

الجريمة الإلكترونية وآليات التصدي لها في القانون الجزائري *Cybercrime and mechanisms to address it in Algerian law*

د. قيرة سعاد

د. سي حمدي عبد المومن*

جامعة محمد البشير الإبراهيمي برج

جامعة محمد البشير الإبراهيمي برج

بوعرييج الجزائر

بوعرييج الجزائر

souad.g123@gmail.com

Abdelmoumene.sihamdi@univ-bba.dz

تاريخ النشر: 2022 / 06 / 15

تاريخ القبول: 2022 / 05 / 08

تاريخ الاستلام: 2022 / 04 / 27

ملخص:

لقد أدت التطور التكنولوجي والثورة التكنولوجية إلى ظهور مجموعة من الأفعال والتصرفات التي مست بالحياة الخاصة للأفراد، وكذلك الإضرار ببرامج الحواسيب وبأنظمتها المعلوماتية، مما جعل ضرورة ملحة على وضع آليات قانونية تجرم مثل هذه الجرائم التي ترتبط بالوسائل الإلكترونية وأهمها الحاسوب. والجزائر مثلها مثل جميع دول العالم أصبحت تعاني من استفحال الجرائم الإلكترونية بكل أنواعها في المجتمع الجزائري والتي باتت تهدد أمن المجتمعات وذلك لخطورتها وخاصة أنها جرائم عابرة للحدود، ولهذا سارع المشرع الجزائري إلى وضع مجموعة من الآليات القانونية للوقاية من الجرائم الإلكترونية

الكلمات المفتاحية: الجريمة الإلكترونية، القرصنة، الأمن المعلوماتي، البيانات الشخصية.

Abstract:

Technological development and the technological revolution have led to the emergence of a set of actions and behaviors that affected the private lives of individuals, as well as harming computer programs and their information systems, which made an urgent need to establish legal mechanisms that criminalize such crimes that are related to electronic means, the most important of which is the computer. Algeria, like all countries of the world, is suffering from the spread of cybercrime of all kinds in Algerian society, which threatens the security of societies due to its seriousness, especially as it is cross-border crimes, and this is why the Algerian legislator hastened to develop a set of legal mechanisms to prevent cybercrime

Keywords: cybercrime, hacking, information security, personal data

مقدمة:

إن استخدام الوسائل الإلكترونية في عصر الرقمنة أدى إلى انتشار ظواهر تشكل تهديدات للمصالح الخاصة للأفراد سواء في انتهاك سرية الحياة الخاصة أو سرية المراسلات أو حتى المساس بالمصالح العامة للدولة، كاختراق أو مسح أو حذف البيانات والمعطيات الإلكترونية، وغيرها من الأفعال المجرمة التي تنطوي تحت تسمية الجرائم الإلكترونية.

وهذا ما دفع بالتشريعات الدولية بوضع نصوص قانونية للحد من الجرائم الإلكترونية على غرار المشرع الجزائري الذي شرع الكثير من القوانين الخاصة بالمعاملات الإلكترونية، وكذا تعديل بعض القوانين مثل قانون العقوبات، وهذا كله من أجل الحد من هذه الجرائم المستحدثة ولخصوصيتها وخطورتها على المجتمعات وكذا مؤسسات الدولة ومصالحها.

وتكمن أهمية الدراسة في ارتباط الجريمة الإلكترونية بحياة الأفراد والمؤسسات، خاصة في ظل صعوبة تطبيق النصوص التقليدية على هذه الجرائم، كل هذا شكل موضوعاً هاماً ذا أولوية يقع في جوهر النشاط المعرفي الإنساني، لتأتي هذه الدراسة كجزء لا يتجزأ من هذا الاهتمام.

وبناء على ما تم التطرق إليه يمكن بلورة إشكالية دراستنا في: ما مدي فعالية القوانين الجزائرية في مكافحة الجريمة المعلوماتية والحد منها؟

وللإجابة على إشكالية الدراسة قمنا بتقسيمها إلى مبحثين الأول يتضمن مفهوم الجريمة الإلكترونية أما

المحور الثاني فيتعلق بأهم الآليات القانونية لمكافحة الجريمة الإلكترونية .

المبحث الأول: مفهوم الجريمة الإلكترونية

أصبحت الجريمة الإلكترونية موضوعاً واسعاً، ورغم صعوبة إيجاد تعريف جامعاً مانعاً لها إلا أن اجتهاد كل من الفقهاء والباحثين أدى إلى تحديد عدة تعريفات لها وغن كانت قد تباينت تبعاً لمحل اهتمام كل فئة، منهم من عرفها بالمفهوم الواسع منهم من عرفها بالمفهوم الضيق ومن خلال تعريف الجريمة الإلكترونية نستخلص خصائصها وعليه سوف نقوم في هذا المحور بتحديد مفهوم الجرائم الإلكترونية، من حيث تعريفها وتحديد خصائص الجريمة الإلكترونية.

المطلب الأول: تعريف الجريمة الإلكترونية

بداية يجب أن نشير إلى أنه لا يوجد مصطلح قانوني موحد للدلالة على الجرائم الناشئة عن استغلال تقنية المعلومات واستخدامها ففي هذا الإطار أثر المشرع الانجليزي في قانون إساءة استخدام الحاسوب عام 1990 عدم وضع تعريف محدد لجرائم الحاسوب بغية عدم حصر القاعدة التجريبية في إطار أفعال معينة تحسباً للتطور العلمي والتقني في المستقبل.

في إطار تعريف الفقه للجريمة الالكترونية نجد أن الاتجاهات تباينت في هذا السياق فمنهم من أخذ بالمفهوم الواسع للجريمة المعلوماتية ومنهم من أخذ بالمفهوم الضيق لها، ومن التعريفات التي وضعها أنصار الاتجاه الضيق هي أن الجريمة الإلكترونية "كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازماً لارتكابه من ناحية لملاحقته وتحقيقه من ناحية أخرى"¹.

وفي نفس السياق يرى الأستاذ Tredman أن "الجريمة الالكترونية تشمل أي جريمة ضد المال مرتبطة بالاستخدام المعالجة الآلية للمعلومات"

ويرى الأستاذ Mass أن المقصود بالجريمة الالكترونية: "الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح.

نلاحظ أن هذه التعريفات ضيققت من مفهوم الجريمة الالكترونية إذ يخرج من نطاقها العديد من الأفعال غير المشروعة يستخدم الحاسب كأداة لارتكابها.²

يمكننا القول أن الجرائم الالكترونية هو كل فعل وكل سلوك غير مشروع أو غير أخلاقي أو غير مسموح به صادر عن إرادة جنائية يقوم به شخص ما لديه دراية ومعرفة بتكنولوجيا المعلومات المختلفة (تكنولوجيا التخزين والاسترجاع وتكنولوجيا الاتصالات الحديثة) ويوجه ضد المصلحة العامة والخاصة عبر وسط الكتروني.³ أما أنصار الاتجاه المفهوم الواسع عرف الجريمة الإلكترونية على أنها "كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات" أو هي "أي نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كان مرتبطاً بتقنية المعلومات".

كما عرف مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبه المجرمين المنعقد في فيينا سنة 2000 فقد عرف الجريمة الإلكترونية بأنها: "أية جريمة يمكن ارتكابها بواسطة نظام حاسوب أو شبكة حاسوبية والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية"⁴.

أما المشرع الجزائري لم يقيم بتعريف الجريمة الإلكترونية رغم كل التشريعات وإنما تبني للدلالة على الجريمة مصطلح المساس بأنظمة المعالجة الآلية للمعطيات معتبرا أن النظام المعلوماتي في حد ذاته وما يحتويه من مكونات غير مادية محلاً للجريمة ويمثل نظام المعالجة الآلية للمعطيات الشرط الأول الذي لابد من تحققه حتى يمكن توافر أركان الجريمة، وحسب قانون العقوبات لا نجد تعريفاً للجريمة الإلكترونية بل اكتفى المشرع بذكر الأفعال المجرمة والعقوبات تحت عنوان "الجرائم الماسة بنظام المعالجة الآلية للمعطيات"⁵.

المطلب الثاني: خصائص الجريمة الإلكترونية

تتميز الجريمة الإلكترونية بعدة خصائص أهمها:

- الجريمة الالكترونية جريمة عابرة للحدود:

تتميز الجرائم الإلكترونية بطابعها الدولي وذلك لأن الطابع العالمي لشبكة الانترنت وما يرتبه من جعل معظم دول العالم في حالة اتصال دائم على الخط On Line ، فالجريمة الالكترونية لا تعترف بالحدود بين الدول والقارات فهي تعتبر شكل جديداً من أشكال الجرائم العابرة للحدود الإقليمية بين دول العالم كافة، إذ يمكن ومن

خلال النظام المعلوماتي ارتكاب العديد من الجرائم مثل: جرائم التعدي على قواعد البيانات، وتزوير وإتلاف المستندات الإلكترونية، الاحتيال المعلوماتي، وسرقة بطاقات الائتمان، القرصنة، وغسيل الأموال.

- صعوبة إثبات الجريمة الإلكترونية

فالجرائم المعلوماتية تتصف بالخفاء، أي عدم وجود آثار مادية يمكن متابعتها، وهي خطيرة وصعبة الاكتشاف أو هي صعبة في تحديد مكان وقوعها ومكان التعامل معها بسبب اتساع نطاقها المكاني وضخامة البيانات، وترجع صعوبة إثبات الجريمة الإلكترونية إلى عدة أمور أهمها:⁶

- تقع في بيئة الكترونية يتم فيها نقل المعلومات وتداولها بالنبضات الإلكترونية غير المرئية وبدون مستندات ورقية ولا تترك آثار مادية.

- صعوبة الاحتفاظ الفني بدليل الجريمة المعلوماتية.

- تحتاج إلى خبرة فنية والذكاء في ارتكابها، ويصعب على المحقق التقليدي التعامل معها.

- تعتمد على الخداع في ارتكابها والتضليل في التعرف على مرتكبها، وما يساعد من ازدياد عدم التعرف على مرتكبي الجرائم الإلكترونية إحجام البنوك والشركات ومؤسسات الأعمال عن الإبلاغ عما يرتكب من جرائم معلوماتية تجنباً للإساءة لسمعتها وهز ثقة العملاء فيها، وكذلك إخفاء أسلوب ارتكاب الجريمة خوفاً من قيام آخرين بتقليد هذا الأسلوب.

- عدم وجود مفهوم مشترك للجريمة المعلوماتية

من خصائص الجريمة الإلكترونية عدم وجود مفهوم مشترك لماهية الجريمة الإلكترونية، وكذلك عدم وجود تعريف قانوني موحد لها ولعل السبب في ذلك يرجع إلى عدم وجود تنسيق دولي في مجال الجريمة المعلوماتية، ويرجع ذلك إلى عدم وجود معاهدات دولية ثنائية أو جماعية لمواجهة الجريمة الإلكترونية، أو لاختلاف مفهوم الجريمة تبعاً لاختلاف النظم القانونية.

- وقوع الجريمة المعلوماتية أثناء المعالجة الآلية للبيانات:

ويمثل هذا الشرط الأساسي الذي يتعين توافره حتى يمكن البحث في قيام أو عدم قيام أركان الجريمة الإلكترونية الخاصة بالتعدي على نظام معالجة البيانات، ذلك أنه في حالة تخلف هذا الشرط تنتفي الجريمة الإلكترونية.

والجريمة الإلكترونية قد تقع أثناء عملية المعالجة الآلية للبيانات في أي مرحلة من المراحل الأساسية لتشغيل نظام المعالجة الآلي للبيانات سواء عند مرحلة إدخال البيانات، أو أثناء مرحلة المعالجة، أو أثناء مرحلة إخراج المعلومات.⁷

- قلة الإبلاغ عن وقوع الجريمة الإلكترونية

في الغالب نجد أن الأشخاص (الضحايا) أو المجني عليهم يمتنعون عن تبليغ السلطات المختصة وذلك خوفاً على سمعتهم ومكانتهم في المجتمع، وعدم اهتزاز الثقة في كفاءته خاصة إذا كيان أو هيئة معينة، وهذا ما يجعل الكثير من المجرمين يفلتون من العقاب مما يؤدي إلى تفاقم الوضع داخل المجتمع.

- الجريمة الالكترونية جريمة مستحدثة

تعتبر الجرائم الالكترونية -سواء التي تتعرض لها أجهزة الكمبيوتر أو التي تسخر تلك الأجهزة في ارتكابها- من الجرائم المستحدثة، فعلى الرغم من المزايا والمنافع الايجابية المترتبة على العولمة وثورة المجتمع الالكتروني، إلا أنها ساعدت على ظهور وتعزيز أنواع جديدة من الجرائم، من أبرزها جرائم غسيل الأموال، اختراق قطاع الأعمال سرقة الملكيات الفكرية... الخ

- جرائم ناعمة:

تتميز الجريمة الإلكترونية عن الجرائم التقليدية في أنها لا تحتاج إلى أدنى جهد عضلي في إرتكابها، بل تعتمد على المجهود الذهني المحكم، والتفكير العلمي المدروس القائم على معرفة تقنية ممتازة بالحاسب الآلي، والتعامل السليم بالشبكة على أساس أن الجاني في الجرائم الإلكترونية هو إنسان متوافق مع المجتمع ولكنه يقترب هذا النوع من الجرائم بدافع اللهو أو لمجرد إظهار تفوقه على آلة الكمبيوتر أو على البرامج التي يشتغل بها، وأكد لتحقيق مصلحة ما.⁸

- عدم كفاية التعاون الدولي في مجال الجرائم الالكترونية

عدم وجود معاهدات دولية كافية للتسليم أو للمعاونة الثنائية أو الجماعية بين الدول تسمح بالتعاون الدولي، أو عدم كفايتها إن كانت موجودة لمواجهة المتطلبات الخاصة لجرائم الكمبيوتر ودينامية التحريات فيها وكفالة السرعة بها.⁹

المبحث الثاني: الآليات القانونية لمكافحة الجريمة الإلكترونية

لقد وضع المشرع الجزائري عدة آليات تشريعية لمكافحة الجرائم الإلكترونية والحد منها وذلك من خلال إضفاء تعديلات على قانون العقوبات بموجب القانون رقم 15/04 في قسم تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات" وحصرها في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، ولكن هذا التعديل لم يكن كافي لمواجهة الجريمة الإلكترونية ولهذا تم إصدار ترسانة من القوانين للحد منها

المطلب الأول: قانون العقوبات

قام المشرع الجزائري بتعديل قانون العقوبات بموجب القانون رقم 15/04¹⁰ من أجل تجريم الأفعال الماسة بأنظمة الحاسب الآلي، وذلك نتيجة تأثره بما أفرزته الثورة المعلوماتية من أشكال جديدة من الإجرام، حيث جاء التعديل في المواد 394 مكرر إلى المادة 394 مكرر 7، تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات".

ومن خلال استقراء نص المادة يتضح لنا أن المشرع الجزائري قسم الجرائم الإلكترونية إلى أربع فئات تتعدد بحسب المصالح المحمية التي تتمثل اساسا في سرية هذه المعطيات

كما أضاف المشرع الجزائري في سنة 2006 تعديلات جديدة مست القسم السابع مكرر منه، وجاء هذا التعديل لتشديد العقوبة المقررة لهذه الجرائم دون المساس بنص المواد في هذا القسم، وجاء هذا التعديل لزيادة الوعي بخطورة مثل هذه الجرائم المستحدثة، باعتبارها تؤثر على الاقتصاد الوطني وبمؤسسات الدولة بالدرجة

الأولى وشيوع ارتكابها ليس فقط من الطبقة المثقفة بل من قبل جميع الفئات وبمختلف الأعمار وذلك لتبسيط وسائل التكنولوجيا المعلومات وانتشار الانترنت كوسيلة لنقل وتبادل المعلومات.

وتمثل الجرائم التي نصت عليه التعديلات في قانون العقوبات في ما يلي:

- **جريمتا الدخول والبقاء غير مصرح بهما:** حيث نصت المادة 394 مكرر من قانون العقوبات على ما يلي: "يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة مالية من 50000 دج إلى 100000 دج كل من يدخل أو يبقى عن طريق الغش في كل جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك. تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة".

نلاحظ من خلال نص هذه المادة أن المشرع جرم كل دخول غير مصرح به والغير مشروع إلى منظومة المعالجة الآلية للمعطيات، مثل دخول الفاعل إلى النظام دون تصريح من المسؤول عن النظام أو مالكة، وقد يكون الفاعل مصرحاً له بالدخول إلى جزء من النظام إلا أنه يتجاوز التصريح الممنوح له ويدخل إلى كامل النظام أو إلى أجزاء أخرى يحظر عليه الدخول إليها، وهذا الفرض في الغالب يتم من طرف العاملين في المؤسسات التي يوجد بها النظام المعلوماتي ويحصل الدخول غير المصرح به بأي وسيلة من الوسائل كاستخدام كلمة المرور الحقيقية متى كان الجاني غير مخول في استخدامها، أو عن طريق استخدام برامج أو شيفرة خاصة، أو عن طريق استخدام الرقم الكودي لشخص آخر من خلال شخص مسموح له بالدخول سواء تم عن طريق شبكة الاتصال الهاتفية أو غير الانترنت.

أما فيما يخص جريمة البقاء غير المشروع داخل النظام المعلوماتي فيقصد بها التواجد داخل هذا النظام بالمخالفة لإرادة الشخص صاحب النظام أو من له السيطرة عليه، وتحقق في الحالة التي يجد الشخص فيها نفسه داخل النظام عن طريق الخطأ أو الصدفة إلا أنه يقرر لبقاء داخل النظام وعدم قطع الاتصال به، ويمكن تصور ذلك في الحالة التي يكون فيها الشخص في سبيله للدخول إلى نظام معلوماتي له الحق في الدخول إليه. إلا أنه يجد نفسه بسبب استخدام شيفرة خاطئة داخل نظام آخر¹¹.

- **جريمة الاعتداء على المعطيات:** نصت المادة 394 مكرر 1 من قانون العقوبات على ما يلي: "يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 50000 دج إلى 200000 دج كل من أخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها".

نلاحظ من خلال نص المادة أن المشرع الجزائري حصر صور الاعتداء على المعطيات في ثلاثة صور تتمثل في إدخال معطيات جديدة غير صحيحة إلى المعطيات الموجودة داخل النظام والتي تمت معالجتها آلياً، وإزالة معطيات كانت موجودة، أو تعديل وتغيير المعطيات واستبدالها بأخرى من خلال برامج معينة تعمل على إتلاف المعطيات.

- **جريمة التعامل في المعلومات غير مشروعة:** جاءت نص المادة 394 مكرر 2 من قانون العقوبات على أنه: "يعاقب بالحبس من شهرين 2 إلى ثلاثة 3 سنوات وبغرامة من 100000 دج إلى 500000 دج كل من يقوم عمداً أو عن طريق الغش بما يأتي:

- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة، أو معالجة أو مرسله عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم السابقة.

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

المطلب الثاني: القوانين الخاصة لمواجهة الجرائم الإلكترونية

- القانون رقم 04/09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

نظرا لعدم كفاية النصوص القانونية الموجودة في قانون العقوبات كان من الضروري سن قوانين خاصة بهذا النوع من الجرائم، ولهذا جاء المشرع الجزائري بالقانون رقم 04/09¹² حيث نص على مراقبة الاتصالات الإلكترونية وذلك بتحديد الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتيه،¹³ كما نصت المادة 4 منه على الحالات التي يسمح فيها للسلطات الأمنية باللجوء إلى المراقبة الإلكترونية وهي:

- الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو الجرائم الماسة بأمن الدولة.
- حالة توفر معلومات عن احتمال الاعتداء على المنظومة المعلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.
- لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.
- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة والمشرع إجراء عمليات المراقبة بإذن مكتوب من السلطة القضائية المختصة.

كما نص كذلك هذا القانون على قواعد إجرائية تساهم بدورها في كشف الجريمة ومعالمها، من تفتيش وحجز للمعطيات المعلوماتية وحفظ المعلومات المتعلقة بحركة السير.

فيما يخص التفتيش فقد اجازت المادة 5 من القانون 04/09 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية لدخول بغرض التفتيش ولوعن بعد إلي:

- منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.
- منظومة معلوماتية.

نستنتج بأن التفتيش في الوضعيات المشار لها يأخذ مجالين إما أن يكون في مجال أعمال التحقيق تقوم به السلطات القضائية المختصة وإما أن يكون في مجال أعمال الإستدلال يقوم به ضباط الشرطة القضائية بناء على أمر تصدره السلطات المختصة، وفي كلتا الحالتين يكون جهاز الكمبيوتر هو المستهدف بمختلف مكوناته، كما أجاز القانون تسخير كل شخص له دراية بعمل المنظومة المعلوماتية التي تتضمنها، وذلك قصد مساعدة السلطات المكلفة بالتفتيش من خلال تزويدها بكل المعلومات الضرورية لإتمام مهمتها.

كما نصت المادة 13 من القانون رقم 04/09 عن الهيئة الوطنية للرقابة من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وتتولى هذه الهيئة تنشيط وتنسيق عمليات الوقاية من الجرائم، وكذلك مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات، وتبادل المعلومات مع الدول.¹⁴

حيث يعتبر كخطوة أولى للجزائر في مجال مواجهة الجريمة الإلكترونية من جهة وسد الفراغ التشريعي الذي كان يعتري القانون الجزائري من جهة أخرى، لكن هذا لا يكفي لردع الجرائم الإلكترونية بمختلف أنواعها.

• القانون رقم 04/15 المتعلق بالتوقيع والتصديق الإلكترونيين

كما جاء القانون رقم 04/15¹⁵ المتعلق لتحديد القواعد المتعلقة بالتوقيع والتصديق الإلكترونيين، بتجريم بعض الأفعال المرتبطة بالبيانات والمعلومات ذات الطابع الشخصي التي تشكل الاعتداء عليها جريمة يعاقب مرتكبها بأحكام جزائية التي تمثلت فيما يلي:

- 1- جريمة إفشاء البيانات الشخصية أو إساءة استعمالها: حسب نص المادة 68 من نفس القانون يعاقب بالحبس من ثلاثة 3 أشهر إلى ثلاثة 3 سنوات وبغرامة من مليون دينار إلى خمسة ملايين دينار أو بإحدى هاتين العقوبتين فقط، كل من يقوم بحيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني موصوف خاص بالغير.
- 2- جريمة الإخلال بسرية البيانات: وفقا لنص المادة 42 من القانون 04/15 يجب على مؤدي خدمات التصديق الإلكتروني أن يحافظوا على سرية البيانات والمعلومات المتعلقة بشهادات التصديق الإلكترونية الممنوحة، فإذا أخلوا بهذا الواجب يعاقب بالحبس من ثلاثة أشهر إلى سنتين وبغرامة من 200000 دج إلى مليون دينار أو بإحدى هاتين العقوبتين.

لقد أراد المشرع الجزائري أن يضيف حمايته على المعلومات الشخصية التي تؤخذ من الأفراد، وأسبغ عليها صفة السرية لما لها من خصوصية معينة، وحسنا فعل عندما جرم الإخلال بسرية هذه البيانات، فتخزين المعلومات لا يعني أن هذه المعلومات قد انتقلت من الخصوصية إلى العلانية، كما أن الرضا بالتجميع والتخزين لا يعني حرية تداول ونقل المعلومات إلى جميع الناس.

- 3- جريمة جمع البيانات الشخصية للمعني دون موافقة: تنص المادة 43 منه على أنه لا يمكن لمؤدي خدمات التصديق الإلكتروني أن يجمع البيانات الشخصية للمعني إلا بموافقة الصريحة، ومتى أخل بهذا الواجب يعاقب بالحبس من ستة أشهر إلى ثلاثة سنوات، وبغرامة مالية من 200000 دج إلى مليون دينار أو بإحدى هاتين العقوبتين فقط.

• القانون رقم 04/18 المتعلق بالقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية

على غرار القوانين سابقة الذكر التي أصدرها المشرع الجزائري لمكافحة الجرائم الإلكترونية لم تكن كافية لمجابهته هذا النوع من الجرائم، ولهذا اصدر المشرع القانون رقم 04/18¹⁶ الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات التكنولوجية والذي الغى بموجبه رقم 03/2000، والذي أكد فيه على وجوب عدم مساس استعمال شبكات وخدمات الاتصال الإلكترونية بحفظ الحياة الخاصة للأفراد، وفي حالة مخالفة ذلك يتعرض المخالف للأحكام الجزائية التي تضمنها هذا القانون، والمتمثلة فيما يلي:

- إنتهاك سرية المراسلات الإلكترونية: حسب نص المادة 164 من هذا القانون يعاقب بالحبس من سنة إلى خمس سنوات وبغرامة من 500000 دج إلى مليون دينار كل شخص ينتهك سرية المراسلات المرسلة عن طريق البريد أو الاتصالات الإلكترونية أو يفشي مضمونها أو نشره أو استعماله بدون ترخيص.

- تحويل المراسلات الصادرة عن طريق البريد: حسب نص المادة 165 من القانون رقم 04/18 يعاقب بالحبس من سنة إلى ثلاث سنوات وبغرامة من مليون دينار إلى خمس ملايين دينار أو بإحدى هاتين العقوبتين كل متعامل

للاتصالات الإلكترونية يحول بأي طريقة كانت، المراسلات لصادرة أو المرسله أو المستقبله عن طريق الاتصالات الإلكترونية.

• القانون رقم 07/18 المتعلق بتحديد قواعد حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي

في محاولة من المشرع الجزائري لمواكبة التطورات والجرائم التي تمس خصوصية الأفراد أصدر حديثا القانون رقم 07-18¹⁷ المؤرخ في 10 يونيو 2018 والذي هدف من خلاله إلى تحديد قواعد حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي وذلك في إطار احترام الحياة الخاصة للأفراد.

ويقصد بالمعطيات ذات الطابع الشخصي- وفقا لأحكام هذا القانون- "كل معلومة بغض النظر عن دعائها متعلقة بشخص معرف أو قابل للتعريف بصفة مباشرة أو غير مباشرة، لاسيما بالرجوع إلى رقم التعريف أو عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الثقافية أو الإجتماعية".

ويقصد بمعالجة المعطيات على أنها "كل عملية منجزة بطرق أو وسائل آلية أو بدونها على معطيات ذات طابع شخصي، مثل الجمع أو التسجيل أو الحفظ أو الملاءة أو التغيير أو الاستخراج أو الاطلاع أو الاستعمال أو الإيصال عن طريق الإرسال أو النشر وكذا الإغلاق أو التشفير أو المسح أو الإتلاف"¹⁸.

كما تجدر الإشارة إلى أن اس مخالفة لأحكام هذا القانون تعرض المخالف للأحكام الجزائية المتمثلة فيما يلي:

- خرق الحياة الخاصة عند معالجة المعطيات: أو جب المشرع أن تتم معالجة المعطيات ذات الطابع الشخصي مهما كان مصدرها أو شكلها في إطار حماية الحياة الخاصة للأفراد¹⁹ وكل خرق لهذا الواجب يعاقب المخالف بالحبس من سنتين إلى خمس 5 سنوات، وبغرامة من 200000 دج إلى 500000 دج²⁰.

- معالجة المعطيات الشخصية رغم اعتراض الشخص المعني: حسب نص المادة 7 من القانون رقم 07/18 يجب معالجة المعطيات ذات الطابع الشخصي بالموافقة الصريحة للشخص المعني، فإذا تمت معالجة هذه المعطيات رغم اعتراضه يعاقب المخالف بالحبس من سنة إلى ثلاث سنوات وبغرامة من 100000 دج على 300000 دج²¹.

- طبقا للمادة 12 من القانون رقم 07/18 يجب إخضاع كل عملية معالجة معطيات شخصية لتصريح مسبق من السلطة المختصة، وفي حالة القيام بالمعالجة دون الحصول على هذا التصريح يعاقب المسؤول بالحبس من سنتين إلى خمس سنوات وبغرامة من 200000 دينار إلى 500000 دينار.

- الاستعمال غير الشرعي للمعطيات الشخصية: المعلومات والبيانات الإسمية التي يتم تجميعها وتخزينها ومعالجتها في جهاز الحاسوب يتعين أن يكون لها هدف محدد وواضح ومعين سلفا، ولابد من إلزام الجهة القائمة على النظام المعلوماتي بالهدف أو الغاية التي من أجلها قامت بتجميع المعلومات ومعالجتها إلكترونيا، فلا يجوز وصول هذه المعلومات إلى شخص آخر أو جهة أخرى تجمع معلومات لغاية مغايرة لأن هذا من شأنه إلحاق الضرر بالشخص لذا تدخل المشرع الجزائري وعاقبة بالحبس من ستة أشهر إلى سنة وبغرامة من 60000 دج غلي 100000 دينار، أو بإحدى هاتين العقوبتين فقط، كل من قام بإنجاز أو استعمال معالجة معطيات غير تلك المصرح بها أو المرخص لها²²

- جمع المعطيات الشخصية بطريقة غير شرعية: يعاقب من سنة إلى ثلاث سنوات وبغرامة من 100000 دينار إلى 300000 دينار كل من قام بجمع معطيات ذات طابع شخصي بطريقة تدليسية أو غير نزيهة أو غير مشروعة طبقا لنص المادة 59 من هذا القانون، فهذا الفعل فيه انتهاك للحياة الخاصة للأفراد يتمثل في جمع معلومات صحيحة عنهم لكن على نحو غير مشروع وغير قانوني.

ويستمد هذا الجمع صفته غير المشروعة إما الأساليب غير المشروعة المستخدمة للحصول على هذه البيانات أو المعلومات كمراقبة الرسائل المتبادلة واعتراضها عن طريق البريد الإلكتروني أو بتوصيل أسلاك خفية إلى الحاسوب الذي تختزن فيه البيانات، أو من حيث طبيعة مضمونها فتمثل صفة عدم المشروعية في أن البيانات غير صالحة للجميع بسبب مضمونها، كأن تتعلق بالمعتقدات الدينية والسياسية والانتماءات الحزبية والأصل العرقي للأفراد، فلا بد أن تكون بعيدة عن عمليات التجميع في الحواسيب، لأن مضمون هذه البيانات يدخل في نطاق الحياة الخاصة للأفراد.²³

- اللوج غير الشرعي للمعطيات الشخصية: يعاقب بالحبس من 6 اشهر إلى سنتين وبغرامة من 60000 دينار إلى 200000 دينار أو بإحدى العقوبتين فقط، كل من عرقل عمل السلطة الوطنية:

- بالاعتراض على إجراء عملية التحقق في عين المكان.

- عن طريق رفض تزويد أعضائها أو الأعوان الذي وضعوا تحت تصرفها بالمعلومات والوثائق الضرورية لتنفيذ المهمة الموكلة لهم أو إخفاء أو إزالة الوثائق أو المعلومات المذكورة.

- عن طريق إرسال معلومات غير مطابقة لمحتوى التسجيلات وقت تقديم الطلب أو عدم تقديمها بشكل مباشرة واضح.²⁴

- إفشاء المعطيات الشخصية: يعاقب الشخص الذي يقوم بإفشاء معلومات محمية بموجب المادة 301 من قانون العقوبات الخاصة بإفشاء الاسرار المهمة.²⁵

- الاحتفاظ بالمعطيات الشخصية أكثر من المدة القانونية: يعاقب بغرامة من 200000 دج إلى 500000 دينار المسؤول عن المعالجة الذي يحتفظ بالمعطيات ذات الطابع الشخصي بعد المدة المنصوص عليها في التشريع الساري المعمول أو تلك الواردة في التصريح أو الترخيص، وهذا وفقا لمقتضيات المادة 65 من هذا القانون.

- نقل المعطيات الشخصية إلى دولة اجنبية: يعاقب من سنة إلى 5 سنوات، وبغرامة من 500000 دينار إلى 1000000 دينار كل من ينقل معلومات ذات طابع شخصي نحو دولة اجنبية.²⁶

خاتمة

من خلال ما تم التطرق إليه أن الجريمة الإلكترونية جريمة ناعمة ومستحدثة وماهي إلا جريمة مثلها مثل الجرائم التقليدية لكن تختلف عنها من حيث الاداة المستخدمة في ارتكاب هذا النوع من الجرائم، حيث سيطرت التقنية الحديثة على الأفراد وعقولهم مما أفرزت عن ظواهر إجرامية تمس الأمن العام من جهة والحق في الخصوصية من جهة أخرى. ومن أجل التصدي للجريمة الإلكترونية قام المشرع الجزائري بمواكبة هذه التطور من خلال تعديل قانون العقوبات وكذا وضع مجموعة من الترسانة القانونية للحماية الجزائية للمعاملات الإلكترونية كان آخرها في سنة 2018 القانون الخاص بحماية المعاملات الإلكترونية وحماية المعلومات المعالجة ذات الطابع الشخصي وذلك في إطار احترام الحياة الخاصة للأفراد.

لكن رغم هذه الجهود الذي بذلها المشرع الجزائري في مواجهة الجرائم الإلكترونية لكنها غير كافية لتحقيق الأمن المعلوماتي نظرا للتطور السريع للجريمة الإلكترونية، وخاصة خاصية العالمية والعابرة للحدود لهذا لبد من تعزيز التعاون الدولي قضائيا وإجرائيا في مجال الأمن المعلوماتي ومكافحة هذه الجرائم.

التوصيات:

- ضرورة التعاون والتنسيق الدولي من خلال الإجراءات وتسليم المجرمين وكذا المحاكمة القضائية.
- وجوب تضافر الجهود القانونية والاجتماعية لتحقيق المواجهة خاصة إذا ما علمنا أن الظاهرة اجتماعية بامتياز كونها قد تتطور من مجرد شغف بالتكنولوجيا إلي دوافع سيئة لهذا من الضروري التحذير من تنامي الإجرام الإلكتروني.
- ضرورة تكوين رجال الشرطة في كيفية التعامل مع هذا النوع من الجرائم الإلكترونية وكيفية التحقيق متابعة المجرمين.

قائمة المراجع:

- 1- القانون رقم 15/04 المتضمن تعديل قانون العقوبات، المؤرخ في 10 نوفمبر 2004، ج ر العدد 71.
- 2- القانون رقم 04/09 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المؤرخ بتاريخ 25 أوت 2009، ج ر العدد 47.
- 3- القانون رقم 04/15 المحدد للقواعد المتعلقة بالتوقيع والتصديق الإلكترونيين، المؤرخ بتاريخ 01 فبراير 2015، الصادر ب ج ر العدد 05.
- 4- القانون رقم 04/18 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، المؤرخ في 10 ماي 2018، ج ر العدد 27.
- 5- القانون رقم 07/18 المتعلق بتحديد قواعد حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، المؤرخ في 10 يوليو 2018 ج ر العدد 34.
- 6- قورة نائلة، جرائم الحاسب الاقتصادية، الطبعة الأولى، دار النهضة العربية، القاهرة، 2004، ص 21.
- 7- نهلا عبد القادر المومني، الجرائم المعلوماتية، ط1 دار الثقافة، عمان، 2008، ص ص. 46-48.
- 8- جعفر حسين جاسم، حرب المعلومات بين ارث الماضي وديناميكية المستقبل، دار البداية، الأردن 2010.
- 9- محمود إبراهيم الغازي، الحماية الجنائية للخصوصية والتجارة الإلكترونية، مكتبة الوفاء القانونية، الإسكندرية، ط1، 2014.
- 11- فضيلة عقالي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، كتاب أعمال مؤتمر الجرائم الإلكترونية المنعقد في طرابلس/لبنان، يومي 24-25-26-03-2017.
- 12- خالد ممدوح إبراهيم، الجرائم الإلكترونية، ط1، الإسكندرية: دار الفكر الجامعي، 2008.
- 13- عبد الفتاح مراد، شرح التحقيق الجنائي الفني والبحث الجنائي، دار الكتب والوثائق المصرية، سنة 2006.

الهوامش:

¹قورة نائلة، جرائم الحاسب الاقتصادية، الطبعة الأولى، دار النهضة العربية، القاهرة، 2004، ص 21.

²نهلا عبد القادر المومني، الجرائم المعلوماتية، ط1 دار الثقافة، عمان، 2008، ص ص. 46-48.

³جعفر حسين جاسم، حرب المعلومات بين ارث الماضي وديناميكية المستقبل، دار البداية، الأردن 2010، ص 64.

- ⁴محمود إبراهيم الغازي، الحماية الجنائية للخصوصية والتجارة الإلكترونية، مكتبة الوفاء القانونية، الإسكندرية، ط1، 2014، ص 118.
- ⁵فضيلة عقالي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، كتاب أعمال مؤتمر الجرائم الإلكترونية المنعقد في طرابلس/لبنان، يومي 24-25-03-2017، ص 5
- ⁶خالد ممدوح إبراهيم، الجرائم الإلكترونية، ط 1، الإسكندرية: دار الفكر الجامعي، 2008، ص ص 87-89.
- ⁷خالد ممدوح إبراهيم، المرجع نفسه، ص ص 83-85.
- ⁸عبد الفتاح مراد، شرح التحقيق الجنائي الفني والبحث الجنائي، دار الكتب والوثائق المصرية، سنة 2006، ص 46.
- ⁹خالد ممدوح إبراهيم، المرجع نفسه ص ص 86-87.
- ¹⁰القانون رقم 15/04 المتضمن تعديل قانون العقوبات، المؤرخ في 10 نوفمبر 2004، ج ر العدد 71.
- ¹¹نهلا عبد القادر المومني، مرجع سابق، ص 161.
- ¹²القانون رقم 04/09 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المؤرخ بتاريخ 25 أوت 2009، ج ر العدد 47.
- ¹³نص المادة 3 من القانون رقم 04/09
- ¹⁴نص المادة 11 من القانون 04/09 سالف الذكر.
- ¹⁵القانون رقم 04/15 المحدد للقواعد المتعلقة بالتوقيع والتصديق الإلكترونيين، المؤرخ بتاريخ 01 فبراير 2015، الصادر ب ج ر العدد 05.
- ¹⁶القانون رقم 04/18 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، المؤرخ في 10 ماي 2018، ج ر العدد 27.
- ¹⁷القانون رقم 07/18 المتعلق بتحديد قواعد حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، المؤرخ في 10 يوليو 2018 ج ر العدد 34.
- ¹⁸أنظر نص المادة 03 من القانون رقم 07/18.
- ¹⁹أنظر نص المادة 2 من القانون رقم 07/18.
- ²⁰أنظر نص المادة 54 من القانون رقم 07/18.
- ²¹أنظر نص المادة 55 من القانون رقم 07/18.
- ²²أنظر نص المادة 58 من القانون رقم 07/18.
- ²³نهلا عبد القادر المومني، المرجع السابق ص ص 174-175.
- ²⁴أنظر نص المادة 60 من القانون 07/18.
- ²⁵أنظر نص المادة 62 من القانون 07/18.
- ²⁶أنظر نص المادة 67 من القانون 07/18.