الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة محمد بوضياف - المسيلة

كلية الحقـــوق والعلـــوم السياسية
قسم الحقوق
رقم: .....

ميدان: الحقـــوق والعلـــوم السياسية
فرع: الحقوق
تخصص: قانون جنائي

مذكرة مقدمة لنيل شهادة الماستر أكاديمي

إعداد الطالب: أسامة مهمل

تحت عنوان

الإجرام السيبيراني

لجنة المناقشة:

د/ حسين العيساوي	جامعة محمد بوضياف - المسيلة	رئيســا
د/ الطيب بالواضح	جامعة محمد بوضياف - المسيلة	مشرفا ومقررا
د/ محمـد قسمية	جامعة محمد بوضياف - المسيلة	مناقشا

السنة الجامعية: 2018/2017

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي

جامعة محمد بوضياف– المسيلة
كلية الحقوق و العلوم السياسية
قسم الحقوق

Université Mohamed Boudiaf M'sila
Faculté de Droit et de sciences politiques
Département de Droit

إذن بالطبع والإيداع

الأستاذ الطيب بالواضح

وبعد الاطلاع على مذكرة الطالب مهمل أسامة

المعنونة بـ: الإجرام السيبراني

المقدمة لنيل شهادة الماستر تخصص قانون جنائي

تأكدنا من توفر الشروط العلمية الموضوعية والشكلية، وأذنا له بطبع المذكرة وإيداعها قصد مناقشتها.

التاريخ 2018/05/10

الأستاذ المشرف

الـجمهـورية الجـــزائرية الديمـــقراطـية الشـــعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
جامعة محمد بوضياف – المسيلة
Université Mohammed Boudiaf – M'sila
كلية الحقوق والعلوم السياسية
Faculté de Droit et des Sciences Politiques

تصريح باحترام الأمانة العلمية

أنا الموقع أدناه الطالب

الاسم واللقب: أسامة مهمل

رقم التسجيل: 02489932

التخصص: قانون جنائي

مقدم مذكرة التخرج العنوان: الإجرام السيبراني

تحت إشراف الأستاذ: الطيب بالواضح

أصرح بأن ما اشتملت عليه هذه المذكرة هو نتاج جهدي الخاص، وقد احترمت الأمانة العلمية، وفقا للأصول المنهجية المتبعة، حيث راعيت الدقة في نقل الأفكار والإشارة إلى المراجع التي استقيت منها المعلومات.

وأن هذه المذكرة في مجملها أو أي جزء منها لم تقدم من قبل كبحث علمي لدى أي مؤسسة تعلمية أو بحثية أخرى.

وأتحمل كامل المسؤولية في حال ثبوت ما ينافي هذا التصريح.

التاريـــخ: 2018/05/10

التوقيـــع


بسم الله الرحمن الرحيم

إهداء

إلى من أمدني بالحب والنصح والتوجيه، إلى من ضحى من أجلي، وتعب من أجل أن أنجح في دراستي، إلى من لا أقدر على رد ولو جزء صغير من تضحياته إلى والدي حفظه الله وأطال بعمره.

إلى أغلى ما رأت عيناي في الوجود، إلى الصدر الدافئ الذي ضمني في أفراحي وأحزاني، إلى أعذب نبع حنان، إلى والدتي أبقاها الله وأطال بعمرها.

إلى أخواتـــي (أسماء، سارة، مريم)، وجميع أفراد عائلتي وأقاربي.

إلى كل أساتذة كلية الحقوق والعلوم السياسية بجامعة محمد بوضياف بالمسيلة.

إلى كل أساتذة كلية الحقوق والعلوم السياسية بجامعة محمد البشير الإبراهيمي ببرج بوعريريج.

إلى كل من ساعدني في إتمام هذه المذكرة.

إلى كل أصدقائي وزملائي.

أهدي هذا العمل المتواضع

شكر وعرفان

تصديقا لقوله تعالى في محكم التنزيل " لَئِن شَكَرْتُمْ لَأَزِيدَنَّكُمْ " أسجد لله عز وجل على نعمة العلم والتعلم وعلى توفيقه لي في إعداد هذا البحث، فله الحمد والشكر كما ينبغي لجلال وجهه وعظيم سلطانه.

ولا يسعني إلا أن أتقدم بالشكر الجزيل إلى من كان مثلا في التواضع، إلى أستاذي العزيز **الدكتور الطيب بلواضح** الذي أمدني بالنصح والتوجيه، إلى من أعتز به مشرفا على هذه البحث المتواضع، إليه أتقدم بالشكر الجزيل.

كما أتوجه بالشكر الجزيل إلى السادة أعضاء لجنة المناقشة، **الدكتور حسين العيساوي** و**الدكتور محمد قسمية** على تكرمهم وقبولهم مناقشة هذه المذكرة.

ولا أنسى من كانت بحق مثلا يقتدى به في نشر العلم، إلى من كنت أحب كثيرا دروسها، إلى أستاذتي الغالية الدكتورة فريدة بن يونس، أتوجه إليها بهذا الشكر.

ولا يفوتني أن أنحني تقديرا للقاضي الدكتور الطيب سماتي، والأستاذ رفيق زاوي لما بذلوه معنا من جهد، وإمدادهم لنا بالمراجع القيمة، حفظهما الله وسدد خطاهما.

إلى كل هؤلاء أنحني إنحناءة شكر وتقدير، وأرجوا أن أوفق في مذكرتي لأرد لهم ولو جزءا صغيرا من حسن صنيعهم.

قائمة المختصرات

- ق.إ.ج: قانون الإجراءات الجزائية.
- ق.ع: قانون العقوبات.
- المشرع: المشرع الجزائري.
- القانون: القانون الجزائري.
- ج ر: الجريدة الرسمية.
- المادة *&/: المادة * الفقرة &.
- ص: الصفحة.

مقدمة

مقدمة

ساهم التقدم التكنولوجي والأنترنت في التطور المذهل لوسائل الإعلام والإتصال في العالم على جميع الأصعدة والمستويات، الأمر الذي أدى إلى إفراز نوع جديد من الجرائم وهي ما إصطُلح عليها بالجرائم السيبرانية، وقد بدت النصوص الجزائية التقليدية قاصرة عن ملاحقة هذا النوع من الجرائم، ذلك أن التشريع وليد الحاجة.

بدأ المجتمع الدولي في تنظيم تشريعات لمواجهة هذا النوع الجديد من الجرائم الذي ظهر مصاحبا لإستخدام الحاسب الآلي، وإنَّ ثمة تباين كبير بشأن المصطلحات المستخدمة للدلالة على هذه الظاهرة الإجرامية الناشئة في العالم الإفتراضي.

لم تتطرق التشريعات العربية إلى جرائم الحاسب الآلي إلا فيما ندر، ولعل السبب في ذلك أن ثورة الحاسب الآلي في البلدان العربية حديثة النشأة، لأن الإعتماد على تطبيقات الحاسب الآلي فيها بدأ في نهاية العقد الأخير من القرن الماضي، على عكس البلدان الغربية التي إعتمدت الحاسب الآلي منذ عقدين من الزمن أو أكثر.

الجزائر على غرار باقي الدول تشهد حركة متسارعة في مجال الإجرام السيبراني الإلكتروني، خاصة أمام الإستعمال الواسع لشبكة الأنترنت وضعف المراقبة والمتابعة الدورية لإستخدامها، مما يزيد من فُرص قيام هذه الجرائم.

وحرصا من المشرع على التصدي للجريمة السيبرانية، قام بإستحداث آليات إجرائية تتناسب وطبيعة هذه الجريمة، نظرا لعجز الإجراءات التقليدية في مواجهة هذا النوع من الجرائم التي تتميز بالتطور المستمر.

أسباب إختيار الموضوع

ترجع أسباب إختيار موضوع " الإجرام السيبراني " إلى الرغبة في التعرف على هذا النوع الجديد من الجرائم، التي تنتشر اليوم بصورة واسعة وتتفاقم داخل المجتمع الجزائري هذا من جهة، ومن جهة أخرى الفضول لمعرفة الآليات المرصودة لمكافحة مثل هذه الجرائم سواء الدولية منها أو الوطنية.

بالإضافة إلى أن هذا الموضوع مازال محل دراسة وبحث نظرا للتطور التكنولوجي المستمر وتطور إستخدامات الأنترنت كذلك.

أهمية الموضوع

إن أهمية هذا البحث تكمن أساسا في محاولة إعطاء نظرة حول المستجدات الإجرامية في عصر الأنترنت داخل المجتمع الجزائري، وتحديدا حول ما إصطُلح عليه بالإجرام السيبراني.

أهداف الموضوع

يهدف هذا البحث إلى محاولة التعريف بالجريمة السيبرانية وتحديد أنواعها، مع الإشارة إلى المخاطر المترتبة عنها، وفي نفس السياق لابد من التَعرُّف على الآليات الدولية والوطنية المقررة لمكافحة الجرائم السيبرانية، ومدى كفاية القوانين الحالية لمواجهتها.

الإشكالية

إنطلاقا مما سبق يمكن طرح الإشكالية التالية:

- ما هي الإستجابات الجزائية للمشرع الجزائري والهيئات الدولية لمراقبة الأنظمة الإلكترونية وضمان حماية المستخدمين، وهل التدابير والإجراءات المتاحة كفيلة بمواجهة خطر الجرائم السيبرانية؟

المنهج المتبع

من خلال دراسة الإجرام السيبراني وبهدف توضيح موضوع البحث تمت معالجة الإشكالية المطروحة وفق المنهج التحليلي أساسا وذلك بتحليل مختلف النصوص المتعلقة بالجريمة السيبرانية مع الإعتماد على المنهج المقارن في بعض المواطن حيث يمكن إجراء مقارنة حول تصنيف الجريمة السيبرانية في بعض التشريعات، وكذا الآليات المعتمدة في مكافحتها.

الدراسات السابقة

إن البحث في موضوع الإجرام السيبراني يتميز بوفرة المراجع حول هذا الموضوع حيث تم التطرق إليه ومعالجته في العديد من الرسائل ومذكرات الماجيستير فيما يُصطلح عليه بالجرائم الإلكترونية أو الجرائم المعلوماتية.

ولقد تم الإعتماد على البعض منها في إعداد هذا البحث، وبالخصوص في تحديد مختلف التعاريف الفقهية والخصائص المميزة للجريمة السيبرانية والمجرم السيبراني، من بين هذه الدراسات نذكر:

- كتاب بعنوان جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، لمؤلفه الدكتور علي جعفر، حيث بَيَّن من خلاله الأحكام العامة لجريمة تقنية المعلومات ومختلف تقسيمات الجريمة السيبرانية بالنظر لآراء فقهاء القانون الجنائي.
- كتاب بعنوان الجرائم المعلوماتية للدكتور أحمد خليفة الملط، يتحدث فيه عن مختلف صور الجريمة السيبرانية، كجرائم الإعتداء على المال المعلوماتي، وجرائم الغش المعلوماتي، جريمة إتلاف المعلومات وغيرها.
- مذكرة ماجيستير، بعنوان الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والمقارن، من إعداد عبد اللطيف معتوق، حيث بين موقف مختلف التشريعات العربية والأوروبية إتجاه الجريمة السيبرانية.

خطة الدراسة

بهدف الإجابة على إشكالية البحث قُسم موضوع الدراسة إلى فصلين، حيث جاء في الفصل الأول ماهية الإجرام السيبراني والذي من خلاله تم التطرق إلى تعريف الجريمة السيبرانية إضافة إلى خصائصها وصورها وسمات مرتكبها، ثم يأتي بعد ذلك الفصل الثاني تحت عنوان آليات مكافحة الإجرام السيبراني على الصعيدين الدولي والوطني، وأخيرا خاتمة تضمنت أهم النتائج والتوصيات التي خلص إليها البحث.

الفصل الأول

الفصل الأول

ماهية الإجرام السيبراني

إن البحث في موضوع الإجرام السيبراني يَستلزم بالضرورة تحديد مختلف المفاهيم والمصطلحات الدالة عليه، ثم التطرق إلى التطور التاريخي لهذه الجريمة، حيث يعتبر الخطوة الأولى لتوضيح الخصائص المميزة لها ولِسمات مُرتكبيها (المبحث الأول)، مرورا إلى تِبيان الصور المتعددة التي تأخذها الجريمة السيبرانية فقهًا وتشريعًا (المبحث الثاني).

المبحث الأول: مفهوم الإجرام السيبراني

لقد تغيرت أساليب إرتكاب الجريمة، فلم تَعد الإعتداءات تَستهدف المال والنفس فقط، بل مسَّت حتى المعلومات في البيئة الرقمية، حيث أصبح بإمكان المجرمين العصريين إرتكاب أبشع الجرائم في هدوءٍ تام، دون إراقةٍ للدِّماء، بل وحتى دون الإنتقال من أماكنهم [1]، هذا الأسلوب الجديد لإرتكاب الجريمة هو ما يُصطلح عليه بالإجرام السيبراني، ومن أجل فهم هذه الجريمة تم إعطاء تعريف لها، مع عَرضٍ مُوجز للمراحل الزمنية التي مَرّت بها (المطلب الأول) وصولا إلى تحديد مميزات هذه الجريمة عن بقية الجرائم الأخرى، والصفات الخاصة التي يمتاز بها مرتكبوها (المطلب الثاني).

المطلب الأول: تعريف الجريمة السيبرانية وتطورها التاريخي

أُطلقت على الجريمة المرتكبة بواسطة الأنترنت عدة تسميات مختلفة تماشيا مع تطورها الزمني، ولقد عرَّفها الفقه الجنائي بِعدةِ تَعاريف وِفقًا لأُسس مُختلفة، كما عَرَّف المشرع الجزائري أيضا هذا النوع من الجرائم (الفرع الأول)، ولكون الجرائم السيبرانية تتسم بالتطور المستمر، وجب التطرق إلى مختلف المراحل الزمنية لتطورها، والمرتبطة أساسا بتطور تكنولوجيا المعلومات والأنترنت (الفرع الثاني).

(1) سميرة معاشي، " ماهية الجريمة المعلوماتية "، مجلة المنتدى القانوني، جامعة محمد خيضر ببسكرة، العدد السابع، أفريل 2010، ص 275-276.

الفرع الأول: تعريف الجريمة السيبرانية

إن الإجرام السيبراني هو أحد النتائج السلبية التي خلّفها التطور التكنولوجي، وقد أخذت هذه الظاهرة الإجرامية [1] التي فرضت نفسها على المجتمع [2]، حيزا كبيرا من الدراسات من أجل تحديد مفهومها [3]، حيث نجد أن العديد من الأعمال الأكاديمية حاولت وضع تعريف للجريمة المرتكبة عبر الأنترنت [4]، هذه الأخيرة تعد من بين الجرائم التي تباينت تسمياتها عبر المراحل الزمنية لتطورها، والتي إرتبطت بتطور تقنية المعلومات، فقد إصطُلح على تسميتها في بادئ الأمر "بإساءة إستخدام الكمبيوتر"، ثم "جرائم إحتيال الكمبيوتر"، "فالجريمة المعلوماتية" بعدها "جرائم الكمبيوتر" و"الجريمة المرتبطة بالكمبيوتر"، ثم "جرائم التقنية العالية" إلى "جرائم الهاكرز" "فجرائم الأنترنت"، وأخيرا "السيبر كرايم Cyber Crime" [5].

وقبل الخوض في تعريف الفقهاء للإجرام السيبراني، لابدّ من الإشارة إلى المصطلحات التي يأخذ بها القانون الدولي، فمن خلال مصطلح القانون السيبراني Cyber Law، والذي يقصد به القانون الذي يطبق على كل السلوكات التي تتم داخل الفضاء الإلكتروني ، حيث يصبح كل من القانون والأنترنت في رواق واحد، نجد على سبيل المثال مصطلح Cyber behavoir الذي يدل على سلوكيات القانون المدني، ومصطلح Cyber Justice ويعني العدالة السيبرانية، كذلك Cyber Tribunal للدلالة على المحاكمات التي تتم عبر الأنترنت، Cyber Investigation ويعني الإجراءات الجنائية في إطار قانون الأنترنت .... الخ [6].

---

(1) إبتسام حمديني، " أسلوب التحقيق في الجرائم الإلكترونية كآلية لمكافحتها "، مداخلة مقدمة ضمن فعاليات الملتقى الدولي الذي نظمته كلية الحقوق والعلوم السياسية قسم الحقوق جامعة برج بوعريريج، الموسوم بعنوان: الإجرام السيبراني المفاهيم والتحديات، يومي 11 و12 أفريل 2017، ص 02.

(2) علي جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، الطبعة الأولى، منشورات زين الحقوقية، بيروت، 2013، ص 02.

(3) إبتسام حمديني، المرجع السابق، ص 02.

(4) ذياب موسى البداينة، " الجرائم الإلكترونية المفهوم والأسباب "، ورقة علمية مقدمة في الملتقى العلمي الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، خلال الفترة من 02-04 سبتمبر 2014، كلية العلوم الإستراتيجية، الأردن، 2014، ص 05.

(5) ياسمينة بونعارة، " الجريمة الإلكترونية "، مجلة المعيار، جامعة الأمير عبد القادر كلية أصول الدين، المجلد الثاني، العدد 39، جوان 2015، ص 03.

(6) عبد العال الدريبي ومحمد صادق إسماعيل، الجريمة الإلكترونية، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2012، ص 32.

إنطلاقا مما سبق ذكره، يتضح أن المقصود من مصطلح الإجرام السيبراني Cyber Crime، هو السلوكيات المجرمة التي تتم داخل العالم الإفتراضي، والتي تخضع للقانون الجنائي، وهو السبب الرئيسي والدافع لإستخدام مصطلح الجريمة السيبرانية في هذا البحث.

وبالعودة إلى تعريف الفقهاء للإجرام السيبراني، يعتبر عدم إستقرارهم على مصطلح واحد للدلالة على الجريمة المرتكبة عبر الإنترنت، من بين الصعوبات الواردة على دراستها [1]، فالحداثة التي تتميز بها هذه الأخيرة، إضافة إلى الإختلاف في النظم الثقافية والقانونية للدول، نتج عنهما عدم وضع تعريف موحد لهذه الظاهرة الإجرامية [2]، وذلك خشية حصرها في مجال ضيق يضر بها [3]، إذ نجد أن فقهاء القانون الجنائي قد إنقسموا إلى أربعة إتجاهات، لكل إتجاه أُسسه المختلفة التي يعتمدها ويرتكز عليها في تعريفه للجريمة السيبرانية [4] وهي كالآتي:

أولا: التعريف القائم على أساس محل الجريمة

يرتكز أصحاب هذا الإتجاه على وسيلة إرتكاب الجريمة، طالما أن وسيلة إرتكاب الجريمة هي الكمبيوتر أو إحدى وسائل التقنية الحديثة المرتبطة به، فتعتبر الجريمة من ضمن جرائم الأنترنت [5]، حيث يضيق أنصار هذا الإتجاه من نطاق هذه الجريمة، ويَحصُرونها في الحالات التي تمس مكونات الحاسوب غير المادية، كالبرامج والبيانات والمعطيات المخزنة في ذاكرته [6]، ومن ذلك نجد تعريف مكتب تقييم التقنية في الولايات المتحدة الأمريكية حيث يرى بأنها " الجرائم التي تَلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا " [7].

وعرَّفها البعض الآخر بصياغة أخرى وهي: تلك الجرائم الناتجة عن إستخدام التكنولوجيا والتقنية الحديثة المتمثلة في الكمبيوتر والأنترنت، بأعمال وأنشطة إجرامية تهدف إلى تحقيق عوائد

(1) يوسف صغير، الجريمة المرتكبة عبر الأنترنت، مذكرة ماجستير، جامعة مولود معمري بتيزي وزو، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2012-2013، ص 07.

(2) إبتسام حمديني، المرجع السابق، ص 03.

(3) أحمد خليفة الملط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية، 2006، ص 83.

(4) إبتسام حمديني، المرجع السابق، ص 03.

(5) يوسف صغير، المرجع السابق، ص08.

(6) عبد العال الديربي ومحمد صادق إسماعيل، المرجع السابق، ص 42.

(7) المرجع نفسه.

ضخمة جراء أعمال غير شرعية، يعاد ضخها في الإقتصاد الدولي عبر شبكة الأنترنت بإستخدام النقود الإلكترونية (*) أو بطاقات السحب التي تحمل أرقاما سرية للشراء عبر الأنترنت، أو تداول الأسهم وممارسة الأنشطة التجارية عبر هذه الشبكة (1).

يَردُّ في هذا الإطار الأستاذ فاندرسون R. Fanderson على واضعي هذا التعريف بقوله: " ليس لمجرد أن الحاسب قد إستخدم في الجريمة، أن نعتبرها من جرائم الأنترنت " والحجة التي إعتمدها في نقده، مفادها أنه لا يُمكن وضع تعريف لهذا النوع من الجرائم دون الرجوع إلى العامل الأساسي المكون لها، وأن الإعتماد فقط على الوسائل المستخدمة لتحقيقها، لا يكفي لإعتبار مجرد إستخدام الحاسب الآلي في الجريمة أنها من جرائم الإنترنت (2).

ثانيا: التعريف القائم على أساس المعرفة والتحكم في التكنولوجيا

يستند أنصار هذا الإتجاه إلى معيارٍ شخصي، إذ يجب أن يكون القائم بهذه الجرائم مُلِمًا وعارفا بتقنية المعلومات (3)، ومن قبيل هذه التعاريف نجد التعريف الذي أتى به الأستاذ ديفيد تومبسون David Tompson للجريمة المرتكبة عبر الأنترنت بأنها " أي جريمة يكون متطلبا لإقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب " (4)، كما قدم الفقيه ستين سكيولبيرج Stein Schiolberg تعريفه لجرائم الحاسب بقوله: " أي فعل غير مشروع تكون المعرفة بتقنية المعلومات

(*) النقود الإلكترونية: وهي ما يُصطلح عليها بالبيتكوين Bitcoin، وهي عُملة إلكترونية يمكن مقارنتها بالعملات الأخرى كالدولار أو اليورو، لكن مع وجود فارقين أساسيين بينهما، الأول هو أن هذه العملة هي عملة إلكترونية بشكل كامل يتم تداولها عبر الأنترنت فقط وليس لها أي وجود مادي، كما لا توجد هيئة تنظيمية مركزية تقف خلف هذه العملة، ومع ذلك يمكن إستخدامها في عملية الشراء كأي عملة أخرى، بل وحتى يمكن تحويلها إلى عملات تقليدية.

أنظر موقع ويكيبيديا مقال بعنوان بيتكوين، https://ar.wikipedia.org، أطلع عليه بتاريخ 14 أفريل 2018.

(1) عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والإنترنت، منشورات الحلبي الحقوقية، بيروت، 2007، ص15.

(2) يوسف صغير، المرجع السابق، ص 10.

(3) رحيمة نميلي، " خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة "، مداخلة مقدمة في أعمال المؤتمر الدولي الرابع عشر، طرابلس، الموسوم بعنوان: الجرائم الإلكترونية طرابلس، يومي 24 و25 مارس 2017، ص 05.

(4) هشام محمد فريد رستم، " الجرائم المعلوماتية أصول التحقيق الجنائي الفني واقتراح إنشاء آلية حربية موحدة للتدريب التخصصي"، بحوث مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات المتحدة كلية الشريعة والقانون، الطبعة الثالثة (المجلد الثاني)، 2004، ص 407.

أساسية لمرتكبه والتحقيق فيه وملاحقته قضائيا " [1]، ولقد أخذت وزارة العدل الأمريكية بهذا التعريف في التقرير الصادر عنها سنة 1989 والمتعلق بجرائم الأنترنت [2].

حسب منظور أصحاب هذا التعريف، لابد من توفر سمات شخصية لدى مرتكب هذه الجريمة، والمحصورة أساسا في الدراية والمعرفة التقنية.

ثالثا: التعريف المرتكز حول موضوع الجريمة

يرى أصحاب هذا الإتجاه أن الجريمة السيبرانية ليست التي يكون الحاسب أداة إرتكابها، بل هي التي تقع عليه أو في نِظامه، ومن نماذج مسايرة هذه الفكرة تعريف الفقيه روزنبلات Rosenblatt وبعض الخبراء الآخرين، حيث يُعرِّفون الجريمة السيبرانية بأنها " نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تُحوَّل عن طريقهِ "، ومن نفس المنظور يعرفها البعض بأنها غش معلوماتي ينصرف إلى كل سلوك غير مشروع يتعلق بالمعلومات المعالجة ونقلِها [3].

رابعا: التعريف القائم على أساس الجمع بين عدة معايير

نظرا لعدم نجاح الإتجاهات السابقة في وضع تعريف شامل للجريمة المرتكبة عبر الأنترنت، عَمَدَ أصحاب هذا الإتجاه إلى تعريفها عن طريق دمج أكثر من تعريف، وإعتبروا أن الجريمة المرتكبة عبر الأنترنت هي: " الجريمة التي يُستخدم فيها الحاسب الآلي كوسيلة أو أداة لإرتكابها، أو الجريمة التي يكون الحاسب الآلي نَفسُه ضحيتها " [4].

ورغم الإنتقادات التي وجهت لهذا الإتجاه على إعتبار الجمع بين عدّة معايير لتعريف الجريمة السيبرانية، إلا أن هذا التعريف يُعد التعريف الراجح من الناحية العملية نظرا لتعدد صور الجرائم الإلكترونية وتطورها بتطور تقنية المعلومات [5].

---

(1) عبد اللطيف معتوق، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة ماجستير، جامعة العقيد الحاج لخضر بباتنة، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2011-2012، ص07.

(2) سفيان سوير، جرائم المعلوماتية، مذكرة ماجستير، جامعة أبو بكر بلقايد بتلمسان، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2010-2011، ص 12.

(3) هشام محمد فريد رستم، المرجع السابق، ص 407.

(4) إبتسام حمديني، المرجع السابق، ص 05.

(5) المرجع نفسه.

إنطلاقا مما سبق ذكره يتضح أن الجريمة السيبرانية هي التي تتم بواسطة الكمبيوتر أو أحد وسائل التقنية الحديثة على كمبيوتر آخر أو أحد وسائل التقنية الحديثة، مع ضرورة توفر شبكة إتصال فيما بينها.

خامسا: تعريف المشرع الجزائري للإجرام السيبراني

خِلافا للمشرع الفرنسي الذي لم يُعطِ تعريفا للجريمة السيبرانية، فإن المشرع الجزائري قد إصطَلح على تسميتها بالجرائم المتصلة بتكنولوجيا الإعلام والإتصال، وعرفها بموجب الفقرة (أ) المادة 02 من القانون 04/09 على أنها " جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل إرتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية " [1].

الملاحظ على تعريف المشرع الجزائري أنه قد إعتمد على الجمع بين عدّة معايير لتعريف الجريمة السيبرانية، أولها معيار وسيلة الجريمة وهو نظام الإتصالات الإلكتروني، وثانيها معيار موضوع جريمة المساس بأنظمة المعالجة الآلية للمعطيات، وثالثها معيار القانون الواجب التطبيق أو الركن الشرعي للجريمة المنصوص عليها في قانون العقوبات [2].

كما إعتمد المشرع على معيار رابع لتحديد نطاق الجريمة الإلكترونية، حيث نص على أن الجريمة الإلكترونية ترتكب في نظام معلوماتي أو يسهل إرتكابها عليه، وهذا من شأنه أن يوسع من دائرة التجريم في مجال الإجرام السيبراني في القانون الجزائري [3].

(1) القانون رقم 09-04 المؤرخ في 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، الجريدة الرسمية العدد 47، بتاريخ 16 أوت 2009، ص 05.

(2) رحيمة نميلي، المرجع السابق، ص 06.

(3) المرجع نفسه.

الفرع الثاني: مراحل تطور الإجرام السيبراني

مرَّت الجريمة السيبرانية بِعدَّة مراحل إلى غاية وصولها لدرجة التطور التي هي عليه حاليا، وظلّت مُعدَّلاتها في تصاعد منذ عقد التسعينات، وهذا تماشيا مع التطور الذي شهدته التقنية المستخدمة في جرائم الأنترنت [1]، ولعل أهم مراحل تطور الجريمة السيبرانية هي:

أولا: المرحلة الأولى

إرتبطت هذه المرحلة بظهور إستخدام الكمبيوتر وربطه بشبكة الأنترنت، وكان ذلك في الستينات إلى السبعينات من القرن الماضي، وتميزت هذه المرحلة بعدم الإنتشار الواسع لإستخدام الحاسب الآلي والأنترنت وقلة المستخدمين، وقد تم خِلالها رصد عدد قليل من الجرائم بمعدل جريمة واحدة إلى ثلاث جرائم سنويا، كما أن طريقة معالجة هذه الجرائم كانت في شكل مقالات صحفية تناقش التلاعب بالبيانات المخزنة والتدمير الذي يَمسُّ أنظمة الكمبيوتر والتجسس المعلوماتي، والتي بقيت محصورة في إطار السلوك اللاأخلاقي دون النطاق القانوني [2].

ثانيا: المرحلة الثانية

شهد عقد الثمانينات إرتفاعا نسبيا في معدل الإجرام السيبراني، حيث ظهر نوع جديد من الجرائم إرتبط بعمليات إقتحام نظم الحاسوب عن بعد ونشر الفيروسات عبر شبكات الكمبيوتر ما تسبب في تدمير للملفات والبرامج، حيث شاع في هذه الفترة مصطلح الهاكرز [*]، وهو مُصطلح يطلق على مقتحمي النظم، وتعتبر قضية موريس الشهيرة من بين أهم القضايا المسجلة في فترة الثمانينات أين تم نشر فيروس إلكتروني عُرف بدودة موريس [**] عبر آلاف أجهزة الكمبيوتر من خلال الأنترنت [3].

---

(1) عمر حوتية ورحاب فايز، " بناء إستراتيجية للأمن المعلوماتي كمدخل لمواجهة تهديدات ومخاطر الإجرام السيبراني في الجزائر"، مداخلة مقدمة ضمن فعاليات الملتقى الدولي الذي نظمته كلية الحقوق والعلوم السياسية قسم الحقوق جامعة برج بوعريريج، الموسوم بعنوان: الإجرام السيبراني المفاهيم والتحديات، يومي 11 و12 أفريل 2017، ص 07.

(2) نسيمة سحواذ، " الجريمة الإلكترونية مشكلة عالمية "، مجلة الشرطة للمديرية العامة للأمن الوطني، العدد 129، ديسمبر 2015، ص 139.

(*) الهاكرز: أنظر الصفحة 19 من هذا البحث.

(**) موريس روبيرت تابان: هو أول شخص حوكم بموجب قانون الإحتيال الإلكترونى الأمريكي، بسبب تصميمه لفيروس سمي فيما بعد بفيروس دودة موريس يعرف من خلاله عدد المتصلين بشبكة الأنترنت، ثم أضاف موريس تعليمات للفيروس ليقوم بنسخ نفسه عدة مرات ويملأ كل مساحات التخزين الفارغة، وقد تسبب هذا الفيروس في خسائر كبيرة جدا.
أنظر موقع ويكيبيديا مقال بعنوان موريس تابان، https://ar.wikipedia.org، أطلع عليه بتاريخ 26 أفريل 2018.

ثالثا: المرحلة الثالثة

شهدت فترة التسعينات تطورا هائلا في مجال الإجرام السيبراني وتغييرا في نطاقها ومفهومها، حيث أصبحت مواقع الأنترنت التسويقية النشطة أكثر عُرضة للهجمات التي ظهرت بسببها أنماط جديدة من الجرائم [1]، ففي سنة 1995 تم إختراق موقع البيت الأبيض الأمريكي، لتليها بعد ذلك العديد من الحوادث كحادثة شركة أوميغا فيروس وغيرها، ومن أبرز الجرائم في هذه المرحلة قيام صبي بريطاني بإختراق شبكات الحواسيب العسكرية الأمريكية، وكشف عن أدق الإتصالات مما جعل المسؤولين الأمريكيين يصفونهُ بأنه أشد أنواع إختراق أمن شبكات الحاسوب خطورة، حيث أثَّر هذا الإختراق على حالة الإستعداد العسكري [2].

رابعا: المرحلة الرابعة

وهي الفترة الممتدة من سنة 2000 إلى حد الآن، حيث حَفِلت بتطورات كثيرة ومتسارعة مع إرتفاع عدد مستخدمي الأنترنت ومعدلات الجرائم بالتبعية، وضخامة الخسائر المالية، وتواصل الجهود الدولية والوطنية لمواجهة هذه الجرائم، ففي عام 2002 بلغ عدد سكان العالم 6,28 مليار نسمة، وعدد مستخدمي الأنترنت 662 مليون مستخدم، ورغم ذلك لم تتفاعل حكومات دول العالم بالقدر المطلوب لتوفير الحماية اللاّزمة من الإجرام السيبراني، بالرغم من أنها صارت تعتمد بشكل أساسي على شبكات الحاسب الآلي في القطاع العام والخاص وعلى مستوى الأفراد [3].

وبعد الهجمات الإلكترونية الشهيرة على دولة إستونيا عام 2007، إنتبهت الكثير من الدول لهذا الخطر الذي يدمر البنيات التحتية للمعلومات وتقنية الإتصالات والشبكات، ويعطل كل المرافق الحيوية، فبدأت الدول التفكير بجدية في إعداد إستراتيجيات للأمن السيبراني Cyber Security [4].

(3) عبد الكريم بلعزوق، " دراسة في ماهية الإجرام الإلكتروني ومجرم الأنترنت "، مداخلة مقدمة ضمن فعاليات الملتقى الدولي الذي نظمته كلية الحقوق والعلوم السياسية قسم الحقوق جامعة برج بوعريريج، الموسوم بعنوان: الإجرام السيبراني المفاهيم والتحديات، يومي 11 و12 أفريل 2017، ص 04.

(1) نسيمة سحواذ، المرجع السابق، ص 140.

(2) عبد الكريم بلعزوق، المرجع السابق، ص 05.

(3) مجمع البحوث والدراسات بأكاديمية السلطان قابوس لعلوم الشرطة، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، نزوى سلطنة عمان، 2016، ص 05.

(4) عمر حوتية ورحاب فايز، المرجع السابق، ص 07.

وفي السنوات القليلة الماضية أصبحت حماية أمن المعلومات والإتصالات والشبكات ومواجهة الجريمة الإلكترونية ذات أولوية في سياسات العديد من الحكومات، خاصة وأن حجم الجريمة الإلكترونية يزداد بإزدياد عدد مستخدمي الأنترنت حول العالم [1].

المطلب الثاني: خصائص الجريمة السيبرانية والمجرم السيبراني

تختلف الجرائم السيبرانية عن الجرائم التقليدية التي ترتكب في العالم المادي، لذلك فهي تتسم بخصائص جعلت منها ظاهرة إجرامية جديدة لم يعرفها العالم من قبل (الفرع الأول)، كما أن مرتكب هذه الجريمة يتميز ببعض الصفات الخاصة (الفرع الثاني).

الفرع الأول: خصائص الجريمة السيبرانية

من خلال هذا الفرع سيتم توضيح الخصائص التي تميز الجريمة السيبرانية عن غيرها من الجرائم، على النحو التالي:

أولا: جريمة ناعمة

تتسم الجرائم الناشئة عن إستخدام الأنترنت بأنها ناعمة لخفتها ولكونها متسترة في أغلبها، كما أن الضحية لا يُلاحظ إرتكابها رغم أنها قد تقع أثناء وجوده على الشبكة، فالجاني يتمتع بقدرات فنية تُمكنه من تنفيذ جريمته بدقة، ومِثال ذلك إرسال الفيروسات المدمرة وسرقة الأموال والبيانات الخاصة أو إتلافها والتجسس وغيرها من الجرائم [2].

ويستفيد المجرمون في مختلف مناطق العالم من الشبكة في تبادل الأفكار والخبرات الإجرامية فيما بينهم، ويظهر ذلك جليا في مختلف المواقع الإلكترونية ومنتديات قراصنة الهاكرز التي تضمن لهم الإتصال فيما بينهم بهدف تبادل الخبرات في مجال القرصنة، من أجل إرتكابهم لجرائمهم بعيدا عن أعين الأمن [3].

(1) مجمع البحوث والدراسات بأكاديمية السلطان قابوس لعلوم الشرطة، المرجع السابق، ص 14.

(2) يوسف صغير، المرجع السابق، ص 14-15.

(3) عبد المومن بن صغير، " الطبيعة الخاصة للجريمة المرتكبة عبر الأنترنت في التشريع الجزائري والتشريع المقارن "، مداخلة مقدمة ضمن فعاليات الملتقى الوطني الذي نظمته كلية الحقوق والعلوم السياسية قسم الحقوق جامعة محمد خيضر بسكرة، الموسوم بعنوان: الجريمة المعلوماتية بين الوقاية والمكافحة، يومي 16و 17 نوفمبر 2015، ص 08.

ثانيا: إعتبارها أقل عنفا في التنفيذ

لا تتطلب جرائم الأنترنت عنفا لتنفيذها أو مجهودا كبيرا، فهي تنفذ بأقل جهد ممكن مقارنة بالجرائم التقليدية التي تتطلب نوعا من المجهود العضلي، الذي يكون في صور ممارسة العنف والإيذاء كما هو الحال في جريمة القتل والإختطاف، أو في صورة الخلع أو الكسر وتقليد المفاتيح في جريمة السرقة [1].

وتتميز جرائم الأنترنت بأنها جرائم هادئة بطبيعتها [2]، فكل ما تحتاج إليه هو القدرة على التعامل مع جهاز الحاسوب بمستوى تِقني يُوظفُ في إرتكاب الأفعال غير المشروعة، وتحتاج بطبيعة الحال إلى وجود شبكة المعلومات الدولية (الأنترنت)، مع وجود مجرم يُوظِّفُ خِبرته وقُدارته في التعامل مع الشبكة للقيام بجرائم مختلفة كالتجسس أو إختراق خصوصيات الغير أو التغرير بالقاصرين، فمن هذا المنطلق تعد الجريمة المرتكبة عبر الأنترنت من الجرائم النظيفة فلا أثر فيها لأي عنف أو دماء، وإنما مجرد أرقام وبيانات يتم تغييرها من السجلات المخزنة في ذاكرة الحواسيب وليس لها أثر خارجي مادي [3].

ثالثا: جريمة ذات بعد دولي (عابرة للحدود)

بعد ظهور شبكات المعلومات، لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر مختلف الدول، فالمقدرة التي تتمتع بها الحواسيب وشبكاتها في نقل كميات كبيرة من المعلومات وتبادلها بين أنظمة تفصل بينها ألاف الأميال، جعلت من الممكن إرتكاب جريمة من أماكن متعددة في دول مختلفة، ويتحقق الفعل الإجرامي في دولة أخرى بواسطة أنظمة التقنية الحديثة [4]، وذلك راجع إلى مجتمع المعلومات الذي لا يعترف بالحدود الجغرافية، فهو مجتمع منفتح عبر شبكات تخترق الزمان والمكان دون أن تخضع لحرس الحدود.

---

(1) صالح بن محمد المسند وعبد الرحمان بن راشد المهيني، " جرائم الحاسب الآلي الخطر الحقيقي في عصر المعلومات "، المجلة العربية للدراسات الأمنية والتدريب، العدد 29 (المجلد 15)، أفريل 2000، ص 20.

(2) ذياب موسى البداينة، " دور الأجهزة الأمنية في مكافحة جرائم الإرهاب المعلوماتي "، دورة تدريبية في كلية التدريب قسم البرامج التدريبية بالقنطيرة، المغرب، 2006، ص 20.

(3) عبد المومن بن صغير، المرجع السابق، ص 09.

(4) عباس أبو شامة عبد المحمود، عولمة الجريمة الإقتصادية، الطبعة الأولى، جامعة نايف العربية للعلوم الأمنية، الرياض، 2007، ص 52.

هذا وقد لا يقتصر الضرر المترتب عن الجريمة على المجني عليه وحده، وإنما قد يتعداه إلى متضررين آخرين في عدة دول، وهو الملاحظ من خلال جرائم نشر المواد ذات الخطر الديني والأخلاقي والأمني والسياسي والتربوي والثقافي والإقتصادي [1].

تتم الجرائم السيبرانية في الغالب الأعم بواسطة أفعال ترتكب من قبل أشخاص من خارج الحدود، كما أنها تمر عبر شبكات وأنظمة المعلومات، الأمر الذي يُثِير التساؤل حول الإختصاص القضائي لهذه الجرائم، علاوة على أن إمتداد أنشطة الملاحقة والتحري والضبط والتفيش خارج الحدود، أمر يحتاج إلى تعاون دولي شامل يستهدف تحقيق مكافحة هذه الجرائم، مع إحترام السيادة الوطنية للدول المعنية [2].

رابعا: عدم قيام ضحايا الإجرام السيبراني بتقديم الشكوى أو التبليغ

من بين خصائص الجريمة السيبرانية، أنهُ لا يتم في غالب الأحيان تقديم شكوى أو الإبلاغ عند إرتكابها، إما لعدم إكتشاف الضحية لها وإما خوفا من التشهير [3]، لذا نجد أن معظم جرائم الأنترنت تُكتشف بالمصادفة، وأحيانا بعد وقت طويل من إرتكابها، زد على ذلك أن الجرائم التي لم تُكتشف هي أكثر بكثير من تلك التي كُشِفَ السِتارُ عنها، فالرقم المظلم بين حقيقة عدد الجرائم المرتكبة والعدد الذي تم إكتشافه هو رقم خطير [4].

وتبدو هذه الظاهرة أكثر وضوحا في المؤسسات المالية، كالبنوك والمؤسسات الإدخارية ومؤسسات الإقراض والسمسرة، حيث تخشى مجالس إدارتها عادة من أن تؤدي الدعاية السلبية التي قد تنجم عن كشف هذه الجرائم أو إتخاذ الإجراءات القضائية بشأنها إلى نقص ثقة عملائها فيها وإنصرافهم عنها [5].

(1) عبد المومن بن صغير، المرجع السابق، ص 09.

(2) المرجع نفسه، ص 11.

(3) أمير فرج يوسف، الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والأنترنت، الطبعة الأولى، مكتبة الوفاء القانونية، الإسكندرية، 2011، ص 157.

(4) عبد الرحمان جميل محمود حسين، الحماية القانونية لبرامج الحاسب الآلي، مذكرة ماجيستير، جامعة النجاح الوطنية نابلس فلسطين، كلية الدراسات العليا، 2008، ص 09.

(5) محمد عبيد الكعبي، الجرائم الناشئة عن الإستخدام غير المشروع لشبكة الأنترنت، الطبعة الثانية، دار النهضة العربية، القاهرة، 2009، ص 37.

خامسا: صعوبة الوصول إلى الدليل

تكون البيانات والمعلومات المتداولة عبر شبكة الأنترنت على هيئة رموز مخزنة في وسائط تخزين ممغنطة بلغة الصفر والواحد، لا تقرأ إلا بواسطة الحاسب الآلي، والوقوف على الدليل الذي يمكن فَهمه بالقراءة والتوصل عن طريقِه إلى الجاني يَبدُوا أمرا صعبا، خاصة وأن الجاني يسعى إلى عدم ترك أثر لجريمته، ضف إلى ذلك ما يَتطلبُه من فحص دقيق لموقع الجريمة من قبل المتخصصين في هذا المجال، للوقوف على إمكانية وجود دليل ضد الجاني، وما يتبع ذلك من فحص للكم الهائل من الوثائق والمعلومات والبيانات المخزنة [1].

وتتم الجريمة المرتكبة عبر الأنترنت خارج إطار الواقع المادي الملموس، مما يجعل الأمور تزداد تعقيدا لدى سلطات الأمن وأجهزة التحقيق، فداخل هذه البيئة تكون البيانات والمعلومات عبارة عن نبضات إلكترونية غير مرئية، مما يجعل أمر طمس الدليل ومَحوِه كليا من قبل الفاعل أمرا في غاية السهولة [2].

كما يسعى مرتكب الجريمة السيبرانية إلى إعاقة سلطات التحقيق في الوصول إلى الدليل بشتى الوسائل الممكنة، كحذف البرامج أو وضع رموز سرية وكلمات للمرور، وقد يَلجأ لتشفير التعليمات لمنع إيجاد أي دليل يدينه [3].

إنه من السهل مسح الدليل من الكمبيوتر في زمن قياسي بإستخدام البرامج المخصصة لذلك، إذ يتم بمجرد لمسة خاطفة على لوحة المفاتيح، على إعتبار أن الجريمة تتم بأوامر وتعليمات تُصدَر إلى الجهاز [4]، ومن بين صعوبات الوصول إلى الدليل أيضا، قيام كبرى المواقع العالمية بإحاطة البيانات المخزنة على صفحاتها بسياج من الحماية، لمنع التسلل والوصول غير المشروع إليها لتدميرها أو تبديلها أو الإطلاع عليها ونسخها [5].

(1) محمد عبيد الكعبي، نفس المرجع، ص 38.

(2) يوسف صغير، المرجع السابق، ص 45.

(3) عبد المؤمن بن صغير، المرجع السابق، ص 10.

(4) موسى مسعود أرحومة، " الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية "، مداخلة مقدمة ضمن فعاليات المؤتمر المغاربي الأول الذي نظمته أكاديمية الدراسات العليا بطرابلس، الموسوم بعنوان: المعلوماتية والقانون، يومي 28-29 أكتوبر 2010، ص 03.

(5) عبد المؤمن بن صغير، المرجع السابق، ص 11.

سادسا: صعوبة ضبط وتكييف الجرائم السيبرانية

لا شك أن لرجال الشرطة القضائية والمحققين والقضاة أثناء تأدية مهامهم صعوبات كبيرة تتعلق بإجراءات ضبط الجرائم المعلوماتية وإضفاء الوصف القانوني المناسب الذي ينطبق على الوقائع المتعلقة بها، ولعل مردَّ ذلك يرجعُ إلى الطبيعة الخاصة لهذه الجرائم، فهي تتم في فضاء إلكتروني يتميز بالتغيير والديناميكية والإنتشار الجغرافي العابر للحدود [1].

سابعا: تصادم التفتيش عن الأدلة مع الحق في الخصوصية المعلوماتية

إن التفتيش في هذا النوع من الجرائم يتم غالبا على نظم الكمبيوتر وقواعد البيانات وشبكات المعلومات، وقد يتجاوز التفتيش النظام المشتبه فيه إلى عدة أنظمة أخرى مرتبطة به، نظرا لشيوع التشبيك بين الحواسيب وإنتشار الشبكات الداخلية على مستوى المنشآت والشبكات المحلية والإقليمية والدولية على مستوى الدول [2].

ولا شك في أن إمتداد التفتيش إلى نظم غير النظام محل الإشتباه قد يمسُّ في الصميم بالحق في الخصوصية المعلوماتية لأصحاب النظم التي يمتد إليها التفتيش [3].

الفرع الثاني: المجرم السيبراني

إن مرتكب الجرائم السيبرانية شخص تتوفر لديه بعض الميزات التي لا نجدها عند كل الأشخاص، كما أنه ليس بمقدور كل شخص تنفيذ أحد الجرائم السيبرانية وإن أراد ذلك، وقد إختلف الدارسون والباحثون في مجال الجريمة السيبرانية بخصوص تحديد شخصية المجرم السيبراني ومدى جسامة جرمه كدليل لتبرير العقوبة المنجرة عن فعلته، غير أنه لا يوجد نموذج محدد لمجرمي الأنترنت، إلا أنه توجد مجموعة من الصفات المشتركة بين هؤلاء المجرمين [4].

أولا: سمات المجرم السيبراني

يتميز المجرم السيبيراني بالصفات التالية:

(1) أمير فرج يوسف، المرجع السابق، ص 158.

(2) عبد المؤمن بن صغير، المرجع السابق، ص 155.

(3) عبد العال الدريبي ومحمد صادق إسماعيل، المرجع السابق، ص 155.

(4) عبد الكريم بلعزوق، المرجع السابق، ص 07.

1-مجرم متخصص

إن لمجرم الأنترنت القدرة الفائقة والمهارة العالية للتحكم في التقنية المعلوماتية، حيث يستغل كل هذه المكتسبات في إختراق الشبكات وكسر كلمات المرور والشيفرات، ويسبح في عالم الأنترنت ليحصل على كل غالٍ وثمين من البيانات والمعلومات الموجودة على أجهزة الحواسيب المتصلة بالشبكات [1].

2-عائد للإجرام

يتميز المجرم المعلوماتي بأنه عائد للإجرام دائما، إذ يستخدم مهاراته وخبراته وطريقة عمل الحواسيب وكيفية تخزين البيانات والمعلومات فيها، وكذا طريقة التحكم في أنظمة الشبكات عن بُعد، فهو قد لا يرتكب الجريمة بهدف الإيذاء أو سرقة البيانات، إنما هو نوع من أنوع التحدي بهدف إختبار مهاراته ورغبته في تطويرها أكثر فأكثر، خاصة ما لم يتم القبض عليه [2].

3-مجرم محترف

إن مجرمي المعلوماتية يتمتعون بقدر لا يستهان به من المهارة والمعرفة بتقنيات الحاسوب والأنترنت، بل وأكثر من ذلك أن بعض مرتكبي هذه الجرائم هم من المتخصصين في مجال معالجة المعلومات آليا، فالمجرم السيبراني يتمتع بإحترافية كبيرة في تنفيذ جرائمه، حيث أنه يرتكب هذه الجرائم عن طريق الكمبيوتر، الأمر الذي يقتضي الكثير من الدقة والتخصص والإحترافية في هذا المجال، بغية التغلب على العقبات التي أوجدها المتخصصون والمبرمجون لحماية أنظمة الكمبيوتر، كما في حالة البنوك والمؤسسات العسكرية والمواقع الخاصة بالحكومات [3].

4-مجرم ذكي

يتمتع مرتكب الجريمة السيبرانية بنظرة غير تقليدية للإجرام، على إعتبار أنه يوصف غالبا بدرجة عالية من الذكاء المعلوماتي الذي يُمَكِّنُهُ من التعديل والتطوير في الأنظمة الأمنية حتى لا يكون من الممكن ملاحقته وتتبع أعماله الإجرامية عبر الشبكات وداخل أجهزة الحواسيب، مما يجعل من الصعب تصنيفه بحسب التصنيف الإجرامي المعتاد، لذا يُعتمد في تحديد أنواع

(1) مليكة عطوي، " الجريمة المعلوماتية "، حوليات جامعة الجزائر، العدد 21، جوان 2012، ص 13.

(2) عبد الفتاح مراد، شرح جرائم الكمبيوتر والإنترنت، دار الكتب والوثائق المصرية، دون ذكر تاريخ النشر، ص 45.

(3) فتيحة رصاع، الحماية الجنائية للمعلومات على شبكة الأنترنت، مذكرة ماجستير، جامعة أبي بكر بلقايد تلمسان، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2011-2012، ص 51.

الجناة في الجرائم المرتكبة عبر الأنترنت على الهدف المراد تحقيقيه من إرتكاب هذه الجرائم كمعيار للتمييز فيما بينهم [1].

ثانيا: تصنيف مرتكبي الجرائم السيبرانية

يمكن تصنيف مرتكبي الجرائم السيبرانية، حسب الدراسات السابقة لهذا الموضوع إلى ثلاثة مجموعات:

1-الموظفون العاملون في مجال الأنظمة المعلوماتية

بإعتبار أن النظام المعلوماتي هو مجال عملهم الأساسي، ونظرا للمهارات والمعرفة التقنية التي يتمتعون بها، فإنهم يقترفون بعض الجرائم المعلوماتية التي يمكن أن تحقق أهدافهم الشخصية ومنها الكسب المادي، كما أن هذه الفئة يمثلون الغالبية العظمى من مرتكبي هذه الجرائم [2].

2-الحاقدون

أفراد هذا الصنف لا يسعون إلى إثبات مقدرتهم ولا لتحقيق مكاسب مادية أو سياسية أو غيرها، وإنما يرتكبون أنشطتهم الإجرامية بِدافع الرغبة في الإنتقام والثأر، لذا فهم ينقسمون إما إلى مستخدمي النظام بوصفهم على علاقة ما بالنظام محل الجريمة، وإما إلى غرباء عن النظام وتتوفر لديهم أسباب للإنتقام من الشخص المستهدف في نشاطهم، ومثال ذلك من يقومون بإستخدام الكمبيوتر لمسح بعض المعلومات الخاصة بالشركة أو المؤسسة، كطريقة للإنتقام من المؤسسة لأسباب يعرفها مرتكب هذا الفعل [3].

3-القراصنة

وهم عادة المبرمجون من أصحاب الخبرة، حيث يسعون إلى الدخول إلى الأنظمة المعلوماتية غير المسموح لهم بدخولها، وكسر كل الحواجز الأمنية المحيطة بهذه الأنظمة، ويمكن تصنيف القراصنة إلى صنفين [4] هما:

(1) عبد اللطيف معتوق، المرجع السابق، ص 16.

(2) مليكة عطوي، المرجع السابق، ص 13.

(3) علي جعفر، المرجع السابق، ص 117.

(4) صغير يوسف، المرجع السابق، ص 26-27.

أ-القراصنة الهواة (الهاكرز)

يكون هذا الصنف من القراصنة عادة من هواة الحواسيب والتكنولوجيا، ينطلقون من فكرة التسلية والرغبة في المعرفة، ويرون في إختراق الأنظمة المعلوماتية تحديا لقدراتهم الذاتية، فالفضول وحب التعمق في الأنظمة المعلوماتية هو دافعهم الأول، وفي العادة لا تكون لديهم دوافع تخريبية وراء أعمالهم، لكنها قد تتولد بالعودة لإرتكاب الجريمة [1].

وهناك سمة مميزة لهذه الفئة من القراصنة، وهي تبادلهم للمعلومات والخِبرات فيما بينهم، حيث يتم ذلك عن طريق النشرات الإعلانية الإلكترونية ومجموعات الأخبار والمنتديات المخصصة لهذا الغرض [2].

ب-القراصنة المحترفون (الكراكرز)

بالنسبة لهذا الصنف، فهو الأخطر على الإطلاق لأن المجرم يدرك ماذا يريد، وكيفية الوصول إلى أهدافه المحددة مسبقا، وذلك بإستخدام ما لديه من مهارة وعلم يطوره بإستمرار، فهدفه سحب الأموال من الأرصدة، والوصول إلى أخطر المواقع وأكثرها حساسية وإختراقها والتلاعب ببياناتها، فهذه الفئة من المجرمين وبالنظر إلى السلوكات المرتكبة من طرفهم نجد أن لهم ميول إجرامية خطيرة وواضحة، تفصح عن رغبتهم في إحداث التخريب والسرقة والنهب [3].

لكن مهما قيل عن المجرم السيبراني أنه متكيف إجتماعيا وأنه ليس مجرما بطبعه أو أنه لم يكشف عن أي عداء للمجتمع، يبقى رغم ذلك مجرما يتطلب توقيع العقاب عليه، فتعدد الجرائم المعلوماتية وتنوع صورها، يقتضي عدم التهاون في مكافحة مرتكبيها [4].

(1) نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2005، ص 61-62.

(2) مليكة عطوي، المرجع السابق، ص 13.

(3) عبد الفتاح مراد، المرجع السابق، ص 47.

(4) عبد اللطيف معتوق، المرجع السابق، ص 16.

المبحث الثاني: صور الجريمة السيبرانية

إهتم فقهاء القانون الجنائي منذ ظهور الثورة المعلوماتية بوضع تقسيم للجرائم السيبرانية، حيث صنفوها ضمن فئات متعددة تختلف بإختلاف زاوية النظر وبحسب الأساس والمعيار المعتمد في التقسيم (المطلب الأول).

كما حدد المشرع الجزائري صورا للجريمة السيبرانية من خلال بعض النصوص القانونية المتعلقة بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات (المطلب الثاني).

المطلب الأول: صور الجريمة السيبرانية في الفقه الجنائي

إذا بحثنا في تصنيف الفقهاء للجريمة السيبرانية، نجد أن البعض منهم يقسمها إلى جرائم تستهدف نظام المعلومات وأخرى ترتكب بواسطته، والبعض الآخر يصنفها إستنادا إلى الأسلوب المتبع في الجريمة، وآخرون يستندون إلى الباعث أو الدافع لإرتكاب الجريمة، وغيرهم يؤسس تقسيمه على تهديد محل الإعتداء، وكذا تعدد الحق المعتدى عليه، وكلها تصنيفات ودراسات رافقت موجات التشريع في ميدان تقنية المعلومات وعكست التطور التاريخي لهذه الظاهرة الإجرامية، وكما يقول الدكتور علي جعفر " لا نبالغ إن قلنا إن ثمة نظريات ومعايير لتصنيف طوائف جرائم تقنية المعلومات الحديثة بعدد المؤلفين والباحثين في هذا المجال القانوني " [1].

نظرا لعدم وجود معيار محدد ومتفق عليه يتم إعتماده في تصنيف هذه الجرائم وأمام التطور المستمر لتكنولوجيات الإعلام والإتصال سيتم تسليط الضوء على أهم المعايير المعتمدة في تصنيف الجرائم السيبرانية.

الفرع الأول: تصنيف الجريمة السيبرانية بالنظر للغرض من إرتكابها

وهو التصنيف الذي إعتُمد من قبل الهيئة الأكاديمية الأمريكية التي وضعت مشروع القانون النموذجي لجرائم تكنولوجيا المعلومات عام 1998 والمسمى Model State Computer Crimes Code [2]، وتبعا لهذا التقسيم الوارد ضمن مشروع القانون النموذجي الأمريكي نجد:

(1) علي جعفر، المرجع السابق، ص 08.

(2) المرجع نفسه، ص 91.

1-الجرائم السيبرانية التي تستهدف الأشخاص

وتضم هذه الجرائم فئتين رئيسيتين وهي الجرائم غير الجنسية والجرائم الجنسية:

أ-الجرائم السيبرانية غير الجنسية

تستهدف هذه الجرائم الأشخاص وتشمل التشهير بهم سواء المعنويين منهم أو الطبيعيين وذلك ببث أفكار ومعلومات وفضائح ملفقة من شأنها إلحاق ضرر أدبي وأحيانا مادي وشخصي بالجهة المقصودة، كما يتم أيضا إستخدام الحواسيب وشبكة الأنترنت في إنتهاك حقوق الملكية الفكرية خاصة التعدي على برامج الحاسب والمصنفات الرقمية، ومن بين الجرائم التي تتم عبر الأنترنت كذلك التخابر والإتصال من أفراد منظمة أو نشاط يهدد أمن وإستقرار الدول كالدعارة، المخدرات والتهريب ...إلخ [1].

وتندرج في هذا الإطار أيضا جرائم القتل بالكمبيوتر، وذلك عن طريق التسبب في الوفاة بالتحريض على الإنتحار بإستخدام شبكة الأنترنت، ومثال ذلك لعبة "الحوت الأزرق" التي تسببت في إنتحار بعض الأطفال بعد أيام من الإدمان على هذه اللعبة خلال مطلع سنة 2018.

ب-الجرائم السيبرانية الجنسية

وتشمل تحريض القاصرين على أنشطة جنسية غير مشروعة، وإفسادهم بأنشطة جنسية عبر الوسائل الإلكترونية، والتحرش الجنسي بهم عبر الكمبيوتر والوسائل التقنية، ونشر وتسهيل نشر وإستضافة المواد الفاحشة عبر الأنترنت بوجه عام وللقاصرين تحديدا، ونشر الفحش والمساس بالحياء عبر الأنترنت، وتصوير أو إظهار القاصرين ضمن أنشطة جنسية، وكذا الحصول على الصور والهويَّات بطريقة غير مشروعة لإستغلالها في أنشطة جنسية، وبإمعان النظر في هذه الأوصاف نجد أنها تجتمع كلها تحت صورة واحدة هي إستغلال وسائل تقنية المعلومات للترويج للدعارة أو إثارة الفحش وإستغلال الأطفال والقصر في أنشطة جنسية غير مشروعة [2].

2-الجرائم السيبرانية التي تستهدف الأموال

وتشمل أنشطة الإستيلاء على الأموال والمصاريف عن طريق الإحتيال التجاري أو عن طريق الأوراق المالية، وكذا التزوير أو الدخول بهدف إغتصاب الملكية ونقلها عبر النظم

(1) عبد الكريم بلعزوق، المرجع السابق، ص 05-06.

(2) علي جعفر، المرجع السابق، ص 92.

والشبكات، وإستخدام إسم النطاق أو العلامة التجارية أو إسم الغير دون ترخيص، وتشمل جرائم الإحتيال التلاعب بالمعطيات والنظم وإستخدامها في تدمير الكمبيوتر والبطاقات المالية للغير دون ترخيص، وكذا الإختلاس بواسطة الكمبيوتر، وسرقة المعلومات المخزنة فيه، وقرصنة البرامج، وسرقة خدمات الكمبيوتر وأدوات التعريف والهوية عبر إنتحال هذه الصفات، أيضا جرائم تزوير البريد الإلكتروني والوثائق والسجلات والهوية [1].

3-الجرائم السيبرانية المرتبطة بالمقامرة والجرائم المنافية للآداب والأخلاق

وتشمل تَمَلُّك وإدارة أو تسهيل إدارة مشاريع القمار على الأنترنت أو تشجيع المقامرة عبر الأنترنت، وإستخدام الأنترنت لترويج الكحول والمواد المخدرة وكل مواد الإدمان للقصر [2].

4-الجرائم السيبرانية ضد الحكومة

هذه الطائفة تضم كافة جرائم تعطيل الأعمال الحكومية وتنفيذ القانون، والحصول على المعلومات السرية، والإخبار الخاطئ عن جرائم الكمبيوتر، والعبث بالأدلة القضائية أو التأثير فيها، وكذا تهديد السلامة العامة، وبث البيانات من مصادر مجهولة، كما تشمل الإرهاب الإلكتروني والأنشطة الثأرية الإلكترونية [3].

الفرع الثاني: تصنيف الجرائم السيبرانية تبعا لنوع المعطيات ومحل الجريمة

هذا التصنيف هو الذي يتوافق وموجات التشريع في ميدان قانون تقنية المعلومات، وهو كذلك التصنيف الذي يعكس التطور التاريخي لظاهرة جرائم تكنولوجيا المعلومات الحديثة، حيث تُقسَّم جرائم الحاسبات الآلية إلى ثلاث طوائف رئيسية وهي:

جرائم تتعلق بإنتهاك حرمة الحياة الخاصة وجرائم الحاسب الآلي الاقتصادية، والجرائم الماسة بحقوق الملكية الفكرية لبرامج الحاسوب ونظمه [4].

(1) محمد طارق عبد الرؤوف الحن، جريمة الإحتيال عبر الإنترنت، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2011، ص 48-51.

(2) علي جعفر، المرجع السابق، ص 94.

(3) المرجع نفسه.

(4) المرجع نفسه، ص 86.

المطلب الثاني: صور الإجرام السيبراني في التشريع الجزائري

على غرار العديد من الدول، ورغبة من المشرع الجزائري في التصدي لظاهرة الإجرام السيبراني، وما يصاحبها من أضرار معتبرة تمسُّ بالأفراد ومؤسسات الدولة من جهة، ومحاولةً منه لتدارك الفراغ التشريعي القائم في هذا المجال من جهة أخرى، عَمَدَ منذ الألفية الثانية لإصدار بعض القوانين وتعديل البعض الآخر بما فيها قانون العقوبات، وجعلها تتجاوب مع التطورات الإجرامية في مجال تكنولوجيا الإعلام والإتصال، فقام بإستحداث قوانين خاصة لضمان الحماية الجنائية للمعاملات الإلكترونية [1]، وسيتم عرض ذلك كما يلي:

الفرع الأول: الحماية الدستورية من الجرائم السيبرانية

كفل دستور الجزائر لسنة 1996 وكذا القانون 16-01 المتضمن تعديل الدستور مجموعة من المبادئ لحماية الحقوق الأساسية والحريات الفردية، على أن تضمن الدولة عدم إنتهاك حرمة الإنسان وحقوقه، وقد تم تكريس هذه المبادئ الدستورية عن طريق سن نصوص قانونية أوردها المشرع ضمن قانون العقوبات والإجراءات الجزائية وقوانين خاصة أخرى، والتي تحضر كُلَّ مساس بهذه الحقوق [2].

ومن أهم هذه المبادئ الدستورية ما نصت عليه مواد 38[3]، 40[4]، 44[5] و46[6] من القانون 01/16 المؤرخ في 06 مارس 2016.

---

(1) جمال براهيمي، " مكافحة الجرائم الإلكترونية في التشريع الجزائري "، المجلة النقدية للقانون والعلوم السياسية، جامعة مولود معمري تيزي وزو، المجلد الثاني، نوفمبر 2016، ص 124.

(2) فضيلة عاقلي، " الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري "، مداخلة مقدمة في أعمال المؤتمر الدولي الرابع عشر، الموسوم بعنوان: الجرائم الإلكترونية طرابلس، يومي 24 و25 مارس 2017، ص 13.

(3) المادة 38 من القانون 16-01 " الحريات الأساسية وحقوق الإنسان والمواطن مضمونة "، ج ر عدد 14، ص 10.

(4) المادة 40 من القانون 16-01 " تضمن الدولة عدم إنتهاك حرمة الإنسان ". ج ر عدد 14، ص 10.

(5) المادة 44 من القانون 16-01 " حرية الإبتكار الفكري والفني والعلمي مضمونة للمواطن.
حقوق المؤلف يحميها القانون. ج ر عدد 14، ص 11.
لا يجوز حجز أي مطبوع أو تسجيل أو أية وسيلة أخرى من وسائل التبليغ والإعلام إلا بمقتضى أمر قضائي ".

(6) المادة 46 من القانون 16-01 " لا يجوز إنتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه ويحميها القانون. سرية المراسلات والإتصالات الخاصة بكل شكلها مضمونة. لا يجوز بأي شكل المساس بهذه الحقوق دون أمر معلل من السلطات القضائية ويعاقب القانون كل إنتهاك هذا الحكم. حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حق أساسي يضمنه القانون ويعاقب على إنتهاكه "، ج ر عدد 14، ص 11.

الفرع الثاني: الجريمة السيبرانية في قانون العقوبات

ذكرنا في غير موضع أن المشرع الجزائري قد إستحدث نصوصا قانونية لمحاربة الجرائم السيبرانية، حيث أصدر القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 وقد حوى هذا الأخير على قسم خاص، القسم السابع مكرر من الفصل الثالث المتعلق بجرائم الجنايات والجنح ضد الأموال، تحت عنوان المساس بأنظمة المعالجة الألية للمعطيات، وقد شدد المشرع الجزائري في عقوباتها بموجب القانون 06-23 المؤرخ في 20 ديسمبر 2006 المعدل لقانون العقوبات.

أولا: أنواع الجريمة السيبرانية في قانون العقوبات

تضمنت المواد من 394 مكرر إلى 394 مكرر 2 من القانون 23/06 على الأفعال المعتبرة جرائما سيبرانية وهي:

1-الدخول أو البقاء غير المصرح بهما لمنظومة معالجة آلية للمعطيات

نصت المادة 394 مكرر [1] من قانون العقوبات على هذه الصورة البسيطة للإعتداء على نظام المعالجة الآلية للمعطيات، حيث ينطوي تحتها جريمتين:

أ-جريمة الدخول غير المرخص به لنظام معالجة آلية للمعطيات: ويكون هذا الإعتداء بمجرد الولوج داخل نظام للمعالجة مملوك للغير، دون علم هذا الأخير ودون رضاه.

ب-جريمة البقاء غير المرخص به في نظام آلي لمعالجة المعطيات: ويكون بإستمرارية التواجد داخل نظام للمعالجة مملوك للغير دون إذن منه، وتجدر الإشارة أنه من الممكن أن يحصل تداخل مادي بين الجريمتين، كأن يدخل شخص لنظام آلي مملوك للغير مع بقائه داخله دون إذن من صاحبه [2].

نلاحظ من خلال نص المادة 394 مكرر [3] في فقرتيها الثانية والثالثة، أن المشرع الجزائري قد أورد ظرفين لتشديد العقوبة، وهما أن يترتب عن فعل الدخول أو البقاء في المنظومة

(1) المادة 394 مكرر/1 من القانون 04-15 " يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك "، ج ر عدد 71، ص 12.

(2) آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، الطبعة الثانية، دار هومه للطباعة والنشر والتوزيع، الجزائر،2007، ص 102.

(3) المادة 394 مكرر/2 من قانون 06-23 " تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة. =

الآلية إما المحو أو التعديل في بيانات النظام، وإما حصول تخريب في إشتغال النظام وإعاقته عن أداء وظيفته [1].

2-جريمة إدخال أو إزالة أو تعديل معطيات في نظام المعالجة الألية بطرق تدليسية

بحسب المادة 394 مكرر 1 [2] من قانون العقوبات يجرم فعل الدخول أو البقاء عن طريق الغش، الذي يترتب عنه إلحاق ضرر بالمعطيات التي تتضمنها هذه المنظومة المعلوماتية.

3-جريمة حيازة معطيات من أنظمة للمعالجة الآلية عن طريق الغش

بإستقراء المادة 394 مكرر 2 [3] من قانون العقوبات، نجد أن المشرع الجزائري لم يكتفي بتجريم الأفعال المتعلقة بالدخول أو البقاء عن طريق الغش في نظام لمعالجة البيانات، بل كانت له نظرة أبعد من ذلك، ففي الغالب من يرتكب الأفعال المنصوص عليها في المادة 394 مكرر يكون هدفه الحصول على معطيات من النظام المخترق لغرض معين، سواء لإستخدامها في أمور شخصية أو لبيعها أو نشرها ...الخ، ولهذا جرَّم المشرع الجزائري مجرد حيازة هذه البيانات.

ثانيا: الأحكام الخاصة بالجريمة السيبرانية

إلى جانب الجرائم المنصوص عليها في المواد من 394 مكرر إلى 394 مكرر 2، بيَّن المشرع الجزائري مسألة الشروع في إرتكاب الجريمة السيبرانية وعقوبة الشريك فيها وغيرها، كما أورد أيضا عقوبة تكميلية خاصة تطبق وجوبا على هذا النوع من الجرائم، هذه الأحكام الخاصة هي:

= وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام إشتغال تكون العقوبة الحبس من ستة (6) أشهر إلى سنتين (2) والغرامة من 50.000 دج إلى 300.000 دج ". ج ر عدد 71، ص 12.

(1) جمال براهيمي، المرجع السابق، ص 131.

(2) المادة 394 مكرر 1 من قانون العقوبات " يعاقب بالحبس من 06 أشهر إلى 03 سنوات وبغرامة من 500.000 دج إلى 4.000.000 كل من أدخل بطريقة الغش معطيات في نظام أو أزال أو عدل بطريقة الغش المعطيات التي يتضمنها ". ج ر عدد 71، ص 12.

(3) المادة 394 مكرر 2 من قانون العقوبات " يعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من 1.000.000 دج إلى 10.000.000 دج، كل من يقوم عمدا وعن طريق الغش بما يأتي:

- تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.
- حيازة أو إفشاء أو نشر أو إستعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم ". ج ر عدد 71، ص 12.

1-الشروع في إرتكاب الجريمة السيبرانية

إن فعل الشروع أو البدء في إرتكاب الجنحة بحسب نص المادة 31 [1] من قانون العقوبات، لا يعاقب عليه إلَّا بناء على نص صريح في القانون، ونظرا لكون جرائم الإعتداء على نظام المعالجة الآلية ذات وصف جنحي، فإن المشرع أقر لها وبنص خاص نفس العقوبة المقررة للجريمة وهو نص المادة 394 مكرر 7 من نفس قانون [2].

2-الظروف المشددة في للجريمة السيبرانية

إعتبر المشرع بنص المادة 394 مكرر 3 [3] من قانون العقوبات أن الجرائم المعلوماتية التي تستهدف الدفاع الوطني أو أي مؤسسة رسمية، بمثابة ظرف تشديد، فحرص المشرع الجزائري على ضمان حماية مطلقة لهيئات الدفاع الوطني والمؤسسات التابعة للدولة الجزائرية وتَوسَّعَ في هذه الحماية وذلك بنصه على مضاعفة العقوبة المنصوص عليها [4].

3-الشريك في الجريمة السيبرانية

يتضح من خلال نص المادة 394 مكرر5 [5] أن العقوبات تَمسُّ كل من يشارك أي مجموعة أو في أي إتفاقٍ الغرضُ منه التحضير أو الإعداد لإرتكاب الجرائم المعلوماتية، مع توفر القصد الجنائي، كما يستخلص أن مجرد المشاركة أو الإتفاق المجسَّد بفعل مادي يوحي بالتحضير للجريمة، خاصة أن ذلك يمكن أن يتم عبر الشبكات المعلوماتية [6].

---

(1) المادة 31 من الأمر 66-156 " المحاولة في الجنحة لا يعاقب عليها إلا بناء على نص صريح في القانون ". ج ر عدد 49، ص 704.

(2) المادة 394 مكرر7 من القانون 04-15" يعاقب على الشروع في إرتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها "، ج ر عدد 71، ص 12.

(3) المادة 394 مكرر3 من القانون 04-15 " تضاعف العقوبات المنصوص عليها في هذا القسم، إذا إستهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد ". ج ر عدد 71، ص 12.

(4) فاروق خلف، " الآليات القانونية لمكافحة الجريمة المعلوماتية "، مداخلة مقدمة ضمن فعاليات الملتقى الوطني الذي نظمته كلية الحقوق والعلوم السياسية قسم الحقوق جامعة محمد خيضر بسكرة، الموسوم بعنوان: الجريمة المعلوماتية بين الوقاية والمكافحة، يومي 16و17 نوفمبر 2015، ص 131.

(5) المادة 394 مكرر5 من القانون 04-15 " كل من شارك في مجموعة أو في إتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها "، ج ر عدد 71، ص 12.

(6) فضيلة عقيلة، المرجع السابق، ص 16.

4-الجرائم السيبرانية المرتكبة من طرف الشخص المعنوي

طبقا للمادة 394 مكرر 4 من قانون العقوبات، يُسأل الشخص المعنوي عن هذه الجرائم سواء بصفته فاعلا أصليا أو شريكا، ويكون ذلك إذا إرتُكبت الجريمة لحسابه أو بواسطة أحد أعضائه أو مُمثليه [1].

5-العقوبات التكميلية في الجرائم السيبرانية

نص المشرع الجزائري على عقوبات تكميلية وجوبية، تطبق على الجرائم السالف ذكرها، وتتمثل في مصادرة الأجهزة والبرامج والوسائل المستعملة، إضافة إلى غلق المواقع وأماكن الإستغلال، على أن يكون صاحبها على علم بالجريمة مع حفظ حق الغير حسن النية [2].

الفرع الثالث: الجريمة السيبرانية في القوانين الخاصة

إلى جانب القسم السابع مكرر من قانون العقوبات، نص المشرع الجزائري في بعض القوانين الخاصة على تجريم بعض السلوكات المعتبرة من ضمن الجرائم السيبرانية:

أولا: الجريمة السيبرانية في القانون المتعلق بالمواصلات السلكية واللاسلكية

صدر خلال سنة 2000 القانون رقم 03/2000 المتعلق بالبريد والمواصلات السلكية واللاسلكية، وقد تضمن أحكاما جزائية خاصة بمخالفة نظامها القانوني، فالأشخاص المرخص لهم بتقديم خدمة المواصلات السلكية واللاسلكية هم العمال متعاملي الشبكات العمومية الذين ينتهكون سرية المراسلات السلكية واللاسلكية أو المساعدة على ذلك، يعاقبون طبقا لنص المادة 137 [3] من قانون العقوبات وهذا ما نصت عليه المادة 127 [4] من القانون 03/2000.

---

(1) المرجع نفسه.

(2) فاروق خلف، المرجع السابق، ص 16.

(3) المادة 137 من القانون 06-23 " كل موظف أو عون من أعوان الدولة أو مستخدم أو مندوب عن مصلحة البريد يقوم بفض أو إختلاس أو إتلاف رسائل مسلمة إلى البريد أو يسهل فضها أو إختلاسها أو إتلافها، يعاقب بالحبس من ثلاثة (3) أشهر إلى خمس (5) سنوات وبغرامة من 30.000 دج إلى 500.000 دج "، ج ر عدد 84، ص 20.

(4) المادة 127 من القانون 2000-03 " تطبق العقوبات المنصوص عليها في المادة 137 من قانون العقوبات على كل شخص مرخص له بتقديم خدمة البريد السريع الدولي أو كل عون يعمل لديه والذي في إطار ممارسة مهامه يفتح أو يحول أو يخرب البريد أو ينتهك سرية المراسلات أو يساعد في إرتكاب هذه الأفعال،

تسري نفس العقوبات على كل شخص مرخص له بتقديم خدمة مواصلات سلكية ولا سلكية وكل عامل لدى متعاملي الشبكات العمومية للمواصلات السلكية واللاسلكية ..."، ج ر عدد 48، ص 23.

ثانيا: الجريمة السيبرانية في قانون الملكية الأدبية والفنية

وسَّعَ المشرع الجزائري قائمة المؤلفات المحمية بعد إصداره للأمر 05/03 المؤرخ في 2003/07/23، والمتعلق بحقوق المؤلف والحقوق المجاورة، حيث أضاف برامج المعلوماتية ضمن المصنفات الأصلية وذلك بموجب المادة 4 الفقرة (أ) من الأمر سالف الذكر.

ثالثا: الجريمة السيبرانية في قانون عصرنة العدالة

أصدر المشرع الجزائري القانون رقم 03/15 المؤرخ في 10 فيفري 2015، والمتعلق بعصرنة العدالة، وقد تضمن الفصل الخامس المتعلق بالأحكام الجزائية في المادتين 17 [1] و18 [2] منه حماية التوقيع والتصديق الإلكترونيين، وذلك بمعاقبة كل من يستعمل بطريقة غير قانونية العناصر الشخصية المتصلة بإنشاء توقيع إلكتروني خاص بتوقيع شخص آخر.

رابعا: الجريمة السيبرانية في قانون التأمينات الاجتماعية

عاقب المشرع الجزائري كل من يستلم بهدف الإستعمال غير المشروع بطاقة إلكترونية لمؤمن له إجتماعيا، وكذا كل تعديل أو حذف كلي أو جزئي للمعطيات التقنية أو الإدارية المدرجة في البطاقة، أو نسخ البرمجيات المتعلقة بإستعمالها، أو الشروع في إرتكاب أحد هذه الأفعال، وهذا طبقا للمواد 93 مكرر 2، 93 مكرر 3 و93 مكرر 5 من القانون 01/08 [3].

كما وتجدر الإشارة إلى **مشروع القانون المتعلق بالتجارة الإلكترونية** والذي تمت المصادقة عليه بالأغلبية من طرف أعضاء المجلس الشعبي الوطني يوم الثلاثاء 20 فبراير 2018 حيث ينص في المادتين 3 و4 منه على المعاملات المحظورة، والتي رصد لها المشرع عقوبات تطبق على مرتكبها، المواد (من المادة 36 إلى المادة 42) من مشروع القانون [4].

---

(1) المادة 17 من القانون 15-03 " يعاقب بالحبس من سنة (1) إلى خمس (5) سنوات وبغرامة تتراوح بين 100.000 دج إلى 500.000 دج كل شخص يستعمل بطريقة غير قانونية العناصر الشخصية المتصلة بإنشاء توقيع إلكتروني يتعلق بتوقيع شخص آخر "، ج ر عدد 06، ص 06.

(2) المادة 18 من القانون 15-03 " يعاقب بالحبس من سنة (1) إلى خمس (5) سنوات وبغرامة تتراوح بين 100.000 دج 500.000 دج كل شخص حائز شهادة إلكترونية يواصل إستعمالها رغم علمه بإنتهاء مدة صلاحيتها أو إلغائها "، ج ر عدد 06، ص 06.

(3) فاروق خلف، نفس المرجع، ص 11.

(4) ريم بن محمد صادق، نواب البرلمان يصادقون على مشروع قانون التجارة الإلكترونية، مقال في جريدة الجزائر اليوم، http://aljazairalyoum.com، أطلع عليه بتاريخ 20 مارس 2018.

الفصل الثاني

الفصل الثاني

آليات مكافحة الإجرام السيبراني

بدأت المؤسسات التشريعية ومختلف الهيئات والمنظمات على جميع الأصعدة الدولية والإقليمية والوطنية، تهتم بحماية إستخدام الحاسوب وتجريم السلوكات التي تستهدفه، حيث قامت بوضع العديد من الإتفاقيات الدولية والقوانين للتصدي لهذه الظاهرة الإجرامية.

وبناء على ما تقدم تم التطرق في هذا الفصل إلى الإطار الدولي والإقليمي لمكافحة الإجرام السيبراني (المبحث الأول)، مرورا إلى آليات مكافحة الإجرام السيبراني في التشريع الجزائري (المبحث الثاني).

المبحث الأول: الإطار الدولي والإقليمي لمكافحة الجريمة السيبرانية

في إطار الجهد الدولي المبذول وُجِدت العديد من الهيئات والمنظمات والمجالس الدولية التي لها دور ملحوظ في إبرام الإتفاقيات مُحاولةً ترسيخ التعاون الدولي لمواجهة الجرائم السيبرانية وحماية مستخدمي الأنترنت، وهذا ما أكدتهُ الإتفاقيات الدولية والإقليمية (المطلب الأول) ومختلف التشريعات الغربية والعربية (المطلب الثاني) [1].

المطلب الأول: تصدي الهيئات الدولية والإقليمية للجريمة السيبرانية

مع إرتفاع الخسائر الناتجة عن الإجرام السيبراني وتزايد حجم الأضرار الناتجة عنه، والتي تتخطى في أغلب الأحيان حدود الدول لتصل إعتداءاتها لأجهزة الحواسيب المملوكة للأفراد أو المؤسسات المالية أو الحكومات [2]، ورغم تميُّز الجرائم السيبرانية بالبعد الدولي كونها جرائم عابرة للحدود، إلَّا أنها لا تعتبر من بين الجرائم التي تختص المحكمة الجنائية الدولية بالنظر فيها [3].

(1) علي جبار الحسيناوي، جرائم الحاسوب والأنترنت، دار اليازوري العلمية للنشر والتوزيع، عمان، 2009، ص 147.

(2) المرجع نفسه.

(3) عبد اللطيف معتوق، المرجع السابق، ص 98.

إن الجريمة السيبرانية يعاقب عليها من خلال التشريعات الوطنية، والسلوك الإجرامي المكون لها يتم على المستوى الداخلي، فهي جرائم داخلية لكن قد يترتب عنها ضرر على المستوى الدولي، لذا إهتمت الهيئات والمنظمات الدولية بمواجهة هذه الجرائم، وعلى رأسها هيئة الأمم المتحدة والجمعية الدولية لقانون العقوبات (الفرع الأول)، وكذا المجلس الأوربي ومجلس وزراء الداخلية والعدل العرب (الفرع الثاني).

الفرع الأول: مواجهة المنضمات الدولية للجريمة السيبرانية

في سبيل محاولة التصدي للجرائم السيبرانية تبذل كل من الأمم المتحدة (أولا) والجمعية الدولية لقانون العقوبات (ثانيا) جهودا لا يستهان بها، تأكيدا على ضرورة تعزيز العمل المشترك بين جميع الدول.

أولا: القرار الصادر عن الأمم المتحدة بشأن جرائم الكمبيوتر – هافانا 1990

بعد إنعقاد مؤتمر الأمم المتحدة السابع لمنع الجريمة ومعاملة المجرمين في مدينة ميلانو الإيطالية عام 1985، والذي تمت من خلاله الإشارة إلى مشكلة الجريمة السيبرانية، حيث إنبثقت عنه مجموعة من التوجيهات من بينها تكليف لجنة الخبراء العشرين لدى منظمة الأمم المتحدة، بدراسة موضوع حماية نظم المعلومات والإعتداء على الحاسب الآلي، والتي بدورها أقرت جملة من التوصيات والمقترحات والمبادئ، التي تبنَّاها المؤتمر الثامن لمكافحة الجريمة ومعاملة المجرمين المنعقد في أوت 1990 بالعاصمة الكوبية هافانا [1].

تتلخص توصيات مؤتمر هافانا أساسا في التأكيد على ضرورة وضع إطار قانوني دولي بتظافر جهود جميع الدول الأعضاء، من أجل التعاون على الحد من إنتشار وتعاظم آثار هذه الظاهرة الإجرامية المستحدثة [2]، وذلك بأن تقوم كل دولة عضو بتكثيف جهودها لمكافحة إساءة إستخدام الكمبيوتر [3]، وأشار القرار أنه على الدول الأعضاء وفي سبيل مواجهة الإجرام السيبراني إتخاذ مجموعة من الإجراءات تتلخص في:

(1) علي جبار الحسيناوي، المرجع السابق، ص 147.

(2) محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2009، ص 155.

(3) يوسف صغير، المرجع السابق، ص 93.

– تحديث القوانين وأغراضها الجنائية، من أجل ضمان تطبيق الجزاءات والقوانين الراهنة بشأن جهات التحقيق وقبول الأدلة في الإجراءات القضائية على نحو ملائم، وإدخال تغييرات مناسبة إذا دعت الضرورة إلى ذلك، مع تحسين تدابير أمن الحاسب الآلي ومراعاة حماية الخصوصية وإحترام حقوق الإنسان وحرياته الأساسية.

– وضع أحكام وإجراءات تتعلق بالتحقيق والأدلة للتصدي لمثل هذا الشكل الجديد والمعقد من أشكال النشاط الإجرامي، ومصادرة أو رد الأصول الناجمة عن إرتكاب جرائم ذات صلة بالحاسوب.

– إعتماد تدابير لزيادة وعي الجماهير والعاملين في الأجهزة القضائية وأجهزة التنفيذ، بالمشكلة وبأهمية مكافحة الجرائم ذات الصلة بالحاسب الآلي.

– إعتماد تدابير مناسبة لتدريب القضاة والمسؤولين عن منع الجريمة الإقتصادية والجرائم المتعلقة بالحاسب الآلي والتحري والإدعاء فيها.

– الإهتمام بوضع قواعد خاصة بالآداب المتبعة في إستخدام جهاز الحاسب الآلي، وإعتماد سياسات تعالج المشكلات المتعلقة بضحايا جرائم الحاسب الآلي [1].

ثانيا: القرارات الصادرة عن المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات بشأن جرائم الكمبيوتر – ريودي جانيرو 1994

أوصى المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات الذي إنعقد في ريودي جانيرو بالبرازيل في 04 أكتوبر 1994، والذي تم من خلاله مناقشة جرائم الحاسب الآلي بأن تتضمن قائمة الحد الأدنى من الأفعال المشكلة لجرائم الحاسب الآلي والمتعين تجريمها [2] والتي يمكن ذكرها على النحو التالي:

–الإحتيال أو الغش المرتبط بالكمبيوتر،

–تزوير الكمبيوتر أو التزوير المعلوماتي،

(1) عبد الله عبد الكريم عبد الله، المرجع السابق، ص 108–110.

(2) نسيم دردور، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، مذكرة ماجستير، جامعة منتوري قسنطينة، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2012–2013، ص 84.

-الإضرار بالبيانات والبرامج وتشمل المحو والإتلاف والتعطيل للمعطيات،

-تخريب وإتلاف الكمبيوتر،

-الدخول غير المصرح به: وهو الولوج إلى نظام ما عن طريق إنتهاك إجراءات الأمن،

-الإعتراض غير المصرح به: وهو الإعتراض عن طريق وسائل فنية للإتصال توجه لنظام الكمبيوتر أو عدة نظم أو شبكة إتصالات [1].

وقد وضع القرار الصادر عن المؤتمر بعض القواعد الإجرائية لمكافحة الجرائم السيبرانية، كوجوب تحديد السلطات المؤهلة للتفتيش وضبط الأدلة في البيئة المعلوماتية، والسماح لها بإعتراض المراسلات، وكذا ضرورة توفير قدر من التعاون بين الضحايا والشهود ومستخدمي هذه التكنولوجيا لإتاحة إستخدام المعلومات في المتابعة القضائية، كما أكد القرار على ضرورة الأخذ بعين الإعتبار كل الوسائل المتعلقة بإنتهاك حرمة الحياة الخاصة والتجسس والمخاطر والخسائر الإقتصادية أثناء عملية التفتيش وضبط الأدلة [2].

زيادة على هذه الجهود المبذولة، تلعب الوكالات والمنظمات العالمية العاملة تحت لواء الأمم المتحدة دورا في هذا المجال، ومن ذلك المنظمة العالمية للملكية الفكرية WIPO [3]، فبعد تزايد الحاجة إلى إيجاد نصوص قانونية خاصة لحماية البرامج، شكلت المنظمة مجموعة عمل تضم عددا من الخبراء لحماية برامج الحاسب الآلي، وعبر الإجتماعات المتكررة والتي كان آخرها عام 1985 بالتعاون ما بين الويبو واليونيسكو في جنيف، ساد رأي لدى أغلب الدول الصناعية ودول العالم الثالث، وهو خضوع برامج الحاسب الآلي لقوانين حماية المؤلِّف، ومنذ ذلك العام وحتى الآن، عدَّلت معظم الدول تشريعاتها الخاصة بحق المؤلف [*] وأضافت برامج الحاسب الآلي إلى المصنفات الأدبية المحمية وفقا للقانون [4].

(1) عبد اللطيف معتوق، المرجع السابق، ص 100.

(2) المرجع نفسه.

(3) نسيم دردور، المرجع السابق، ص 84-85.

(*) المشرع الجزائري وضع برامج المعلوماتية ضمن المصنفات الأصلية، أنظر الصفحة 28 من هذا البحث.

(4) محمود أحمد عبابنة، المرجع السابق، ص 162.

الفرع الثاني: مواجهة الإجرام السيبراني على المستوى الإقليمي

إلى جانب المنظمات الدولية، إهتمت المجالس الإقليمية كالمجلس الأوربي (أولا) ومجلس وزراء الداخلية والعدل العرب (ثانيا)، بوضع إتفاقيات بغرض التصدي للجريمة المرتكبة عبر الأنترنت.

أولا: إتفاقية بودابست لمكافحة جرائم المعلوماتية والأنترنت – بودابست 2001

لعب المجلس الأوربي دورا هاما في مكافحة الجرائم السيبرانية، وصدرت عنه العديد من التوصيات لحماية تدفق المعلومات، ففي سنة 1981 وقَّع المجلس الأوربي إتفاقية تتعلق بحماية الأشخاص لمواجهة المعالجة الإلكترونية للبيانات ذات الصبغة الشخصية، وفي أفريل 2000 تقدمت اللجنة الأوربية بمشروع إتفاقية حول مشكلات جرائم المعلوماتية والحاسب الآلي، والتي تمت المصادقة عليها سنة 2001 ببودابست عاصمة المجر [1].

تتكون الإتفاقية من مقدمة وأربعة فصول، حيث تم إستعراض أهداف الإتفاقية ومرجعياتها السابقة، وبعض التدابير التشريعية الإقليمية والدولية المتعلقة بجرائم المعلوماتية، كما ثمَّنت المقدمة التعاون الدولي في هذا المجال [2].

حيث تضمَّن الفصل الأول من الإتفاقية تعريف المصطلحات من خلال نص المادة الأولى، أما الفصل الثاني جاء تحت عنوان الإجراءات المتعين إتخاذها على المستوى الوطني وتضمَّن ثلاثة أقسام، يضم القسم الأول منها المواد من 2 إلى 13 ويعالج النصوص الموضوعية للجرائم المعلوماتية [3]، حيث نص على خمس مجموعات:

-المجموعة الأولى، وتتضمن الجرائم التي تستهدف أمن المعلومات وسريتها، وسلامة معطيات المنظومة المعلوماتية وإساءة إستخدام الأجهزة.

-المجموعة الثانية، الجرائم المرتبطة بالكمبيوتر وهي التزوير والإحتيال المرتبطين به.

(1) هشام عبد الكريم، " التمييز العنصري وصور الإستخدامات الجديدة للأنترنت "، مداخلة مقدمة ضمن فعاليات الملتقى الدولي الذي نظمته كلية الحقوق والعلوم السياسية قسم الحقوق جامعة برج بوعريريج، الموسوم بعنوان: الإجرام السيبراني المفاهيم والتحديات، يومي 11 و12 أفريل 2017، ص 08.

(2) عبد الله عبد الكريم عبد الله، المرجع السابق، ص 124-125.

(3) عبد اللطيف معتوق، المرجع السابق، ص 101.

-المجموعة الثالثة، وتتضمن الجرائم المرتبطة بالمحتوى، وتنطوي تحتها صورة واحدة وهي جرائم دعارة الأطفال وتشمل تجريم أي نشاط متعلق بهذا الموضوع.

-المجموعة الرابعة، وهي الجرائم المرتبطة بحقوق المؤلف والملكية الفكرية.

-المجموعة الخامسة، تحوي المساهمة والشروع والمسؤولية الجزائية للأشخاص المعنوية [1].

ثانيا: الإتفاقية العربية لمكافحة جرائم تقنية المعلومات

بتاريخ 21 ديسمبر 2010، وافق مجلس وزراء الداخلية والعدل العرب في إجتماعهم المشترك المنعقد بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة، على الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، تحتوي هذه الإتفاقية على 43 مادة، وجاء في المادة الأولى منها " تهدف هذه الإتفاقية إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات لدرء أخطار هذه الجرائم، حفاظا على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها "، ونجد في الفصل الثاني تفصيلا للأفعال التي تعد مجرمة، أما الفصل الثالث منها فقد تم التعرض من خلاله إلى نطاق تطبيق الأحكام الإجرائية، وفي الفصل الرابع نُصَّ على التعاون القانوني والقضائي، أما الفصل الخامس فتضمن أحكاما ختامية [2].

المطلب الثاني: تصدي التشريعات الغربية والعربية للجريمة السيبرانية

كان للإتفاقيات الدولية والإقليمية، الأثر البالغ على تشريعات العديد من دول العالم، حيث قامت هذه الأخيرة بتبني فكرة الحماية الجزائية لمستخدمي الأنترنت وكذا البيانات المخزنة في النظم المعلوماتية، وعليه سنتطرق من خلال هذا المطلب لأبرز النماذج التشريعية الغربية (الفرع الأول)، والعربية (الفرع الثاني).

الفرع الأول: تشريعات بعض الدول الغربية

من خلال هذا الفرع سنتناول مكافحة التشريع البريطاني للجريمة المعلوماتية وذلك لريادته في النظام الأنجلوسكسوني (أولا)، وكذا التشريع الفرنسي بإعتباره الرائد في النظام اللاتيني (ثانيا).

(1) محروس نصار غايب، " الجريمة المعلوماتية "، مجلة هيئة التعليم التقني الأكاديمية، المجلد 24، العراق، 2011، ص 20-21.

(2) فاروق خلف، المرجع السابق، ص 08.

أولا: التشريع البريطاني

تأتي بريطانيا كثالث دولة تَسُنُّ قوانين خاصة بجرائم الحاسب الآلي، حيث أقرَّت قانون مكافحة التزوير والتزييف سنة 1981، والذي شمل في تعاريفه الخاصة، تعريف تزوير وسائط التخزين الحاسوبية المتنوعة أو أي أداة أخرى يتم التسجيل عليها، سواء بالطرق التقليدية أو الإلكترونية أو بأي طريقة أخرى [1].

ثم أصدرت بعد ذلك قانونا خاص بإساءة إستخدام الحاسوب الآلي سنة 1990، الذي نظم جرائم الحاسب الآلي ضمن ثلاث فئات، تتعلق الأولى بالدخول غير المصرح به إلى معطيات الحاسب الآلي وبرامجه المخزنة، والثانية فقد تناولت تجريم الدخول غير المصرح به مع وجود نية إرتكاب أو تسهيل إرتكاب جرائم أخرى، أما الثالثة فتتعلق بتجريم الإتلاف المعلوماتي وذلك من خلال نص المادة الثالثة من هذا القانون [2].

ثانيا: التشريع الفرنسي

نص المشرع الفرنسي من خلال قانون العقوبات الفرنسي، على تجريم الإعتداء على أنظمة معالجة البيانات، وذلك بموجب الفصل الثالث من الباب الثاني منه، ومن ضمن الجرائم التي نصَّ عليها هذا الفصل، إدخال أو مسح أو تغيير معلومات بطرق الغش، المادة 323-3، كما نص أيضا على تجريم عدة أفعال تقع ضد المصالح العليا للدولة، وذلك إذا إنصبت على المعلومات أو البيانات التي تمت معالجتها إلكترونيا، المواد من 411-6 إلى 411-10، وإلى جانب هذه النصوص، فإن المشرع الفرنسي قد نص على بعض الجوانب المتصلة بالمستند الإلكتروني في قوانين متفرقة أهمها، قانون الإثبات والتوقيع الإلكتروني الصادر سنة 2000، واللائحة الصادرة سنة 2001 التي أقرَّ من خلالها الأخذ بالدليل الإلكتروني في الإثبات والتوقيع الإلكتروني [3].

(1) علي جبار الحسيناوي، المرجع السابق، ص 165.

(2) عبد اللطيف معتوق، المرجع السابق، ص 90.

(3) فتيحة رصاع، المرجع السابق، ص 94.

الفرع الثاني: تشريعات بعض الدول العربية

سنعرض من خلال هذا الفرع إلى التجربة العربية في مجال مكافحة للإجرام السيبراني من خلال تشريع الإمارات العربية المتحدة (أولا)، والتشريع المصري (ثانيا).

أولا: تشريع دولة الإمارات العربية المتحدة

تعد دولة الإمارات العربية المتحدة من الدول العربية القليلة والرائدة في مجال التشريع الخاص بحماية النظم المعلوماتية، وقد تناول القانون الإتحادي رقم 02 لسنة 2006 المتعلق بمكافحة جرائم المعلوماتية، مجموعة من الجرائم، كجريمة إختراق المواقع والأنظمة الإلكترونية، أين تم التمييز بين الأنظمة المعلوماتية وبين الإختراق، وتَرتُب نتيجة متعلقة بالإلغاء أو الحذف أو تدمير المعلومات، إذ جعل العقوبة في الحالة الثانية أشد وتُقدر بالحبس لمدة لا تقل عن 6 أشهر مع غرامة مالية، وفي حالة إختراق النظم المعلوماتية يترتب عن ذلك إنتهاك للمعلومات الشخصية، وتكون العقوبة هي الحبس لمدة لا تقل عن سنة وغرامة مالية مقدرة بعشرة آلاف درهم [1].

لكن هذا القانون تعرض للنقد في حلقة نقاشية نظمها معهد التدريب والدراسات القضائية بالإمارات العربية المتحدة، حيث أن المشاركين من قضاة ووكلاء نيابة أكدوا في ختام النقاش أن مواد هذا القانون تتعارض فيما بينها، ودعوا لإيجاد محاكم مختصة للبت في جرائم تقنية المعلومات وعقد المزيد من برامج التدريب والتظافر لتوعية الشباب بالقانون [2].

ثانيا: التشريع المصري

لقد وضع المؤتمر التأسيسي الأول لجمعيات قانون الأنترنت الذي عقد بالقاهرة في 27 سبتمبر 2004 اللبنة الأولى لإنشاء جمعيات ومنظمات للعمل التطوعي في مجال قانون الأنترنت، ثم تم عقد المؤتمر الدولي الأول لقانون الأنترنت بمدينة الغردقة في أوت 2005 وبدأ الإهتمام في مصر بمكافحة الجرائم المعلوماتية [3].

(1) عبد اللطيف معتوق، المرجع السابق، ص 95-96.

(2) عبد الله عبد الكريم عبد الله، المرجع السابق، ص 79.

(3) عبد الفتاح بيمو حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2006، ص 556.

ثم تأسست الجمعية المصرية لمكافحة جرائم المعلوماتية في نفس السنة، وهي منظمة غير حكومية تعمل على نشر الوعي وإعداد الدراسات والمؤتمرات حول هذه الجرائم [1]، وتعتبر حركة التشريع في مجال مكافحة الجريمة السيبرانية في مصر، ضعيفة مقارنة بدولة الإمارات العربية المتحدة، إلا أن تطبيق بعض النصوص التقليدية المتعلقة بالتزوير والإحتيال والسرقة والمساس بإعتبار الأشخاص، لا يزال مستمرا في القانون المصري [2].

ويعتبر قانون التوقيع الإلكتروني الصادر سنة 2004، أول قانون يصدر بشأن الأفعال المتعلقة بالنظم المعلوماتية في مصر، حيث جرم أفعالا بموجب المادة 23 منه، تتعلق بالحصول على توقيع أو وسيط أو محرر إلكتروني بدون وجه حق، أو إعتراضه أو تعطيله عن أداء وظيفته وقد عُرِّف الوسيط الإلكتروني في الفقرة الرابعة من المادة الأولى من قانون التوقيع الإلكتروني المصري بأنه " أداة أو أدوات أو أنظمة إنشاء التوقيع الإلكتروني"، فهو عبارة عن نظام معلوماتي يساعد على إنشاء التوقيع الإلكتروني وإصدار المحررات الإلكترونية [3].

من خلال ما سبق عرضه يتضح أن مختلف الإتفاقيات الدولية والإقليمية وكذا التشريعات الوطنية قد أولت إهتماما كبيرا لموضوع الجريمة السيبرانية، وذلك بهدف تحقيق مجموعة من الأهداف المتمحورة أساسا حول توفير الحماية اللازمة لمستخدمي الأنترنت وللنظم المعلوماتية، حيث سعت هذه الإتفاقية إلى بناء سياسة جنائية مشتركة من أجل مكافحة الجرائم المعلوماتية في جميع أنحاء العالم من خلال تنسيق وإنسجام التشريعات الوطنية ببعضها البعض، و تعزيز قدرات القضاء وكذا تحسين التعاون الدولي في هذا الإطار، إضافة إلى تحديد عقوبات للجرائم السيبرانية في إطار القوانين الداخلية.

(1) عبد الله عبد الكريم عبد الله، المرجع السابق، ص 93.

(2) عبد اللطيف معتوق، المرجع السابق، ص 97.

(3) علي عدنان الفيل، الإجرام الإلكتروني، الطبعة الأولى، منشورات زين الحقوقية، بيروت، 2011، ص 231-242.

المبحث الثاني: آليات مكافحة الإجرام السيبراني في التشريع الجزائري

تعتبر الجزائر من بين الدول التي تسير على نهج مكافحة الجريمة السيبرانية، وذلك من خلال تعديل قوانينها، بدأً بتعديل قانون العقوبات، بموجب القانون رقم 04-15 المؤرخ في 25 أوت 2004، والذي تم من خلاله إدراج جرائم المساس بأنظمة المعالجة الآلية للمعطيات ضمن نطاق الأفعال المجرَّمة، وصولا إلى إصدار القانون رقم 09-04 المؤرخ في 05 أوت 2009، والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتهما، وفي هذا الإطار سنتناول الإجراءات التقليدية التي أقرها المشرع الجزائري لمكافحة الجريمة السيبرانية (المطلب الأول)، ثم الآليات المستحدثة التي تتماشى وطبيعة الجريمة السيبرانية (المطلب الثاني).

المطلب الأول: مكافحة الجريمة السيبرانية بالوسائل الإجرائية التقليدية

لقد أثارت الإجراءات التقليدية المعتمدة جدلا فقهيا كبيرا من ناحية صلاحيتها في البيئة الرقمية، وسنكتفي بدراسة الإجراءات التقليدية المتمثلة في التفتيش والمعاينة والخبرة، وذلك لعلاقتها المباشرة بالوسط الرقمي وقابلية تطبيق قواعدها من جهة، ومن جهة أخرى إستبعاد الإعتراف والشهادة والاستجواب، كونها لا تثير أي صعوبات ونظرا لخضوعها للقواعد العامة المقررة قانونا [1].

الفرع الأول: التفتيش في البيئة الرقمية

إن التفتيش في البيئة الرقمية هو إجراء يسمح بجمع الأدلة المخزنة أو المسجلة بشكل إلكتروني، والبحث عن معطيات الحاسب الآلي غير المادية المخزنة في الجهاز أو في الأقراص المضغوطة [2]، بهدف إثبات الجريمة السيبرانية ونسبتها إلى مرتكبها.

(1) سليمان النحوي، " آليات مكافحة الجريمة السيبرانية في التشريع الجزائري "، مداخلة مقدمة ضمن فعاليات الملتقى الدولي الذي نظمته كلية الحقوق والعلوم السياسية قسم الحقوق جامعة برج بوعريريج، الموسوم بعنوان: الإجرام السيبراني المفاهيم والتحديات، يومي 11 و12 أفريل 2017، ص 03.

(2) خالد عياد الحلبي، إجراءات والتحقيق في جرائم الحاسوب والأنترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن، 2011، ص 157.

أولا: خضوع أنظمة الحاسب الآلي للتفتيش

بناء على ما سبق ذكره، يمكن القول أن تفتيش أنظمة الحاسب الآلي يكون بإحدى الصورتين:

1-تفتيش المكونات المادية للكمبيوتر

تتمثل المكونات المادية لجهاز الحاسب الآلي [1]، في مجموعة من الوحدات المتصلة فيما بينها بشكل يجعلها تعمل كنظام متكامل [2] وهي: وحدات الإدخال مثل الفأرة ولوحة المفاتيح ووحدات الإخراج مثل شاشة الحاسب الآلي والطابعة، وأخيرا الذاكرة [3].

وعليه لا توجد أية صعوبة عند معاينة القائمين بالتفتيش لمسرح الجريمة الواقعة على المكونات المادية للحاسب الآلي، نظرا لعدم وجود تعارض بين تفتيش المُكوِّن المادي لجهاز الحاسب الآلي، مع مفهوم التفتيش التقليدي، لأنه يمثل في ذاته بحثا عن الأدلة المادية، وكل ما يتطلبه إجراء التفتيش في هذه الحالة أن يتم وفقا للقواعد القانونية [4].

2-تفتيش المكونات المعنوية للكمبيوتر

المكونات المعنوية لجهاز الحاسب الآلي، هي عبارة عن مجموعة من البرامج والملفات المتعلقة بتشغيل وحدة معالجة البيانات، وتنقسم إلى كيانات أساسية تضم البرامج الضرورية التي يتم من خلالها تشغيل وإستخدام جهاز الحاسب الآلي، وكيانات تطبيقية تضم برامج تُمكِّن المستخدم من أن ينفذ بواسطتها عملا معينا بإستخدام جهاز الحاسوب [5].

ولقد ثار خلاف فقهي بخصوص إمكانية تفتيش العناصر المعنوية للحاسب الآلي، حيث يرى جانب من الفقه أنه متى كانت الغاية من التفتيش هي ضبط الأدلة المادية التي تفيد في الكشف عن الحقيقة، فإن هذا المفهوم يمتد ليشمل جميع المعلومات والبيانات الرقمية بمختلف

(1) بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2011، ص 67.

(2) خالد عياد الحلبي، المرجع السابق، ص 158.

(3) علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والإنترنت، الطبعة الأولى، عالم الكتب الحديث، الأردن، 2004، ص 19.

(4) بكري يوسف بكري، المرجع السابق، ص 68.

(5) علي حسن محمد الطوالبة، المرجع السابق، ص 24.

أشكالها [1]، وسبب ذلك أن القوانين الإجرائية عندما تنص على إصدار الإذن بضبط أي شيء، فإن ذلك يجب تفسيره بصورة واسعة، حيث يشمل جميع المعلومات والبيانات المادية أو المعنوية هذا من جهة، ومن جهة أخرى ذهب رأي آخر إلى عدم إنطباق المفهوم المادي على بيانات الحاسب الآلي أي المكونات المعنوية، لذلك فهو يقترح مواجهة هذا القصور التشريعي والنص صراحة على أن تفتيش الحاسب الآلي لا بد أن يشمل المواد المعالجة عن طريق الحاسب الآلي، أي بياناته [2].

موقف المشرع الجزائري من خلال القانون 09-04 واضح، إذ نص صراحة على تفتيش أنظمة الحاسب الآلي، وذلك بموجب نص المادة 05 منه، حيث يجوز للسلطات القضائية المختصة وكذا الشرطة القضائية، في إطار قانون الإجراءات الجزائية الدخول بغرض التفتيش إلى منظومة معلوماتية أو جزء منها ولو عن بعد، وكذا المعطيات والمعلومات المخزنة فيها [3].

ثانيا: خضوع شبكات الإتصال للتفتيش

إن طبيعة الجريمة السيبرانية تزيد من صعوبة القيام بهذا الإجراء، فالبيانات التي تتضمن أدلة قد تتوزع عبر شبكات الحاسب الآلي في أماكن قد تكون على مسافات بعيدة عن الموقع المادي الذي يتم فيه التفتيش هذا من جهة، ومن جهة ثانية قد يكون الموقع الفعلي للبيانات ضمن دولة أخرى، وهو ما يُصعِّب تنفيذ هذه العملية [4].

الفرع الثاني: المعاينة في الوسط الإلكتروني

يقصد بالمعاينة في علم التحقيق الجنائي " مشاهدة المكان الذي إرتكبت فيه الجريمة وعمل وصف شامل له، سواء بالكتابة أو بالرسم التخطيطي أو التصوير، لإثبات حالته كما تركه الجاني " [5]، لذا تعتبر المعاينة وسيلة جد هامة لتكوين الفكرة الأولى عن كيفية إرتكاب الجريمة، بالإضافة إلى أنها تعد من أهم مصادر الأدلة الجنائية المادية.

(1) عبد الفتاح بيومي حجازي، المرجع السابق، ص 378.

(2) خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2010، ص 182.

(3) النحوي سليمان، المرجع السابق، ص 04.

(4) المرجع نفسه.

(5) خالد ممدوح إبراهيم، المرجع السابق، ص 149.

أولا: دور المعاينة في كشف الجريمة السيبرانية

المعاينة تعتبر من أهم إجراءات التحقيق، إلا أن دورها في الكشف عن الجريمة السيبرانية يتضاءل، وسبب ذلك أن الجريمة التقليدية تجري غالبا على مسرح جريمة وتخلف آثار مادية، هذا المسرح يفتح المجال أمام جهات البحث والتحري للكشف عن غموض الجريمة، على عكس مسرح الجريمة السيبرانية الذي يتضاءل فيه دور المعاينة، بسبب أن هذا النوع من الجرائم قلَّما يترك آثار مادية، بالإضافة إلى إمكانية التلاعب بالأدلة عن بعد عن طريق محوها أو إتلافها أو تغييرها، وعليه يمكن القول أنه ينبغي على القائمين بالمعاينة التعامل مع مسرح الجريمة السيبرانية على أنه مسرحان، مسرح مادي وآخر معنوي، فالأول يشمل جميع المكونات المادية للحاسب الآلي التي من الممكن أن تحوي آثار مادية مثل بصمات الجاني أو وسائط تخزين رقمية أو أوراق ....الخ، أما الثاني فهو مسرح إفتراضي ما يقع داخل البيئة الإلكترونية (الرقمية) لجهاز الحاسب الآلي، ويحتوي على جميع المعلومات والبيانات الرقمية المخزنة فيه والتي قد تفيد في التحقيق [1].

ثانيا: إجراءات المعاينة في الوسط الإلكتروني

حتى تكون لمعاينة مسرح الجريمة السيبرانية فائدة عملية في الكشف عن ملابسات الجريمة، لابد من مراعاة العديد من الإجراءات والخطوات التقنية، للقيام بإجراء المعاينة ومنها:

1-الإجراءات المتخذة قبل إجراء المعاينة

عادة ما تكون هذه الإجراءات والخُطوات تحضيرية، غرضها تهيئة الوسائل البشرية والمادية للقيام بإجراء المعاينة، ويتم ذلك بإعداد خطة عمل تحتوي على إعداد شامل للأدوات المستعملة في المعاينة، وتقسيم المهام بين الفنيين القائمين على هذا الإجراء [2]، بالإضافة إلى توفير معلومات مسبقة عن مكان الجريمة وعن نوع وعدد الأجهزة المراد معاينتها، وذلك لتحديد إمكانيات التعامل معها فنيا من حيث الضبط والتأمين وحفظ المعلومات، وتأمين التيار الكهربائي تجنبا

(1) فاطمة زهرة بوعناد، " مكافحة الجريمة الإلكترونية في التشريع الجزائري "، مجلة الندوة للدراسات القانونية، جامعة جيلالي اليابس سيدي بالعباس، العدد الأول، 2013، ص 68.

(2) كاظم محمد عطيات، محمد رضوان هلال، " كيفية التعامل التقني والآمن مع أوعية الجريمة الرقمية في مسرح الجريمة لضمان حيدة الدليل المستخلص"، المجلة العربية الدولية للمعلوماتية، العدد الخامس، المجلد 3، السعودية، 2014، ص 45.

لتلفها، كما أنه يجب في هذه المرحلة توفير الإحتياجات الضرورية من الأجهزة والبرامج للاستعانة بها في الفحص والتشغيل وفك التشفير [1].

2-الإجراءات المتخذة أثناء القيام المعاينة

بعد القيام بالإجراءات التحضيرية التي سبق ذكرها، يقوم الفنيون القائمون على إجراء المعاينة بتصوير جهاز الحاسب الآلي وكافة مكوناته المادية [2]، مع التركيز على تصوير الأجزاء الخلفية له ومراعاة تسجيل وقت وتاريخ ومكان التقاط كل صورة [3]، زيادة على ذلك القيام بملاحظة وإثبات حالة توصيلات الأسلاك المتصلة بكل ملحقات الحاسب الآلي، وأيضا التحفُّظ على محتويات سلة المهملات من الأوراق الملقاة أو الممزقة، وكذا الشرائط والأقراص المضغوطة وفحصها، بعد ذلك يتم البحث في جهاز الحاسب الآلي عن الآثار الرقمية التي خلفها المستخدم، وفي هذه المرحلة يجب تعطيل حركة الإتصالات السلكية واللاسلكية بشبكة الإنترنت تجنبا لتلف الدليل الجنائي الرقمي أو التلاعب به وتخريبه عمدا عن بعد، وفي حالة ضبط معلومات أو بيانات رقمية، يجب مراعاة قواعد تحريز الأدلة الجنائية الرقمية التي يتطلب تخزينها عناية فائقة للدعائم المادية وفحصها وإستعمالها لاحقا [4].

الفرع الثالث: الخبرة في مجال الجريمة السيبرانية

الخبرة القضائية هي إستشارة فنية يستعين بها القاضي أو المحقق لمساعدته في تكوين عقيدته نحو المسائل التي يحتاج تقديرها إلى معرفة أو دراية علمية خاصة [5]، ومنه فالخبرة هي وسيلة لتحديد التفسير الفني للأدلة عن طريق ربطها بالعلوم، وهي في حقيقتها ليست دليلا مستقلا وإنما هي تقييم فني لهذا الدليل [6].

---

(1) نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الإستدلالات، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2007، ص 199.

(2) كاظم محمد عطيات، محمد رضوان هلال، المرجع السابق، ص 45.

(3) خالد ممدوح إبراهيم، المرجع السابق، ص 172.

(4) سليمان النحوي، المرجع السابق، ص 06.

(5) فاطمة زهرة بوعناد، المرجع السابق، ص 71.

(6) عبد الفتاح بيومي حجازي، المرجع السابق، ص 321.

أولا: قيمة الخبرة في مجال الجريمة السيبرانية

يستطيع الخبير من خلال ما لديه من معلومات وخبرة إبداء رأي في أمر من الأمور المتعلقة بالقضية التي تحتاج إلى خبرة فنية خاصة [1]، وإذا كانت الإستعانة بخبير فني في المسائل الفنية البحتة في الجرائم التقليدية أمرا ضروريا، فإن الإستعانة به في مجال الجريمة السيبرانية أكثر من ضروري [2]، وذلك للطبيعة التقنية للجريمة من جهة، وخصوصية الأدلة الفنية التي تتطلب مهارة ودراية كبيرة في مجال الحاسب الآلي من جهة أخرى، ولهذا كان لزاما أن يتم اللجوء إلى خبير فني ومتخصص.

ونظرا لطبيعة عمل الخبير في هذا المجال، إهتم المشرع الجزائري بتنظيم أعمال الخبرة وكيفية اللجوء إليها وذلك من خلال المواد من 143 إلى المادة 156 ق.إ.ج، بحيث نصت المادة 143 منه على أنه " لجهات التحقيق أو الحكم عندما تعرض عليها مسألة ذات طابع فني أن تأمر بندب خبير إما بناء على طلب النيابة العامة وإما من تلقاء نفسها ".

ومن جهة أخرى نص المشرع من خلال نص المادة 04/05 المستحدثة بالقانون رقم 09-04 أنه " يمكن للسلطات 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 " [3].

ومنه يمكن القول أنه يوجد دائما هناك حاجة ماسة إلى خبراء وفنيين من أجل القيام بالعديد من المهام التقنية مثل الكشف عن الأدلة الجنائية الرقمية وتحليلها، أو إصلاح الدليل وإعادة تجميعه من المكونات المادية للحاسب الآلي، أو التأكد من أن الدليل لم يتم العبث به [4].

(1) خالد ممدوح إبراهيم، المرجع السابق، ص 285.

(2) نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجستير، جامعة الحاج لخضر باتنة، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2012-2013، ص 166.

(3) القانون رقم 09-04 المؤرخ في 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من جرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، ج ر عدد 47، بتاريخ 16 أوت 2009، ص 05.

(4) خالد ممدوح إبراهيم، المرجع السابق، ص 302.

ثانيا: دور الخبير في مجال الجريمة السيبرانية

عند قيام الخبير بمزاولة مهامه يجب أن تتوفر لديه مجموعة من الضوابط القانونية والفنية وهي أن يتم إختياره من قائمة الخبراء المعدة مسبقا، وهذا ما نصت عليه المادة 144 من قانون الإجراءات الجزائية، حيث يُختار الخبراء من الجدول الذي تُعِدُهُ المجالس القضائية بعد إستطلاع رأي النيابة العامة، وإستثناءً يجوز للجهات القضائية أن تختار بقرار مسبب وبصفة إستثنائية خبراء ليسوا مقيَّدين في أي من هذه الجداول، ويجب على الخبير أيضا أن يكون قد أدى اليمين القانونية حتى لا يشوبَ عمله البطلان، وهو ما نصت عليه المادة 145 من نفس القانون، وذلك بأن يحلف الخبير المقيد لأول مرة بالجدول الخاص بالمجلس القضائي، اليمين القانونية أمام المجلس[1].

يقوم الخبير بعد ذلك بمزاولة مهامه المحددة، وبمجرد إنتهائه من عمله يُعِدُّ تقريرا كتابيا مفصلا لما توصل إليه من نتائج، ويودعه خلال المدة المحددة في الأمر أو الحكم بالندب، كما يجب على الخبير أن يكون ملما بكل ما يتعلق بالحاسب الآلي وملحقاته، إضافة إلى وجوب تمكنه وفهمه للبيئة التي يعمل فيها، وقدرته على أداء المهام الموكلة إليه دون أن يترتب على ذلك أي ضرر للدليل الجنائي الرقمي المراد إستخلاصه [2].

تماشيا مع إتجاه تطوير وتكوين خبراء متخصصين في مجال مكافحة الجريمة السيبرانية، بادرت مختلف الدول بإنشاء وحدات متخصصة في مجال البحث والتحري، وكانت الجزائر من بين هذه الدول التي أنشأت وحدات متخصصة ضمن جهازي الشرطة والدرك الوطني لمكافحة الجريمة السيبرانية، وتجسد ذلك بعد إنشاء المعهد الوطني للأدلة الجنائية وعلم الإجرام تحت وصاية القيادة العامة للدرك الوطني، بموجب المرسوم الرئاسي رقم 04-183 المؤرخ في 27 جوان 2004 ، بحيث نصت المادة 04 منه على العديد من المهام الموكلة للمعهد، أهمها إجراء الخبرات والفحوص العلمية بناء على طلب من القضاة، بالإضافة إلى المساعدة التقنية والفنية أثناء القيام بالتحريات بإستخدام مناهج الشرطة العلمية والتقنية الرامية إلى تجميع وتحليل الأشياء

(1) إبراهيم بلعليات، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري، الطبعة الأولى، دار الخلدونية، الجزائر، 2007، ص 304.

(2) عبد الفتاح بيومي حجازي، المرجع السابق، ص 331.

والآثار والوثائق المأخوذة من مسرح الجريمة، ويضم هذا المعهد قسم الإعلام الآلي المختص بالتحقيق من خلال جمع الأدلة الجنائية الرقمية وتحليلها [1].

إلى جانب المعهد الوطني للأدلة الجنائية وعلم الإجرام، تم إستحداث المعهد الوطني للبحث في علم التحقيق الجنائي تحت وصاية المديرية العامة للأمن الوطني، بموجب المرسوم الرئاسي رقم 04-432 المؤرخ في 29 ديسمبر 2004 ، حيث نص في المادة 05 منه على مجموعة من المهام من بينها إعداد تقارير الخبرة، وأيضا القيام بالتكوين وتجديد المعارف في ميدان علم التحقيق الجنائي والإجرام، ويحتوي هذا المعهد على مصلحة الخبرات الخاصة بالدلائل التكنولوجية، حيث تقوم بتحليل الدلائل المادية التي تم جمعها أثناء معاينة المخالفات والتحريات في مسرح الجريمة السيبرانية وإعداد تقارير الخبرة [2].

كما إستحدث القانون رقم 09-04 أيضا، من خلال المادة 13 منه، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، حيث تتولى هذه الأخيرة العديد من المهام التي تدخل ضمن إطار مكافحة الجريمة السيبرانية، ولعل أهمها ما أتت به المادة 14 الفقرة (ب)، إذ تتولى " مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والإتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية "، وقد صدر التنظيم الخاص بهذه الهيئة من خلال المرسوم الرئاسي رقم 15-261 المؤرخ في 2015/10/08 المحدد لتشكيلة وتنظيم وكيفيات سير هذه الهيئة [3].

المطلب الثاني: الوسائل الإجرائية المستحدثة لمكافحة الجريمة السيبرانية

إن الوسائل الإجرائية المستحدثة لمكافحة الجريمة السيبرانية هي أساليب محددة بموجب القانون، تهدف إلى إثبات وقوع الجريمة وتكشف عن شخصية مرتكبها، عن طريق إستخدام برامج وتقنيات إلكترونية مختلفة، وذلك تماشيا مع إرادة المشرع في مكافحة الجريمة السيبرانية.

فقد إستحدث المشرع وسائل إجرائية، بموجب القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006، المعدِل والمتمم للأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية، وهي نظام إعتراض المراسلات (الفرع الأول) ونظام التسرب (الفرع الثاني) هذا من جهة، ومن جهة أخرى

(1) نعيم سعيداني، المرجع السابق، ص 188.

(2) المرجع نفسه، ص 189.

(3) سليمان النحوي، المرجع السابق، ص 08.

تم إستحداث الإجراء المتمثل في نظام المراقبة الإلكترونية (الفرع الثالث) والمساعدة القضائية الدولية لمكافحة الجريمة السيبرانية (الفرع الرابع) وذلك بموجب القانون رقم 09-04 [1].

الفرع الأول: إعتراض المراسلات

تعتبر عملية إعتراض المراسلات من بين أهم الإجراءات المستحدثة، لما لها من أهمية وفائدة في جمع الأدلة الجنائية الرقمية، ومنه وجب التطرق لهذا الإجراء من خلال مفهومه (أولا) وشروطه (ثانيا) وكيفية القيام به (ثالثا) [2].

أولا: مفهوم عملية إعتراض المراسلات

نظام إعتراض المراسلات والتسجيل والإلتقاط للمراسلات والأصوات والصور، من بين أهم الآليات المعتمدة من قبل المشرع الجزائري، حيث أنه بالرجوع لنص المادة 65 مكرر 5 من القانون رقم 22/06 ، والتي جاء فيها " إذا إقتضت ضرورات التحري في الجريمة المتلبس بها، أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بالمعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد، يجوز لوكيل الجمهورية المختص أن يأذن بما يأتي:

- إعتراض المراسلات التي تتم عن طريق وسائل الإتصال السلكية واللاسلكية،

- وضع الترتيبات التقنية، دون موافقة المعنيين من أجل إلتقاط الصور وتثبيت وبث وتسجيل الكلام المُتفوه أو إلتقاط صور لشخص أو عدة أشخاص يتواجدون في أماكن خاصة أو عمومية أو إلتقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص... ".

يتضح من خلال نص المادة أن المشرع الجزائري لم يُعرف نظام إعتراض المراسلات هذا من جهة، ومن جهة أخرى قام بتحديد مجال تطبيق هذا النظام، حيث جعله يطبق على جرائم مُحددة بذاتها، من بينها الجرائم الماسة بالمعالجة الآلية للمعطيات.

(1) عبد اللطيف، معتوق المرجع السابق، ص 106.

(2) سليمان النحوي، المرجع السابق، ص 09.

حيث يمكن أن يتعدى هذا النظام إلى جرائم أخرى فهو يتعلق فقط بالجرائم المذكورة في المادة سالفة الذكر، ويبدو أن المشرع الجزائري قد راعى الكثير من الإعتبارات للأخذ بالمفهوم الحصري للجرائم في هذا الخصوص وذلك يعود للأسباب التالية:

– أن الجرائم المذكورة تعد الأخطر بذاتها، وهي جرائم يَرتكبها أشخاص محترفون وتتوافر لديهم مؤهلات خاصة بالإضافة إلى صعوبة إثبات هذا النوع من الجرائم.

– أن نظام إعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور، يعد من الناحية الشكلية إعتداءا واضحا على الكثير من المبادئ الدستورية المستقرة، وخاصة حرمة الحياة الخاصة والحق في الخصوصية وضرورة الحصول على الأدلة بالطرق المشروعة وغيرها [1].

ثانيا: شروط القيام بعملية إعتراض المراسلات

حدد المشرع من خلال ق.إ.ج شروطا للقيام بالإجراء إعتراض المراسلات، كونه يشكل إنتهاكا لحرمة الحياة الخاصة للأفراد، وإعتداءً على سرية مراسلاتهم وإتصالاتهم، لذا فقد وضع المشرع شروطا قانونية بهدف منع التعسف في إستعمالها، وتتمثل في الحصول على إذن من وكيل الجمهورية أو من قاضي التحقيق في حالة فتح تحقيق قضائي، زيادة على ذلك أن يكون الإذن مكتوبا ولمدة أقصاها 4 أشهر، قابلة للتجديد حسب مقتضيات البحث والتحري، مع وجوب تضمنه على كل العناصر التي تسمح بالتعرف على الإتصالات المطلوب إلتقاطها والأماكن المقصودة، وأخير أن يطبق هذا الإجراء في الجرائم المحددة بموجب المادة 65 مكرر 5، والتي من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات [2].

ثالثا: كيفية إعتراض المراسلات في الجريمة السيبرانية

يمكن القول أن هذه العملية تنصب عادة على رسائل البريد الإلكتروني، حيث يعتبر هذا الأخير من أهم الوسائل الحديثة للإتصال في مجال الأنترنت، وهو بمثابة نظام للتراسل عن طريق شبكة الأنترنت، إذ يحتوي على العديد من المعلومات كتاريخ إنشاء الرسالة وتاريخ إرسالها أو تلقيها، وكذا عنوان المُرسِل وعنوان المُرسَل إليه، ولكن تبقى المعلومات التي تحتويها حاشية رسالة البريد الإلكتروني هي الأهم، بحيث تتضمن على عنوان التعريف لمرسِل

(1) سليمان النحوي، المرجع السابق، ص 10.

(2) جمال براهيمي، المرجع السابق، ص 124.

الرسالة، بحيث يتكون هذا العنوان من أربعة أجزاء، يشير الجزء الأول من اليسار إلى المنطقة الجغرافية، والجزء الثاني لمزود الخدمة، والثالث لمجموعة الحاسبات الآلية المترابطة، وأما الجزء الرابع فيحدد الحاسب الآلي الذي تم الإتصال بواسطته [1].

الفرع الثاني: نظام التسرب

نظم المشرع الجزائري هذا الإجراء من خلال المواد 65 مكرر 11 إلى غاية المادة 65 مكرر 18 من ق.إ.ج، وسنتناول فيما يلي مفهوم هذا الإجراء وشروطه وكيفية تطبيقه.

أولا: مفهوم نظام التسرب

عرفت المادة 65 مكرر 12 من ق.إ.ج التسرب بأنه: " قيام ضابط عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص والمشتبه في إرتكابهم جناية أو جنحة، بإيهامهم أنه فاعل معهم أو شريك لهم "، فالتسرب إذن هو تلك العملية المُحَضر لها مسبقا، تهدف إلى التوغل داخل خلية إجرامية ومعرفة نشاطاتها، والكشف عن الأشخاص المتورطين سواء كانوا فاعلين أصليين أم شركاء، وذلك بتوفير جميع الوسائل البشرية والتقنية اللازمة [2].

ثانيا: شروط القيام بعملية التسرب

تتمثل شروط القيام بعملية التسرب وفقا لنصوص قانون الإجراءات الجزائية في الإجراءات التالية:

– مباشرة التسرب من طرف ضابط أو عون شرطة قضائية تحت مسؤولية ضابط الشرطة القضائية، والواضح بالنسبة لهذا الشرط أن المشرع الجزائري قد وسع المجال من حيث الأشخاص المعتمد عليهم في نظام التسرب، على عكس نظام المراقبة الإلكترونية، أين حصره في نطاق ضباط الشرطة القضائية دون غيرهم من الأعوان بعد إستصدار إذن مكتوب بالتسرب.

(1) زيدان زيبحة، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى للطباعة والنشر والتوزيع، عين مليلة، 2011، ص 159.

(2) سليمان النحوي، المرجع السابق، ص 12.

فطبقا لنص المادة 65 مكرر 11 من ق.إ.ج " يجوز لوكيل الجمهورية أو لقاضي التحقيق بعد إخطار وكيل الجمهورية أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب، وكغيره من الأذون المتعلقة بالإجراءات، فهو إذن مقيد بالشروط التالية:

- ضرورة أن يكون الإذن مكتوبا لا شفاهة،

- ضرورة أن يكون الإذن محدِدا لأسباب إصداره،

- ضرورة أن يشتمل الإذن على كل البيانات المطلوبة من تحديد نوع الجريمة وهوية الفرد المتسرب والإجراءات المطلوبة،

- ضرورة تحديد المدة في الإذن، والتي لا يمكن أن تتجاوز أربعة (4) أشهر قابلة للتمديد،

- ضرورة إيداع نسخة من الإذن بالتسرب في ملف الإجراءات بعد إنتهاء عملية التسرب [1].

ثالثا: كيفية التسرب في الجريمة السيبرانية

إن عملية التسرب في نطاق الجريمة السيبرانية تتمثل في دخول ضابط أو عون الشرطة القضائية إلى العالم الرقمي، وذلك بإختراقه لمواقع معينة وفتح ثغرات إلكترونية فيها، أو إشتراكه في محادثات غرف الدردشة، والظهور بمظهر كما لو كان فاعلا مثلهم، مستخدما أسماء أو صفات وهمية [2]، وذلك بهدف الحصول على معلومات تفيد في التحقيق.

الفرع الثالث: نظام المراقبة الإلكترونية

نظام المراقبة الإلكترونية هو نظام قام المشرع الجزائري بإستحداثه بموجب القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، وسنتناول فيما يلي مفهومه وكذا شروط تطبيقه.

أولا: مفهوم نظام المراقبة الإلكترونية

من خلال إستقراء نصوص القانون رقم 09-04، نجد أن المشرع لم يعرف المراقبة الإلكترونية بل ترك أمر تعريفها للفقه، حيث أنها " عمل أمني أساسي له نظام معلومات إلكتروني يقوم فيه المراقِب بمراقبة المراقَب بواسطة الأجهزة الإلكترونية عبر شبكة الإنترنت، لتحقيق غرض

(1) زيدان زيبحة، المرجع السابق، ص 169-170.

(2) عبد اللطيف معتوق، المرجع السابق، ص 107.

محدد وإفراغ النتيجة في ملف إلكتروني، وتحرير تقارير بالنتيجة " [1] وعليه يمكن القول أن المراقبة الإلكترونية وسيلة من وسائل جمع البيانات والمعلومات عن المشتبه فيه، بحيث يقوم بها ضابط من ضباط الشرطة القضائية ذو كفاءة تقنية عالية وباستخدام تقنيات وبرامج إلكترونية.

ومن جهة أخرى بالرجوع لذات القانون نجد أن المشرع الجزائري لم يعتبر هذا الإجراء طريقة من طرق الحصول على الأدلة الجنائية الرقمية فقط، بل أدرجه أيضا ضمن التدابير الوقائية من الجريمة السيبرانية حمايةً للنظام العام من التهديد، وهذا وفقا لما نصت عليه المادة 04 من هذا القانون، إذ يمكن القيام بهذا الإجراء للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، وكذا في حالة توفر معلومات عن إحتمال الإعتداء على منظومة معلوماتية، على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني [2].

ثانيا: شروط القيام بعملية المراقبة الإلكترونية

بالرجوع إلى نص المادة 04 من القانون رقم 09-04، نجد أن المشرع الجزائري قد حدد شروطا للجوء إلى إجراء المراقبة الإلكترونية، وهي أن يتم تنفيذ هذه العملية تحت سلطة القضاء وبإذن منه، بحيث لا يجوز إجراء عمليات المراقبة إلا بإذن مكتوب من السلطة القضائية المختصة، حيث جاء في المادة " لا يجوز إجراء عمليات المراقبة في الحالات المذكورة إلا بإذن مكتوب من السلطات القضائية المختصة ".

وقد حدد المشرع في نفس المادة الحالات التي يطبق فيها إجراء المراقبة الإلكترونية [3] وهي:

" يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 03:

أ-للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

ب-في حالة توفر معلومات عن إحتمال إعتداء على منظومة معلوماتية على نحو يهدد النظام العام والدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

(1) سليمان النحوي، المرجع السابق، ص 14.

(2) زيدان زيبحة، المرجع السابق، ص 127-128.

(3) سليمان النحوي، المرجع السابق، ص 06.

ج-لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.

د-في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة ".

يتم منح الإذن لمدة 6 أشهر قابلة للتجديد، على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها، زيادة على ذلك أن تكون هناك ضرورة تتطلب هذا الإجراء وذلك عندما يكون من الصعب الوصول إلى نتيجة تهم مجريات التحري أو التحقيق دون اللجوء إلى المراقبة الإلكترونية، وهو ما نصت عليه المادة 4 من خلال الفقرة "ج" من نفس القانون [1].

الفرع الرابع: المساعدة القضائية الدولية لمكافحة الجريمة السيبرانية

أكد القانون 09-04 في المادة 16 [2] منه على أنه وفي إطار التحقيقات والتحريات القضائية التي تمت مباشرتها، وتتبُّع الجرائم المنصوص عليها في هذا القانون والكشف عن مرتكبيها، فإنه بإمكان السلطات الجزائية المختصة تبادل المساعدات القضائية على المستوى الدولي، فيما يتعلق بجمع الأدلة، ويمكن أن يكون بواسطة الدخول إلى المنظومة المعلوماتية المشكوك في تخزينها للمعلومات المبحوث عنها، وأنه نظرا للطابع الخاص لهذا النوع من الجرائم وما يتطلبه تعقبها من سرعة، فإن المشرع أجاز في حالة الإستعجال قبول طلبات المساعدة القضائية الدولية حتى وإن وردت عن طريق وسائل الإتصال السريعة، كالفاكس أو البريد الإلكتروني، شريطة التأكد من صحتها [3].

(1) أمنة أمحمدي بوزينة، " إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية "، مداخلة مقدمة ضمن فعاليات الملتقى الوطني الذي نظمه مركز جيل البحث العلمي بالجزائر، الموسوم بعنوان: آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، يوم 29 مارس 2017، ص 74-75.

(2) المادة 16 من القانون 09-04 المتضمن الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها " في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المشمولة بهذا القانون وكشف مرتكبيها، يمكن للسلطات المختصة تبادل المساعدات القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني ... "، الجريدة السمية عدد 47، ص 8.

(3) زيدان زيبحة، المرجع السابق، ص 144.

خاتمة

خاتمة

لقد بات لزامًا على دول العالم مواكبة التطور التكنولوجي الحاصل في العالم الإفتراضي الجديد، الذي صارت المعلومة فيه سيدة دون مُنازع ومصدرا للقوة والمعرفة والسلطة والمال، بل وأكثر من هذا أصبحت معيارًا لتطور الشعوب.

إزاء هذا التطور العلمي، فإن مزايا الأنترنت جلبت معها مخاطر جمة طورها المجرم السيبراني وصارت سلاحا لا يستهان به لممارسة نشاطاته الإجرامية، إضافة إلى إمكانية إرتكاب الجرائم التقليدية بطرق حديثة، وبهذا ظهرت طائفة جديدة من الجرائم المستحدثة، وباتت القوانين الجزائية الموضوعية منها والإجرائية، تسعى لمواجهة الجرائم المرتكبة بواسطة الحاسب الآلي.

من خلال هذا البحث لوحظت الصعوبات القانونية التي قد تواجه رجال القانون، وخاصة القضاة في تطبيق النصوص الجزائية التقليدية، سيما ما يتعلق بطبيعة المال المعلوماتي بإعتباره مالا معنويا، في حين أن الحماية الجزائية في أغلب الدول تقتصر على المال المادي.

إن قواعد الإجراءات الجزائية تبدو قاصرة عن مواجهة الإجرام السيبراني، كفشلها في مجال الضبط والتحري والتحقيق وتفتيش النظام المعلوماتي وإستنباط الأدلة وإثبات الجريمة السيبرانية وصعوبة إثبات الجرائم الالكترونية بالنظر إلى طبيعة الدليل الذي يُتحصل منها، إذ قد يكون هذا الدليل غير مرئي وقد يَسهل إخفاؤه أو تدميره، وقد يكون متصلا بدول أخرى فتكون هناك صعوبة للحصول عليه نظرا لتمسك كل دولة بسيادتها. كما وأن هذا الإثبات قد يحتاج إلى معرفة علمية وفنية قد لا تتوافر لدى ضباط الشرطة القضائية والقضاة.

ومن خلال هذا البحث تمت معالجة إشكالية تطبيق النصوص التقليدية والمستحدثة في مجال الجريمة المعلوماتية وصعوبة إثبات الجرائم التي تقع على العمليات الالكترونية، وقد خلص البحث إلى مجموعة من النتائج يمكن إجمالها فيما يلي:

- رغم أن المشرع الجزائري تصدى لهذا النوع من الجرائم، إلا أنه لم يخصها بقانون خاص بها.

- قصور النصوص التقليدية سواء الموضوعية منها أو الإجرائية، أمام هذه الجرائم المستحدثة.

- إن حماية حقوق المؤلف والحقوق المجاورة فيما يتعلق بالمصنفات الرقمية، تعتبر غير كافية لمواجهة الإعتداءات الواقعة عليها عبر الأنترنت، وبالأخص قرصنة البرامج وإستعمالها.

من خلال ما تقدم وبهدف مواصلة السير في إتجاه تفعيل مكافحة الجريمة السيبرانية، تم إقتراح بعض التوصيات بخصوص هذا الموضوع:

– رغم سير المشرع الجزائري في مجال تخصص القوانين، ورغم حرصه على التصدي للجريمة السيبرانية، إلا أنه لم يخصها بقانون خاص قائم بذاته، حيث نجد أنه قد جرم السلوكات المشكلة للجريمة السيبرانية في قانون العقوبات، بينما نص على آليات مكافحتها في الأمر 66–155 والقانون 09–04، لذا نقترح على المشرع دمج جميع النصوص القانونية المتعلقة بهذه الجريمة سواء الموضوعية منها أو الإجرائية، وتنظيمها في قانون خاص بها كما هو الشأن في القانون رقم 04–18 المتعلق بالوقاية من المخدرات والمؤثرات العقلية وقمع الإستعمال والإتجار غير المشروعين بها، وكذا القانون رقم 06–01 المتعلق بالوقاية من الفساد ومكافحته، وغيرها من القوانين الخاصة.

– على الدولة التغيير في المناهج الدراسية إبتداءا من كليات الحقوق، لذلك نقترح إدراج مقياس خاص بالقانون الجنائي السيبراني، إقتداءا بالجامعات الأجنبية التي تدرس مقياس Cybercriminalité، وكذا العمل على تحضير القاضي خلال تكوينه في المدرسة العليا للقضاء وصولا إلى تكوينه أثناء تأدية مهامه.

– ضرورة تدريب وتأهيل أفراد الشرطة القضائية على كيفية التعامل مع هذا النوع من الجرائم، وذلك بالتعاون مع التقنيين والفنيين من أصحاب الخبرة، مع ضمان تحقيق التوازن بين مكافحة الجريمة السيبرانية وحماية الحق في الخصوصية.

– الإعتماد على وسائل الإعلام في توعية المواطن بمخاطر الجريمة السيبرانية، وتشجيعه على التبليغ عنها.

قائمة المصادر والمراجع

قائمة المراجع

أولا: النصوص القانونية

1-الدساتير

- دستور 1996 المؤرخ في 08 ديسمبر 1996، الجريدة الرسمية العدد 76، بتاريخ 28 نوفمبر 1996.

- القانون 16-01 المؤرخ في 06 مارس 2016 يتضمن تعديل دستور 1996، الجريدة الرسمية العدد 14، بتاريخ 07 مارس 2016.

2-الإتفاقيات الدولية والإقليمية

- إتفاقية مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين، الصادرة في أوت 1990.

- إتفاقية بودابست لمكافحة جرائم المعلوماتية والأنترنت، الصادرة في 23 نوفمبر 2001.

- الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، الصادرة في 21 ديسمبر 2010.

3-القوانين العادية

- القانون 03/2000 المؤرخ في 05 أوت 2000 يتضمن القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، الجريدة الرسمية العدد 48، بتاريخ 06 أوت 2000.

- القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 يتضمن تعديل قانون العقوبات، الجريدة الرسمية العدد 71، بتاريخ 10 نوفمبر 2004.

- القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 يتضمن تعديل قانون الإجراءات الجزائية، الجريدة الرسمية العدد 84، بتاريخ 24 ديسمبر 2006.

- القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006 يتضمن تعديل قانون العقوبات، الجريدة الرسمية العدد 84، بتاريخ 24 ديسمبر 2006.

- قانون رقم 09-04 مؤرخ في 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، الجريدة الرسمية العدد 47.

- القانون 15-03، المؤرخ في 01 فيفري 2015 يتعلق بعصرنة العدالة، الجريدة الرسمية العدد 06، بتاريخ 10 فيفري 2015.

4-الأوامر

- الأمر رقم 66-155 المؤرخ في 08 جوان 1966 يتضمن قانون الإجراءات الجزائية المعدل والمتمم، الجريدة الرسمية العدد 48، بتاريخ 10 جوان 1966.

- الأمر رقم 66-156 المؤرخ في 10 جوان 1996 يتضمن قانون العقوبات المعدل والمتمم، الجريدة الرسمية العدد 49، بتاريخ 11 جوان 1966.

5-المراسيم الرئاسية

- المرسوم الرئاسي رقم 04-183، المؤرخ في 26 جوان 2004، يتضمن إحداث المعهد الوطني وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، الجريدة الرسمية العدد 41، بتاريخ 27 جوان 2004.

- المرسوم الرئاسي رقم 04-432، المؤرخ في 29 ديسمبر 2004، يتضمن إنشاء المعهد الوطني للبحث في علم التحقيق الجنائي، الجريدة الرسمية العدد 84، بتاريخ 29 ديسمبر 2004.

- المرسوم الرئاسي رقم 15-361، المؤرخ في 08 أكتوبر 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، الجريدة الرسمية العدد 53، بتاريخ 08 أكتوبر 2015.

ثانيا: الكتب

- إبراهيم بلعليات، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري، الطبعة الأولى، دار الخلدونية، الجزائر، 2007.

- أحمد خليفة الملط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية، 2006.

- آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، الطبعة الثانية، دار هومه للطباعة والنشر والتوزيع، الجزائر،2007.

- أمير فرج يوسف، الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والأنترنت، الطبعة الأولى، مكتبة الوفاء القانونية، الإسكندرية، 2011.

- بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2011.

- خالد عياد الحلبي، إجراءات والتحقيق في جرائم الحاسوب والأنترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن، 2011.

- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2010.

- زيدان زيبحة، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى للطباعة والنشر والتوزيع، عين مليلة، 2011.

- عبد العال الدريبي ومحمد صادق إسماعيل، الجريمة الإلكترونية، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2012.

- عبد الفتاح بيمو حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2006.

- عبد الفتاح مراد، شرح جرائم الكمبيوتر والإنترنت، دار الكتب والوثائق المصرية، دون ذكر تاريخ النشر.

- عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والإنترنت، منشورات الحلبي الحقوقية، بيروت، 2007.

- علي جبار الحسيناوي، جرائم الحاسوب والأنترنت، دار اليازوري العلمية للنشر والتوزيع، عمان، 2009.

- علي جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، الطبعة الأولى، منشورات زين الحقوقية، بيروت، 2013.

- علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والإنترنت، الطبعة الأولى، عالم الكتب الحديث، الأردن، 2004.

- علي عدنان الفيل، الإجرام الإلكتروني، الطبعة الأولى، منشورات زين الحقوقية، بيروت، 2011.

- محمد طارق عبد الرؤوف الحن، جريمة الإحتيال عبر الإنترنت، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2011.

- محمد عبيد الكعبي، الجرائم الناشئة عن الإستخدام غير المشروع لشبكة الأنترنت، الطبعة الثانية، دار النهضة العربية، القاهرة، 2009.

- محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2009.

- نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الإقتصادية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2005.

- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الإستدلالات، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2007.

ثالثا: المقالات

- إبتسام حمديني، " أسلوب التحقيق في الجرائم الإلكترونية كآلية لمكافحتها "، مداخلة مقدمة ضمن فعاليات الملتقى الدولي الذي نظمته كلية الحقوق والعلوم السياسية قسم الحقوق جامعة

برج بوعريريج، الموسوم بعنوان: الإجرام السيبراني المفاهيم والتحديات، يومي 11 و12 أفريل 2017.

- أمنة أمحمدي بوزينة، " إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية "، مداخلة مقدمة ضمن فعاليات الملتقى الوطني الذي نظمه مركز جيل البحث العلمي بالجزائر، الموسوم بعنوان: آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، يوم 29 مارس 2017.

- جمال براهيمي، " مكافحة الجرائم الإلكترونية في التشريع الجزائري "، المجلة النقدية للقانون والعلوم السياسية، جامعة مولود معمري تيزي وزو، (المجلد الثاني)، نوفمبر 2016.

- ذياب موسى البداينة، " الجرائم الإلكترونية المفهوم والأسباب "، ورقة علمية مقدمة في الملتقى العلمي الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، خلال الفترة من 02-04 سبتمبر 2014، كلية العلوم الإستراتيجية، الأردن، 2014.

- ذياب موسى البداينة، " دور الأجهزة الأمنية في مكافحة جرائم الإرهاب المعلوماتي "، دورة تدريبية في كلية التدريب قسم البرامج التدريبية بالقنطيرة، المغرب، 2006.

- رحيمة نميلي، " خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة"، مداخلة مقدمة في أعمال المؤتمر لدولي الرابع عشر، طرابلس، الموسوم بعنوان: الجرائم الإلكترونية طرابلس، يومي 24و25 مارس 2017.

- زهرة بوعناد فاطمة، " مكافحة الجريمة الإلكترونية في التشريع الجزائري "، مجلة الندوة للدراسات القانونية، جامعة جيلالي اليابس سيدي بالعباس، العدد الأول، 2013.

- سليمان النحوي، " آليات مكافحة الجريمة السيبرانية في التشريع الجزائري "، مداخلة مقدمة ضمن فعاليات الملتقى الدولي الذي نظمته كلية الحقوق والعلوم السياسية قسم الحقوق جامعة برج بوعريريج، الموسوم بعنوان: الإجرام السيبراني المفاهيم والتحديات، يومي 11 و12 أفريل 2017.

- سميرة معاشي، " ماهية الجريمة المعلوماتية "، مجلة المنتدى القانوني، جامعة محمد خيضر بسكرة، العدد السابع، أفريل 2010.

- صالح بن محمد المسند، عبد الرحمان بن راشد المهيني، " جرائم الحاسب الآلي الخطر الحقيقي في عصر المعلومات "، المجلة العربية للدراسات الأمنية والتدريب، العدد 29، (المجلد 15)، أفريل 2000.

- عباس أبو شامة عبد المحمود، " عولمة الجريمة الاقتصادية "، الطبعة الأولى، جامعة نايف العربية للعلوم الأمنية، الرياض، 2007.

- عبد الكريم بلعزوق، " دراسة في ماهية الإجرام الإلكتروني ومجرم الأنترنت "، مداخلة مقدمة ضمن فعاليات الملتقى الدولي الذي نظمته كلية الحقوق والعلوم السياسية قسم الحقوق جامعة برج بوعريريج، الموسوم بعنوان: الإجرام السيبراني المفاهيم والتحديات، يومي 11 و12 أفريل 2017.

- عبد الكريم هشام، " التمييز العنصري وصور الإستخدامات الجديدة للأنترنت "، مداخلة مقدمة ضمن فعاليات الملتقى الدولي الذي نظمته كلية الحقوق والعلوم السياسية قسم الحقوق جامعة برج بوعريريج، الموسوم بعنوان: الإجرام السيبراني المفاهيم والتحديات، يومي 11 و12 أفريل 2017.

- عبد المؤمن بن صغير، " الطبيعة الخاصة للجريمة المرتكبة عبر الأنترنت في التشريع الجزائري والتشريع المقارن "، مداخلة مقدمة ضمن فعاليات الملتقى الوطني الذي نظمته كلية الحقوق والعلوم السياسية قسم الحقوق جامعة محمد خيضر بسكرة، الموسوم بعنوان: الجريمة المعلوماتية بين الوقاية والمكافحة، يومي 16و17 نوفمبر 2015.

- عمر حوتية ورحاب فايز، " بناء إستراتيجية للأمن المعلوماتي كمدخل لمواجهة تهديدات ومخاطر الإجرام السيبراني في الجزائر"، مداخلة مقدمة ضمن فعاليات الملتقى الدولي الذي نظمته كلية الحقوق والعلوم السياسية قسم الحقوق جامعة برج بوعريريج، الموسوم بعنوان: الإجرام السيبراني المفاهيم والتحديات، يومي 11 و12 أفريل 2017.

- فاروق خلف، " الآليات القانونية لمكافحة الجريمة المعلوماتية "، مداخلة مقدمة ضمن فعاليات الملتقى الوطني الذي نظمته كلية الحقوق والعلوم السياسية قسم الحقوق جامعة محمد خيضر بسكرة، الموسوم بعنوان: الجريمة المعلوماتية بين الوقاية والمكافحة، يومي 16و17 نوفمبر 2015.

- فضيلة عاقلي، " الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري "، مداخلة مقدمة في أعمال المؤتمر الدولي الرابع عشر، طرابلس، الموسوم بعنوان: الجرائم الإلكترونية طرابلس، يومي 24و25 مارس 2017.

- كاظم محمد عطيات، محمد رضوان هلال، " كيفية التعامل التقني والآمن مع أوعية الجريمة الرقمية في مسرح الجريمة لضمان حيدة الدليل المستخلص"، المجلة العربية الدولية للمعلوماتية، العدد الخامس، المجلد 3، السعودية، 2014.

- مجمع البحوث والدراسات بأكاديمية السلطان قابوس لعلوم الشرطة، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، نزوى سلطنة عمان، 2016.

- محروس نصار غايب، " الجريمة المعلوماتية "، مجلة هيئة التعليم التقني الأكاديمية، المجلد 24، العراق، 2011.

- محمد عبد الرحيم سلطان العلماء، " جرائم الأنترنت والإحتساب عليها"، الطبعة الثالثة، بحوث مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات المتحدة كلية الشريعة والقانون، (المجلد الثالث)، 2004.

- مليكة عطوي، " الجريمة المعلوماتية "، حوليات جامعة الجزائر، العدد 21، جوان 2012.

- موسى مسعود أرحومة، " الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية "، مداخلة مقدمة ضمن فعاليات المؤتمر المغاربي الأول الذي نظمته أكاديمية الدراسات العليا بطرابلس، الموسوم بعنوان: المعلوماتية والقانون، يومي 28-29 أكتوبر 2010.

- نسيمة سحواذ، " الجريمة الإلكترونية مشكلة عالمية "، مجلة الشرطة للمديرية العامة للأمن الوطني، العدد 129، ديسمبر 2015.

- هشام محمد فريد رستم، " الجرائم المعلوماتية أصول التحقيق الجنائي الغني واقتراح إنشاء آلية حربية موحدة للتدريب التخصصي"، الطبعة الثالثة، بحوث مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات المتحدة كلية الشريعة والقانون، (المجلد الثاني)، 2004.

- ياسمينة بونعارة، " الجريمة الإلكترونية "، مجلة المعيار، جامعة الأمير عبد القادر كلية أصول الدين، المجلد الثاني، العدد 39، جوان 2015.

رابعا: المذكرات والأطروحات الجامعية

- سفيان سوير، جرائم المعلوماتية، مذكرة ماجستير، جامعة أبو بكر بلقايد تلمسان، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2010-2011.

- عبد الرحمان جميل محمود حسين، الحماية القانونية لبرامج الحاسب الآلي، مذكرة ماجيستير، جامعة النجاح الوطنية نابلس فلسطين، كلية الدراسات العليا، 2008.

- عبد اللطيف معتوق، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة ماجستير، جامعة العقيد الحاج لخضر باتنة، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2011-2012.

- فتيحة رصاع، الحماية الجنائية للمعلومات على شبكة الأنترنت، مذكرة ماجستير، جامعة أبي بكر بلقايد تلمسان، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2011-2012.

- نسيم دردور، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، مذكرة ماجستير، جامعة منتوري قسنطينة، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2012-2013.

- نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجستير، جامعة الحاج لخضر باتنة، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2012-2013.

- يوسف صغير، الجريمة المرتكبة عبر الأنترنت، مذكرة ماجستير، جامعة مولود معمري تيزي وزو، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2012-2013.

خامسا: المواقع الإلكترونية

- أنظر موقع https://ar.wikipedia.org/wiki/

- أنظر موقع http://aljazairalyoum.com

الفهرس

الفهرس

ملخص

إن الجريمة السيبرانية أصبحت تشكل خطورة على مصالح الدول والأفراد، بعد أن تحولت المجتمعات برمتها إلى مجتمعات إلكترونية تستخدم التكنولوجيا في كثير من مجالات الحياة، لذا وجب مجابهة هذا النوع من الجرائم بما يتوافق مع طبيعتها، وتماشيا مع هذا التوجه الدولي القاضي بمكافحة الجريمة السيبرانية قام المشرع الجزائري بإستحداث آليات إجرائية لمكافحة الجريمة السيبرانية، نظرا لعدم فاعلية الإجراءات التقليدية في مكافحة هذا النوع من الجرائم المتسم بالتطور المستمر.

Résumé

Le cybercrime est devenu dangereux sur les intérêts de l'Etat et des membres après que l'ensemble des sociétés deviennent des sociétés électroniques qui utilisent la technologie dans la plupart des domaines de la vie. L a raison pou laquelle il est nécessaire de faire face à ce type d'infractions via de moyens conformes à sa nature. Et en parallèle de ce acheminement international tendant à la lutte contre le cybercrime, le législateur algérien a actualisé des mécanismes de procédures pour la lutte contre le cybercrime, à cause de l'inefficacité des procédures traditionnels à la lutte contre ce type des infractions qui est en évolution durable.

Abstract

Cybercrime has become a danger to the interests of states and individuals, after the entire society has become electronic communities using technology in many areas of life, so this type of crime must be confronted in accordance with its nature. In line with this international trend to combat cybercrime, Algerian initiative to develop procedural mechanisms to combat cybercrime, in view of the ineffectiveness of traditional measures to combat this type of crime characterized by continuous development.