

التأصيل القانوني للجرائم السيبرانية المرتكبة عبر الوسائط الرقمية

Legal Rooting of Cybercrimes Committed through Digital Media

تاريخ استلام المقال: 2023/04/01 تاريخ قبول المقال للنشر: 2023/06/20 تاريخ نشر المقال: 2023/06/30

د/ مباركة حنان كركوري

– مخبر قانون الأسرة ، جامعة الجزائر ، (الجزائر)، m.karkouri@univ-alger.dz

ملخص:

تعالج هذه الدراسة موضوع التأصيل القانوني للجرائم السيبرانية المرتكبة عبر الوسائط الرقمية؛ حيث يتجلى من خلال استقراء الأحكام المنظمة لها والتي تحدد الإطار المفاهيمي لهذا النوع من الجرائم المستحدثة، وكذا تبين موقف المشرع الجزائري منها والذي أقره صراحة من خلال استحداثه لقسم خاص معنون بالمساس بأنظمة المعالجة الآلية للمعطيات في قانون العقوبات رقم 15/04 المعدل والمتمم للأمر رقم 156/66، وكذا تحديد طرق ارتكابها التي تتم عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية وفقا لأحكام القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها هذا من ناحية.

ومن ناحية أخرى تسليط الضوء على الآليات الإجرائية التي استحدثها المشرع لمكافحة الجرائم السيبرانية بحيث نص عليها في التشريعات العقابية العامة الواردة في القانون رقم 15/04 و 02/16 المعدلين والمتممين للأمر رقم 156/66 المتضمن قانون العقوبات الجزائري، إضافة إلى إقراره لجملة من الاستراتيجيات الفعالة في مضامين القوانين الخاصة والمتمثلة في القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وكذا القانون رقم 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، وقد هدف المشرع الجزائري من خلال سَنَ هذه القوانين إلى تجريم كافة أشكال الاعتداء على حقوق الأفراد في البيئة المعلوماتية فضلا عن تحقيقه لمبدأ الأمن السيبراني.

الكلمات المفتاحية: الجرائم السيبرانية؛ الوسائط الرقمية؛ تكنولوجيا الإعلام والاتصالات؛ آليات مكافحة؛ قانون العقوبات؛ التشريع الجزائري.

Abstract:

This study deals with the issue of the legal rooting of cybercrimes committed through digital media, as it is reflected through the extrapolation of the provisions regulating them that define the conceptual framework for this type of new crimes, as well as clarifying the position of the Algerian legislator on them, which he explicitly approved through the development of a special section entitled to prejudice to automated data processing systems in the Penal Code N°. 04/15 amending and supplementing Order N°. 66/156, It also determines the methods of their commission carried out through an information system or an electronic communications system in accordance with the provisions of the law containing special rules for the prevention and combating of crimes related to information and communication technologies, on the one hand.

On the other hand, highlighting the procedural mechanisms developed by the legislator to combat cybercrime, as stipulated in the general penal legislation contained in Law N°. 04/15 and 16/02 amending and supplementing Order N°. 66/156 on the Algerian Penal Code, in addition to approving a number of effective strategies in the contents of special laws, represented in Law N°. 09/04 containing special rules for the prevention and combating of crimes related to information and communication

technologies. Law N°. 18/07 on the protection of natural persons in the processing of personal data, through the enactment of these laws, the Algerian legislator aimed to criminalize all forms of infringement of the rights of individuals in the information environment, as well as to achieve the principle of cybersecurity.

Keywords: Cybercrime; digital media; information and communication technology; control mechanisms; penal code; Algerian legislation.

مقدمة:

إن استخدام تكنولوجيا المعلومات والاتصالات من قبل الأفراد والمؤسسات في مختلف المجالات العامة والخاصة أصبح ضرورة حتمية لا غنى عنها في وقتنا الحالي، نظرا لما تحققه هذه الوسيلة من يُسر وسرعة في أداء وإدارة الأعمال التي تتجزأ بواسطة النظام المعلوماتي الذي يساهم في ربح الوقت والجهد، وعليه كان لزاما على المشرع الجزائري أن يسنّ قوانين خاصة ويضع القواعد الملزمة لتسيير الأنشطة والمهام بطريقة منظمة تساهم في الاستفادة من هذه التقنية الرقمية.

وتتجلى الأهمية العلمية والعملية لهذه الدراسة في تكريس القوانين التي تجرم الأفعال التي من شأنها إحداث ضرر بالمصلحة العامة أو الخاصة في تحقيق وتكريس مبدأ الأمن السيبراني وحماية الحقوق المالية والشخصية والفكرية للأفراد والمؤسسات من أيّ إعتداء، حيث يعتبر الهجوم على النظام المعلوماتي بمثابة تهديد قانوني محقق ونوع جديد من الجرائم المستحدثة في القرن الواحد والعشرين وقد أطلق عليها تسمية "الجرائم السيبرانية"، ذلك أن مرتكبي هذا النوع من الجرائم يستخدمون تقنيات وطرق الاتصال الحديثة بطريقة غير مشروعة كوسيلة لتسهيل عملياتهم التي قد تنتقل من البعد الوطني لتتخذ بُعداً عالمياً في ارتكابها، حيث تتسم هذه الجريمة الناعمة بالدقة في التخطيط والتنظيم والسرعة وصعوبة وجود أدلة لإثباتها.

وتجدر الإشارة إلى أن النصوص الواردة في أحكام قانون العقوبات أصبحت قاصرة نوعا ما في التصدي لهذا النوع من الجرائم السيبرانية، لذلك حرص المشرع في التصدي لظاهرة الجريمة السيبرانية المرتكبة عبر الوسائط الرقمية وما يصاحبها من أضرار وتهديدات قانونية، على تعديل المنظومة التشريعية العقابية.

وفي هذا الصدد قام باستحداث آليات إجرائية تجرم كل فعل يمسّ بالنظام المعلوماتي يتناسب وطبيعة الجريمة السيبرانية وذلك في الأحكام الواردة في القانون رقم 15/04 و 02/16 المعدلين والمتممين للأمر رقم 156/66 المتضمن قانون العقوبات الجزائري، فضلا عن إقراره لمجموعة من القوانين الخاصة التي تهدف إلى مكافحة الجرائم السيبرانية ومن بينها القانون رقم 04/09 المتضمن القواعد الخاصة للحماية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وكذا القانون رقم 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، وعليه فإن الإشكالية المطروحة في هذا الصدد هي: فيم تتمثل الجرائم السيبرانية وما مدى كفاية التشريعات العقابية في التصدي لهذا النوع من الجرائم المرتكبة عبر الوسائط الرقمية؟

وللإجابة على الإشكالية المطروحة تم الاعتماد على المنهج الوصفي والتحليل أداة له وذلك من خلال وصف وتحليل المعطيات والآراء الفقهية ذات الصلة بموضوع التأصيل القانوني للجرائم السيبرانية المرتكبة عبر الوسائط الرقمية، وكذا مختلف النصوص الواردة في التشريعات العقابية وعلى وجه الدقة في القسم الخاص بالجرائم المتعلقة بمسائل أنظمة المعالجة الآلية للمعطيات.

وتهدف هذه الدراسة إلى البحث في مختلف الأحكام المنظمة للجرائم السيبرانية المرتكبة عبر الوسائط الرقمية ومدى اعتبارها تهديد قانوني يمس بمبدأ استقرار الأمن السيبراني، فضلا عن تحديد إستراتيجية المشرع الجزائري في التصدي لهذه الجريمة ذات الطابع المعلوماتي في النصوص التشريعية العقابية، وقد قسمت هذه الدراسة إلى بدورها بحثين أساسيين؛

جاء المبحث الأول منها تحت عنوان الأحكام المنظمة للجرائم السيبرانية المرتكبة عبر الوسائط الرقمية والذي يعالج في البداية تحديد الإطار المفاهيمي لها وكذا موقف المشرع الجزائري منها والذي أورده في قانون العقوبات والقانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

أما المبحث الثاني فعنون ب: آليات مكافحة المشرع الجزائري للجرائم السيبرانية المرتكبة في البيئة الرقمية، وقد سلطت مضامين هذا المبحث الضوء على آليات التدخل بالنصوص العقابية العامة لمكافحة الجرائم السيبرانية وفقا للمقتضيات التي جاء بها القانون رقم 15/04 المعدل والمتمم لقانون العقوبات، إضافة إلى تبيان مختلف الآليات والاستراتيجيات المقررة لمكافحة الجرائم السيبرانية وفقا لأحكام القوانين الخاصة والمتمثلة على وجه الخصوص في القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وكذا القانون رقم 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، وسيتم التفصيل في جميع هذه المسائل تباعا في المباحث الآتية:

المبحث الأول: الأحكام المنظمة للجرائم السيبرانية المرتكبة عبر الوسائط الرقمية

تعد الجرائم السيبرانية من بين الجرائم التي استحضرتها الممارسات السلبية لتكنولوجيا المعلومات والاتصالات، حيث تختلف هذه الجرائم المرتكبة عبر الوسائط الرقمية عن الجرائم التقليدية سواء من حيث طبيعتها ووسيلة ارتكابها أو حتى الأحكام المنظمة لها؛ ولذلك كان لابد من توضيح الأحكام المنظمة للجرائم السيبرانية والتي تتجلى بداية في تحديد الإطار المفاهيمي لها المتضمن تعريفها وموقف المشرع الجزائري منها والذي أبداه صراحة في مضامين نصوص القانونين رقم 15/04 و 02/16 المعدلين والمتممين للأمر رقم 156/66 المتضمن قانون العقوبات الجزائري، كما تجسد أيضا في نصوص أحكام القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها هذا من ناحية (المطلب الأول).

ومن ناحية أخرى كان لابد من تسليط الضوء على مختلف الخصائص التي تتميز بها الجريمة السيبرانية والمتمثلة في اعتبار هذه الجريمة من بين الجرائم الخفية إضافة إلى تميزها بالطابع العالمي العابر للحدود، فضلا عن صعوبة الإثبات والوصول إلى دليل مادي ملموس يدل على قيام وارتكاب الجريمة السيبرانية في البيئة الرقمية (المطلب الثاني)، وسيتم التفصيل في مجموع هذه المسائل في المطالب الموالية:

المطلب الأول: الإطار المفاهيمي للجريمة السيبرانية

تعتبر الجرائم السيبرانية من الجرائم المستحدثة، فلم يستقر فقهاء القانون على وضع تعريف محدد للجرائم الناشئة في بيئة الحاسب الآلي أو بيئة الشبكات، وذلك بسبب نشأة وتطور ظاهرة الإجرام المرتبط بتقنية المعلومات، فمنهم من يطلق عليها جرائم الإنترنت، في حين أن جانب آخر من الفقه من يطلق عليها الجريمة المرتبطة بالكمبيوتر، أو جرائم التقنية العالية، أو الجرائم المعلوماتية المتصلة بتكنولوجيا المعلومات والاتصالات، أو جرائم الشبكة العنكبوتية، حتى أصبح أخيراً يطلق عليها مصطلح الجرائم السيبرانية.

وقبل البدء في تعريف الجرائم المتصلة بتكنولوجيا المعلومات والاتصالات أو السيبرانية، فإنه من المهم البدء بتعريف الجريمة السيبرانية لغةً واصطلاحاً، وكذلك توضيح موقف المشرع الجزائري منها، وذلك على النحو الآتي بيانه.

أولاً: تعريف الجريمة السيبرانية في اللغة والاصطلاح

تُعرّف الجريمة في اللغة بأنها الأصل الواحد الذي ترجع إليه الفروع؛ فالجُرْمُ القطعُ، وجَرَمَ كَسب، والجريمةُ هي الذنب¹، وقد جاء ذكر الجريمة في القرآن الكريم في قوله تَعَالَى في الآية 40 من سورة الأعراف [حَتَّى يَلِجَ الْجَمَلُ فِي سَمِّ الْخِيَاطِ وَكَذَلِكَ نَجْزِي الْمُجْرِمِينَ]².

ومن الناحية الاصطلاحية تعرف الجريمة في الشريعة الإسلامية بأنها "المحظورات الشرعية التي زجر الله تعالى عنها بحد أو تعزير"، في حين عرفها فقهاء القانون بأنها "كل فعل ايجابي نص القانون على منعه، أو امتناع سلبي عن أداء فعل أمر القانون به واعتبره جريمة وخصص له عقوبة معينة ذات

¹ - ابن منظور محمد بن مكرم بن علي أبو الفضل جمال الدين جمال الدين الأنصاري الرويفعي الإفريقي، لسان العرب، المجلد الثاني، طبعة صادر، دار صادر، بيروت، ص 90.

² - سورة الأعراف، الآية 40.

ألم معين يوقع على الشخص المسؤول عنها جنائياً¹، إذن فالجريمة حسب فقهاء القانون تتمثل في الفعل أو الترك الذي نصّ القانون على عقوبة مقدرة له².

وقبل تعريفنا للجريمة السيبرانية لابد من الإشارة في البداية إلى مصدر مصطلح كلمة "Cyber"؛ حيث تشير المراجع العلمية إلى أن عالم الرياضيات "توريرت وينر" هو أول من استخدم مصطلح السيبرانية عام 1948 أثناء دراسته لموضوع القيادة والسيطرة في حقل الهندسة الميكانيكية³، أما بالنسبة لمصدرها في المعاجم الأجنبية فيعني الارتباط بالحاسوب أو شبكات الحاسوب، وتعني أيضاً فضاء الانترنت، أما معناها في اللغة اليونانية فهي كلمة مشتقة من "kybernetes" وتعني القيادة أو التحكم عن بعد⁴.

ويمكننا القول بأن هذه الجريمة هي عبارة عن أحد أهم النتائج السلبية التي خلفها التطور التكنولوجي المتسارع في القرن العشرين، وقد اختلف الفقهاء في تحديد تسمية محددة لهذه الجريمة منذ نشأتها نظراً لارتباطها الوثيق بتقنية المعلومات، فقد اصطلح على تسميتها في بادئ الأمر "بجريمة إساءة استخدام الكمبيوتر"، ثم أطلق عليها "جريمة احتيال الكمبيوتر"، لتتطور تسميتها بعد ذلك إلى "الجريمة المعلوماتية أو جرائم الكمبيوتر"، ثم "جرائم التقنية العالية وجرائم الهاكرز"، ليستقر الفقه بعد ذلك على تسميتها "بالجريمة السيبرانية Cyber Crim"⁵، وفي هذا الصدد نجد هيئة الأمم المتحدة قد عرفت الجريمة السيبرانية بأنها "جميع السلوكات الغير قانونية التي تستخدم عمليات الكترونية تستهدف امن النظام المعلوماتي والمعطيات التي يعالجها"⁶.

¹ - طلال أبو عفيفه، أصول علمي الإجرام والعقاب وآخر الجهود الدولية والعربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية، ط 1، دار الجندي للنشر والتوزيع، فلسطين 2013، ص 31.

² - الإمام محمد أبو زهرة، الجريمة والعقوبة في الفقه الإسلامي -العقوبة-، دار الفكر العربي، الإسكندرية، 2008، ص 22.

³ - الفتلاوي عبيس نعمة، الهجمات السيبرانية: دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، ط 1، منشورات زين الحقوقية، بيروت 2018، ص 11.

⁴ - بن مرزوق عنتر وحرشاي محي الدين، الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية، ورقة علمية مقدمة في فعاليات المؤتمر الدولي المعنون "استراتيجيات الدفاع الوطني"، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، الجزائر 2017، ص 66.

⁵ - البدائية ذياب موسى، الجرائم الإلكترونية: المفهوم والأسباب، ورقة علمية مقدمة في فعاليات الملتقى العلمي المعنون "الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية"، كلية العلوم الإستراتيجية، جامعة الأردن، 2-4/09/2014، ص 05.

⁶ - Romain Beas, La lutte contre la cybercriminalité au regard de l'action des états, doctorat de droit privé et sciences criminelles, université de lorraine, Faculté de droit, Paris, 2016, p 25-26.

وهي أيضا جميع الأفعال المخالفة للقانون التي ترتكب بواسطة الحاسوب من خلال شبكة الانترنت، وهي تتطلب إلمام خاص بتقنيات ونظم المعلومات سواء لارتكابها أو للتحقيق فيها، ويقصد بها أيضا أي نشاط غير مشروع ناشئ من مكونات الانترنت وتسمى أيضا بالجرائم السيبرانية أو السيبرانية لارتباطها بالعالم الافتراضي.

ومن خلال ما سبق ذكره يمكننا أن نعرف الجريمة السيبرانية بأنها السلوك غير المشروع أو المنافي للأخلاق أو غير المسموح به المرتبط بالشبكات المعلوماتية العالمية، أي أنها كل فعل أو امتناع يقوم به الشخص بصفة عمدية يتمثل في فعل الاستخدام غير المشروع لتقنية المعلومات بحيث يهدف من خلاله إلى تحقيق مصالح شخصية تتمثل في الاعتداء على الأموال المادية أو المعنوية، كما قد ينصب موضوعها أيضا في الاعتداء على خصوصية الأفراد والمؤسسات، فهي كل عمل أو امتناع يأتيه الشخص قصد الإضرار بمكونات الحاسب وشبكات الاتصال الخاصة به هذا من جهة، ومن جهة أخرى فإن هذه الجريمة هي التي يكون النظام المعلوماتي فيها وسيلة أساسية لارتكاب جريمة تقليدية، إما ضد الأموال كالتحويل الإلكتروني غير المشروع للأموال أو ضد الأشخاص كجريمة السب أو القذف عبر شبكة الإنترنت.

ثانيا: موقف المشرع الجزائري من الجرائم السيبرانية

بالإشارة إلى القانون الجزائري فإننا نجد بأن المشرع الجزائري قد أبدى موقفاً واضحاً وصريحاً بشأن هذه المسألة؛ حيث عالج مسألة تحديد الإطار المفاهيمي للجريمة السيبرانية وأطلق عليها مصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال في مختلف التعديلات الواردة في النصوص التشريعية العقابية والتي تضمنت فرض عقوبات رادعة على مرتكبي هذه الجرائم¹، كما نرى أيضا بأن سبب هذه التعديلات المتتالية لنصوص قانون العقوبات الجزائري يعود بالدرجة الأولى إلى ازدياد وعي المشرع الجزائري بمدى خطورة هذا النوع من الجرائم المستحدثة التي تضر بمصالح الأفراد على وجه الخصوص وبأمن وسلامة الدولة واقتصادها الوطني على وجه العموم².

¹ - طالة لامية، التهديدات والجرائم السيبرانية: تأثيرها على الأمن القومي للدول واستراتيجيات مكافحتها، مقال منشور في مجلة معالم للدراسات القانونية والسياسية، المركز الجامعي تندوف، الجزائر، المجلد 04، العدد 02، 2020، ص 65.

² - إن ارتكاب الجرائم المتصلة بتكنولوجيا الإعلام والاتصال في البيئة الرقمية يؤثر على اقتصاديات الدول ويظهر هذا التأثير جليا من خلال ارتكاب الجرائم المالية والاقتصادية وكذا جرائم الأعمال والمتمثلة في السطو على حسابات الأفراد والمؤسسات المالية ومن بينها بنوك الدول وكذا أرقام البطاقات الائتمانية، فضلا عن جرائم التزوير وغسل الأموال وتحويلها من حسابات العملاء بطرق غير مشروعة وكل ذلك يتم من خلال شبكة الانترنت، لمزيد من التفصيل بهذا الخصوص ينظر: جاب الله حكيم، انعكاسات الجريمة السيبرانية على البيئة الرقمية: دراسة في آليات واستراتيجيات مكافحتها، مقال منشور في مجلة حوليات جامعة الجزائر 1، جامعة الجزائر 01 بن يوسف بن خدة، الجزائر، المجلد 35، العدد 03،

ففي سنة 2004 أصدر المشرع الجزائري القانون رقم 15/04 المتمم للأمر رقم 156/66 المتضمن قانون العقوبات بحيث أدرج فيه قسماً مخصصاً وهو القسم السابع مكرر والذي نص على الفصل في أحكام الجرائم المتعلقة بمساس أنظمة المعالجة الآلية للمعطيات¹.

أما في سنة 2006 أدخل تعديلاً جديداً على قانون العقوبات وذلك بموجب أحكام القانون رقم 23/06²، وقد تعلق هذا التعديل بالقسم السابع مكرر المتعلق بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، بحيث تم تشديد العقوبة على الأفعال الماسة بهذه الأنظمة دون المساس بالنصوص التجريبية التي أوردتها أحكام القانون 15/04، كما أدخل المشرع تعديلاً جديداً في سنة 2016 وذلك بموجب أحكام القانون رقم 02/16 المعدل والمتمم لقانون العقوبات³، حيث تضمن هذا التعديل مادتين؛ هما 87 مكرر 12 المتعلقة باستخدام تكنولوجيات الإعلام والاتصال لتجنيد الأشخاص لصالح إرهابي، والمادة 394 مكرر 08 المتعلقة بمقدم خدمات الانترنت.

كما نجد أيضاً المادة 02 الفقرة (أ) من القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها قد عرفت الجرائم السيبرانية بأنها "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية"⁴.

والجدير بالذكر أن الموقف الذي حدده المشرع الجزائري للجريمة السيبرانية قد اعتمد بالدرجة الأولى على الجمع بين معايير عديدة في تبيانها لمعالم هذه الجريمة ذات الطابع الخاص، ففي البداية اعتمد على معيار الوسيلة المتعمدة في الجريمة والتي تتمثل في نظام الاتصالات الإلكترونية ثم اعتمد على المعيار القائم على أساس الموضوع والمتمثل في المساس بأنظمة المعالجة الآلية للمعطيات، يليها بعد ذلك معيار القانون الواجب التطبيق أو ما يطلق عليه بالركن الشرعي في الجريمة.

2021، ص 656، وانظر أيضاً: قنديلجي عامر إبراهيم، الحكومة الالكترونية، ط 1، دار المسيرة، الأردن 2015، ص 312.

¹ - للمزيد من التفصيل ينظر القسم السابع مكرر يتضمن 08 مواد؛ من المادة 394 مكرر إلى 394 مكرر 07 ويتعلق بـ "المساس بأنظمة المعالجة الآلية للمعطيات" من القانون رقم 15/04 المتضمن قانون العقوبات الجزائري المعدل والمتمم للأمر رقم 156/66، الجريدة الرسمية عدد 71، المؤرخة في 10 نوفمبر 2004.

² - القانون رقم 23/06 المتضمن قانون العقوبات الجزائري المعدل والمتمم للأمر رقم 156/66، الجريدة الرسمية عدد 84، المؤرخة في 24 ديسمبر 2006.

³ - القانون رقم 02/16 المتضمن قانون العقوبات الجزائري المعدل والمتمم للأمر رقم 156/66، الجريدة الرسمية عدد 37، المؤرخة في 22 جوان 2016.

⁴ - المادة 02 الفقرة (أ) من القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية عدد 47، المؤرخة في 05 أوت 2009.

وقد تم النص على الأحكام المنظمة للركن الشرعي للجريمة في النصوص التشريعية الواردة في قانون العقوبات في القسم المتعلق "بالمساس بأنظمة المعالجة الآلية للمعطيات"، وفيما يتعلق بالمعيار الأخير في تحديد نطاق الجريمة الإلكترونية، فقد أقر المشرع الجزائري بأن الجريمة السيبرانية ترتكب في نظام معلوماتي أو يسهل ارتكابها عليه، وهو الأمر الذي من شأنه أن يوسع دائرة التجريم على الأفعال المجرمة والمكونة لقيام الجريمة السيبرانية في مضمون الأحكام العقابية المنصوص عليها في نصوص التشريع الجزائري.

المطلب الثاني: خصائص الجرائم السيبرانية

تتميز الجريمة السيبرانية بعدة خصائص تميزها عن غيرها من الجرائم التقليدية، وهو الأمر الذي يجعل منها تمثل تهديدا قانونيا وحقيقيا في هذا الفضاء الافتراضي أو الرقمي، ومن بين الخصائص المميزة لهذه الجريمة هو أنها تعتبر من بين أهم الجرائم الخفية التي يصعب اكتشاف ارتكابها في البيئة الافتراضية، كما أنها جريمة عالمية ذات بعد دولي وعابرة للحدود، فضلا عن صعوبة الإثبات والوصول إلى دليل مادي ملموس يدل على قيام الجريمة السيبرانية؛ وسيتم التفصيل في مجموع هذه الخصائص في النقاط التالية:

أولا: الجريمة السيبرانية جريمة خفية يصعب اكتشافها

تختص الجريمة السيبرانية بالخفاء؛ لأنها تقع في بيئة رقمية أو فضاء سيبراني لا حدود له وفي الغالب لا يشعر بها المجني عليه كسرقة البيانات أو إرسال الفيروسات إلى الجهاز المضيف، فمن ناحية تقنية يتم نقل المعلومات بواسطة النبضات الإلكترونية في صيغة أوامر رقمية¹.

حيث يلاحظ بأنها تتسم بالحدوث في البيئة الافتراضية لأنها تعد من الجرائم الناعمة، وذلك بسبب خفتها لأن الجاني مرتكب هذه الجريمة يتمتع بقدرات فنية تمكنه من تنفيذ جريمته بدقة دون إحداث أي فوضى ذات طابع مادي وهو الأمر الذي يؤدي إلى صعوبة كشف هوية الفاعل، لأن الجرائم السيبرانية لا يمكن إثباتها إلا بدليل ذو طبيعة خاصة تنتمي إلى نفس الفضاء السيبراني الذي تقع فيه الجريمة، ذلك أن الجاني يحرص على عدم الظهور في مسرح الجريمة ومواجهة المجني عليه أو الجهة المستهدفة لخوفه من اكتشاف هويته.

وتجد هذه الجريمة أساسها القانوني في أحكام قانون العقوبات في القسم السابع من الفصل الثالث الخاص المتعلق بجرائم الجنايات والجنح ضد الأموال والمعنونات بالمساس بأنظمة المعالجة الآلية للمعطيات، حيث يتضمن هذا القسم على وجه الخصوص جرائم الولوج إلى المعطيات المعالجة آليا عن طريق الغش والتزوير وكذا جريمة الحذف والتغيير والتخريب في هذه المعطيات، والجرائم الإلكترونية

¹ - الكعبي محمد عبيد، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت، ط 2، دار النهضة العربية، القاهرة 2009، ص 38.

بواسطة النظام المعلوماتي وأهمها استعمال أو إفشاء أو نشر معلومات منصوص عليها في قانون العقوبات وكذا البحث أو التجميع في معطيات مخزنة في نظام معلوماتي كجرائم التحويل الإلكتروني والسطو والنصب والاحتيال والسلب وغيرها، والجرائم المتعلقة بأمن الدولة ومؤسساتها كجرائم التجسس والإرهاب، والجرائم الإلكترونية للشخص المعنوي.

ثانيا: الجريمة السيبرانية عابرة للحدود الوطنية والدولية

وهذه هي إحدى الخصائص الهامة التي تتميز بها الجرائم السيبرانية، حيث أن المسرح الجنائي الخاص بها لا ينحصر في مكان معين أو دولة معينة؛ لأنها تتم في بيئة افتراضية لا حدود لها، وبالتالي يُعد الفضاء السيبراني حول العالم كله مسرحاً لها، وبإمكان المجرم السيبراني تنفيذ هجماته في أي مكان وزمان بالعالم، أي أنها جريمة دولية ذات بعد عالمي؛ حيث يعد البعد الدولي في الجريمة السيبرانية من أهم التحديات التي تواجه الجزائر في سبيل تحقيقها للأمن السيبراني الذي لا يخضع لإجراءات الحراسة الجمركية للحدود فهي حراسة تقليدية، فبعد ظهور شبكة الانترنت العالمية لم تعد هناك حدود مرئية أو حتى ملموسة تمنع تبادل المعلومات عبر الشبكة العنكبوتية العابرة للحدود.

والسبب الرئيسي في ذلك هو قدرة أجهزة الحواسيب في المساعدة على انتقال المعلومات بين الأفراد في مختلف أنحاء العالم، وهو الأمر الذي ساعد بشكل كبير في انتشار ارتكاب الجرائم السيبرانية عبر شبكات الانترنت العابرة لحدود الزمان والمكان سواء في الجزائر أو في العديد من الدول المختلفة عبر العالم، وتجدر الإشارة إلى أن الفعل المجرّم لا يتحقق إلا بواسطة استخدام أنظمة تقنية حديثة¹.

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 والاقتصادي²، والمقصود بذلك أن الجريمة السيبرانية كما هو معلوم ذات طابع دولي عابر للحدود لذلك فإن المجرم السيبراني قد ينتج عن قيامه بهذه الجريمة تضرر شخص واحد أو العديد من الأشخاص، أو مؤسسة واحدة أو العديد من المؤسسات وسواء كانوا داخل حدود دولة واحدة كالجزائر، أو أن الضرر قد يتعدى أثره إلى العديد من الدول بحيث يربطهم قاسم مشترك واحد يهدف المجرم من خلاله إلى الإضرار بمصالحهم الشخصية أو تحقيقاً لمنافعه الخاصة.

¹ - أبو شامة عباس عبد المحمود، عولمة الجريمة الاقتصادية، ط 01، جامعة نايف العربية للعلوم الأمنية، الرياض، 2007، ص 52.

² - بن صغير عبد المومن، الطبيعة الخاصة للجريمة المرتكبة عبر الانترنت في التشريع الجزائري والتشريع المقارن، ورقة علمية مقدمة في فعاليات الملتقى الوطني المعنون الجريمة المعلوماتية بين الوقاية والمكافحة، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر، 16-17/11/2015، ص 09.

ونظرا لوقوع الجريمة السيبرانية ذات البعد العالمي في بيئة افتراضية لا تعرف قيود الزمان والمكان جعلها تكتسب طبيعة خاصة تتميز بالتغيير والديناميكية، وهو الأمر الذي يصعب على رجال الشرطة القضائية والمحققين وحتى القضاة أثناء تأدية مهامهم إضفاء الوصف أو التكييف القانوني المناسب الذي ينطبق على الوقائع المتعلقة بارتكاب هذه الجريمة في الفضاء الافتراضي¹.

وتجدر الإشارة إلى أن الجريمة السيبرانية قد ترتكب بواسطة أشخاص يقيمون خارج حدود الدولة فيثور التساؤل في هذه الحالة حول الاختصاص القضائي لهذا النوع من الجرائم المستحدثة، وعلاوة على ذلك فإن امتداد أنشطة الملاحقة والتحري والضبط وإجراءات التفتيش التي تتم خارج الحدود تحتاج إلى تعاون دولي شامل وقائم على اتفاقيات ومعاهدات دولية مبرمة بين الدول الأعضاء التي تهدف إلى مكافحة هذه الجرائم وتحقيق الأمن السيبراني²، مع الأخذ بعين الاعتبار احترام السيادة الوطنية للدول المعنية بإبرام هذه المعاهدات والمقصود بذلك هو عدم تعارض أحكام هذه الاتفاقيات مع مضمون تشريعاتها الداخلية التي تعاقب على ارتكاب الجرائم السيبرانية أو المشاركة في ارتكابها ضد الأفراد والمؤسسات الخاصة وضد أمن الدولة ودفاعها ومؤسساتها العامة.

ثالثا: صعوبة إثبات وقوع الجرائم السيبرانية المرتكبة في البيئة الرقمية

تختص الجرائم المرتكبة عبر استخدام شبكات الإنترنت بالغموض وصعوبة الاكتشاف³، على غرار الجرائم التقليدية كالسرقة أو الاختلاس أو التخريب، حيث يعد إثبات السلوك غير المشروع الذي يهدف إلى المساس بالأمن السيبراني من أهم التحديات وذلك بفعل طبيعة الجاني والمجني عليه وكذلك وسيلة تنفيذ الجريمة السيبرانية التي تتم في بيئة رقمية، فالمجرم في غالب الحالات محترف وذكي لا يترك آثاراً لاقتراف الجرم والمجني عليه في غالب الحالات مؤسسات عامة أو خاصة تفضل الإحجام عن الإبلاغ حفاظا على سمعتها وثقة عملائها ومركزهم الاجتماعي فضلا عن إمكانية تدمير الدليل في مدة زمنية قياسية⁴.

حيث أن السبب الرئيسي الكامن في صعوبة إثبات الجريمة السيبرانية يتمثل في أن البيانات الموجودة عبر شبكة الانترنت تكون على هيئة نبضات إلكترونية غير مرئية ورموز مخزنة في وسائط تخزين ممغنطة بلغة الصفر والواحد، ولا يتم قراءة مضمونها إلا بواسطة جهاز الحاسب الآلي، مما

¹ - بن صغير عبد المومن، المرجع السابق، ص 11.

² - غادة نصار، الإرهاب والجريمة الإلكترونية، ط 1، العربي للنشر والتوزيع، القاهرة 2017، ص 38.

³ - بدوي عبد المحسن محمد، الجرائم المعلوماتية، مقال منشور في مجلة الأمن والحياة، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية، المجلد 29، العدد 335، 2010، ص 67.

⁴ - نمديلي رحيمة، خصوصية الجريمة الإلكترونية في القانون الجزائري والقانون المقارن، ورقة علمية مقدمة في فعاليات المؤتمر الدولي الرابع عشر المعنون "الجرائم الإلكترونية"، مركز جيل البحث العلمي، لبنان، 24-25/03/2017، ص 102.

يصعب عملية فهم وقراءة الدليل إن كان موجوداً، خاصة وأن الجاني مرتكب الجريمة السيبرانية باعتباره محترفا يسعى دائماً إلى تدمير الدليل المتمثل في ملفات الوثائق الالكترونية المحفوظة في جهاز الحاسب الآلي فضلاً عن حذف المعلومات والبيانات المخزنة فيه وعدم ترك أي أثر لجريمته.

إذ أنه من السهل مسح الدليل من الكمبيوتر في زمن قياسي باستخدام البرامج المخصصة لذلك، حيث تتم بمجرد لمسة خاطفة على لوحة المفاتيح، على اعتبار أن الجريمة السيبرانية تتم بأوامر وتعليمات تصدر إلى الجهاز¹، لأن الجريمة المرتكبة عبر الوسائط الرقمية تتم خارج إطار الواقع المادي الملموس، مما يجعل الأمور تزداد تعقيداً في الكشف عن ملابسات الجريمة السيبرانية لدى سلطات الأمن وأجهزة التحقيق²، لأنها جريمة تعتمد على نسبة ذكاء عالية في ارتكابها وهو الأمر الذي يصعب على سلطات الأمن والتحقيق ورجال الضبطية القضائية التقليدية التعامل مع هذا النوع من الجرائم المستحدثة ذلك أن الوصول لحقيقة وهوية مرتكبها يستوجب خبرة فنية عالية المستوى في المجال استخدام برامج الحاسب الآلي.

ومن بين صعوبات الوصول إلى الدليل في الجرائم السيبرانية المرتكبة أيضاً، هو قيام كبرى المواقع العالمية بإحاطة البيانات المخزنة على صفحاتها بسياج من الحماية أو يسمى بجدار الحماية الناري، لمنع التسلل والوصول غير المشروع إليها لتدميرها أو تبديلها أو الإطلاع عليها ونسخها³.

المبحث الثاني: آليات مكافحة المشرع الجزائري للجرائم السيبرانية المرتكبة في البيئة الرقمية

إن الجرائم السيبرانية المرتكبة عبر منظومة المعالجة الآلية للمعطيات تتميز بنوع من الخصوصية باعتبارها مرتكبة في الفضاء الافتراضي، وعليه أقر لها المشرع الجزائري في البداية مجموعة من الآليات العقابية المنصوص عليها في القواعد العامة الواردة في القانون رقم 15/04 المعدل والمتمم لقانون العقوبات وذلك من خلال تسليط الضوء على مختلف صور الاعتداء على هذه المنظومة، وكذا تبيانته لمختلف العقوبات المقررة على الجرائم التي تستهدف مؤسسات القطاع العام فضلاً عن تلك التي يتم ارتكابها من طرف الأشخاص المعنويين، إضافة إلى مصادرة الجهات المختصة لكافة الوسائل المستخدمة في ارتكاب هذه الجرائم وتوقيع العقاب على فعل الشروع في ارتكاب الجرائم السيبرانية والجرائم المتعلقة بإساءة استغلال تكنولوجيات الإعلام والاتصال وجرائم مقدمي خدمات الانترنت وفقاً لمقتضيات القانون رقم 02/16 المعدل والمتمم لقانون العقوبات (المطلب الأول).

¹ - أرحومة موسى مسعود، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، ورقة علمية مقدمة في فعاليات المؤتمر المغاربي في طبعته الأولى المعنون "المعلوماتية والقانون"، أكاديمية الدراسات العليا، المغرب، 28-2010/10/29، ص 03.

² - صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة مقدمة لنيل شهادة الماجستير في القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، الجزائر، السنة الجامعية 2012، ص 45.

³ - انظر: بن صغير عبد المومن، المرجع السابق، ص 11.

ونظرا لعدم كفاية النصوص العقابية العامة بسبب تطور أساليب ارتكاب الجرائم السيبرانية، استدعى الأمر المشرع إلى ضرورة سن تشريعات خاصة تتضمن آليات واستراتيجيات فعالة لمكافحة هذا النوع من الجرائم المستحدثة، وفي هذا الصدد لجأ المشرع الجزائري إلى صياغة نصوص قانونية خاصة تتمثل على وجه الخصوص في إقراره للقانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وكذا القانون رقم 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، وتهدف هذه القوانين في مجملها إلى تجريم كافة أشكال الاعتداء على حقوق الأفراد في البيئة المعلوماتية وتحقيق الأمن السيبراني ومكافحة الأنماط المختلفة للجريمة السيبرانية (المطالب الثاني)، وسيتم البحث بشيء من التفصيل في آليات مكافحة هذه الجرائم في المطالب الآتية:

المطلب الأول: آليات التدخل بالنصوص العقابية العامة لمكافحة الجرائم السيبرانية

تعتبر الجزائر من بين الدول التي تسير على نهج مكافحة الجريمة السيبرانية وقمعها، وذلك من خلال اعتماد أسلوب خاص لمكافحة هذه الجرائم التي خصص لها المشرع الجزائري قسم خاص في أحكام القانون رقم 14/05 المعدل والمتمم لقانون العقوبات، وقد ورد القسم السابع مكرر تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات" حيث يحتوي على عدة مواد مخصصة تجرم سلوك الاعتداء على الأنظمة المعلوماتية؛ والمتمثلة في كل الأفعال الماسة بنظم المعالجة الآلية للمعطيات وما يقابلها من جزاء وعقوبة.

وتتدرج هذه الأفعال تحت وصف الاعتداء على نظام المعالجة الآلية للمعطيات عن طريق الدخول أو البقاء غير المرخص في المنظومة بالإضافة إلى تغيير معطياتها وسير نظامها، كما يمكن أن تأخذ هذه الجرائم وصف الاعتداء على سير نظام المعالجة الآلية المستهدفة للدولة ولمؤسسات القطاع العام وكذا المرتكبة من طرف الأشخاص المعنويين، وفي الأخير كان لابد من تسليط الضوء على مساعي الجهات المختصة في مصادرة الوسائل المستخدمة في ارتكاب الجرائم السيبرانية فضلا عن توقيع العقاب على فعل الشروع في ارتكاب هذه الجرائم المرتكبة في البيئة الرقمية، وسيتم التفصيل في جميع هذه المسائل تباعا في النقاط الموالية:

أولاً: صور الاعتداء على منظومة المعالجة الآلية للمعطيات

لقد نصت المادة 394 مكرر من القانون رقم 15/04 المعدل والمتمم لقانون العقوبات على أن "يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك، تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة. وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة (6) أشهر إلى سنتين (2) والغرامة من 50.000 دج إلى 150.000 دج".

نلاحظ جليا من نص المادة المذكورة أنفا بأن المشرع الجزائري قد اعتبر فعل الدخول غير المرخص به إلى نظام المعالجة الآلية للمعطيات كله أو جزئه، وسواء تم هذه الدخول بقصد أو بغير قصد، فإنه يعد أساسا لقيام هذه الجريمة، أما فيما يتعلق بفعل البقاء غير المرخص فيقصد به عموما استمرارية التواجد داخل نظام المعالجة الآلية دون موافقة أو إذن أو الحصول على ترخيص من صاحب النظام، بمعنى آخر هو بقاء شخص داخل نظام المعالجة المملوك للغير بعد الدخول إليه عن طريق الخطأ أو الصدفة رغم علمه بأن بقاءه فيه غير مرخص¹، وعليه فإن العقوبة المقررة على مرتكبي هذه الأفعال الموصوفة بالدخول أو البقاء في نظام المعالجة الآلية للمعطيات تتمثل في فرض عقوبة الحبس المتراوح من ثلاثة أشهر إلى سنة، أما الغرامة المالية فتتراوح من 50.000 دج إلى 100.000 دج كأقصى حد.

وتجدر الإشارة إلى أنه في حالة ترتب عن الدخول أو البقاء نتائج غير مشروعة ضد معطيات النظام كحذفها أو تغييرها أو تخريب نظام اشتغال المنظومة تضاعف عقوبة الحبس من ستة أشهر إلى سنتين، أما الغرامة المالية فتضاعف من مبلغ 50.000 دج إلى 150.000 دج.

في حين أن المادة 394 مكرر 01 من نفس القانون نصت على أن "يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها"، ومن خلال نص المادة المذكورة نلاحظ جليا بأن المشرع الجزائري قد أقر بصفة صريحة توقيع العقاب المتمثل في الحبس والغرامة المالية على كل شخص قام بإحداث تغييرات في المنظومة عن طريق قيامه بالإدخال بطريق الغش معطيات في نظام المعالجة الآلية للمعطيات، أو القيام بإزالتها أو تعديلها عن طريق الغش المصحوب بسوء نية هذا المجرم السيبراني².

في حين أن المادة 394 مكرر 02 من نفس القانون قد نصت على أنه "يعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج، كل من يقوم عمدا أو عن طريق الغش بما يأتي:

1- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

¹ - عيمور راضية، الجريمة الالكترونية واليات مكافحتها في التشريع الجزائري، مقال منشور في المجلة الأكاديمية للبحوث القانونية والسياسية، جامعة عمار ثليجي الأغواط، الجزائر، المجلد 06، العدد 01، 2022، ص 100.

² - المادة 394 مكرر 01 من القانون رقم 15/04 المعدل والمتمم لقانون العقوبات، وانظر أيضا: قارة آمال، الحماية الجزائية للمعلوماتية في التشريع الجزائري، ط 2، دار هومة، الجزائر 2007، ص 44 وما يليها.

2- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم".

من خلال استقراءنا لنص المادة أعلاه نجد بأن المشرع الجزائري قد فرض عقوبات وغرامات مالية مشددة على كل شخص يقوم عن طريق العمد والغش بتصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلّة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في القسم الأول، فضلا عن حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان، المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.

ثانيا: العقوبات المقررة على الجرائم السيبرانية المستهدفة لمؤسسات القطاع العام والمرتبكة من طرف الأشخاص المعنويين

لقد أقرت المادة 394 مكرر 03 من رقم 15/04 المعدل والمتمم لقانون العقوبات على مضاعفة العقوبات المنصوص عليها في هذا القسم إذا كانت الجريمة الالكترونية أو السيبرانية تستهدف الدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام وذلك دون الإخلال بتطبيق عقوبات أشد إن اقتضى الأمر ذلك¹.

في حين أن المادة 394 مكرر 04 من القانون رقم 15/04 المعدل والمتمم لقانون العقوبات قد أقرت بصفة صريحة على تشديد المشرع الجزائري على معاقبة كل شخص معنوي يقوم بارتكاب هذه الجرائم -السيبرانية- وذلك بغرامة تعادل خمس (05) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي، كما جاء في نص المادة 394 مكرر 05 من نفس القانون على معاقبة كل من شارك في مجموعة أو قام بالاتفاق مع الجاني بغرض الإعداد للجريمة وكان الإعداد أو التحضير مجسدا بفعل أو عدة أفعال مادية وذلك بمعاقبته بنفس العقوبة المقررة للمجرم الأصلي².

ثالثا: مصادرة الوسائل المستخدمة في ارتكاب الجرائم الالكترونية وتوقيع العقاب على فعل الشروع في ارتكاب الجرائم السيبرانية والجرائم المتعلقة بإساءة استغلال تكنولوجيات الإعلام والاتصال وجرائم مقدمي خدمات الانترنت

لقد أقرت المادة 394 مكرر 06 من القانون رقم 15/04 المعدل والمتمم لقانون العقوبات على أنه مع الاحتفاظ بحق الغير حسن النية، يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها علاوة على إغلاق المحل أو مكان الاستغلال

¹ - انظر: المادة 394 مكرر 03 من القانون رقم 15/04 المعدل والمتمم لقانون العقوبات.

² - انظر: المادتين 394 مكرر 04 و 394 مكرر 05 من القانون رقم 15/04 المعدل والمتمم لقانون العقوبات.

إذا كانت الجريمة قد ارتكبت بعلم مالکها، وأخيراً أقرت المادة 394 مكرر 07 على معاقبة فعل الشروع في ارتكاب الجرح المنصوص عليها بالعقوبات المقررة للجنة¹.

وتجدر الإشارة أيضاً إلى أن القانون رقم 02/16 المعدل والمتمم لقانون العقوبات قد تضمن مادتين؛ هما 87 مكرر 12 المتعلقة باستخدام واستغلال تكنولوجيات الإعلام والاتصال لتجنيد الأشخاص لصالح إرهابي والتي قضت بأن "يعاقب بالسجن المؤقت من خمس (5) سنوات إلى عشر (10) سنوات وبغرامة من 100.000 دج إلى 500.000 دج كل من يستخدم تكنولوجيا الإعلام والاتصال لتجنيد الأشخاص لصالح إرهابي أو جمعية أو تنظيم أو جماعة أو منظمة يكون غرضها أو تقع أنشطتها تحت طائلة أحكام هذا القسم، أو ينظم شؤونها أو يدعم أعمالها أو أنشطتها أو ينشر أفكارها بصورة مباشرة أو غير مباشرة".

أما المادة 394 مكرر 08 من القانون رقم 02/16 قد نصت على جملة العقوبات الجزائية المفروضة على مقدم خدمات الانترنت²، وعلى وجه التحديد الغير مستجيب لأعدار الهيئات المختصة أو للأوامر والأحكام القضائية والتي تلزمه بسحب أو تخزين المحتويات التي يتيح الاطلاع عليها أو جعل الدخول إليها غير ممكن عندما تتضمن محتويات تشكل جرائم أو قيامه بمقدم الخدمات - بوضع ترتيبات تقنية تسمح بسحب أو تخزين المحتويات المتعلقة بالجرائم المرتكبة³.

حيث تقضي المادة المذكورة أعلاه بأنه "دون الإخلال بالعقوبات الإدارية المنصوص عليها في التشريع والتنظيم الساري المفعول، يعاقب بالحبس من سنة إلى ثلاث (3) سنوات وبغرامة من 2.000.000 دج إلى 10.000.000 دج، أو بإحدى هاتين العقوبتين فقط، مقدم خدمات "الانترنت" بمفهوم المادة 02 من القانون رقم 04/09 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الذي لا يقوم رغم إعداره من الهيئة المنصوص عليها في القانون أو صدور أمر أو حكم قضائي يلزمه بذلك: أ- بالتدخل الفوري لسحب أو تخزين المحتويات التي يتيح الاطلاع عليها أو جعل الدخول إليها غير ممكن عندما تتضمن محتويات تشكل جرائم منصوص عليها قانوناً. ب- بوضع

¹ - انظر: المادتين 394 مكرر 06 و 394 مكرر 07 من القانون رقم 15/04 المعدل والمتمم لقانون العقوبات.

² - لقد عرفت المادة 02 الفقرة (د) من القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها مقدمو الخدمات بأنهم "أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية و/ أو نظام للاتصالات، وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعملها".

³ - انظر: المادة 394 مكرر 08 من القانون رقم 02/16 المتضمن قانون العقوبات الجزائي المعدل والمتمم، وانظر أيضاً:

Touidjini Med Kamel Addine, la repense légale et judiciaire a la cybercriminalité, CERIST, Alger 2012, p 14.

ترتيبات تقنية تسمح بسحب أو تخزين المحتويات التي تتعلق بالجرائم المنصوص عليها في الفقرة (أ) من هذه المادة أو لجعل الدخول إليها غير ممكن¹.

وبناء على ما سبق ذكره ومن خلال استقراءنا للنصوص القانونية السالفة الذكر نتوصل إلى القول بأن استحداث المشرع الجزائري للنصوص التشريعية لمكافحة الجرائم السيبرانية ساهم بشكل جد فعال في الحد النسبي من انتشار الجرائم السيبرانية بصفة خاصة والمعلوماتية بصفة عامة، مما جعل منها بمثابة نصوص ردعية لمعاقبة مرتكبي هذه الجرائم فضلا عن الحد من انتشارها نوعا ما بسبب العقوبات المشددة على مرتكبي هذا النوع من الجرائم سواء كانوا فاعلين أصليين أم شركاء في ارتكاب الجريمة وسواء تم ارتكابها داخل حدود الدولة أو خارجها ففي كل الحالات يتم معاقبته على ارتكاب الفعل المجرّم المتمثل في ارتكاب الجريمة السيبرانية.

المطلب الثاني: الآليات والاستراتيجيات المقررة لمكافحة الجرائم السيبرانية وفقا لأحكام القوانين الخاصة
تتجلى آليات واستراتيجيات مكافحة الفعالة للجرائم السيبرانية المرتكبة عبر الوسائط الرقمية، من خلال سن ترسانة من النصوص القانونية الخاصة فضلا عن النصوص العقابية العامة التي يهدف المشرع الجزائري من خلالها إلى فرض الحماية الجنائية للأفراد والمؤسسات ذات الطابع العام والخاص من أي اعتداء على حقوقهم في هذا الفضاء السيبراني.

وعليه فإن القوانين الخاصة التي أقرها المشرع الجزائري لمكافحة الجرائم السيبرانية تتمثل بداية في فرض أحكام القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، فضلا عن مكافحتها من خلال تجريم الاعتداء على حقوق الأفراد في البيئة السيبرانية على ضوء أحكام القانون رقم 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، وفيما يلي سنوضح مضمون هذه الآليات والاستراتيجيات على النحو الآتي بيانه:

أولا: مكافحة الجرائم السيبرانية على ضوء أحكام القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

لقد استحدث المشرع الجزائري أحكام القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها بهدف الوقاية من الجرائم المعلوماتية والسيبرانية

¹ - لقد تضمنت أحكام المادة 02 من القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها -والتي تمت الإشارة إليها في المادة 394 مكرر 08 من القانون رقم 02/16 المعدل والمتمم لقانون العقوبات- تعريف مجموعة من المصطلحات والمتمثلة أساسا في تحديد المقصود بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وكذا المنظومة المعلوماتية، والمعطيات المعلوماتية، ومقدمي الخدمات، والمعطيات المتعلقة بحركة السير، وأخيرا الاتصالات الالكترونية.

التي تقع في الفضاء الافتراضي، حيث تتميز الأحكام الواردة في هذا القانون بأنها الإطار التشريعي الأكثر ملائمة مع خصوصية الجرائم السيبرانية المرتكبة في البيئة الرقمية أو الافتراضية، ومن خلال استقراءنا للنصوص الواردة فيه يظهر لنا جليا بأن المشرع الجزائري قد أقر مجموعة من التدابير الوقائية والإجرائية المستحدثة للوقائية من الجرائم السيبرانية ومكافحتها.

وفي هذا الصدد نصت أحكام المادة 04 من القانون رقم 04/09 السالف الذكر، على التدابير الوقائية من خلال تبيان الحالات المحددة التي يسمح فيها القيام بعمليات المراقبة الالكترونية من طرف الهيئات المختصة لتفادي وقوع أو ارتكاب الجرائم السيبرانية أو الكشف عنها وعن مرتكبيها في وقت مبكر؛ وتتمثل هذه الحالات في الوقاية من الأفعال الإرهابية أو التخريبية أو الجرائم الماسة بأمن الدولة، أو في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، أو لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى إجراء المراقبة الالكترونية، و يمكن الاستعانة بالمراقبة الالكترونية في إطار تنفيذ المساعدة القضائية الدولية المتبادلة. والجدير بالذكر أنه لا يمكن إجراء عمليات المراقبة الالكترونية في الحالات التي سبق الإشارة إليها إلا بموجب إذن مكتوب من السلطات القضائية المختصة، بحيث يختص النائب العام لدى مجلس قضاء الجزائر بمنح الإذن لضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها للقيام بإجراء المراقبة الالكترونية¹.

إضافة إلى التدابير الوقائية السالفة الذكر تبنى المشرع مجموعة من التدابير الإجرائية تهدف للوقاية من الجرائم السيبرانية ومكافحتها، حيث تتمثل على وجه الخصوص في تفتيش وحجز المنظومة المعلوماتية عن طريق السماح للجهات القضائية المختصة وكذا لضباط الشرطة القضائية بالدخول لغرض التفتيش والحجز ولو عن بعد للمنظومة المعلوماتية أو جزء منها والمعطيات المعلوماتية المخزنة فيها واستنساخها مع إمكانية تمديد التفتيش ليشمل المعطيات المخزنة في منظومة معلوماتية أخرى².

إضافة إلى التدابير المتعلقة بتمديد الاختصاص بنظر هذه الجرائم، يؤول الاختصاص للمحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني، في حالة ارتكاب الجريمة من أجنبي وكانت الجريمة تستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني، فضلا عن إمكانية تبادل المساعدة القضائية الدولية فقد سمح

¹ - للمزيد من التفصيل ينظر: المادة 13 من القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

² - انظر: المادة 03 من القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

المشرع الجزائري بإمكانية تبادل المساعدة القضائية الدولية لجمع الأدلة المتعلقة بالجريمة في شكلها الإلكتروني، مع إمكانية الاستجابة لطلبات المساعدة الرامية إلى تبادل المعلومات أو اتخاذ أي إجراءات تحفظية وذلك طبقا لما تقضي به نصوص الاتفاقيات الدولية ومبدأ المعاملة بالمثل.

أما التدبير الإجرائي الأخير فيتمثل في إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته بموجب أحكام المرسوم الرئاسي الساري المفعول رقم 439/21 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها¹، ففي هذا الصدد أوضحت المادة 14 من هذا القانون مهام هذه الهيئة والمتمثلة في القيام بالتنسيق وتنسيق عمليات الوقاية من الجرائم السيبرانية المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، فضلا عن مساعدة الجهات القضائية المختصة ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية، وأخيرا تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي هذه الجرائم وتحديد مكان تواجدهم بدقة².

ثانيا: مكافحة الجرائم السيبرانية على ضوء أحكام القانون رقم 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي

لقد استحدث المشرع الجزائري بموجب أحكام القانون رقم 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي، مجموعة من الآليات والمتمثلة أساسا في:

¹ - لقد استحدث المشرع الجزائري الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته في الفصل الخامس من أحكام القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ويتضمن هذا الفصل مادتين هما 13 و14؛ حيث حددت أحكام المادة 13 منه إنشاء الهيئة كما أوضحت المادة منه 14 مهامها، أما فيما يتعلق بتشكيلتها وتنظيمها وكيفية سيرها فقد تم تحديدها عن طريق التنظيم، وذلك بموجب أحكام المرسوم الرئاسي رقم 183/20 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية عدد 40، المؤرخة في 18 جويلية 2020، ثم المرسوم الرئاسي رقم 439/21 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية عدد 86، المؤرخة في 11 نوفمبر 2021، ويعد هذا الأخير -المرسوم الرئاسي رقم 439/21- بمثابة الإطار القانوني المنظم لهذه الهيئة والتي عرفها بأنها عبارة عن سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلالية المالية توضع تحت سلطة رئيس الجمهورية، ويحدد مقرها في الجزائر العاصمة ويمكن نقله إلى أي مكان من التراب الوطني بموجب مرسوم رئاسي.

² - انظر: المادة 14 من القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

أ- استحداث سلطة وطنية لحماية المعطيات ذات الطابع الشخصي بالإضافة إلى وضع مجموعة من الالتزامات الملقاة على عاتق المسؤول عن المعالجة الآلية للمعطيات ذات الطابع الشخصي¹.

ب- اتخاذ السلطة الوطنية مجموعة من الإجراءات ذات الطابع الإداري في حالة خرق أحكام القانون من طرف المسؤول عن المعالجة كما يمكن لهذه السلطة أيضا القيام بالتحريات ومعاينة المحلات والأماكن التي تتم فيها المعالجة باستثناء محلات السكن، كما يمكنها الولوج إلى المعطيات المعالجة وجميع المعلومات والوثائق أيا كانت دعامتها، والجدير بالذكر أنه لا يعتد أمام السلطة الوطنية بالسر المهني².

ت- تنص المادة 52 من القانون رقم 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي على أنه "يمكن لكل شخص يدعي أنه تم المساس بحق من حقوقه المنصوص عليها في هذا القانون، أن يطلب من الجهة القضائية المختصة اتخاذ أي إجراءات تحفظية لوضع حد لهذا التعدي أو للحصول على تعويض"، فمن خلال نص المادة المذكورة نرى بأن أحكام هذا القانون قد فرضت آليات قانونية وإجرائية لحماية حقوق الأشخاص الطبيعيين في البيئة الرقمية.

ث- تأهيل أعوان الرقابة للقيام ببحث ومعاينة الجرائم المتعلقة بالمعطيات ذات الطابع الشخصي تحت إشراف وكيل الجمهورية³، كما تختص الجهة القضائية الجزائية أيضا بمتابعة هذه الجرائم التي ترتكب خارج إقليم الجمهورية من طرف مواطن جزائري أو شخص أجنبي مقيم في الجزائر أو أي شخص معنوي خاضع للقانون الجزائري، كما تختص بمتابعة الجرائم المنصوص عليها في هذا القانون وفقا لقواعد الاختصاص المنصوص عليها في أحكام المادة 588 من قانون الإجراءات الجزائية⁴.

ج- جرّم المشرع الجزائري بموجب أحكام القانون رقم 07/18 السالف الذكر كافة أشكال الاعتداء على المعطيات ذات الطابع الشخصي عن طريق استحداثه للفصل الثالث المعنون بالأحكام الجزائية، وبموجب هذه الأحكام أقر عقوبة الحبس والغرامة؛ حيث تتمثل عقوبة الحبس السالبة للحرية في فرض

¹ - تم استحداث السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي في الباب الثالث وعلى وجه التحديد المواد من 22 إلى 31 من القانون رقم 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي، الجريدة الرسمية عدد 34، المؤرخة في 10 جوان 2018؛ وقد تضمنت الأحكام الواردة في هذا الباب إنشاء السلطة الوطنية وتشكيلها وكيفية أداء أعضائها لليمين، ومهامها وواجبها حفاظها على الطابع السري للمعطيات ذات الطابع الشخصي وغيرها من التعليمات التي تخص تنظيمها وسيرها.

² - لمزيد من التفصيل ينظر: المادة 49 من القانون رقم 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي.

³ - لمزيد من التفصيل ينظر: المادة 50 من القانون رقم 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي.

⁴ - المادة 53 من القانون رقم 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي.

عقوبة الحبس المتراوح من شهرين (2) كأدنى حد إلى خمس (5) سنوات كأقصى حد، أما العقوبات المالية فتتراوح ما بين 60.000 دج كأدنى حد و 1.000.000 دج كأقصى حد، كما يمكن فرض إحدى هاتين العقوبتين¹.

خاتمة:

في ختام هذه الدراسة يظهر لنا جليا بأن موضوع التأصيل القانوني للجريمة السيبرانية المرتكبة في عبر الوسائط الرقمية، يتوقف على تحديد الأحكام المنظمة لها وكذا معايير قيامها ومدى اعتبارها كتهديد قانوني يمس بمبدأ استقرار الأمن السيبراني، وهو الأمر الذي استدعى المشرع الجزائري لإبداء موقفه منها عن طريق التصدي لهذه الظاهرة ومكافحتها بموجب النصوص التشريعية الخاصة ذات الطابع العقابي، والواردة على وجه الخصوص في أحكام القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وفي القانون رقم 15/04 المعدل والمتمم لقانون العقوبات، وقد توصلنا بهذا الخصوص إلى جملة من النتائج نردها فيما يلي:

1- تعتبر الجريمة السيبرانية من بين الجرائم المستحدثة التي ظهرت في بواخر القرن العشرين لأن وجودها يرتبط أساسا بوجود نظام معلوماتي، وتُرتكب هذه الجريمة من طرف مجرم متميز يملك دراية كافية بطريقة عمل وتسيير النظام المعلوماتي واستغلاله في القيام بأعمال غير مشروعة، إما لدوافع شخصية يكون الغرض منها غالبا الحصول على معلومات لتحقيق مكاسب مادية، أو تغيير وتعديل برامج النظام المعلوماتي أو حذفها لإحداث أضرار للأفراد أو المؤسسات الخاصة، أو المؤسسات العامة المتمثلة في مؤسسات الدفاع الوطني للدولة الجزائرية.

2- تتجلى معالم التهديدات القانونية المميزة لقيام الجريمة السيبرانية المرتكبة عبر الوسائط الرقمية من خلال إبراز العلاقة التي تربط المنظومة القانونية بالنظم المعلوماتية، حيث ظهرت الضوابط القانونية التي تعمل على الحد من قيام هذه الجريمة الناعمة في مجال تكنولوجيا المعلومات والمتميزة بصعوبة إثباتها في النظام المعلوماتي، فضلا على عدم القدرة على حصرها ضمن حدود معينة فهي جريمة عابرة للحدود، خاصة بعد أن أصبح استخدام الوسائل المعلوماتية ضرورة لا غنى عنها لدى الأفراد والشركات والمؤسسات ومختلف أجهزة الدولة سواء في الجزائر أو في كافة أنحاء العالم.

3- نظرا لخصوصية الجريمة السيبرانية، وسّع المشرع الجزائري من مجال الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، بإدراجها في القسم السابع من الفصل الثالث من قانون العقوبات والمعنون بقواعد "المساس بأنظمة المعالجة الآلية للمعطيات"، حيث حدد كل الأفعال الماسة بنظم المعالجة الآلية

¹ - لمزيد من التفصيل حول العقوبات المقررة مرتكبي جرائم الاعتداء على المعطيات ذات الطابع الشخصي: ينظر الفصل الثالث وعلى وجه التحديد المواد من 54 إلى 74 من القانون رقم 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي.

للمعطيات وما يقابلها من عقوبات مقررة على مرتكبيها، وتأخذ هذه الأفعال إما وصف الاعتداء على نظام المعالجة الآلية أو وصف الاعتداء على معطيات نظام المعالجة الآلية للمعطيات، كما يمكن لها أن تأخذ أيضا وصف الاعتداء على سير نظام المعالجة الآلية للمعطيات، ومكافحتها تكون بتوقيع أشد العقوبات المالية والسالبة للحرية على مرتكبيها وشركائهم إن وجدوا.

4- تكمن آليات واستراتيجيات الجرائم السيبرانية في توقيع الجزاء المقرر في التشريعات العقابية، فهذه النصوص التشريعية من شأنها أن تواكب التحديات الناتجة عن التطور الهائل للتكنولوجيات الحديثة في مجال النظم المعلوماتية وجعلها أكثر تجاوبا مع الطبيعة الخاصة للجريمة السيبرانية المرتكبة في النظام المعلوماتي وهذا التنوع التشريعي الوارد في أحكام قانون العقوبات في المواد من 394 مكرر إلى 394 مكرر 07 من شأنه أن يساهم بشكل فعال على الأقل في الوقت الراهن في الحد من تفاقم ظاهرة الجرائم الالكترونية أو السيبرانية في الدولة الجزائرية.

5- استحداث المشرع الجزائري لقوانين خاصة أكثر تجاوبا مع طبيعة الجرائم السيبرانية حيث تتضمن مجموعة من التدابير الفعالة لمكافحة الجرائم السيبرانية والحد من تفاقمها في الدولة الجزائرية، وتتمثل هذه القوانين على وجه الخصوص في القانون رقم 15/04 المعدل والمتمم لقانون العقوبات، وكذا القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

ومن خلال النتائج المتوصل إليها في دراستنا لموضوع التأصيل القانوني للجرائم السيبرانية المرتكبة عبر الوسائط الرقمية، نعترف حقيقةً بالجهود الجبارة التي يبذلها المشرع الجزائري في سبيل مكافحته للجرائم السيبرانية المرتكبة في النظام المعلوماتي أو الرقمي، إلا أنها غير كافية لبلوغ الهدف الذي يتطلع إليه، ولعل السبب الرئيسي في ذلك يرجع إلى الطبيعة الخاصة لهذه الجريمة باعتبار أنها تتطور تماشيا مع التطور الهائل الذي يشهده نظام تكنولوجيا الإعلام والاتصال في وقتنا الحاضر أو حتى المستقبلي، وعليه نرى أنه من المفيد تقديم جملة من المقترحات العلمية والعملية تتمثل في:

1- استحداث مشروع قانون خاص أو منظومة قانونية خاصة تعنى بدراسة مفاهيم الجرائم السيبرانية ونطاق تطبيقها وجميع السبل الواردة لمكافحتها بغية تحقيق الأمن السيبراني، وتعديل هذه المنظومة بصفة دورية من طرف لجان تتضمن رجال قانون وهيئات متخصصة في البرمجة والنظم المعلوماتية لتقييم هذه اللجنة ماهية ومدى فعالية العقوبات المقررة على الجرائم المرتكبة في برامج النظام المعلوماتي، خاصة في ظل التطورات السريعة والمستمرة التي تعرفها ظاهرة الجريمة السيبرانية المرتكبة في النظام المعلوماتي هذا من جهة.

2- ومن جهة أخرى الأخذ بعين الاعتبار خصوصية الجريمة السيبرانية باعتبارها جريمة ذات طبيعة ديناميكية تتطور أساليب وكيفيات ارتكابها بصفة دورية تماشيا مع تطور استخدام تكنولوجيا المعلومات والاتصالات، لذلك لابد من التفكير في التوجه بالاستعانة والاستفادة من خبرات الدول المتقدمة

في مجال مكافحة هذه الجرائم عن طريق البحث والتحري وجمع الأدلة للكشف عن مرتكبي الجرائم المتصلة بتكنولوجية الإعلام والاتصال واتخاذ مختلف التدابير الاحترازية لمكافحتها وذلك في إطار الاتفاقيات والمعاهدات الدولية.

قائمة المصادر والمراجع:

باللغة العربية

أولاً: المصادر

1- القرآن الكريم:

✓ سورة الأعراف.

2- المعاجم اللغوية:

✓ ابن منظور محمد بن مكرم بن علي أبو الفضل جمال الدين جمال الدين الأنصاري الرويفعي الإفريقي، لسان العرب، المجلد الثاني، طبعة صادر، دار صادر، بيروت.

3- المراسيم الرئاسية:

✓ المرسوم الرئاسي رقم 439/21 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية عدد 86، المؤرخة في 11 نوفمبر 2021.

✓ المرسوم الرئاسي رقم 183/20 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية عدد 40، المؤرخة في 18 جويلية 2020.

4- القوانين:

✓ القانون رقم 02/16 المتضمن قانون العقوبات الجزائري المعدل والمتمم للأمر رقم 156/66، الجريدة الرسمية عدد 37، المؤرخة في 22 جوان 2016.

✓ القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية عدد 47، المؤرخة في 05 أوت 2009.

✓ القانون رقم 15/04 المتضمن قانون العقوبات الجزائري المعدل والمتمم للأمر رقم 156/66، الجريدة الرسمية عدد 71، المؤرخة في 10 نوفمبر 2004.

✓ القانون رقم 23/06 المتضمن قانون العقوبات الجزائري المعدل والمتمم للأمر رقم 156/66، الجريدة الرسمية عدد 84، المؤرخة في 24 ديسمبر 2006.

✓ القانون رقم 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي، الجريدة الرسمية عدد 34، المؤرخة في 10 جوان 2018.

ثانياً: المراجع

1- الكتب:

✓ أبو شامة عباس عبد المحمود، عولمة الجريمة الاقتصادية، ط 01، جامعة نايف العربية للعلوم الأمنية، الرياض، 2007.

✓ الإمام محمد أبو زهرة، الجريمة والعقوبة في الفقه الإسلامي -العقوبة-، دار الفكر العربي، الإسكندرية، 2008.

✓ طلال أبو عفيفه، أصول علمي الإجرام والعقاب وآخر الجهود الدولية والعربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية، ط 1، دار الجندي للنشر والتوزيع، فلسطين 2013.

- ✓ غادة نصار، الإرهاب والجريمة الالكترونية، ط 1، العربي للنشر والتوزيع، القاهرة 2017.
- ✓ الفتلاوي عبيس نعمة، الهجمات السيبرانية: دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، ط 1، منشورات زين الحقوقية، بيروت 2018.
- ✓ قارة آمال، الحماية الجزائية للمعلوماتية في التشريع الجزائري، ط 2، دار هومة، الجزائر 2007.
- ✓ قنديلجي عامر إبراهيم، الحكومة الالكترونية، ط 1، دار المسيرة، الأردن 2015.
- ✓ الكعبي محمد عبيد، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت، ط 2، دار النهضة العربية، القاهرة 2009.

2- المقالات العلمية:

- ✓ بدوي عبد المحسن محمد، الجرائم المعلوماتية، مقال منشور في مجلة الأمن والحياة، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية، المجلد 29، العدد 335، 2010.
- ✓ جاب الله حكيمة، انعكاسات الجريمة السيبرانية على البيئة الرقمية: دراسة في آليات واستراتيجيات مكافحتها، مقال منشور في مجلة حوليات جامعة الجزائر 1، جامعة الجزائر 01 بن يوسف بن خدة، الجزائر، المجلد 35، العدد 03، 2021.
- ✓ طالة لامية، التهديدات والجرائم السيبرانية: تأثيرها على الأمن القومي للدول واستراتيجيات مكافحتها، مقال منشور في مجلة معالم للدراسات القانونية والسياسية، المركز الجامعي تندوف، الجزائر، المجلد 04، العدد 02، 2020.
- ✓ عباوة نجا، الإشكالات القانونية في تجريم الاعتداء على أنظمة المعلومات، مجلة دفاتر السياسة والقانون، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، العدد 16، 2017.
- ✓ عيمور راضية، الجريمة الالكترونية واليات مكافحتها في التشريع الجزائري، مقال منشور في المجلة الأكاديمية للبحوث القانونية والسياسية، جامعة عمار ثلجي الأغواط، الجزائر، المجلد 06، العدد 01، 2022.

3- الرسائل العلمية:

- ✓ صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة مقدمة لنيل شهادة الماجستير في القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، الجزائر، السنة الجامعية 2012.

4- المداخلات العلمية:

- ✓ أرحومة موسى مسعود، الإشكاليات الإجرائية التي تنثيرها الجريمة المعلوماتية عبر الوطنية، ورقة علمية مقدمة في فعاليات المؤتمر المغربي في طبعته الأولى المعنون "المعلوماتية والقانون"، أكاديمية الدراسات العليا، المغرب، 28-2010/10/29.
- ✓ البداينة ذياب موسى، الجرائم الإلكترونية: المفهوم والأسباب، ورقة علمية مقدمة في فعاليات الملتقى العلمي المعنون "الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية"، كلية العلوم الإستراتيجية، جامعة الأردن، 2-2014/09/4.
- ✓ بن صغير عبد المومن، الطبيعة الخاصة للجريمة المرتكبة عبر الانترنت في التشريع الجزائري والتشريع المقارن، ورقة علمية مقدمة في فعاليات الملتقى الوطني المعنون الجريمة المعلوماتية بين الوقاية والمكافحة"، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر، 16-2015/11/17.
- ✓ بن مرزوق عنترة وحرشاي محي الدين، الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية، ورقة علمية مقدمة في فعاليات المؤتمر الدولي المعنون "استراتيجيات الدفاع الوطني"، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، الجزائر 2017.

✓ نمديلي رحيمة، خصوصية الجريمة الالكترونية في القانون الجزائري والقانون المقارن، ورقة علمية مقدمة في فعاليات المؤتمر الدولي الرابع عشر المعنون "الجرائم الالكترونية"، مركز جيل البحث العلمي، لبنان، 24-25/03/2017.
باللغة الأجنبية:

1- Les Ouvrages:

- ✓ Romain Beas, La lutte contre la cybercriminalité au regard de l'action des états, doctorat de droit privé et sciences criminelles, université de lorraine, Faculté de droit, Paris, 2016.
- ✓ Toudjini Med Kamel Addine, la repense légale et judiciaire a la cybercriminalité, CERIST, Alger 2012.