

الجريمة الالكترونية وتداعياتها على أمن الوطن والمواطن
بين المكافحة القانونية وأجهزة الكشف والتحري

**ELECTRONIC CRIME AND ITS REPERCUSSIONS ON THE SECURITY OF THE
HOMELAND AND THE CITIZEN BETWEEN LEGAL CONTROL AND DETECTION AND
INVESTIGATION DEVICES**

تاريخ النشر: 2022/06/01

تاريخ القبول: 2022/05/04

تاريخ الاستلام: 2022/02/17

د. فرج الحسين¹

جامعة حسيبة بن بوعلي الشلف، الجزائر، e.feredj@univ-chlef.dz

1

الملخص

يعرف زماننا هذا العديد من التطورات الظاهرة من الناحية العلمية، ولعل أبرزها على الإطلاق ما تشهده الثورة المعلوماتية والالكترونية وانتشار لا محدود للشبكة العنكبوتية، بغية تطوير الحياة وتسهيلها هذا الجانب الايجابي، غير أنه مقابل ذلك أنتجت هذه الطفرة العلمية جرائم معاصرة تخالف الجانب الكلاسيكي لها التي اصطلح عليها بالجريمة الالكترونية أو المعلوماتية، جريمة تمس عمق قيم الأفراد والهيئات وحتى سيادة الدول وهذا جانبها السلبي، مما استدعى الإسراع إلى الحد من عواقب التطور العلمي بالتشخيص الدقيق والكامن بغية ضبط حدودها ومنه سهولة التحكم فيها.

الكلمات المفتاحية : الجريمة؛ الجريمة الالكترونية؛ النصوص العقابية؛ الأجهزة المكلفة والمتخصصة.

ABSTRACT

Our time knows many visible developments from a scientific point of view, and perhaps the most prominent of them are what the information and electronic revolution is witnessing and the unlimited spread of the World Wide Web, in order to develop and facilitate life and this positive aspect. It is an electronic or information crime, a crime that affects the depth of the values of individuals and bodies and even the sovereignty of states, and this is its negative side, which necessitated a rush to reduce the consequences of scientific development by accurate and latent diagnosis in order to control its borders and thus ease of control.

Keywords: the crime; cyber crime; Punitive texts; commissioned and specialized devices.

1. المقدمة

لا ريب أنّ التقدم الجلي في وسائل الاتصال الالكتروني بمختلف صورها قد تبعته تطور في الجريمة كنتيجة بديهية، غير أنّ ما يميز هذه الجريمة هي اتصافها بخطورة الظاهرة في ساحة العلوم الجنائية، ناهيك عن ذلك بروز نوع جديد من المجرمين المستغلين لهاته الشبكة في ارتكاب جرائمهم مما يجعل امن وسلامة المجتمع في المحك.

وتأسيسا على ما سبق، يعتبر العقاب من أبرز الأساليب مجابهة الظاهرة والحد من انتشارها، كونها أقدم الآليات التي أثبتت فعاليتها في ردع المجرمين عن القيام بأنشطة إجرامية والتقليل من معدلات ارتكابها، الأمر الذي جعل من النصوص القانونية السبيل الوحيد حاليا في خضم غياب آليات حديثة تناسب مع هذا النوع المستحدث من الجرائم.

أهمية الدراسة

ينهل الموضوع أهميته وفائدته في كونه يسعى لتجلية الدور البالغ الأهمية للقانون والأجهزة المختصة في ضبط الجريمة الالكترونية وكيفية الحد من تداعياتها، بتزامن مع زيادة الاهتمام بمعالجة هذا النوع من القضايا لتأثيرها الجلي على مجالات متعلقة بالأمن القومي للدولة اقتصاديا واجتماعيا وثقافيا وأمنيا.

أهداف الدراسة

تبرز أهداف الدراسة من خلال رغبتنا الملحة لمعرفة حدود الجريمة الالكترونية كأحدث صور الجريمة، ومدى تأهب المشرع الجزائري والأجهزة الأمنية لمواجهتها، وهذا لن يتأتى إلا بـ:

- فهم حقيقة الجريمة الالكترونية بكل حدودها منعا للجهالة بشأنها؛
- إبراز مجالات الجريمة الالكترونية والضبط الدقيق لأشكالها؛
- معرفة مقدار تبني المشرع الجزائري لأحكام رادعة لجريمة الالكترونية؛
- محاولة التعرف على الأجهزة المختصة بكشف الجريمة الالكترونية.

وعليه، ونحن بصدد التعرض إلى أبرز المواضيع القانونية المعاصرة سنحاول الإجابة على الإشكالية التالية: ما مدى كفاية واستطاعة النصوص القانونية والأجهزة المتواجدة في مجابهة الجريمة الالكترونية والحد من سرعة انتشارها؟

وتم اعتماد في هذه الدراسة على المنهج الوصفي التحليلي من خلال معالجة الإشكالية في بحثين رئيسين، أولها نأصل فيه محل الموضوع ألا وهي الجريمة الالكترونية بكل حدودها، وأما المبحث الثاني سنخصصه لبحث عن سبل مجابهة هذه الظاهرة من حيث القدرات القانونية والمؤسسية.

2. الجريمة الالكترونية: دراسة مفاهيمية

يكون من حسن تأصيل الموضوعات لما لها من أهمية قصوى في إيجاد السبل السليمة لحلحلة القضايا والمشكلات، وعليه سنتطرق إلى تأصيل الجريمة الالكترونية (المطلب الأول) ومن ثمة نستنتج أبرز مجالاتها (المطلب الثاني). كما سنوضحه فيما يلي:

1.2 تأصيل الجريمة الالكترونية

الجرائم الالكترونية ظاهرة مستشرية في مجال الجريمة، تبذل الجهود الوطنية والدولية لأجلها الكثير، وذلك لما لها من انعكاسات خطيرة تمس أكثر من مجال؛ لاسيما اجتماعيا واقتصاديا وسياسيا، وتقتضي المسألة لتعريفها ضبط معنى الجريمة (أولا)، ومن ثمة التعرض إلى هذا النوع من الجرائم لدى الفقه (ثانيا)، وكذا في التشريع الجزائري (ثالثا). كما سنوضحه فيما يلي:

1.1.2 تعريف الجريمة الالكترونية:

في تعريفنا للجريمة سنتطرق للجانب اللغوي للمصطلح، ومن ثمة المرور عبر محطة الاصطلاحية، لننتهي بالجانب القانوني. كما سنوضحه أكثر فيما يلي:

1.1.1.2 الجريمة لغة:

الجريمة في اللغة العربية مشتقة من الفعل جَرَمَ، بمعنى: أذنب واكتسب الإثم، والجُرْمُ: بمعنى الذنب والإثم والتعدي، يقال: أُجْرِمُ فلان إذا جنى جناية (أبوزهرة، 1998، ص 19).

أي الجريمة هي كل فعل يجانب الحق والاستقامة، وتسحق الاستهجان، ومن الشواهد التي تعزز الأصل اللغوي ما ورد في القرآن الكريم، في قول الله تعالى:

"كلوا وتمتعوا قليلا إنكم مجرمون" (سورة المرسلات، آية 46)؛

"وما أضلنا إلا المجرمون" (سورة الشعراء، آية 99)؛

"ويحق الله الحق بكلماته ولو كره المجرمون" (سورة يونس، آية 82).

2.1.1.2 الجريمة الالكترونية اصطلاحا:

الجريمة عموما تتباين تعريفاتها بين الفقهاء القانونيين وبينهم وبين علماء الاجتماع، إلا أنّ التعريف الكامل هو الذي جاء به الفقه الذي يحدد عناصر الجريمة مع بيان أثرها؛ فالتعريف الجريمة هي بيان سلوك والسلوك غير المشروع وفق القانون (سوري، 2005/2004، ص 04).

وهنا ارتكز الباحثين والمختصين على ثلاثة معايير أساسية في تعريفهم للجريمة الالكترونية، أولهما حاول تعريفها بالارتكاز على الوسائل المستخدمة للجرم وتم تعريفها بأنها: "كل نشاط إجرامي تستخدم فيه التقنية الالكترونية المتمثلة في الحاسوب الآلي الرقمي وشبكة الإنترنت بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الفعل الإجرامي المستهدف" (بهلول، 2020، ص 139)، وأما المعيار الثاني فيقوم على مستوى المعرفة بالتقنيات الحديثة وحينئذ عرفت بأنها: "كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازما لارتكابه من ناحية، وملاحقته وتحقيقه من ناحية أخرى" (نائلة، 2003، ص 21)، وأما المعيار الثالث فيستند في تعريفه للجريمة الالكترونية على حسب موضوعها أو محلها ومنه فإن: "الجرائم الالكترونية هي الجرائم التي ترتكب ضد الأنظمة الالكترونية والشبكات المعلوماتية"، والبعض الآخر في ذات

الجزئية ذهب إلى القول بأنها: "كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسوب الالكتروني أو التي تحول عن طريقه" (أشرف، 2000، ص 04).

3.1.1.2 الجريمة الالكترونية قانونا:

تعرف الجريمة قانونا بأنها: "الفعل المجرم قانونا ويقرله جزاءً جنائياً، أو هي فعل أو امتناع يخالف قاعدة جنائية تحظر السلوك المكون لها وترتب لمن يقع منه جزاءً جنائياً (رحماني، دون تاريخ نشر، ص 83).

فالجريمة في القانون الوضعي الجنائي هي الفعل أو الامتناع الذي جاء منصوصا عليه ومقرر في قانون العقوبات، يستوجب معه أن يشكل عدوانا على المجتمع برمته، والقول بخلاف هذا أي إذا لا يوجد أي نص قانوني وارد فلا تعد الأفعال تستوجب العقاب (بوالماين، 2008/2007، ص 17).

ومع استفحال ظاهرة الجريمة الالكترونية واتساع نطاقها تدخل المشرع الجزائري بغية التصدي لمخلفات السلبية للجريمة، وتخصيص عقوبات لأجلها، وعلى اعتبار أن المشرع ليس من اختصاصه ضبط المفاهيم القانونية؛ في بداية العمل على تجريمها بمقتضى تعديل قانون العقوبات سنة 2004 باستحداث قسما خاصا للعقوبات المطبقة على الجرائم المتعلقة بالمساس بأنظمة معالجة المعلومات والمعطيات (قانون رقم 15/04، المتضمن قانون العقوبات، 2004)، ليصدر المشرع في سنة 2009 أول نص قانوني متعلق بالجرائم الالكترونية ومكافحتها، والذي من خلاله ورد تعريف للجريمة الالكترونية تحت تسمية الجرائم المتصلة بتكنولوجيات الإعلام والاتصال توخيا لاستبعاد الغموض وعرفها على النحو التالي: "الجرائم المتصلة بتكنولوجيات الإعلام والاتصال هي جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية" (قانون رقم 04/09، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها).

2.1.2 الجريمة الالكترونية لدى الفقه:

لم يتفق الفقه على إيجاد تعريف جامع مانع للجريمة الالكترونية، انطلاقا من غياب أي نص قانوني في أغلب التشريعات لهذا النوع من الجرائم، ناهيك عن تنوع المصطلحات القانونية الموحدة لدلالة عليه، فالبعض يطلق عليها الغش الالكتروني والبعض الآخر الاختلاس المعلوماتي، والبعض الآخر الجريمة الالكترونية (فكري، 2014، ص 09)، زيادة على تنوع المجالات التي تمسها، وفي ظل هذا الفراغ حاول بعض رجال الفقه الإحاطة ببعض حدود هاته الجريمة، وفي ذلك انقسموا لفتنتين، أولهما عرفتها تعريفا ضيقا، وأما الأخرى فعرفت تعريفا واسعا. كما سنوضحه فيما يلي:

1.2.1.2 الاتجاه المضيق لتعريف الجريمة الالكترونية:

يرى أنصار هذا الاتجاه أن الجريمة الالكترونية بأنها: "كل سلوك غير مشروع يكون العلم بتكنولوجيات الحاسبات الآلية بقدر كبير لازما لارتكابه من ناحية، وملاحقته وتحقيقه من ناحية أخرى، كما عرفوها كذلك بأنها: "نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسوب الآلي أو تلك التي يتم تحويلها عن طريقها"، ويعاب على أنصار هذا الاتجاه أن نطاق الجريمة الالكترونية من وجهة نظرهم في نطاق الجريمة الالكترونية إلى عدة أفعال

إجرامية غير مشروعة، وانتقد كذلك لأنه يحصر الجريمة في ضرورة توفر قدر عالي من التحكم في التقنية (ابراهيم، 2015، ص213).

2.2.1.2 الاتجاه الموسع لتعريف الجريمة الالكترونية:

بينما يرى جانب آخر من الفقه ضرورة توسيع فكرة تعريف الجريمة الالكترونية، وعرفوها بأنها: "كل فعل أو امتناع عمدي ينشأ عن استخدام غير مشروع لتقنية المعلوماتية، يهدف إلى الاعتداء على الأموال المادية والمعنوية"، كما عرفت بأنها: "كل نشاط إجرامي يؤدي فيه نظام حاسب الآلي دوراً لإتمامه على أن يكون هذا الدور على قدر من الأهمية"، وترتبا على ذلك فإن الجريمة الالكترونية وفق ما ذكر أعلاه عموماً هي كل سلوك إجرامي يرتكب باستخدام الحاسوب (ابراهيم، 2015، ص213).

3.1.2 سمات الجريمة الالكترونية:

تتسم الجريمة الالكترونية بسمات تميزها عن غير من الجرائم، نذكر منها ما يلي: (ابراهيم، 2015، ص214)

- صعوبة كشفها وإثباتها: تتسم الجريمة الالكترونية بصعوبة بالغة في كشفها، وان تم كشفها فهي من محض الصدفة، بسبب عدم ترك مرتكبها في غالب أي أثر خارجي مرئي، أو قيام الجاني بتدمير الدلائل في ثواني معدودة.

- جريمة متعددة للحدود: هذا نوع من الجرائم يعتبر عابر للحدود ولا يعترف بها، فقد تمتد إلى أكثر من دولة مما يني قضايا عدة مثل الاختصاص والإجراءات والتحري .

- أساليب ارتكابها: تتميز الجريمة الالكترونية عن الجرائم التقليدية أكثر من خلال أسلوب ارتكابها؛ فإذا كان متعارف عليه أن الجرائم التقليدية تستدعي للقيام بها نوع من الجهد العضلي في صور مختلف مثل السرقة والتعدي والاختطاف والعنف، فإن الجرائم الالكترونية تحتاج إلى ذكاء وحنكة واستطاعة على التعامل مع جهاز الحاسوب في مستويات تقنية توظف لفعل غير مشروع.

4.1.2 خصائص المجرم الالكتروني:

كما يتميز مرتكب الجريمة بمميزات خاصة تميزه عن غيره من مرتكبي الجرائم الأخرى التقليدية. كما سنوضحه فيما يلي:

1- الذكاء والتخصص: على الغالب مرتكبي هذا النوع من الجرائم أذكيا ولهم من المهارات التي تأهلهم لقيام بذلك، لاسيما قدرتهم على تطوير الأنظمة الأمنية الالكترونية، والقدرة على التخفي حتى لا تتم ملاحظته وتتبع أفعاله الإجرامية عبر شبكات الانترنت لعلمه المسبق بظروف المحيطة (رحموني، 2018، ص443).

2- شخص سوي واجتماعي: عادة ما يتميز المجرم الالكتروني بسلوك حسن وسط المجتمع، ولا يضع نفسه وسط عداء مجتمعي، غير أنه مقابل ذلك وبدافع اللهو أحيانا أو بدافع الحصول على الأموال والانتقام أحيانا أخرى يصبح مجرم الكتروني (رحموني، 2018، ص444).

2.2 الجريمة الالكترونية: مجالاتها وأركانها

تشمل الجريمة الالكترونية جميع مجالات نواحي الحياة بدأ بحياة الأشخاص الخاصة وصولاً إلى أموال الأفراد والمؤسسات و جرائم الالكترونية تطل أمن الدول. كما سنوضحه فيما يلي:

1.2.2 المجال الذي يمس حياة الأشخاص:

لقد أضحت حياة الأشخاص في ظل التطور العلمي والتكنولوجي في خطورة نتيجة حالات السطو والاطلاع على أدق تفاصيلهم واستعمال السلبى ضدّهم. كما سنوضحه فيما يلي: (دوادي، 2020، ص 49-50)

1- التهديد: بمعنى المضايقة وزرع في نفس الأفراد أضرار تمسهم شخصياً أو من تحت رعايتهم أو من بصلّة بهم، لاسيما من خلال إرسال المجرم الالكتروني رسائل تنطوي على تخويف وتهديد بغية ابتزاز الضحية أو رغبة في تحكّم فيه؛

2-انتحال الشخصية: من خلال قيام المجرم الالكتروني باستغلال شخصية فرد من أفراد لأجل الاستفادة من سلطته أو سمعته أو ماله ويجد هذا المجال انتشاراً في الميدان التجاري؛

3-ترويج الإباحة: من خلال إرسال أو نشر أي نشاط إباحي أو إعداده أو طبعه أو نشره وترويجه لصور جنسية فاضحة التي تستهدف الأطفال والشباب عموماً كونهم أقلّ تحصيناً.

2.2.2 المجال الذي يمس أموال أفراد ومؤسسات:

وهي من أبرز القضايا المستشرية في شبكات الانترنت بعد أن باتت أغلب المعاملات المالية تتم عبر الانترنت، وأبرز مجالاتها ما يلي: (دوادي، 2020، ص 51)

1- بطاقات الائتمان والتحويلات المالية الالكترونية: حيث يتم كسر الكلمة السرية للبطاقات الالكترونية أو من خلال فك شفرة الصراف الآلي وقيام بتحويلات مالية من المصدر إلى رصيده أو رصيد متعامل آخر أو الحصول من خلالها على سلع وخدمات من بطاقات مثل ماستر كارد؛

2- سرقة البنوك: والذي يتم من خلال استغلال المجرم الالكتروني الحاسوب للدخول عبر الشبكة لنظام معلومات البنوك أو المؤسسات المالية و مباشر القيام بتحويلات من حساب العملاء إلى حسابات أخرى من خلال كميات قليلة حتى لا يتم اكتشافه أو دفعة واحدة؛

3- غسيل الأموال: تشير إحصائيات الأمم المتحدة وصندوق البنك الدولي أن ما قيمته 30مليار أمريكي من الأموال تغسل سنوياً عبر شبكة الانترنت، مختربة ما يقرب 70دولة، تتولاه شبكات منظمة على درجة عالية من التخطيط والتنسيق بينها.

3.2.2 جرائم الالكترونية تطل أمن الدول:

وتعتبر أخطر مجالات الجرائم الالكترونية على الإطلاق، في كونها تهدد استقرار الدولة، وأهم صورها ما يلي: (دوادي،

2020، ص 51)

1-الإرهاب: استفحل مصطلح الإرهاب في عشرية الأخيرة، وأضح ظاهرة عالمية لاسيما بظهور تنظيمات عالمية تتبنى الفكرة وتسميات مختلفة، وبخصوص صلة الجريمة الالكترونية بالإرهاب فإنها تعتبر أداة لتجنيد وتجييش لأعضاء جدد عبر مختلف منصات التواصل الاجتماعي؛

2-التجسس: لقد سهل التطور العلمي والتكنولوجي ممارسة التجسس من قبل أفراد أو تنظيمات وحتى دول في مجالات عدة اقتصادية وعسكريا وسياسيا.

4.2.2 أركان الجريمة الالكترونية:

للجريمة الالكترونية ثلاثة أركان، أولها الركن الشرعي وهو الصفة الغير المشروعة للجرم، وتتجسد قاعدتها التجريبية وعقابية من خلال ما ورد من أحكام في قانون المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الاتصال والإعلام ومكافحتها، وأما الركن الثاني فهو مادي يقصد به الماديات الإجرامية التي تظهر العالم الخارجي، وأخير الركن المعنوي وهي توفر الإرادة على الفعل بقصد أو بدون قصد (العجمي، 2014، ص36).

3. مواجهة الجريمة الالكترونية بين جهود القانون وهياكل الدعم:

في ظل الحركة التشريعية الدولية لمجابهة الجريمة الالكترونية لم يبقى المشرع الجزائري في وضع المتفرج؛ بل أسوة بالنهج الدولي في هذا المجال حاول ضبط انتشار هذه الجريمة. لذا سنخصص هذا المبحث للحديث عن النصوص القانونية لمواجهة تفشي الظاهرة (المطلب الأول)، ونتحدث كذلك عن الأجهزة المكلفة والمختصة بمبحث والتحري (المطلب الثاني). كما سنوضحه فيما يلي:

1.3 مواجهة الجريمة الالكترونية في التشريع الجزائري

تمت مواجهة الجريمة الالكترونية عبر العديد من الأحكام القانونية لعل أبرزها القانون المتعلق بتكنولوجيات المعلومات والاتصال ومكافحتها، وكذا عبر الأحكام المقررة في قانون العقوبات. كما سنوضحه فيما يلي:

1.1.3 مواجهة الجريمة الالكترونية من خلال القانون 04/09 المتعلق بتكنولوجيات المعلومات والاتصال ومكافحتها:

كفل المشرع من خلال القانون 04/09 نصوص معالجة وواقية لمختلف الجرائم الالكترونية، فبعد انتشار اعتداءات على معطيات الأفراد والمؤسسات والدولة على شبكة إنترنت تدخل المشرع بمقتضى نصوص خاصة، إذ أجاز المشرع مراقبة اتصالات الالكترونية بنصه: "...يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية ووفقا لقانون الإجراءات الجزائية وفي هذا القانون وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية" (المادة 03، قانون رقم 04/09).

غير أنّ، هذه المراقبة غير مطلقة؛ فقد نص المشرع على حالات خاصة لذلك؛ لاسيما في الحالات التالية: (المادة 04، قانون رقم 04/09).

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

- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية؛
- لمقتضيات التحريات والتحقيقات القضائية؛
- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة؛

كما نص المشرع على بعض ترتيبات التفتيش في ذات القانون، لاسيما عند اكتشاف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها، على أن يتم ذلك مع السهر على صحة المنظومة المعلوماتية (المواد 05، 06، 07، 08، 09، 10، 11، 12، 13، 14، 15، 16، 17، 18، 19، 20، 21، 22، 23، 24، 25، 26، 27، 28، 29، 30، 31، 32، 33، 34، 35، 36، 37، 38، 39، 40، 41، 42، 43، 44، 45، 46، 47، 48، 49، 50، 51، 52، 53، 54، 55، 56، 57، 58، 59، 60، 61، 62، 63، 64، 65، 66، 67، 68، 69، 70، 71، 72، 73، 74، 75، 76، 77، 78، 79، 80، 81، 82، 83، 84، 85، 86، 87، 88، 89، 90، 91، 92، 93، 94، 95، 96، 97، 98، 99، 100). قانون رقم 049/09.

وبصرف ذلك، نص المشرع على إحداث هيئة وطنية لغرض الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، توكل لها مجموعة من المهام أبرزها: (المادتين 13، 14، قانون رقم 04/09)

- تنشيط وتنسيق عمليات الوقاية من الجرائم الالكترونية؛
- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجرئها بما في ذلك تجميع المعلومات وانجاز خبرات قضائية؛
- تبادل المعلومات مع نظيراتها في الخارج بقصد جمع المعطيات المفيدة.

2.1.3 مواجهة الجريمة الالكترونية من خلال قانون العقوبات

تولى المشرع من خلال قانون العقوبات رقم 15/04 المعدل والمتمم للأمر 155/66 لاسيما الكتاب الثالث الباب الثاني منه الفصل الثالث بتحديد بمعالجة مجموعة من أفعال الإجرامية الالكترونية نستحضرها فيما يلي:

فيما يتعلق بالدخول للمنظومات المعلوماتية عن طريق الغش فقد وصفها بجريمة البسيطة وقرر لأجلها عقوبة الحبس من 03 أشهر إلى سنة وغرامة مالية قدرها من 50.000 دج إلى 100.000 دج، على أن تضاعف العقوبة إن كان هنالك حذف أو تعديل، وإن كان هنالك تخريب لنظام اشتغال المنظومة يعاقب الفاعل من 06 أشهر إلى سنتين وغرامة من 50.000 دج إلى 150.000 دج (المادة 394 مكرر، الأمر 155/66)، أما إذا كانت هناك إزالة لمعطيات تتضمنها المنظومة المعلوماتية الآلية فتتم المعاقبة بالحبس من 06 أشهر إلى 03 سنوات زائد غرامة مالية قدرها 500.000 دج إلى 2.000.000 دج (المادة 394 مكرر، الأمر 155/66).

وبصرف ذلك، تعرض المشرع إلى نوع آخر ألا وهو التصرف العمد في المعطيات عن طريق الغش، وهنا يعاقب المجرم بالحبس من شهرين إلى 03 سنوات وبغرامة مالية مقدارها 1.000.000 دج إلى 5.000.000 دج (المادة 394 مكرر، الأمر 155/66)، كما نص على حالات تضاعف فيها العقوبة وهي:

- استهداف الجريمة الدفاع الوطني أو المؤسسات الخاضعة للنظام العام؛

- إذا كان الفاعل شخص معنوي؛

- إذا كانت هناك مشاركة في الجرم أو اتفاق على تنفيذ الجريمة.

ناهيك عن ذلك، هناك العقوبات المتعلقة بمصادرة كل الأجهزة ومختلف البرامج التي استعملت كماديات في الجريمة مع الاحتفاظ بحقوق الغير ذوي نية الحسنة.

2.3 الأجهزة المكلفة والمختصة ببحث والتحري:

كان لتطور الجريمة الالكترونية الأثر البالغ في حتمية تطوير الأجهزة المختصة والمكلفة ببحث والتحري دوليا ووطنيا، لذا سنخصص الحديث عن الأجهزة المكلفة ببحث والتحري (أولا)، ومن ثمة نتطرق لأجهزة المختصة ببحث والتحري (ثانيا). كما سنوضحه فيما يلي:

1.2.3 الأجهزة المكلفة ببحث والتحري الدولية:

لا ريب في أنّ الدول الغربية كانت السبّاقة لإحداث هذا النوع من الأجهزة المكلفة ببحث والتحري في الجرائم الالكترونية، تأسيسا على تقدمها من الناحية التقنية وتوفر لديها الإمكانيات اللازمة لإحداثها؛ وتتصدر الولايات المتحدة المشهد أين قامت بإحداث العديد منها (سعيداني، 2013/2012، ص104). نذكر منها: (سعيداني، 2013/2012، ص105)

- شرطة واب: وهي عبارة عن نقطة مراقبة لأنشطة التي تجرى في انترنت، ناهيك عن مهامها في تلقي الشكاوي وملاحقة القرصنة، والبحث عن الأدلة وتقديم للعدالة؛

- نيابة الجرائم الحاسوب والاتصالات: وتتكون من مجموعة من القضاة النيابة العامة كانوا قد تلقوا تكويننا مكثف على أنظمة معالجة الآلية البيانية، أوكلت لهم صلاحيات معتبرة في مجال الجرائم الالكترونية والعدوان بالملكيات الفكرية؛

- مركز تلقي شكاوي جرائم الانترنت: والذي تم استحداثه من طرف مكتب التحقيقات الفيدرالي، والذي يشتغل بمشاركة مع المركز الوطني للجرائم الياقات البيضاء، وعملها يكمن في تلقي الشكاوي عبر موقعه عبر الانترنت من خلال ملء استمارة الكترونية ثم يتولى المتخصصون تحليل هذه الشكاوي وربطها مع شكاوي أخرى مقدمة.

وبالعودة للجزائر؛ فإنّ الوضع بالنظر لخصوصيته كان محتما المبادرة بتوفير كوادرم مؤهلة لمجابهة هذه الجريمة الالكترونية، وكذا وضع لأجهزة مكلفة بذلك، والتي تتجسد في كل من جهاز الشرطة أو جهاز الدرك؛ فأما الأول فقد استحدث على مستوى المديرية العامة للأمن الوطني بشاطوناف مخبرا مركزيا للشرطة العلمية ومخبرين جهويين في كل من وهران وقسنطينة، وتحتوي هذه الفروع على خلية للإعلام الآلي، ناهيك عن ذلك تتواجد على مستوى أمن الولايات في الوطن فرق متخصصة بالتحقيق في الجريمة الالكترونية تشتغل بالتنسيق مع المخابر السالفة الذكر، وأما جهاز الدرك فيتوفر على معهد وطني للأدلة الجنائية ببوشاوي تابع لقسم الإعلام والإلكترونيك له اختصاص أصيل في الجرائم الالكترونية (سعيداني، 2013/2012، ص107).

2.2.3 أجهزة مختصة ببحث والتحري دوليا:

على الصعيد الدولي تعد المنظمة الدولية للشرطة الجنائية الأنتربول أبرز تلك هيئات المتخصصة دوليا في مجابهة الجرائم الالكترونية من خلال التعاون بين مختلف أجهزة الشرطة لدى الدول؛ لاسيما من ناحية تجميع المعلومات أو من خلال التعاون في ملاحقة الفارين والقبض عليهم وتسليم للدول المعنية (سعيداني، 2013/2012، ص107).

ناهيك عن ذلك، توجد الشرطة الأوروبية أوروبول، وهو جهاز تابع للإتحاد الأوروبي مقره مدينة لاهاي أنشأ سنة 1992 ليكون جهاز كحلقة وصل بين دول الأعضاء في كل الجرائم عموماً والجرائم الالكترونية على وجه الخصوص، من خلال المساعدة في تجميع البيانات وتحليلها والتحقيق بشأنها والقبض على مرتكبها (سعيداني، 2013/2012، ص108).

4. الخاتمة

في ختام هذه الدراسة التي تمحورت حول موضوع من مواضيع الساعة ألا وهي الجريمة الالكترونية، نجتمع بأنّ عالم الجريمة قد تطور وانتقل إلى عالم متطور جداً سريع التفشي من الأفراد إلى المؤسسات وصعب في مكافحته لتنوع صوره، ولما كان أقدم أساليب المواجهة والردع تتأسس على إيقاع العقاب، كان لزاماً البحث عن مخرج قانوني يناسب الظاهرة باعتماد على هيئات متخصصة للبحث والتحري بشأنها. ومن جملة ما أمكننا التوصل إليه النتائج التالية:

- الجرائم الالكترونية هي عمل غير مشروع واعتداء على نظم المعالجة الآلية للمعطيات؛

- أنّها جريمة تنصب على محل خاص يختلف عن الجرائم التقليدية؛ مثل حياة الأشخاص، أموال الأفراد ومؤسسات، وأمن الدولة؛

- تبين كذلك بالنظر لتمييزها أنها تحتاج إلى نصوص عقابية خاصة تنصب على محل مادي ملموس؛

- توجد الكثير من الأجهزة المكلفة ببحث والتحري بشأنها دولياً ووطنياً (جهاز الشرطة وجهاز الدرك)؛

- توجد كذلك أجهزة متخصصة أحدثت لمجابهة الجريمة الالكترونية؛ لاسيما أنتربول.

هذا، وقد سمحت لنا الدراسة محل البحث من تبلور في مخيلتنا مجموعة من اقتراحات للحد أو القضاء على ظاهرة الجريمة الالكترونية. نستحضر بعض منها:

- ضرورة توعية وتحسيس الأفراد بمفهوم الجريمة الالكترونية والخطر القائم من وراءها؛

- ضرورة إحاطة المواطن من العناوين الالكترونية التي تتطلب معلومات سرية مثل بطاقات الائتمان؛

- ضرورة عدم الإفصاح عن كلمة سر لأي شخص، وحرص على تغييرها دورياً؛

- ضرورة زيادة الوازع الديني وسط المجتمع؛

- عدم حفظ صور وفيديوهات الشخصية في الحاسوب؛

- عدم تحميل أي برنامج مصدره غير معروف؛

- ضرورة تطوير الأجهزة المكلفة بمكافحة الجريمة الالكترونية؛

- ضرورة تكييف القوانين من جانب المشرع وجعلها زاجرة أكثر لمن تخول له نفسه المبادرة بعمل غير مشروع اتجاء الأفراد والمؤسسات العامة.

5. قائمة المراجع

• المؤلفات:

- (1) أبوزهرة محمد، (1998)، الجريمة والعقوبة في الفقه الإسلامي، القاهرة، مصر، دار الفكر العربي، دون طبعة.
- (2) رحمانى منصور، (دون تاريخ نشر)، الوجيز في القانون الجنائي العام، الجزائر، دار العلوم للنشر والتوزيع، دون طبعة.
- (3) فكري أيمن عبد الله، (2014)، الجرائم الالكترونية دراسة مقارنة في التشريعات العربية والأجنبية، الرياض، السعودية، مكتبة القانون والاقتصاد، الطبعة الأولى.
- (4) أشرف جمال محمود عبد العاطي، (2000)، الإدارة الالكترونية للمرافق العامة، القاهرة، مصر، دار النهضة العربية، بدون طبعة.

• الأطروحات:

- (1) نائلة عادل محمد فريد، (2003)، جرائم الحاسب الاقصادية، أطروحة دكتوراه، كلية الحقوق، جامعة القاهرة، مصر.
- (2) العجمي عبد الله دغش، (2014)، المشكلات العملية والقانونية للجرائم الالكترونية، رسالة ماجستير، جامعة الشرق الأوسط، الأردن.
- (3) سعيداني نعيم، (2013/2012)، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، الجزائر.

• المقالات:

- (1) عبد الحكيم مولاي إبراهيم، (2015)، الجرائم الالكترونية، مجلة الحقوق والعلوم الإنسانية، العدد 23.
- (2) رحموني محمد، (2017)، خصائص الجريمة الالكترونية ومجالاتها استعمالها، مجلة الحقيقة للعلوم الإنسانية والاجتماعية، المجلد 16، العدد 03.
- (3) دواوي نعيمة، (2020)، الجريمة الالكترونية (خصائصها ومجالات استخدامها، وأهل سبل مكافحتها)، مجلة مهد اللغات، المجلد 02، العدد 01.

• القوانين:

- (1) القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر 155/66 المؤرخ في 08 جوان 1966، المتضمن قانون العقوبات، الجريدة الرسمية، العدد 71، المؤرخة في 10 نوفمبر 2004.
- (2) القانون رقم 04/09، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، المؤرخة في 16 أوت 2009.