجلة العلوم الإنسانية، جامعة منتوري، قسنطينة، عدد 33، جوان 2010.

312- فوزي لواتي، التسرب كآلية للتحقيق في جرائم الاتجار بالمخدرات في الجزائر: المتطلبات القانونية والإشكالات العملية"، مجلة آفاق للعلوم، جامعة زيان عاشور بالجلفة، العدد الثاني (02)، 2016.

313- قارة ملاك، الجريمة المعلوماتية في القطاع البنكي وأساليب مكافحتها إشارة لحالة الجزائر، مجلة الحكمة للدراسات الإعلامية والاتصالية، تصدر عن مؤسسة كنوز الحكمة للنشر والتوزيع، العدد السابع، الجزائر، 2016.

314- قصعة خديجة، جمال بن زروق، تفعيل آليات الحماية القانونية للحد من انتشار الجريمة الإلكترونية في العالم الجزائر، مجلة تاريخ العلوم والدراسات والأبحاث الايستمولوجية، جامعة زيان عاشور بالجلفة، العدد السادس، 2017.

315- كحيل حـياة، حجية الإثبات الإلكتروني، مجلة البحوث والدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة لونيسي علي، البليدة 02، الجزائر، العدد التاسع (09)، اوت 2016.

316- لدغش رحيمة، ضوابط تفتيش الحاسب الآلي، مجلة الحقوق والعلوم السياسية، جامعة زيان عاشور بالجلفة، الجزائر، العدد الرابع (04)، تاريخ النشر: 2015/12/15.

317- لطرش فيروز، بن عزوز حاتم، الجريمة الإلكترونية في الجزائر من جريمة فردية إلى جريمة منظمة، مجلة آفاق للعلوم، جامعة زيان عاشور بالجلفة، العدد 01، 2016.

318- لموسخ محمد، تـنازع الاختصاص في الـجريمة الإلكترونية، مجلة دفاتر السياسة والقانون، جامعة قاصدي مرباح بورقلة، الجزائر، العدد الثاني (02)، جوان 2009.

319- لورنس سعيد الحوامدة، الجريمة المعلوماتية أركانها وآلية مكافحتها "دراسة تحليلية مقارنة"، مجلة الميزان للدراسات الإسلامية والقانونية، جامعة العلوم الإسلامية العالمية، المملكة العربية السعودية، 2016-2017.

320- لينداا بن طالب، التفتيش في الجريمة المعلوماتية، مجلة العلوم القانونية والسـياسية، كـلية الحـقوق والعلوم السـياسية، جامعة الشـهيد حمه لخضر بالوادي، الجزائر، العدد ستة عشر (16)، جوان 2016.

321- لينده بـوسيف، آليات وسـبل مكافحة الـجريمة الإلكترونية، مجلة الاتصال والصحافة، تصـدر عن المدرسة الوطنية العليا للصحافة وعـلوم الإعلام، المجلد الرابع، العدد الثاني، الجزائر، 2017/06/15.

322- ماجدة غريب، حسن الأمير، مدى الوعي لدى الفئة العمرية الشابة بنظام عقوبات الجرائم المعلوماتية السعودي، المجلة العربية الدولية للمعلوماتية، المملكة العربية السعودية، المجلد الخامس (05)، العدد التاسع (09)،2017.

323- مجاهدي خديجة، إستراتيجية المنظمة الدولية للشرطة الجنائية في مكافحة الجريمة المنظمة، مجلة الدراسات القانونية، مخبر السيادة والعولمة، جامعة يحي فارس، المدية الجزائر، المجلد الثاني، العدد الثاني، جوان 2015.

324- محمد احمد سليمان عيسى، التعاون الدولي لمواجهة الجريمة الإلكترونية، المجلة الأكاديمية للبحث القانوني،كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميره، بجاية، الجزائر، المجلد الرابع عشر (14)، العدد الثاني (02)، 2016.

325- محمد احمد السويحلي، تكاثف الجهود العربية لمكافحة الجريمة الإلكترونية، مجلة الدراسات المالية والمصرفية، السنة الثالثة والعشرون، العدد الأول، الأردن، مارس 2015.

326- محمد بن سالم محمد القرني، إدمان الإنترنت وعلاقته ببعض الاضطرابات النفسية لدى عينة من طلاب جامعة الملك عبد العزيز، مجلة كلية التربية، جامعة المنصورة، مصر، الجزء الثالث، العدد الخامس والسبعون(75)، يناير 2011.

327- محمد علي سالم، حسون عبيد هجيج، الجريمة المعلوماتية، مجلة جامعة بابل، كلية العلوم الإنسانية، جامعة بابل، العراق، المجلد 14، العدد 06، 2007.

328- محمد مروان، وضعية الشخص المشتبه فيه أثناء المرحلة البوليسية في الدعوى الجنائية في القانون الجزائري والمقارن، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية، كلية الحقوق والعلوم الإدارية، جامعة الجزائر، الجزء تسعة وثلاثون (39)، العدد رقم 02، سنة 2001.

329- محمودي سماح، مشكلات التفتيش الجنائي عن المعلومات في الكمبيوتر والإنترنت، مجلة الحقوق والعلوم السياسية، جامعة عباس لغرور خنشلة، الجزائر، الجزء الأول، العدد الثامن، جوان 2017.

330- محي الدين حسيبة، سماع الشهود عن طريق المحادثة المرئية عن بعد بين الحق في الحماية وحـقوق الدفاع، مجـلة البحوث والدراسات القانونية والسياسـية، كلية الحقوق والعلوم السياسية، جامعة لونيسي علي، البليدة 02، الجزائر، العدد العاشر (10)، جانفي 2017.

331- مختار الاخضري، الإطار القانوني لمواجهة جرائم المعلوماتية وجرائم الفضاء الافتراضي، مجلة نشرة القضاة، المديرية العامة للشؤون القضائية والقانونية، مديرية الدراسات القانونية والوثائق، وزارة العدل، الجزائر، العدد 66، 2011.

332- مريم لوكال، الحماية القـانونية الدولية والـوطنية ذات الطابع الشخصي في الفضاء الرقمي: في ضوء قانون حـماية المعطيات رقم 18-07، مجـلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمة لخضر بالواد، الجزائر، المجلد العاشر (10)، العدد الأول (01)، افريل 2019.

333- مزيود سليم، الجريمة المعلوماتية واقعها في الجزائر وآليات مكافحتها، المجلة الجزائرية للاقتصاد والمالية، مخبر الاقتصاد الكلي والمالية الدولية، جامعة الدكتور يحي فارس، المدية، الجزائر، العدد الأول، افريل 2014.

334- معاشي سميرة، الجـريمة المعلوماتية (دراسـة تحليلية لمفهوم الجريمة المعلوماتية)، مجـلة المفكر، كلية الحقوق والعـلوم السياسية، جامـعة محـمد خيضر ببـسكرة، الجزائر، العدد سبعة عشر (17)، جوان 2018.

335- معزيز أمينة، التسرب في قانون الإجراءات الجزائية، مجلة القانون والمجتمع، مخبر القانون والمجتمع، جامعة احمد دراية ادرار، الجزائر، العدد الخامس، 2015.

336- معمري عبد الرشيد، ضوابط مشروعية أساليب التحري الخاصة، المجلة الأكـاديمية للبحث القانوني، كلية الحقوق والعـلوم السياسية لجامعة عبد الرحمان ميره، بجاية، المجلد 11، العدد الأول، 2015.

337- ممدوح حسن مانع العدوان، نادر عبد الحليم السلامات، مشروعية وحجية الدليل المستخلص من التفتيش الإلكتروني في التشريع الجزائي الأردني، مجلة دراسات، حقل علوم الشريعة والقانون، عمادة البحث العلمي، الجامعة الأردنية، المجلد الخامس والأربعون (45)، العدد الرابع (4)، الملحق الثاني (2)، الأردن، 2018.

338- منيرة عبيزة، بوبكر مصطفى، الـدليل الإلكتروني والسلطة التقديرية للقاضي، مجلة العلوم الـقانونية والسياسية، كـــلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر بالوادي، الجزائر، المجلد التاسع (09)، العدد الثالث (03)، ديسمبر 2018.

339- ميسوم ليلى، إدمان الإنترنت والاضطراب الجنسي، مجلة الحوار الثقافي، مخبر حوار الحضارات والتنوع الثقافي وفلسفة السلم، كلية العلوم الاجتماعية، جامعة عبد الحميد بن باديس، مستغانم، الجزائر، المجلد السادس (06)، العدد الرابع (04)، 2017/09/15.

340- ناجية شيخ، حول مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر بالوادي، الجزائر، المجلد التاسع(09)، العدد الثاني(02)، جوان 2018.

341- ناصري سميرة، بسمة ترغيني، دور المجتمع الـمدني في مـكافحة الجـريمة المنظمة، مجـلة الحقوق والعلوم السياسية، جـــامعة عباس لغرور خنشلة، الجزائر، المجـلد الأول، العدد الثاني، جويلية 2014.

342- نبيل دريس، الجريمة السيبرانية بين المفاهيم والنصوص التشريعية الجزائر أنموذجا، مجلة القانون والمجتمع، مخبر الـــقانون والمجـــتمع، جـــامعة احـمد دراية ادرار، الجزائر، العدد العاشر (10)، ديسمبر 2017.

343- نزيهة مكاري، إثبات الاعتداء على حق المؤلف عبر الإنترنت في التشريع الجزائري (دراسة مقارنة)، مجلة العلوم الاقتصادية وعلوم التسيير، كلية العلوم الاقتصادية والتجارية وعلوم التسيير بجامعة سطيف1،العدد التاسع (09)، 2009.

344- نديم محمد حسن الترزي، سلطات النيابة العامة في الجرائم المعلوماتية (المعاينة – التفتيش)، مجلة الأندلس للعلوم الإنسانية والاجتماعية، صنعاء، اليمن، العدد الثالث عشر (13)، المجلد الخامس عشر (15)، ابريل 2017.

345- نقادي حفيظ، أساليب البحث والتحري الخاصة، المجلة الجزائرية للعلوم القانونية والسياسية، كلية الحقوق، جامعة الجزائر01 بن يوسف بن خدة، المجلد (50)، العدد الرابع (4)، 2013/12/01.

346- نقموش محمد، ميلودية أحمد، الجريمة المعلوماتية: المفهوم – حتمية تطوير آليات التعاون الدولي في مجال مكافحتها، مجلـة الـدراسات الـقانونية والسياسية، جامعة عمار ثليجي بالأغواط، الجزائر، المجلد الرابع (04)، العدد الثاني (02)، جوان 2018.

347- نور الدين بن سولة، الجريمة الإلكترونية في ضوء التشريع الجزائري، مجلة الحـوار المتوسطي، جامعة الجيلالي ليابس سيدي بلعباس، المجلد التاسع، العدد الأول، الجزائر، مارس 2018.

348- نور الدين الواهلي، الاختصاص في الجريمة الإلكترونية، تأثير الجريمة الإلكترونية على الائتمان المالي، سلسلة ندوات محكمة الاستئناف بالرباط، العدد السابع، 2014.

349- نور الهدى محمودي، حجية الدليل الرقمي في إثبات الجريمة المعلوماتية، مجلة الباحث للـدراسات الأكـاديمية، كلية الحقوق والعلوم السياسية، جامـعة الحاج لخضر (جامعة باتنة 1)، الجزائر، العدد الحادي عشر (11)، جوان 2017.

350- وداعي عز الدين، التسرب كأسلوب البحث والتحري الخاصة على ضوء قانون الإجراءات الجزائية الجزائري والمقارن، المجلة الأكاديمية للبحث القانوني،كلية الحقوق والـعلوم السـياسية، جـامعة عـبد الرحمن ميرا بجاية، الجـزائر، المجلد (16)، العدد الثاني (02)، 2017.

351- وردة شرف الدين، مجالات لمساعدة القضائية المتبادلة فيما يخص جمع الأدلة الرقمية – وفقا للاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 – مجلة العلوم السياسية والقانون، المجلد الثلث (03)، العدد الخامس عشر (15)، المركز الديمقراطي العربي، المانيا، ماي 2019.

352- وعلى جمال، حقوق المشتبه فيه عند اللجوء إلى إجراءات البحث والتحري الخاصة، مجلة الدراسات الحقوقية، جامعة الدكتور الطاهر مولاي، سعيدة، الجزائر، العدد الثالث (03)، جوان 2015.

353- ياسمينة بونعارة، الجريـمة الإلكترونية، مجلة جامعة الأمير عبد القادر للـعلوم الإسـلامية، قسنطينة، العدد تسعة وثلاثون (39)، 21 جوان 2016.

354- يحياوي محمد، مخاطر القرصنة على الحكومة الإلكترونية، مجلة البحوث والدراسات العلمية، المركز الجامعي الدكتور يحي فارس، المدية، الجزائر، العدد الخامس (05)، جويلية 2011.

355- الطيب بلواضح، الجهود الدولية لحماية البريد الإلكتروني جنائيا، مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور، الجلفة، الجزائر، العدد تسعة عشر (19)، 2014/06/01.

356- العيداني محمد، يوسف زروق، حماية المعطيات الشخصية في الجزائر على ضوء القانون رقم 18-07 (المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي)، مجلة معالم للدراسات القانونية والسياسية، المركز الجامعي علي كافي تندوف، الجزائر، العدد الخامس (05)، ديسمبر 2018.

357- المتولي عطيه عبد الباقي إبراهيم، أداء الشهادة بوسائل الاتصال الحديثة في منظور الفقه الإسلامي، مجلة كلية الشريعة والقانون بطنطا، العدد الثلاثون، الجزء الرابع، مصر، ديسمبر 2015.

358- المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، تشكيل عملياتي لمحاربة الجريمة عبر الشبكة العنكبوتية، مجلة الشرطة، المؤسسة الوطنية للاتصال والنشر والإشهار وحدة الطبع رويبة، الجزائر، العدد مائة وأربعة وأربعون (144)، سبتمبر 2019.

هـ)- بحـوث مـؤتمرات ونـدوات:

359- إبراهيم محمد قاسم الميمن، العقوبات البديلة الفقه الإسلامي، ورقة بحثية مقدمة للمشاركة في ندوة بعنوان: بدائل العقوبات السالبة للحرية، المنعقدة بالتعاون بين مركز الدراسات والبحوث بجامعة نايف العربية للعلوم الأمنية وإدارة السجون الجزائرية بوزارة العدل، الجزائر، الفترة ما بين 10 و12 ديسمبر 2012.

360- أحمد عبد الكريم سلامة، الإنترنت والقانون الدولي الخاص فراق أم تلاق، مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، المجلد الأول، الطبعة الثالثة، الإمارات العربية المتحدة، من 01 إلى 03 مايو 2004.

361- أحمان لبني، جنوح الأحداث بين العوامل النفسية والتنشئة الاجتماعية، الملتقى الوطني: جنوح الأحداث "قراءة في الواقع وآفاق الظاهرة وعلاجها، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة باتنة 01، يومي 04 و05 ماي 2016.

362- آمال بن صويلح، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام خطوة هامة نحو مكافحة الإرهاب الإلكتروني بالجزائر، ورقة بحثية مقدمة في إطار الملتقى الدولي حول" الإجرام السيبراني المفاهيم والتحديات"، كلية الحقوق والعلوم السياسية،جامعة محمد البشير الإبراهيمي، برج بوعريرج، يومي 11-12 افريل 2017.

363- أيسر محمد عطية، ورقة علمية بعنوان: دور الآليات الحديثة للحد من الجرائم المستحدثة الإرهاب الإلكتروني وطرق مواجهته، كلية العلوم الإستراتيجية، الملتقى العلمي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، عمان، الأردن، من 02 إلى 04 سبتمبر 2014.

364- بارة سمير، الدفاع الوطني والسياسات الوطنية للأمن السيبراني (Cyper Security) في الجزائر: الدور والتحديات، ورقة بحثية مقدمة في إطار أشغال الطبعة الثانية من الملتقى الدولي حول: سياسات الدفاع الوطني بين الالتزامات السيادية والتحديات الإقليمية، كلية الحقوق والعلوم السياسية ومخبر التحولات السياسية والاقتصادية والاجتماعية والقانونية في التجربة الجزائرية، جامعة قاصدي مرباح، ورقلة، يومي الاثنين والثلاثاء 30 و31 جانفي 2017.

365- ثامر على النويران، الجرائم الإلكترونية وطرق الحد منها: تجربة الأردن، ورقة بحثية مقدمة في إطار أشغال المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية ICACC، كلية علوم الحاسب والمعلومات، جامعة الإمام محمد بن سعود الإسلامية، الرياض، المملكة العربية السعودية، نوفمبر 2015.

366- خالد كاظم أبو دوح، المخدرات الرقمية: مقاربة للفهم، الندوة العلمية" المخدرات الرقمية وتأثيرها على الشباب العربي"، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، الفترة من 16 إلى 18 فيفري 2016.

367- خضراوي الهادي، بوقرين عبد الحليم، تجربة الجزائر في مكافحة الجريمة الإلكترونية، ورقة بحثية مقدمة في إطار أشغال المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية ICACC،كلية علوم الحاسب والمعلومات، جامعة الإمام محمد بن سعود الإسلامية، الرياض، المملكة العربية السعودية، نوفمبر 2015.

368- ذياب موسى البدانية، الجرائم الإلكترونية: المفهوم والأسباب، ورقة مقدمة في الملتقى الخاص بالجرائم المستحدثة في ظل المتغيرات والتحولات الإقليـمية والـدولية، كلية العلوم الإستراتيجية، جامعة عمان ،الأردن، الأيام من 02 إلى 04 سبتمبر 2014.

369- رابحي لخضر، بن بعلاش خاليدة، معالجة الجرائم المعلوماتية في ظل التعاون الدولي والاستجابة الوطنية، مداخلة في إطار أشغال الملتقى الوطني المتعلق بالجريمة المعلوماتية بين الوقـاية والمـكافحة، المنظم من قبل قـسم الحـقوق ومخبر الحقوق والحريات في الأنـظمة المقارنة، بجامعة بسكرة يومي 16-17 نوفمبر 2015.

370- رضا هميسي، أحكام الشاهد في الجريمة المعلوماتية، مداخلة في إطار أشغال الملتقى الوطني المتعلق بالجريمة المعلوماتية بين الوقاية والمكافحة، المنظم من قبل قسم الحقوق ومخبر الحقوق والحريات في الأنظمة المقارنة، بجامعة بسكرة يومي 16-17 نوفمبر 2015.

371- سلامي اسعيداني، التشريعات القانونية لدولية لحماية حقوق الملكية الفكرية الافتراضية رؤية نقدية من منظور إعلامي قانوني، الملتقى الدولي حول التعليم في عصر التكنولوجيا الرقمية، طرابلس، لبنان، من 22 إلى 24 أفريل 2015.

372- سالم بن محمد السالم، السرقات العلمية في البيئة الإلكترونية: دراسة للتحديات والتشريعات المعنية بحماية حقوق التأليف، المؤتمر السادس لجمعية المكتبات والمعلومات السـعودية، الـبيئة المعلوماتـية الآمنة: المـفاهـيم والتشـريعات والتطبـيقات، المنـعقد بالـرياض، السعودية، خلال الفترة من 06 إلى 07 أبريل 2010.

373- سومية عكور، الجرائم المعلوماتية وطرق مواجهتها: قراءة في المشهد القانوني والأمني، ورقة عـلمية مقدمة في الملتقى العـلمي حـول الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، كلية العلوم الإستراتيجية، عمان، الأردن، خلال الفترة من 02 إلى 04 سبتمبر 2014.

374- شرف الدين وردة، مشـكلة تـنازع الاختصاص الدولي في مجال الجريمة المعلوماتية، مداخلة في إطار أشغال الملتقى الوطني المتعلق بالجريمة المعلوماتية بين الوقاية والمكافحة، المنظم من قبل قسم الحقوق ومخبر الحقوق والحريات في الأنظمة المقارنة، بجامعة بسكرة يومي 16-17 نوفمبر 2015.

375- طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي، ورقة عمل مقدمة للمؤتمر المغاربي الأول حول المعلوماتية والـقانون، أكـاديمية الـدراسات الـعليا، طرابلس، ليبيا، يومي 28 و29 اكتوبر 2009.

376- عبد الرؤوف احمد بني عيسى، الخطط المقترحة للوقاية من المخدرات الرقمية في المجال التربوي، الندوة العلمية "المخدرات الرقمية وتأثيرها على الشباب العربي"، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، الفترة من 16 إلى 18 فيفري 2016.

377- عبد الكريم خالد الردايدة، المعوقات التي تؤثر على سير التحقيق في مسرح الجريمة، قسم البرامج التدريبية، كلية لتدريب، الدورة التدريبية حول إجراءات التحري والمراقبة والبحث الجنائي، الرياض، السعودية، خلال الفترة من 05 إلى 16 جويلية 2012.

378- عبد الله عويدات، الآثار النفسية والاجتماعية للمخدرات الرقمية ودور مؤسسات الضبط الاجتماعي في الحد من آثارها، الندوة العلمية" المخدرات الرقمية وتأثيرها على الشباب العربي، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، الفترة من 16 إلى 18 فيفري 2016.

379- عبد الناصر محمد فرغلي، محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية دراسة تطبيقية مقارنة، المؤتمر العربي الأول لعلوم الأدلة الجـنائية والـطب الشرعي، جامعة نايـف العربية للـعلوم الأمـنية، الرياض، السعودية، الأيام من 12 إلى 14 نوفمبر 2007.

380- عبد المومن بن صغير، الطبـيعة الخـاصة للـجريمة المرتكبة عبر الإنترنت في التشريع الجزائري والتشريع المقارن، مداخلة في إطار أشغال الملتقى الوطني المتعلق بالجريمة المعلوماتية بين الوقاية والمكافحة، المنظم من قبل قـسم الحقوق ومخبر الحقوق والحريات في الأنـظمة المقارنة، بجامعة بسكرة يومي 16-17 نوفمبر 2015.

381- عمر عبد العزيز موسى الدبور، آليات تفعيل الحماية والوقاية من الجرائم الإلكترونية (إنشـاء ضبطية خاصة بالجـرائم الإلكترونية)، المـؤتمر الدولي الرابع عشر حول الجرائم الإلكترونية، طرابلس، 24-25 مارس 2017.

382- فضيلة عاقلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، المؤتمر الدولي الرابع عشر حول الجرائم الإلكترونية، طرابلس، 24-25 مارس 2017، ص من 115 إلى 136.

383- مانع سلمى، دور الأمن المعلوماتي في مكافحة الجرائم المعلوماتية، مداخلة في إطار أشغال الملتقى الوطني المتعلق بالجريمة المعلوماتية بين الوقاية والمكافحة، المنظم من قبل قسم الحقوق ومخبر الحقوق والحريات في الأنظمة المقارنة، بجامعة بسكرة يومي 16-17 نوفمبر2015.

384- محمد أبو العلا عقيدة، التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، ورقة بحثية مقدمة في إطار المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، المنظم من قبل أكاديمية شرطة دبي، مركز البحوث والدراسات، الإمارات العربية المتحدة، الفترة من 26 إلى 28 افريل 2003.

385- محمد بن احمد بن على المقصودي، الجرائم المعلوماتية خصائصها وكيفية مواجهتها قانونيا التكامل الدولي المطلوب لمكافحتها، ورقة بحثية مقدمة في إطار أشغال المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية ICACC، كلية علوم الحاسب والمعلومات، جامعة الإمام محمد بن سعود الإسلامية، الرياض، المملكة العربية السعودية، نوفمبر 2015.

386- محمد فهاد الشلالدة، عبد الفتاح أمين ربعي، الجرائم الإلكترونية في دولة فلسطين المحتلة في ضوء التشريعات الوطنية والدولية، بحث مقدم إلى المؤتمر العلمي الحادي عشر حول الجرائم المعلوماتية، لكلية القانون، جامعة جرش، فلسطين، الأيام من 05 إلى 07 ماي 2015.

387- محمد مرسي محمد مرسي، إدمان المخدرات الرقمية عبر الإنترنت وتأثيرها علي الشباب العربي" دراسة ميدانية مطبقة على الشباب العربي بجامعة الأزهر بالقاهرة"، الندوة العـلمية" المخدرات الرقمية وتأثيرها على الشباب العربي"، جامعة نايف العـربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، الفترة من 16 إلى 18 فيفري 2016.

388- محمد الأمين البشري، تأهيـل المحققين في جرائم الحـاسب الآلي وشبكات الإنترنت، الحلقة العلمية (الإنترنت والإرهاب)، كلية التدريب، جامعة نايف العربية للعلوم الأمنية بالتـعاون مع جامعة عين شمس (مصر)، الرياض، السعـودية، خـلال الفترة من 15 إلى 19 نوفمبر 2008.

389- مديحة فخري محمود محمد، دراسة مستقبلية لدور الجامعات المصرية في مواجهة الجرائم الإلكترونية لدي الطلاب، ورقة بحثية مقدمة في إطار أشغال أبحاث مؤتمر التربية في عالم متغير، محور الإدارة التربوية، المقام في الجامعة الهاشمية، الأردن، يومي 07 و08 افريل 2010.

390- محمود على السرطاوي، موقف الشريعة الإسلامية من استعمال الوسائل العلمية في تعذيب المتهم، الندوة العلمية (الجوانب الشرعية والقانونية لاستخدام الوسائل العلمية في التحقيق الجنائي)، مركز الدراسات والبحوث قسم الندوات واللقاءات العلمية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2007.

391- مصطفى محمد مرسي، قواعد وإجراءات البحث الجنائي لكشف غموض الجرائم المعلوماتية والتخطيط لها، الدورة التدريبية (إجراءات التحري والمراقبة والبحث الجنائي)، قسم البرامج التدريبية،كلية التدريب، الرياض، السعودية، من 2012/05/26 إلى 2012/06/06.

392- موسى مسعود أرحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، ورقة بحثية مقدمة في إطار اشغال المؤتمر المغاربي الأول حول: المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، الفترة بين 28 و29 اكتوبر 2009.

393- نشناش منية، الركن المفترض في الجريمة المعلوماتية، مداخلة في إطار أشغال الملتقى الوطني المتعلق بالجريمة المعلوماتية بين الوقاية والمكافحة، المنظم من قبل قسم الحقوق ومخبر الحقوق والحريات في الأنظمة المقارنة، بجامعة بسكرة يومي 16-17 نوفمبر 2015.

394- السيد إيهاب ماهر السنباطي، الجرائم الإلكترونية (الجرائم السيبيرية): قضية جديدة أم فئة مختلفة؟ التناغم القانوني هو السبيل الوحيد!، مداخلة في أعمال الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر في إطار برنامج تعزيز حكم القانون في بعض الدول العربية "مشروع تحديث النيابات العامة"، المقام بالدار البيضاء، المملكة المغربية، يومي 19 و20 يونيو 2008.

395- القاضي وليد العاكوم، مفهوم وظاهرة الإجرام المعلوماتي، بحوث مؤتمر القانون والكمبيوتر والإنترنت بالتعاون مع مركز الإمارات للدراسات والبحوث الإستراتيجية ومركز تقنية

المعلومات بالجامعة، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، المجلد الأول، من 01 إلى 03 مايو 2004.

و)– الأيام الدراسية:

396- لوجاني نور الدين، أساليب البحث والتحري الخاصة وإجراءاتها، يوم دراسي حول عـلاقة النيابة الـعامة بالـشرطة القضائية (احترام حقوق الإنسان ومكافحة الجريمة)، إيليزي 12 ديسمبر 2007.

ز)– التـقارير :

397- تقرير عـن اجتمـاع فـريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، الذي عُقد في فيينا في الفترة من 27 إلى 29 مارس 2019.

398- فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، دراسة شاملة عن مشكلة الجريمة السيبرانية والتدابير التي تتَّخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدي لها، فيينا، 25-27 فبراير 2013 (UNODC/CCPCJ/EG.4/2013/2).

399- مركز هردو لدعم التعبير الرقمي (www.hrdoegypt.org ، info@hrdoegypt.org)، الجريمة الإلكترونية وحجية الدليل الرقمي في الإثبات الجنائي، القاهرة، 2013.

400- الانتربول، مكافحة الجريمة في القرن الحادي والعشرين (2000-2010)، ليون، فرنسا، 2010.

401- المركز الـوطني للدراسات والعـلوم القانونية، مجـلة الـقضاء الجنائي، العـدد الثاني، السـنة الأولى، مطبعة المعارف الجديدة وتوزيع دار الآفاق المغربية، الرباط، المغرب، صيف/خريف 2014.

ح)– اليوميات والجرائد:

402- جمال بن رجم، الفضاء السيبرياني الجزائري معرض للهجومات الداخلية والخارجية، يومية الاتحاد، العدد 1502، الصادر بتاريخ 15 فيفري 2018، ص 05، الموقع الإلكتروني:

– *http://www.elitihadonline.com/files.php?file=1502_9855 01177.pdf*

403- وسام. ك، الإخبارية، يومية وطنية، العدد 1397 ليوم الأربعاء 28 مارس 2018، الموضوع موجود على الموقع الإلكتروني الموالي:
- *http://www.elikhbaria.com/a/wp-content /uploads/elikhbariaPDF.*

ط)- النصوص القانونيــة:

1- الدستور:

404- التعديل الدستوري، المصادق عليه في استفتاء أول نوفمبر سنة 2020، المؤرخ في 15 جمادى الأولى عام 1442 الموافق 30 ديسمبر سنة 2020، الصادر بالمرسوم الرئاسي رقم 20-442، المنشور بالج.ر.ج، العدد 82، بتاريخ 30 ديسمبر سنة 2020، والمعدل للدستور الجزائري الصادر بموجب استفتاء شعبي في 28 نوفمبر 1996، الصادر بموجب المرسوم الرئاسي رقم 96-438 الممضي في 07 ديسمبر1996، المنشور بالج.ر.ج، عدد 76 مؤرخة في 08 ديسمبر 1996، الصفحة 6، ومعدل:
- بالقانون رقم 02-03 المؤرخ في 10 أبريل 2002، الج.ر.ج، عدد 25 المؤرخة في 14 أبريل 2002، الصفحة 13،
- والقانون رقم 08-19 المؤرخ في 15 نوفمبر 2008، الج.ر.ج، عدد 63 المؤرخة في 16 نوفمبر2008، الصــفحة 8،
- والمـعدل بالـقانون رقم 16-01 المؤرخ في 26 جمادى الأول عام 1437 الموافق 06 مارس 2016، المنشور بالج.ر.ج، عدد 14 المؤرخــة في 07 مارس 2016 ص 02.

2- المعاهدات والاتفاقيات:

405- الاتفاقية المتعلقة بالتعاون القضائي في المجال الجزائي بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وحكومة الجـمهورية الايطالية، المؤرخة في 04 محرم عام 1426 الموافق 13 فبراير 2005، الموقعة بالجزائر في 22 جويلية سنة 2003، المصادق عليها بالمرسوم الرئاسي رقم 05-73، الصادر في الج.ر.ج رقم 13 المؤرخة في 16 فبراير سنة 2005.
406- الاتفاقية المتعلقة بتسليم المجرمين بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وحـكومة الجمهورية الايطالية، المؤرخة في 04 محرم عام 1426 الموافق 13 فبراير 2005،

الموقعة بالجزائر في 22 جويلية سنة 2003، المصادق عليها بالمرسوم الرئاسي رقم 05-74 الصادرة في الج.ر.ج رقم 13 المؤرخة في 16 فبراير سنة 2005.

407- الاتفاقية المتعلقة بتسليم المجرمين بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وحكومة المملكة المتحدة لبريطانيا العظمى وإيرلندا الشمالية، المؤرخة في 20 ذي القعدة عام 1427 الموافق 11 ديسمبر 2006، الموقع بلندن في 11 جويلية سنة 2006، المصادق عليها بالمرسوم الرئاسي رقم 06-464، الصادر في الج.ر.ج رقم 81 المؤرخة في 13 ديسمبر سنة 2006.

408- الاتفاقية المتعلقة بالتعاون القضائي في المجال الجزائي بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وحكومة المملكة المتحدة لبريطانيا العظمى وإيرلندا الشمالية، المؤرخة في 20 ذي القعدة عام 1427 الموافق 11 ديسمبر 2006، الموقع بلندن في 11 جويلية سنة 2006، المصادق عليها بالمرسوم الرئاسي رقم 06-465، الصادر في الج.ر.ج رقم 81 المؤرخة في 13 ديسمبر سنة 2006.

409- الاتفاقية بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وجمهورية الصين الشعبية المتعلقة بالتعاون القضائي في المجال الجزائي، المؤرخة في 20 جمادى الأولى عام 1428 الموافق 06 جوان 2007، الموقعة ببيكين في 06 نوفمبر سنة 2006، المصادق عليها بالمرسوم الرئاسي رقم 07-175، الصادر في الج.ر.ج رقم 38 المؤرخة في 10 جوان سنة 2007.

410- اتفاقية التعاون القضائي والإعلانات والإنابات القضائية وتنفيذ الأحكام وتسليم المجرمين بين الجمهورية الجزائرية الديمقراطية الشعبية ودولة الإمارات العربية المتحدة، المؤرخة في 11 شوال عام 1428 الموافق 23 اكتوبر 2007، الموقعة بالجزائر في 12 اكتوبر سنة 1983، المصادق عليها بالمرسوم الرئاسي رقم 07-323، الصادرة في الج.ر.ج رقم 67 المؤرخة في 24 اكتوبر سنة 2007.

411- اتفاقية تسليم المجرمين بين الجمهورية الجزائرية الديمقراطية الشعبية ومملكة إسبانيا، المؤرخة في أول ربيع الأول عام 1429 المـــوافق 09 مـــارس 2008، الموقعـة بالجزائر في 12 ديسمبر

سنة 2006، المصادق عليها بالمرسوم الرئاسي رقم 08-85، الصادر في الج.ر.ج رقم 14 المؤرخة في 12 مارس سنة 2008.

412- معاهدة المنظمة العالمية للملكية الفكرية (الويبو) بشان حق المؤلف، المؤرخة في 22 جمادى الأولى عام 1434 هـ، الموافق 03 ابريل سنة 2013، المنعقدة بجـنيف بتاريخ 20 ديسمبر سنة 1996، المصادق عليها بالمرسوم الرئاسي رقم 13-123، الصادر في الج.ر.ج العدد 27، الصادر في 22 مايو 2013.

413- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر سنة 2010، المؤرخة في 13 ذي القعدة عام 1435 الموافق 8 سبتمبر سنة 2014، المصادق عليها بالمرسوم الرئاسي رقم 14-252، الصادر في الج.ر.ج رقم 57 بتاريخ 28 سبتمبر 2014، ص 04.

414- اتفاقية تسليم المتهمين والمحكوم عليهم بين الجمهورية الجزائرية الديمقراطية الشعبية والمملكة العربية السعودية، المؤرخة في 04 شوال عام 1436 الموافق 20 جويلية سنة 2015، الموقعة بالرياض في 13 ابريل سنة 2013، المصادق عليها بالمرسوم الرئاسي رقم 15-192، الصادر في الج.ر.ج رقم 43 المؤرخة في 12 اوت سنة 2015.

415- اتفاقية التعاون القانوني والقضائي في المجال الجزائي بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وحكومة دولة الكويت، المؤرخة في 21 ذي الحجة عام 1436 الموافق 5 اكتوبر سنة 2015 الموقعة بالجزائر في 12 اكتوبر سنة 2010، المصادق عليها بالمرسوم الرئاسي رقم 15-255، الصادر في الج.ر.ج رقم 53 المؤرخة في 8 اكتوبر سنة 2015.

416- الاتفاقية المتعلقة بالتعاون القضائي في المجال الجزائي بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وحكومة الجمهورية الفرنسية، المؤرخة في 9 جمادى الثانية عام 1439 الموافق 25 فبراير سنة 2018، الموقعة بباريس في 5 اكتوبر سنة 2016، المصادق عليها بالمرسوم الرئاسي رقم 18-73، الصادر في الج.ر رقم 13 المؤرخة في 28 فبراير سنة 2018.

417- الاتفاق المتعلق بتسليم المجـرمين بين الجمهورية الجزائرية الديمقراطية الشعبية وجمهورية أذربيجان، المؤرخ في 03 شـوال عـام 1440 المـوافق 06 يونيو سنة 2019، المـوقع بباكو

بتاريخ 21 يونيو سنة 2018، المصادق عليه بالمرسوم الرئاسي رقم 19-178، الصادر في الج.ر.ج العدد 40، بتاريخ 23 يونيو سنة 2019.

418- الاتفاقية المتعلقة بالتعاون القضائي في المجال الجزائي بين الجمهورية الجزائرية الديمقراطية الشعبية والبوسنة والهرسك، المؤرخة في 16 شوال عام 1441 الموافق 08 يونيو سنة 2020، الموقعة بالجزائر في 20 سبتمبر سنة 2011، المصادق عليها بالمرسوم الرئاسي رقم 20-148، الصادر في الج.ر.ج رقم 36 المؤرخة في 17 يونيو سنة 2020.

3- القوانـــــين والأوامـر والمراسيم الرئاسية:

أ- القوانين والأوامر:

419- الأمر رقم 66-155، المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966، المتضمن قانون الإجراءات الجزائية الجزائري، المنشور في الج.ر.ج عدد 48 المؤرخة في 10 يونيو 1966، الصفحة 622.

420- الأمر رقم 66-156، المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966، المتضمن قانون العقوبات المعدل والمتمم، المنشور بالج.ر.ج عدد 49 مـؤرخة في 11 يـونيو 1966، الصفحة 702.

421- الأمر رقم 73-14، المؤرخ في 03 ابريل 1973، المتعلق بحق المؤلف، الصادر في الج.ر.ج عدد 29، مؤرخة في 10 أبريل 1973، الصفحة 434.

422- القانون رقم 91-23، المؤرخ في 29 جمادى الأولى عام 1412 الموافق 6 ديسمبر سنة 1991، المتعلق بمساهمة الجيش الوطني الشعبي في مهام حماية الأمن العمومي خارج الحالات الاستثنائية، المنشور في الج.ر.ج العدد 63، الصادرة بتاريخ 7 ديسمبر سنة 1991، ص 2396.

423- الأمر رقم 97-10، الممضى في 06 مارس 1997، والمتعلق بحقوق المؤلف والحقوق المجاورة، الصادر في الج.ر.ج عدد 13، المؤرخة في 12 مارس 1997، الصفحة 3.

424- الأمر رقم 03-05، المؤرخ في 19 يوليو 2003، المتعلق بحقوق المؤلف والحقوق المجاورة، الصادر في الج.ر.ج المؤرخة في 23 يوليو 2003، العدد 44، ص 03.

425- القانون 04-15، المؤرخ في 10 نوفمبر 2004، الصادر في الج.ر.ج رقم: 71، المتضمن تعديل قانون العقوبات لسنة 2004، ص.ص: 11 و12، والذي أضيفت بموجبه المواد من 394 مكرر إلى 394 مكرر 07.

426- القانون رقم 05-10، المؤرخ في 13 جمادى الأولى عام 1426 الموافق 20 يونيو سنة 2005، يعدل ويتمم الأمر رقم 75-58 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975 والمتضمن القانون المدني المعدل والمتمم، الصادر بالج.ر.ج، العدد 44 بتاريخ 26 يونيو سنة 2005.

427- القانون رقم 06-01، المؤرخ في 20 فبراير 2006، المتعلق بالوقاية من الفساد ومكافحته ، الصادر في الج.ر.ج، عدد 14، مـؤرخة في 08 مارس 2006، الصـفحة 4، متمم بالأمر رقم 10-05 ممضي في 26 غشت 2010، الصادر بالج.ر.ج، عدد 50، مؤرخة في 01 سبتمبر 2010، الصفحة 16، القانون رقم 10-11 ممضي في 27 أكتوبر 2010، الصادر في الج.ر.ج، عدد 66 مؤرخة في 03 نوفمبر 2010، الصفحة 5، يتضمن الموافقة على الأمر رقم 10-05 الذي يتمم القانون رقم 06-01، المتعلق بالوقاية من الفساد ومكافحته، القانون رقم 11-15، يعدل ويتمم القانون رقم 06-01، المتعلق بالوقاية من الفساد ومكافحته، مؤرخ في 02 رمضان عام 1432، الموافق 02 غشت سنة 2011، الصادر في الج.ر.ج عدد 44، بتاريخ 10 غشت سنة 2011.

428- القانون 06-23، المؤرخ في 20 ديسمبر 2006، الذي يعدل ويتمم قانون العقوبات المعدل والمـتمم (الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966، الصادر في الج.ر رقم 84، المنشور بالج ر.ج عدد 49 مؤرخة في 11 يونيو 1966، الصفحة 702)، المنشور بالج.ر.ج بتاريخ 24 ديسمبر سنة 2006.

429- القانون رقم 09 – 04، المؤرّخ في 14 شعبان عام 1430، الموافق 5 غشت سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المنشور بالج.ر.ج العدد 47 بتاريخ 16 غشت سنة 2009، ص05.

430- الأمر رقم 11-03، المؤرخ في 20 ربيع الأول عام 1432 الموافق 23 فبراير سنة 2011، يعدل ويتمم القانون رقم 91-23، المؤرخ في 29 جمادى الأولى عام 1412 الموافق 6

ديسمبر سنة 1991، والمتعلق بمساهمة الجيش الوطني الشعبي في مهام حماية الأمن العمومي خارج الحالات الاستثنائية، المنشور في الج.ر.ج العدد 12، الصادرة في 23 فبراير سنة 2011.

431- القانون رقم 13-07، المؤرخ في 24 ذي الحجة عام 1434 هـ الموافق 29 اكتوبر سنة 2013، المتضمن تنظيم مهمة المحاماة، الصادر في الج.ر.ج عدد 04، بتاريخ 30 اكتوبر 2013، ص 03.

432- الأمر رقم 15-02 المؤرخ في 23 يوليو 2015 يعدل ويتمم الأمر رقم 66-156 المؤرخ في 8 يونيو 1966، والمتضمن قانون الإجراءات الجزائية، المنشور في الج.ر.ج العدد 40 بتاريخ 23 يوليو 2015.

433- القانون رقم 15-03، المؤرخ في 11 ربيع الثاني عام 1436 الموافق أول فبراير سنة 2015، المتعلق بعصرنة العدالة، المنشور بالج.ر.ج العدد 06، بتاريخ 10 فبراير سنة 2015.

434- القانون رقم 15-04، المؤرخ في 11 ربيع الثاني عام 1436 الموافق أول فبراير سنة 2015، الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، المنشور بالج.ر.ج عدد 6 مؤرخة في 10 فبراير 2015، ص 6.

435- القـانون رقم 16-02، المؤرخ في 19 يونيو سنة 2016، يـعدل ويتمم قانون العقوبات، المادة الثانية (02 تتم قانون العقوبات بثلاث مواد منها المادة 87 مكرر 12)، المنشور بالج.ر.ج العدد 37، المؤرخة في 22 يونيو سنة 2016.

436- القانون رقم 18-01، المؤرخ في 12 جمادى الأولى عام 1439 الموافق 30 يناير سنة 2018، يتمم القانون رقم 05-04 المؤرخ في 27 ذي الحجة عام 1425 هـ الموافق 06 فبراير سنة 2005، والمتضمن قانون تنظيم السجون وإعادة الإدماج الاجتماعي للمحبوسين، المنشور بالج.ر.ج العدد 05، الصادر في 30 يناير سنة 2018.

437- القانون رقم 18-04، المؤرخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018، الذي يحدد القواعد العـامة المتعلقة بالبريد والاتصالات الإلكترونية، الصادر في الج.ر.ج العدد 27، بتاريخ 13 مايو 2018، ص 03.

438- القــانون رقـم 18-05، المؤرخ في 24 شعبان عام 1439 الموافق 10 ماي سنة 2018، المتعلق بالتجارة الإلكترونية، المنشور بالج.ر.ج رقم 28، الصادرة يوم 16 ماي 2018.
439- القانون رقم 18-07، المؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الصادر في الج. ر.ج العدد 34، بتاريخ 10 يونيو 2018، ص 11.
440- الأمر رقم 20-01، المــؤرخ في 09 ذي الحجة عام 1441 المـوافق 30 يوليو سنة 2020، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 08 يونيو سنة 1966 والمتضمن قانون العقوبات، الصادرة في الج.ر.ج، العدد 44 المؤرخة في 30 يوليو سنة 2020.
441- القانون رقم 20-05، المؤرخ في 05 رمضان عام 1441 المـوافق 28 أبريل سنة 2020، المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما، الصادرة في الج.ر.ج رقم 25 المؤرخة في 29 أبريل سنة 2020.
442- القانون رقم 20-06، المؤرخ في 05 رمضان عام 1441 المـوافق 28 أبريل سنة 2020، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 08 يونيو سنة 1966 والمتضمن قانون العقوبات،الصادرة في الج.ر.ج رقم 25 المؤرخة في 29 أبريل سنة 2020.

ب- المراسيم الرئاسية:

443- المرسوم الرئاسي رقم 04-183، المؤرخ في 08 جمادى الأولى عام 1425 الموافق 26 يونيو سنة 2004، يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، المنشور في الج.ر.ج العدد 41، بتاريخ 27 يونيو سنة 2004.
444- المرسوم الرئاسي رقم 04-432، المؤرخ في 17 ذي القعدة عام 1425 الموافق 29 ديسمبر سنة 2004، يتضمن إنشاء المعهد الوطني للبحث في علم التحقيق الجنائي، المنشور بالج.ر.ج، العدد 84، بتاريخ 29 ديسمبر سنة 2004.

445- المرسوم الرئاسي رقم 08-151، المؤرخ في 20 جمادى الأولى علم 1429 الموافق 26 مايو سنة 2008، المتضمن إحداث مدرسة للشرطة القضائية تابعة للـدرك الوطني، المنشور بالج.ر.ج العدد 27، الصادر بتاريخ 28 مايو سنة 2008.

446- المرسوم الرئاسي رقم 09-143، المؤرخ في 2 جمادى الأولى عام 1430 الموافق 27 ابريل سنة 2009، يتضمن مهام الدرك الوطني وتنظيمه، الصادر في الج.ر.ج العدد 26، بتاريخ 03 مايو سنة 2009، ص 17.

447- المرسوم الرئاسي رقم 15-261، المؤرخ في 24 ذي الحجة عـام 1436 الموافق 8 أكتوبر سنة 2015، والذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المنشور بالج.ر.ج العدد 53 بتاريخ 08 أكتوبر 2015، ص 16، (ملغى).

448- المرسوم الرئاسي رقم 17-145، المؤرخ في 22 رجب عام 1438 الموافق 19 ابريل سنة 2017، المتضمن إحداث معهد الدراسات العليا في الأمن الوطني ومهامه وتنظيمه وسيره، المنشور بالج.ر.ج العدد 26، بتاريخ 23 ابريل سنة 2017.

449- المرسوم الرئاسي رقم 19-172، المؤرخ في 3 شوال عام 1440، الموافق 2 جوان سنة 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها، الصادر في الج.ر.ج العدد 37، المؤرخة في 09 جوان سنة 2019، (ملغى).

450- المرسوم الرئاسي رقم 19-278، المؤرخ في 21 صفر عام 1441 الموافق 20 اكتوبر سنة 2019، يتضمن مهام معهد الدراسات العليا في الأمن الوطني وتنظيمه وسيره، المنشور بالج.ر.ج العدد 65، بتاريخ 24 اكتوبر سنة 2019.

451- المرسوم الرئاسي رقم 20-05، المؤرخ في 24 جمادى الأول علم 1441 الموافق 20 جانفي سنة 2020، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، المنشور بالج.ر.ج العدد 04، بتاريخ 26 جانفي سنة 2020، ص 05.

ج- المراسيم التنفيذية والقرارات :

* المراسيم التنفيذيـــة:

452- المرسوم التنفيذي رقم 10-322، المؤرخ في 16 محرم عام 1432 الموافق 22 ديسمبر سنة 2010، المتضمن القانون الأساسي الخاص بالموظفين المنتمين للأسلاك الخاصة بالأمن الوطني، الصادر بالج.ر.ج العدد 78، بتاريخ 26 ديسمبر سنة 2010، ص 04.

453- المرسوم التنفيذي رقم 16-134، مؤرخ في 17 رجب عام 1437 الموافق 25 أبريل 2016، الذي يحدد تنظيم المصالح التقنية والإدارية للسلطة الوطنية للتصديق الإلكتروني وسيرها ومهامها، المنشور بالج.ر.ج عدد 26 مؤرخة في 28 أبريل 2016، الصفحة 6.

454- المرسوم التنفيذي رقم 20-61، المؤرخ في 20 رجب عام 1441 الموافق 15 مارس سنة 2020، المتضمن الموافقة على رخصة لإقامة واستغلال شبكة مفتوحة للجمهور للاتصالات الشخصية النقالة العالمية، عبر السواتل من نوع GMPCS، ولتوفير خدمات الاتصالات الإلكترونية للجمهور، الممنوحة على سبيل التنازل لشركة " اتصالات الجزائر الفضائية، شركة ذات أسهم"، وتجديدها، الصادر في الج.ر.ج العدد 17 المؤرخة في 28 مارس سنة 2020.

455- المرسوم التنفيذي رقم 20-62، المؤرخ في 20 رجب عام 1441 الموافق 15 مارس سنة 2020، المتضمن الموافقة على تجديد رخصة لإقامة واستغلال شبكة مفتوحة للجمهور، عبر الساتل V.SAT، ولتوفير خدمات الاتصالات الإلكترونية للجمهور، الممنوحة لشركة " اتصالات الجزائر الفضائية، شركة ذات أسهم"، الصادر في الج.ر.ج العدد 17 المؤرخة في 28 مارس سنة 2020.

* القرارات الوزارية:

456- القرار الوزاري المشترك، المؤرخ في 26 ربيع الأول عام 1428 الموافق 14 أبريل سنة 2007، يتعلق بتنظيم الأقسام والمصالح والمخابر الجهوية للمعهد الوطني للبحث في علم التحقيق الجنائي، المنشور بالج.ر.ج العدد 36 بتاريخ 03 يونيو سنة 2007، ص 14.

457- القرار الوزاري المشترك، المؤرخ في 28 ربيع الأول عام 1439، الموافق 17 ديسمبر سنة 2017، يحدد التنظيم الداخلي لهياكل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الصادر في الج.ر.ج العدد 14، المؤرخة في 04 مارس سنة 2018.

4- مناقشات المجلس الشعبي الوطني الجزائري:

458- المجلس الشعبي الوطني، الجلسة العلنية لمناقشة مشروع القانون المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي المنعقدة يوم الأربعاء 21 مارس 2018، الجريدة الرسمية للمناقشات (الفترة التشريعية الثامنة، الدورة البرلمانية العادية "2017-2018")، السنة الأولى رقم 52، الجزائر، الاحد 08 ابريل سنة 2018، ص 04.

459- المجلس الشعبي الوطني، السنة الثالثة رقم 122، الفترة التشريعية السادسة، الدورة العادية الرابعة، الجلسة العلنية المنعقدة يوم السبت 27 يونيو 2009، المنشور بالج.ر.ج للمناقشات، الجزائر، 06 يوليو سنة 2009، ص.ص: 21-22

5- قوانين دول أخرى:

460- أقر نظام مكافحة الجرائم المعلوماتية مجلس الوزراء في جلسته الأسبوعية يوم الاثنين 1428/03/07 هـ الموافق 2007/03/26، وصدر بموجب المرسوم الملكي رقم (م/17) بتاريخ 1428/3/8هـ.

461- المملكة الأردنية الهاشمية:

- قانون الجرائم الإلكترونية رقم 27 لسنة 2015 للمملكة الأردنية الهاشمية.
- قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية، الصادر بموجب المرسوم التشريعي رقم 17 لعام 2012، والصادر بموجب القرار رقم 290 بتاريخ 08 ماي 2012، والمتضمن التعليمات التوضيحية والتنفيذية، لقانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية.

- قانون مكافحة جرائم تقنية المعلومات رقم (63) لسنة 2015، الصادر يوم الأحد 12 يوليو 2015، العدد 1244.

462- قانون الإجراءات الجزائية اليمني: قرار جمهوري بالقانون رقم (13) لسنة 1994م، بشأن الإجراءات الجزائية اليمنية معدل ومتمم، الصادر في الج.ر رقم 19 ج 4 لسنة 1994.

463- نصوص قانونية لجمهورية مصر العربية:

- دستور جمهورية مصر العربية، الصادر في 17 ربيع أول 1435 هـ، الموافق 18 يناير 2014م.
- قـانون العقوبات المصري، معدل ومتمم.
- قانون الإجراءات الجنائية (طبقاً لأحدث التعديلات بالقانون 95 لسنة 2003)، الصادر بالقانون رقم 150 لسنة 1950.
- القانون رقم 10 لسنة 2003، الخاص بإصدار قانون تنظيم الاتصالات – المـصري–، الصادر في الجريدة الرسمية العدد 5 مكرر(أ)، في 04 فبراير سنة 2003، ص 03.
- القـرار الرئاسي رقم 276 لسنة 2014، بـشان الـموافقة على انضمام جمهورية مـصر العربية إلى الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الموقعة في القاهرة بتاريخ 21 ديسمبر 2010، الصادرة في الج.ر للجمهورية مصر العربية، العدد 46 الصادرة في 13 نوفمبر سنة 2014.
- الـقانون رقم 26 لسنة 2015، الصادر في الج.ر العدد 25 مكرر (ب) في 22 يـونيو سنة 2015، يعدل ويتمم أحكام قانون حماية الملكية الفكرية الصادر بالقانون رقم 82 لسنة 2002.
- قانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات، الصادر في الج.ر العدد 32 مكرر (ج) في 14 اغسطس سنة 2018، ص 03.
- القانون رقم 151 لسنة 2020، المتعلق بإصدار قانون حماية البيانات الشخصية، الصادر في الجريدة الرسمية المصرية، العدد 28 مكرر (هـ)، بتاريخ 15 يولية سنة 2020.
- قرار رئيس مجلس الوزراء رقم 1453 لسنة 2015، بإنـشأ مجلس أعلى للمجتمع الرقمي، الصادر في الج.ر العدد 24، بتاريخ 11 يونيو سنة 2015، ص 83.

- قــرار رئيس مجلس الوزراء رقم 994 لسنة 2017، الصــادر في الج.ر العدد 17 مكرر (ب)، بتاريخ 02 مايو سنة 2017، ص 02.

464- **نصوص قانونية للجمهورية التونسية:**

- قانون أساسي عدد 63 لسنة 2004، يتعلق بحماية المعطيات الشخصية، مؤرخ في 27 جويلية 2004، الصــادر بالــرائد الرسمي للجمهورية التونسية، بتاريخ 30 جويلية 2004، العدد 61، ص 2084.
- أمر عدد 3003 لسنة 2007، يتعلق بضبط طرق سير الهيئة الوطنية لحماية المعطيات الشخصية، مؤرخ في 27 نوفمبر 2007، الصادر بالرائد الرسمي للجمهورية التونسية، بتاريخ 30 نوفمبر 2007، العدد 96، ص 4214.
- أمر عدد 3004 لسنة 2007، يتعلق بضبط شروط وإجراءات التصريح والترخيص لمعالجة المعطيات الشخصية، مؤرخ في 27 نوفمبر 2007، الصادر بالرائد الرسمي للجمهورية التونسية، بتاريخ 30 نوفمبر 2007، العدد 96، ص4215.

465- **قوانين المملكة المغربية:**

- دستور المملكة المغربية: ظـهير شريف رقم 1.11.91، الخاص بتنفيذ الدستور، الصادر في 27 من شعبان 1432، الموافق 29 يوليو 2011، المنشور بالج.ر، العدد 5964 مكرر، السنة المائة، الصادرة في 30 يوليو 2011، ص 3600.
- القانون 03-07 القاضي بتتميم مجموعة القانون الجنائي في ما يتعلق بالجرائم المتعلقة بنظم المعالجة الآلية للمعطيات، الصادر بتنفيذ الظهير الشريف رقم 1.03.197 بتاريخ 16 رمضان 1424 الموافق 11 نوفمبر 2003، بالج.ر عدد 5171 بتاريخ 27 شوال 1424 الموافق 22 ديسمبر 2003، الصفحة 4284.
- ظهير شريف رقم 1.02.255 صادر في 25 من رجب 1423، المـوافق 03 أكتوبر 2002، الخاص بتنفيذ القانون رقم 22.01 المتعلق بالمسطرة الجنائية المغربية، الصادر في الج.ر عدد 5078 بتاريخ 30 يناير2003، ص 315، معدل ومتمم بالقانون رقم 32.18، الصادر بتنفيذه الظهير الشريف رقم 1.19.92 بتاريخ 5 ذي القعدة 1440، الموافق 8 يوليو 2019، الصادر في الج.ر عدد 6796 بتاريخ 18 يوليو 2019، ص 5036.

- ظهير شـريف رقم 1.02.255 صـادر في 25 من رجب 1423، الموافق 03 أكتوبر 2002، الخاص بتنفيذ القانون رقم 22.01 المتعلق بالمسطرة الجنائية المغربية، الصادر في الج.ر عدد 5078 بتاريخ 30 يناير2003، ص 315، معدل ومتمم بالقانون رقم 32.18، الصادر بتنفيذه الظهير الشريف رقم 1.19.92 بتاريخ 5 ذي القعدة 1440، الموافق 8 يوليو 2019، الصادر في الج.ر عدد 6796 بتاريخ 18 يوليو 2019، ص 5036.
- قانون المسطرة الجنائية المغربي،كما تم تعديله وتتميمه بمقتضى القانون رقم 23.05 والقانون رقم 24.05، الجريدة الرسمية عدد 5374 بتاريخ 28 من شوال 1426 (فاتح ديسمبر2005).
- القانون رقم 09-08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، الصادر بتنفيذه الظهير الشريف رقم 1.09.15، صادر في 22 من صفر 1430 الموافق 18 فبراير 2009، الصادر بالج.ر للمملكة المغربية، عدد 5711 بتاريخ 27 صفر 1430 الموافق 23 فبراير 2009، ص 552.
- مرسوم رقم 2.09.165، الخاص بتطبيق القانون رقم 09-08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، صادر في 25 من جمادى الأولى 1430 الموافق 21 ماي 2009، الصادر بالج.ر للمملكة المغربية، عدد 5744 بتاريخ 24 جمادى الأخيرة 1430 الموافق 18 يونيو 2009، ص 3571.
- مقرر للوزير الأول رقم 3.62.10، المتعلق بشان تنصيب اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي، صادر في 20 من رمضان 1431 الموافق 31 أغسطس 2010، الصـادر بالج.ر للـمملكة المغربية، عدد 5891 بتاريخ 08 ذو الحجة 1431 الموافق 15 نوفمبر 2010، ص 5007.
- ظهير شريف رقم 1.11.169، القاضي بتغيير وتتميم القانون رقم 22.01 المتعلق بالمسطرة الجنائية، صادر في 19 من ذي القعدة 1432 الموافق 17 اكتوبر 2011، بتنفيذ القانون رقم 35.11 الصادر في الج.ر رقم 5990 المؤرخة في 27 اكتوبر 2011، ص 5237.
- ظهير شريف رقم 1.14.85 صادر في 12 من رجب 1435 الموافق 12 ماي 2014، بتنفيذ القانون رقم 136.12 المـوافق بموجبه على اتفاقية الجرائم المعلوماتية، الموقعة ببودابست في

23 نوفمبر 2001 وعلى البروتوكول الإضافي لهذه الاتفاقية، المـوقع بسـتراسبوغ في 28 يناير 2003، الصـادر في الج.ر العدد 6260، السنة الثالثة بعد المائة، 29 ماي 2014.

ي)– الاجتهادات والأحكام القضائيـة:

466- حـكم محكمة النقض المصرية، في الطعن المقيد بجدول المحكمة رقم 3860 لسنة 57 القضائية، في الجلسة العلنية المنعقدة بدار القضاء العالي بمدينة القاهرة، في يوم الثلاثاء 14 يناير سنة 1988.

467- من أحكام المحكمة الدستورية العليا المصرية، لجلسة 18 مـارس سنة 1995، في القضية رقم 23 لسنة 16 قضائية"دستورية".

468- حكم محكمة النقض المصرية، في الطعن المقيد بجدول المحكمة رقم 27735 لسنة 72 القضائية، في الجلسة العلنية المنعقدة بدار القضاء العالي بمدينة القاهرة، في يوم 07 ديسمبر سنة 2003.

469- حكم محكمة النقض المصرية، في الطعن المقيد بجدول المحكمة رقم 13196 لسنة 76 القضائية، في الجلسة العلنية المنعقدة بدار القضاء العالي بمدينة القاهرة، في جلسة 18 مايو سنة 2006.

470- حكم محكـمة النقض المصرية، في الطـعن المـقيد بجدول المحكمة رقم 132 لسنة 78 القضائية، في الجلسة العلنية المنعقدة بدار القضاء العالي بمدينة القاهرة، جلسة 12 ابريل سنة 2014.

471- حكم محكمة النـقض المصرية، الـدائرة الجنـائية (دائـرة الثلاثاء (ج)، غرفة المشـورة)، في الـطعن المقيد بجدول المحـكمة رقم 18572 لسنـة 84 القضائيـة، في الجلسة العلنية المنعقدة بدار القضاء العالي بمدينة القاهرة، في يوم الثلاثاء 27 يناير سنة 2015.

472- حكم محكمة النقض المصرية، الدائرة الجنائية، في الطعن المقيد بجدول المحكمة رقم 15854 لسنة 84 القضائية، في الجلسة العلنية المنعقدة بدار القضاء العالي بمدينة القاهرة، في يوم الاثنين 23 فبراير سنة 2015.

473- حكم محكمة النقض المصرية، في الطعن المقيد بجدول المحكمة برقم 31330 لسنة 83 القضائية، في الجلسة العلنية المنعقدة بدار القضاء العالي بمدينة القاهرة، جلسة 05 مايو سنة 2015.

474- حكم محكمة النقض المصرية، الدائرة الجنائية" غرفة المشورة"، في الطعن المقيد بجدول المحكمة رقم 25992 لسنة 84 القضائية، في الجـلسة العلنية المنعقدة بدار القضاء العالي بمدينة القاهرة، في يوم الثلاثاء 01 سبتمبر سنة 2015.

475- حكم محكمة النقض المصرية، الدائرة الجنائية، في الطعن المقيد بجدول المحكمة رقم 24908 لسنة 84 القضائية، في الجلسة العلنية المنعقدة بدار القضاء العالي بمدينة القاهرة، في يوم السبت 10 اكتوبر سنة 2015.

476- حكم محكمة النقض المصرية، في الطعن المقيد بجدول المحكمة برقم 21819 لسنة 85 القضائية، في الجلسة العلنية المنعقدة بدار القضاء العالي بمدينة القاهرة، جلسة 03 ديسمبر سنة 2015.

477- حكم محكمة النقض المصرية، الدائرة الجنائية، في الطعن المقيد بجدول المحكمة رقم 37025 لسنة 85 القضائية، في الجلسة العلنية المنعقدة بدار القضاء العالي بمدينة القاهرة، في يوم الاربعاء 16 نوفمبر سنة 2016.

478- حكم محكمة النقض المصرية، الدائرة الجنائية، الخميس (ج)، في الطعن المقيد بجدول المحكمة رقم 29953 لسنة 86 القضائية، في الجـلسة العلنية المنعقدة بدار القضاء العالي بمدينة القاهرة، في يوم الخميس الأول من شعبان سنة 1438هـ الموافق 27 ابريل 2017.

479- حكم محكمة النقض، الدائرة الجنائية، في الطعن المقيد بجدول المحكمة برقم 29953 لسنة 86 القضائية، في الجلســة العلنية المنعقدة بــدار القــضاء العالي بمــدينة القاهرة، في يوم الخميس 28 من ابريل سنة 2017.

480- حكم محكمة النقض المصرية، الدائرة الجنائية، الأربعاء (أ)، في الطعن المقيد بجدول المحكمة رقم 29658 لسنة 86 القضائية، في الجلسة العلنية المنعقدة بدار القضاء العالي بمدينة القاهرة، في يوم الأربعاء 12 رمضان سنة 1438هـ الموافق 07 جوان 2017.

481- حكم محكمة النقض المصرية، الدائرة الجنائية، في الطعن المقيد بجدول المحكمة رقم 26463، لسنة 86 القضائية، في الجلسة العلنية المنعقدة بدار القضاء العالي بمدينة القاهرة، في يوم الأحد 22 أكتوبر سنة 2017.

482- حكم محكمة النقض المصرية، الدائرة الجنائية، في الطعن المقيد بجدول المحكمة رقم 8426 لسنة 87 القضائية، في الجلسة العلنية المنعقدة بدار القضاء العالي بمدينة القاهرة، في يوم السبت 04 نوفمبر سنة 2017.

483- حكم محكمة النقض المصرية، الدائرة الجنائية، الأربعاء (أ)، في الطعن المقيد بجدول المحكمة رقم 9680 لسنة 86 القضائية، في الجلسة العلنية المنعقدة بدار القضاء العالي بمدينة القاهرة، في يوم الأربعاء 03 رجب سنة 1439هـ الموافق 21 مارس 2018.

484- حكم محكمة النقض المصرية، الدائرة الجنائية، في الطعن المقيد بجدول المحكمة رقم 7843 لسنة 87 القضائية، في الجلسة العلنية المنعقدة بدار القضاء العالي بمدينة القاهرة، في يوم الأحد 20 يناير سنة 2019.

ك)- المواقع الإلكترونية الرسميـــة:

485- الموقع الرسمي للمجلس الشعبي الوطني الجزائري: http://www.apn.dz/ar/plus-ar/

486- موقع وزارة العدل للمملكة المغربية: https://www.justice.gov.ma/

487- الموقع الرسمي للمديرية العامة للأمن الوطني الجزائري: https://www.algeriepolice.dz/

ل)- المواقع الإلكترونيـــــة:

488- محمد على قطب، الجرائم المعلوماتية وطرق مواجهتها، مركز الإعلام الأمني، الأكاديمية الملكية للشرطة، بدون سنة نشر، المقال منشور على الموقع الإلكتروني الموالي: *http://www.policemc.gov.bh/mcms-store/pdf/ff7a6162-3aba_%D8%pdf*، والذي تم تصفحه في: 2016/05/15.

489- مركز هردو لدعم التعبير الرقمي *www.hrdoegypt.org*، *info@hrdoegypt.org* ، الجريمة الإلكترونية وحجية الدليل الرقمي في الإثبات الجنائي، القاهرة، 2013، بتصرف: وضع كلمة الإلكترونية بدل المعلوماتية.

490- محروس نصار غايب، الجريمة المعلوماتية، المعهد التقني، الانبار، العراق، الموقع الإلكتروني الموالي: http://www.iasj.net/iasj?func=fulltext&aId=28397، والذي تم تصفحه في: 2016/03/10.

491- بن دعاس فيصل، إشكالات الجريمة المعلوماتية في التشريع الجزائري، محاضرة في إطار التكوين المحلي المستمر للقضاة، مجلس قضاء قسنطينة، وزارة العدل، 2011/2010، ص 03 و04، الموقع الإلكتروني الموالي: https://courdeconstantine.mjustice.dz ، والذي تم الاطلاع عليه يوم: 2018/04/25.

492- لعوارم وهيبة، مشروعية الدليل الإلكتروني الناشئ عن التفتيش الجنائي، مجلة الفقه والقانون، العدد العشرون (20)، المغرب، يونيو 2014، ص 104، مجلة إلكترونية مديرها الدكتور: صلاح الدين دكداك، المجلة موجودة على الموقع الموالي: https://www.marocdroit.com/ تاريخ الاطلاع: 2020/06/13.

493- حسين بن سعيد الغافري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الإنترنت، متاح على الموقع الإلكتروني الموالي: http://previous.eastlaws.com/Uploads/Morafaat/33.pdf والذي تم تصفحه في 2018/07/30.

494- عبد الكبير الميناوي، لقاء بمراكش يتدارس إجراءات التعاون الدولي لمكافحة الجريمة المعلوماتية، دعا إلى اعتماد التقنيات الحديثة في التحقيق الجنائي والارتقاء بقدرات المحققين، جريدة الشرق الاوسط، العدد 14616، بتاريخ: 04 ديسمبر 2018، متاحة على الرابط الإلكتروني التالي: https://aawsat.com/home/article/1489666/، تاريخ الإطلاع: 2020/06/15.

495- عبد الفتاح محمود كيلاني، مدى المسئولية القانونية لمقدمي خدمة الإنترنت، ص509، على الموقع الإلكتروني الموالي: http://www.flaw.bu.edu.eg/flaw/imagesp والذي تم تصفحه في يوم 2016/10/24.

496- قانون الألفية الجديدة لحقوق طبع ونشر للمواد الرقمية (DMCA) هو تشريع سنه كونغرس الولايات المتحدة في أكتوبر 1998، معلومات من الموقع الإلكتروني لجامعة إنديانا الأمريكية: https://kb.iu.edu/d/alik

497- التوجـيه EC 31/2000 / الصادر عن البرلمـان والمجلس الأوروبي في 8 يونيو 2000، بشأن بعـض الجوانـب القانـونية لخدمـات مجتمع المعلومات، ولاسيما التجارة الإلكترونية، في السوق الداخلية، موجود على الموقع الإلكتروني الموالي والخاص بالمنظمة العالمية للملكية الفكرية (WIPO): *https://wipolex.wipo.int/ru/text/443174* .

498- نوار الطيب، إشكالية العوامل في جريمة القتل (الحلقة الأولى)، مجلة الشرطة، العدد 62، مارس 2001، متاح على الموقع الإلكتروني الموالي:

- *https:// www.dgsn.dz/IMG/pdf/4recherche-2.pdf*

499- فايزة بلال، الشروط الأساسية المتعلقة بالجريمة في نظام تسليم المجرمين، المجلة الجزائرية للقانون والعدالة، المقال على الموقع الإلكتروني المـوالي:

https*://crjj.mjustice.dz/sem_ar_crjj/revue1_2017p10.pdf*، والذي تم تصفحه في 2020/03/01.

500- عثمان بكر عثمان، المسئولية عن الاعتداء على البيانات الشخصية لمستخدمي شبكات التواصل الاجتماعي، كلية الحقوق، جامعة طنطا، القاهرة، 2016، بحث متاح على الموقع الإلكتروني الموالي: *http://law.tanta.edu.eg/files/conf4/* جلسة رابعة يوم ثاني/المسئولية عن الاعتداء على البيانات الشخصية، والذي تم الاطلاع عليه يوم: 2018/07/15.

501- أنفاس بريس، إستراتيجية المديرية العامة للأمن الوطني في محاربة الجرائم الإلكترونية، الأحد 10 نوفمبر 2019، بحث على الموقع الإلكتروني الموالي:

https://anfaspress.com/news/voir/57929-2019-11-10-04-48-49، تاريخ الاطلاع: 2019/12/27.

502- مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC)، كوفيد-19: تحليل التهديدات الإلكترونية، برنامج مكافحة الجرائم الإلكترونية بالمكتب الإقليمي للشرق الأوسط وشمال إفريقيا، 01 مايو 2020، على الموقع الإلكتروني الموالي: *https://www.unodc.org/documents/middleeastandnorthafrica/2020/COVID19/COVID19_MENA_Cyber_Report_AR2.pdf*، تاريخ الاطلاع: 2021/02/07.

ثانياً– المراجع الأجنبيـــــة:

I. Les Ouvrages :

503- Ali ElAZZOUZI, La cybercriminalité au Maroc, Bishops solutions, Casablanca, Maroc, Juin 2010.

504- Mohamed CHAWKI, Essai sur la notion de cybercriminalité, IEHEI, juillet 2006.

505- Rachid JANKARI, Les technologies de l'information au Maroc, en Algérie et en Tunisie, vers une filière euromaghrébine des TIC ?, vers une filière euromaghrébine des TIC, Etudes & Analyse, l'Institut de Prospective économique du Monde Méditerranéen, France, Octobre 2014.

506- Roberts, Kevin J, Cyber junkie, Printed in the United States of America, Published 2010.

II. Les Thèses :

507- Anmonka Jeanine-Armelle TANO-BIAN, La répression de la cybercriminalite dans les etats de L'UNION européenne et de l'Afrique de l'ouest, Thèse pour le Doctorat en Droit Public de l'Université de Paris Descartes, Jeudi 28 mai 2015.

508- Bouchelit Rym , « Les perspectives d'E-banking dans la stratégie E- Algérie 2013 », thèse de doctorat en sciences économiques, faculté des sciences économiques, Commerciales et de gestion, université Abou Bekr Belkaid, Tlemcen, 2014-2015.

509- Eric LAURENT-RICARD, Rétablir la confiance dans les messages électroniques , Le traitement des causes du "spam", Thèse de doctorat, école doctorale d'informatique, Université Panthéon-Assas, France, soutenue le 9 décembre 2011.

510- François Charlet**,** Responsabilité en droit d'auteur des intermédiaires : de l'hébergeur aux plateformes interactives, Mémoire en vue de l'obtention de la Maîtrise universitaire en Droit, criminalité et sécurité des technologies de l'information, Faculté de droit et des sciences criminelles, Université de Lausanne, Année académique, Université de Lausanne , 2011-2012.

511- LIANG Jiansheng, Criminalité informatique, Diplôme professionnel supérieur en Sciences de l'information et des Bibliothèques, Rapport de stage, Ecole Nationale Supérieure des Sciences de 1'information et des Bibliothèques, 1999.

512- Mira Carignan, L'origine géographique en tant que facteur explicatif de la cyberdélinquance, mémoire présenté à la faculté des études supérieures en vue de

l'obtention de M.SC.en criminologie, Université de Montréal Faculté des études supérieures, Septembre 2015.

III. Les Articles:

513- Adel Azzam Saqf Al-Hait, Jurisdiction in Cybercrimes: A Comparative Study, Journal of Law, Policy and Globalization, *www.iiste.org*, ISSN 2224-3240 (Paper) ISSN 2224-3259 (Online), Vol.22, 2014.

514- Bertrand Warusfel , Procédure pénale et technologies de l'information: de la convention sur la cybercriminalité à la loi sur la sécurité quotidienne, Revue droit et défense, Numéro 2002/1, (pp.17-22), France.

515- Brigitte Pereira, La lutte contre la cybercriminalité: de l'abondance de la norme à sa perfectibilité, Distribution électronique Cairn.info pour De Boeck Supérieur., Article disponible en ligne à l'adresse, 2016/3 t. XXX | pages 387 à 409, p : 408, sur le site : *https://www.cairn.info/revue-internationale-de-droit-economiq ue-2016-3-page-387.htm.*

516- Catherine CHABERT, Fiche pratique : RGPD (le règlement européen relatif a la protection des personnes physiques a l'égard du traitement des données a caractère personnel et a la libre circulation de ces données), Saint-Étienne Roanne, France, Rédigée en Avril 2017, Mise à jour en Juin 2018.

517- Chilstein David , Législation sur la cybercriminalité en France, Revue internationale de droit comparé, Vol. 62 N°2,2010. pp. 553-606, France, 2010.

518- David Bénichou, Cybercriminalité: jouer d'un nouvel espace sans frontière, La base de données juridique des Éditions Dalloz, France, AJ Pénal 2005.

519- Emilie Bailly, Emmanuel Daoud, Cybercriminalité et réseaux sociaux : la réponse pénale, La base de données juridique des Éditions Dalloz, France, AJ Pénal 2012.

520- François-Guillaume, La contrefaçon sur internet : nouvelles difficultés, nouveaux enjeux, La base de données juridique des Éditions Dalloz, France, AJ Pénal 2012.

521- John Ashcroft, Electronic Crime Scene Investigation:A Guide for First Responders, Written and Approved by the Technical Working Group for Electronic Crime Scene Investigation, Washington, July 2001.

522- Kristiina Milt, La protection des données à caractère personnel, Fiches techniques sur l'Union européenne - 2018 , Strasbourg, France, 06/2018.

523- Laurent Latapie, La responsabilité de l'hébergeur, lundi 4 juin 2018, article sur le site : *https://www .village-justice .com /articles/responsabilite-hebergeu r,28664.html.*

524- Laurent Latapie, La responsabilité de l'hébergeur, lundi 4 juin 2018, article sur le site : *https://www .village-justice .com /articles/responsabilite-heberg u r,28664.html.*

525- Maurizio De Arcangelis, La responsabilité des « fournisseurs d'hébergement » - Etude de droit comparé entre la France et l'Italie, http://www.droit-technologie .org, Date de mise en ligne :7 novembre 2001, p :17**.**

526- Michel Richardot, Interpol, Europol, Distribution électronique Cairn.info pour Le Seuil, France, 2002.

527- Myriam Quéméner, Concilier la lutte contre la cybercriminalité et l'éthique de liberté, Revue des directeurs sécurité d'entreprise (Club des Directeurs de Sécurité des Entreprises, Sécurité et stratégie), N°5, France, Mars 2011.

528- Myriam Quéméner, Les nouvelles dispositions de lutte contre la cybercriminalité issues de la loi du 13 novembre 2014 renforçant la lutte contre le terrorisme, La base de données juridique des Éditions Dalloz, France, AJ Pénal 2015.

529- Sizwe Snail , Cyber Crime in South Africa – Hacking, cracking, and other unlawful online activities, Journal of Information, Law & Technology (JILT), 28/05/2009.

IV. Conférence :

530- Anastasios Papathanasiou1, Alexandros Papanikolaou, and others, Legal and Social Aspects of Cyber Crime in Greece, Conference Paper, October 2014,p 10-11, On the website: https:// www. researchgate.net /publication /260390705 _Legal_and _Social _Aspects_of_Cyber_Crime_in_Greece.

531- BOUASRIA OMAR, lutte contre les atteintes aux systèmes de traitements automatisés de données à la lumière de la loi 09/04, les actes de la 14ème Conférence internationale sur la Cybercriminalité, Tripoli, Lebanon , 25 - 24 mars 2017.

532- Déclaration d' Alger relative a la création du mécanisme africain de coopération policière AFRIPOL، Conférence africaine des directeurs et inspecteurs généraux

de police sur AFRIPOL, Alger, les 10 et 11 fevrier 2014, p :01 , sur le site *: http://www.peaceau.org/ uploads /algiers -declaration-afripol-french.pdf.*

533- Déclaration de l'Algérie ،Segment Ministériel de la 62ème session de la Commission des Stupéfiants Vienne, 14 et 15 mars 2019, sur le site : *https ://www.unodc.org/documents/commissions/CND/2019/2019_MINISTERIAL_SEG MENT/19March/ALGERIA.pdf.*

V. Les rapports:

534- Aled Williams, EUROJUST News, Issue No. 5 -, Eurojust News is produced by Eurojust's Press & PR Service., Catalogue no: QP-AB-11-002-EN-C, ISSN: 1831-5623, EUROJUST, Maanweg 174, NL - 2516 AB The Hague December 2011, On the following website: *http:// www.eurojust.europa.eu/Practitioners/operational Child-protection/Pages/child-protection-at-eurojust.aspx;*

535- Comite européen de coopération juridique (CDCJ), L'UTILISATION DES PREUVES ELECTRONIQUESDANS LES PROCEDURES CIVILES ET ADMINISTRATIVESET SON =IMPACT SUR LES REGLES ET MODES DE PREUVE, Etude comparative et analyse Rapport préparé par Stephen MASON avec le concours de Uwe RASMUSSEN, Strasbourg le 27 juillet 2016, sur le site : *https://rm.coe.int/16807007ca*.

536- La Commission nationale de l'informatique et des libertés, 31e rapport d'activité 2010, Direction de l'information légale et administrative – Paris, 2011.

537- Marine vaLzer, La cybercriminalité et les infractions liées à l'utilisation frauduleuse d'internet éléments de mesure et d'analyse pour l'année 2014, Rapport de l'Observatoire national de la délinquance et des réponses pénales (l'ONDRP), France, juillet 2015, p:06 " En 2014.

538- Myriam Quéméner, Le rapport sur la cybercriminalité et la protection des internautes, La base de données juridique des Éditions Dalloz, France,,AJ Pénal 2014.

539- Office of the Inspector General, The Department of Justice, Audit of the Federal Bureau of Investigation's Philadelphia Regional Computer Forensic Laboratory Radnor, Pennsylvania, U.S, April 2015.

540- Pierre PEREZ, Jean DUCHAINE, La Commission Nationale de l'Informatique et des Libertés Principes de la protection des données à caractère personnel, École supérieure de l'éducation nationale, de l'enseignement supérieur et de la recherche (ESENESR), France, 2009 – actualisation : 2013.

541- Rapport explicatif, de la Convention sur la cybercriminalité (Budapest, 23.XI .2001), Série des traités européens - n° 185.

542- Société Financière de la Nef, RGPD - Notice d'information sur la Protection des Données Personnelles, France, Version du 05/06/2018, sur le site souvent : *https:// www.lanef.com/wp-content/uploads /2018 /06 /2018 _06_06_Notice-RGPD.pdf.*

543- Stéfan Lollivier et Christophe Soullez, La criminalité en France (L'activité des offices centraux de police judiciaire de la police et de la gendarmerie nationales), Rapport annuel 2015 de l'ONDRP, France, octobre 2015.

544- Sujit Raman, Chair, John P. Cronan, and athers, **Report of the** Attorney General Cyber-Digital Task Force, United States Department of Justice, Washington, July 2, 2018.

VI. Les textes juridiques :

1- Les conventions :

545- Conseil de l'Europe - Convention sur la cybercriminalité (STE n° 185) ; Budapest, 23.XI.2001, sur le site : https://rm.coe.int/168008156d.

VERSION CONSOLIDÉE DU TRAITÉ SUR LE FONCTIONNEMENT DE L'UNION EUROPÉENNE, sur le site *: https://eur-lex.europa.eu/resource .htm l?uri=cellar:88f94461-564b-4b75-aef7-c957de8e339d.0010.01/DOC3& format =PDF*

2- Les Lois :

546- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *https://www.legifrance.gouv.fr/affichTexte.do ?cidTexte=JORFTEX T000 000886460 .*

547- Loi n° 88-19 du 5 janvier 1988. relative à la fraude informatique (LOI GODFRAIN).

548- Code civil, Article 1366, Modifié par Ordonnance n°2016-131 du 10 février 2016 - art. 4 .

549- Code pénal français.

550- Code de procédure pénale français.

551- LOI n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, Modifie Loi n° 78-17 du 6 janvier 1978.

552- The Digital Millennium Copyright Act (DMCA) OF 1998 U.S. Copyright Office Summary, Pub. L. No. 105-304, 112 Stat. 2860 (Oct. 28, 1998), sur le site : *https://www.copyright.gov /legislation/dmca.pdf.*

3- Les décrets :

553- Décret n° 2000-405 du 15 mai 2000 portant création d'un office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (JORF 16 mai 2000) ; http://www.cil.cnrs .fr/CIL/spip .php ?article2661.

554- Décret n° 2006-580 du 23 mai 2006 portant publication de la Convention sur la cybercriminalité, faite à Budapest le 23 novembre 2001, JORF n°120 du 24 mai 2006 page 7568 texte n° 2, NOR: MAEJ06 30050DELI: *https://www.legifrance .gouv .fr/eli/decret/2006/5/23/MAEJ0630050D.*

555- Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé, «Agence nationale de la sécurité des systèmes d'information» , NOR: PRMD0914748D Version consolidée au 02 février 2020, sur le site : *https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT 000020 82821 2.*

556- DIRECTIVE 2000/31/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIl of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), in the web site : *https://wipolex.wipo.int/ru/text/443174*

557- https://codes.findlaw.com/us/title-18-crimes-and-criminal-procedure/18-usc-sect-2510.html, 18 U.S.C. § 2510 - U.S. Code - Unannotated Title 18. Crimes and Criminal Procedure § 2510. Definitions.

558- Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime (OJ L 63, 6.3.2002, p. 1). 2Council Decision 2003/659/JHA of 18 June 2003 amending Decision 2002 /1 87/JHA setting up Eurojust with a view to reinforcing the fight against serious

crime (OJ L 245, 29.9.2003, p. 44). 3Council Decision 2009/426/JHA of 16 De cember 2008 on the strengthening of Eurojust and amending Decision 2002 /18 7/ HA setting up Eurojust with a view to reinforcing the fight against serious crime (OJ L 138, 4.6.2009, p. 14).

559- REGULATION (EU) 2018/1727 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA, Official Journal of the European Union, L 295/138, 21.11.2018.

3- Les Décisions Judiciaires :

560- Cour de cassation, chambre criminelle, Audience publique du 7 février 2007, N° de pourvoi: 06-87753 , Bulletin criminel 2007 N° 37 p. 241, sur le site : *https://www .legifrance.gouv.fr/affichJuriJudi.do?idTexte =JURITEXT000017 637398.*

561- Cour de cassation , chambre civile 1, Audience publique du 19 juin 2008, N° de pourvoi: 07-12244 (Publié au bulletin), sur le site : *https://www.legifrance .gouv .fr/affichJuriJudi.do?oldAction=re .chJuriJudi&idTexte =JUR ITEXT0000190346 52&fastReqId=15 34992964&fastPos=2.*

562- Cour de cassation, chambre criminelle, Audience publique du 27 octobre 2009, N° de pourvoi: 09-82346 (Publié au bulletin).

563- Cour de cassation, chambre civile 1, Audience publique du 17 février 2011, N° de pourvoi: 09-13202 (Publié au bulletin), sur le site : *https://www.legifrance.gouv.fr /affichJuriJudi. do?old Action =rech JuriJu di&idTexte =JU R ITEXT0000236072 35 &fas tReqId=1534992 964&fastPos=1.*

564- Cour de cassation, chambre criminelle, Audience publique du 28 mars 2012, N° de pourvoi: 11-83012(Non publié au bulletin).

565- Cour de cassation, chambre criminelle, Audience publique du 23 avril 2013, N° de pourvoi: 13-82467, ECLI:FR:CCASS:2013:CR02491(Non publié au bulletin).

566- Cour de cassation, chambre criminelle, Audience publique du 24 avril 2013, N° de pourvoi: 12-80331, ECLI:FR:CCASS:2013:CR01858.

567- Cour de cassation, chambre criminelle, Audience publique du 6 novembre 2013, N° de pourvoi: 12-87130, ECLI:FR:CCASS:2013:CR05362 (Publié au bulletin).

568- Cour de cassation, chambre criminelle, Audience publique du 30 avril 2014, N° de

pourvoi: 13-88162, ECLI:FR:CCASS:2014:CR02211(Publié au bulletin).

4- Les Sites:

569- Bach Xuan Tran, et al, A study on the influence of internet addiction and online interpersonal influences on health-related quality of life in young Vietnamese, BMC Public Health, Published online 2017 Jan 31, sur le site: *https://www.ncbi .nlm.nih .gov/pmc /articles/PMC5282902/, view date: 18/09/2019.*

570- Danny Vena, «How Social Media Is Using AI to Fight Terrorism », The Motley Fool, 26 June 2017. In the web set :*https://www.fool.com/investing /2017/06/26/ how-social-media-is-using-ai-to-fight-terrorism.aspx*

571- Meriem ALI MARINA, Pour que le crime ne reste pas impuni, Police judicaire, *http://www.eldjazaircom.dz/index .php?id_rubrique=313&id _article =37 45* , N° 114 - Juin 2018.

572- Michael Fenichel, Ph.D., "Internet Addiction": Addictive Behavior, Transference or More?, in the web site *: http://www.fenichel.com/addiction.shtml*.

573- Vincent Lemoine Chef du Groupe Cybercriminalité de la B.R Nanterre Expert non inscrit, La Cybercriminalité (Les acteurs les infractions Cas concret et retour d'expérience), *http://www .andsi.fr/wp- content/uploads /2010/01/29, dapresention _andsi _091208.pdf.*

فـــــهرس المحتويـــــات

فـهرس الـمحتويات:

العنـــــــــــوان	الصفحة
اهـــــــــــداء	/
شكـر وعـــــرفان	/
قائمـــة المختصرات	/
مقدمـــــة	01
الفصل التمهيدي: **المضامين الفكرية للجريمة الإلكترونية والمجرم الإلكتروني**	06
المبحث الأول: **الإطار المفاهيمي للجريمة الإلكترونية.**	07
المطلب الأول: تعريف الجريمة الإلكترونية وبيان خصائصها.	08
الفرع الأول: تعريف الجريمة الإلكترونية.	09
الفرع الثاني: الجريمة الإلكترونية في التشريع الجزائري والمقارن.	11
الفرع الثالث: خصائص الجريمة الإلكترونية.	14
أولاً: خفاء الجريمة وسرعة ارتكابها.	14
ثانياً: اعتبارها أقل عنفا في التنفيذ.	15
ثالثاً: جريمة عابرة للحدود.	15
رابعاً: امتناع المجني عليهم عن التبليغ.	17
خامساً: سرعة محو الدليل وصعوبة الوصول إليه.	17
المطلب الثاني: محل الجريمة الإلكترونية.	19

الفرع الأول: المعلومات كمحل للجريمة الإلكترونية.	19
الفرع الثاني : الأجهـزة كمحل للجريمة الإلكترونية.	24
الفرع الثالث: الأشخاص أو الجهات كمحل للجريمة الإلكترونية	25
المبحث الثانـــي: **الإطار المفاهيمي للمجرم الإلكترونـــي.**	31
المطلب الأول: مفهوم المجرم الإلكتروني وسماتــه.	32
أولاً: الذكاء.	32
ثانياً: المعرفة والمهارة والخبرة.	32
ثالثاً: المجرم الإلكتروني إنسان اجتماعي.	33
رابعاً: المجرم الإلكتروني مجرم عائد للإجرام.	33
المطلب الثاني: دوافع ارتكاب المجرم الإلكتروني للجريمة الإلكترونية.	34
الفرع الأول: ارتكاب الجريمة الإلكترونية من أجل كسب المال.	34
الفرع الثاني: ارتكاب الجريمة الإلكترونية رغبة في التعلم وإثبات الذات.	35
الفرع الثالث: ارتكاب الجريمة الإلكترونية رغبة في الانتقام.	36
الفرع الرابع: دوافـع أخرى وراء ارتكاب المجرم الإلكتروني للجريمة الإلكترونية.	37
الباب الأول: **الآليات الإجرائية لمكافحة الجريمة الإلكترونية**	41
الفصل الأول: **آليات التحقيق الجنائي التقليدية المعتمدة لمكافحة الجريمة الإلكترونية**	44
المبحث الأول: **الدليل الإلكتروني وسلطة القاضي في تقديره**	46
المطلب الأول: مفهوم الدليل الإلكتروني.	46
الفرع الأول: تعريف الدليل الإلكتروني.	47

الفرع الثاني: أقسام الدليل الإلكتروني.	49
المطلب الثاني: شروط صحة الدليل الإلكتروني وسلطة القاضي في تقديره.	50
الفرع الأول: شروط صحة الدليل الإلكتروني.	51
الفرع الثاني: سلطة القاضي في تقدير الدليل الإلكتروني.	57
المبحث الثانـــي: **المعاينة والتفتيش ودورهما في جمع الأدلة الإلكترونية**	63
المطلب الأول: المعاينة في الجريمة الإلكترونية.	64
الفرع الأول: معاينة مسرح الجريمة الإلكترونية.	64
الفرع الثاني: الضوابط الواجب مراعاتها عند معاينة مسرح الجريمة الإلكترونية.	68
المطلب الثاني: التفتيش والضبط في مجال الجريمة الإلكترونية.	71
الفرع الأول: التفتيش في الجريمة الإلكترونية.	72
البند الأول: شروط إجراء عملية التفتيش في الجريمة الإلكترونية.	77
البند الثاني: التفتيش داخل وخارج الدولة.	93
الفرع الثاني: الضبط أو الحجز في الجريمة الإلكترونية.	101
البند الأول: الأشياء محل الضبط في الجريمة الإلكترونية.	107
البند الثاني: الاستعانة بالخبرة من أجل ضبط الأدلة الإلكترونية.	110
الفصل الثاني: **الآليات الإجرائية الحديثة المعتمدة للحصول على الدليل الإلكتروني.**	119
المبحث الأول: **اعتراض المراسلات وتسجيل الأصوات والتقاط الصور.**	121
المطلب الأول: اعتراض المراسلات.	123
المطلب الثاني: تسجيل الأصوات والتقاط الصور.	129
المبحث الثاني: **التسرب أو الاختراق.**	132

المطلب الأول: شروط التسرب.	135
المطلب الثاني: الحماية القانونية للمتسرب.	136
المبحث الثالث: دور مقدم الخدمات في كشف الجريمة الإلكترونية وجمع الأدلة الإلكترونية.	139
المطلب الأول: مقدم خدمة الإنترنت في القانون الوطني والمقارن.	140
المطلب الثاني: التزام مقدم خدمــة الإنترنت اتجـاه المحتوى غير المشروع.	143
الباب الثاني: الآليات المؤسساتية لمكافحة الجريمة الإلكترونية	154
الفصل الأول: المكافحة المؤسساتية الوطنية للجريمة الإلكترونية	156
المبحث الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.	157
المطلب الأول: تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.	159
المطلب الثاني: مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.	163
المبحث الثاني: السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي.	171
المطلب الأول: نشأة وتشكيلة السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي.	172
المطلب الثاني: مهام السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي.	173
المطلب الثالث: حماية البيانات الشخصية في التشريع الجزائري والمقارن.	176
المبحث الثالث: المنظومة الوطنية لأمن الأنظمة المعلوماتية.	181
المطلب الأول: المجلس الوطني لأمن الأنظمة المعلوماتية.	183
المطلب الثاني: وكالة أمن الأنظمة المعلوماتية.	184

المبحث الرابع: **وحدات الأمن الوطني المتخصصة في مكافحة الجريمة الإلكترونية.**	191
المطلـب الأول: الشرطـة الجزائرية ودورها في مكافحة الجريمـة الإلكترونية.	191
المطلب الثاني: الدرك الوطني ودوره في مكافحة الجريمة الإلكترونية.	200
الفصل الثاني: **آليات مؤسساتية خارجية لمكافحة الجريمة الإلكترونية.**	206
المبحث الأول: **المكافحة المؤسساتية الدولية والإقليمية للجريمة الإلكترونية.**	207
المطلب الأول: المكافحة الدولية للجريمة الإلكترونية.	208
الفرع الأول: المنظمة الدولية للشرطة الجنائية (الانتربول).	208
البند الأول: مهام المنظمة الدولية للشرطة الجنائية (الانتربول).	210
البند الثاني: دور الانتربول في مكافحة الجريمة الإلكترونية.	212
الفرع الثاني: التعاون الدولي ودوره في مكافحة الجريمة الإلكترونية.	214
البند الأول: الصعوبات التي تعيق التعاون الدولي في مكافحة الجريمة الإلكترونية.	215
البند الثاني: حلول للصعوبات التي تعيق التعاون الدولي في مكافحة الجريمة الإلكترونية.	220
البند الثالث: الدعوة لإنشاء محكمة جنائية دولية للجرائم الإلكترونية	239
المطلب الثاني: المؤسسات الإقليمية لمكافحة الجريمة الإلكترونية.	244
الفرع الأول: الآفريبول كمؤسسة إقليمية لمكافحة الجريمة الإلكترونية.	244
الفرع الثاني: اليوروبول والأوروجيست آليتين إقليميتين لمكافحة الجريمة الإلكترونية.	246
البند الأول: اليوروبول وكالة إقليمية لمكافحة الجريمة الإلكترونية.	247
البند الثاني: الأوروجيست كوكالة إقليمية لمكافحة الجريمة الإلكترونية.	250
المبحث الثاني: **الآليات المساعدة على مكافحة الجريمة الإلكترونية.**	254
المطلب الاول: الجمعيات كآلية مساعدة على مكافحة الجريمة الإلكترونية.	255

الفرع الأول: نماذج عن جمعيات مكافحة الجريمة الإلكترونية.	256
الفرع الثاني: دور جمعيات مكافحة الجريمة الإلكترونية في الحد منها.	258
المطلب الثاني: معالجة الإدمان من الإنترنت كآلية مساعدة على مكافحة الجريمة الإلكترونية.	261
الفرع الأول: سلبيات الإدمان على الإنترنت.	262
الفرع الثاني: آليات الحد من الإدمان على الإنترنت.	269
البند الأول: مراكز معالجة الإدمان على الإنترنت.	270
البند الثاني: حجب المواقع الإلكترونية.	271
البند الثالث: السوار الإلكتروني كآلية لمراقبة مدمني الإنترنت.	275
خاتمـــــــة.	277
قائمة المراجع.	283
فـــهرس الـمحتويات.	357
الملخـــــص.	364

المـــــــلخص

الملخص:

عرفت البشرية في الأزمنة القليلة الماضية مرحلة من التطور التكنولوجي خاصة المعلوماتي، والذي كثر معه استعمال الوسائل الإلكترونية المختلفة؛ التي عملت على تسهيل العديد من المسائل الحياتية، ولكن في المقابل ظهر معها نوع مستجد من الجرائم الخطيرة كالجرائم الإلكترونية؛ التي تعد من أشدها خطورة كونها تشكل تهديداً كبيراً على أمن الدول والمجتمعات معاً، الأمر الذي جعل منها إحدى مواضيع البحث العلمي القانوني، كونها تثير عدة إشكاليات تستوجب الوقوف عندها.

وما دراستنا هاته إلا نموذج عن تلك الدراسات، إذ تضمنت هذه الأطروحة مجموعة من الآليات القانونية التي سيكون لها دور كبير في مكافحة هذه الظاهرة الإجرامية، خاصة وأنها اشتملت على أهم ما تستلزمه تلك الآليات من قواعد وضوابط حتى تكون الأدلة الإلكترونية المبحوث عنها ذات دلالة ثبوتية أمام الجهات القضائية الناظرة في الجرائم الإلكترونية، وضمت أيضاً آليات عملياتية وطنية وإقليمية وكذا دولية، تساعد السلطات المختصة على ملاحقة مرتكبي الجرائم الإلكترونية وتسهل القبض عليهم، بالإضافة إلى آليات مساعدة على مكافحة الجريمة الإلكترونية، كالجمعيات ومراكز معالجة الإدمان على الإنترنت.

كلمات مفتاحية: جريمة إلكترونية، تطور معلوماتي، أدلة إلكترونية، آليات مكافحة.

Abstract :

In the past few times, mankind has known a stage of technological development, especially information, which has increased the use of various electronic means. Which has facilitated many life issues, but on the other hand, a new type of serious crime such as cybercrime appeared with it; Which is one of the most dangerous because it poses a great threat to the security of states and societies together, which made it one of the topics of legal scientific research, as it raises several problems that need to be addressed,

Our study of this is nothing but an example of those studies, as this thesis included a set of legal mechanisms Which will have a major role in combating this criminal phenomenon, especially as it included the most important rules and controls required by these mechanisms so that the electronic evidence searched for would have evidentiary evidence before the judicial authorities looking at cybercrime, and it also included national, regional and international operational mechanisms that help Competent authorities to pursue cybercrime perpetrators and facilitate their arrest, in addition to mechanisms to help combat cyber crime, such as associations and Internet addiction treatment centers.

Key words: Electronic Crime, Information Development, Electronic Evidence, Control Mechanisms.