

التكييف القانوني لجرائم المعلوماتية والإشكالات العملية المترتبة عنها

The legal Characterization of cybercrimes and the practical Issues arising therefrom

سويسي فتيحة

قاضية باحثة بمركز البحوث القانونية والقضائية

ملخص

أدى التطور التكنولوجي المتسارع بفضل الاستخدام الواسع للتكنولوجيات الحديثة للإعلام والاتصال في جميع المجالات (NTIC)، Les nouvelles technologies d'information et communication، إلى بروز نمط جديد من الإجرام وهو الإجرام المعلوماتي أو ما يعرف بالجريمة الإلكترونية أو الجريمة السيبرانية. إذ يعتبر هذا النوع من الجرائم بشق صورته وأنواعه من أكبر التحديات التي تواجهها الدول بسبب انتشاره الواسع لكونه يتسم بالطابع الدولي أي عابر للحدود وأصبح يهدد اليوم الأمن المعلوماتي للأفراد والمؤسسات مما تستدعي الضرورة للتصدي لهذا النوع من الإجرام.

ينطوي هذا المقال على مناقشة أحد أهم الجرائم المطروحة أمام القضاء والتي تتسم بالخطورة البالغة وهي: الجرائم المعلوماتية، وذلك من خلال تسليط الضوء على الإطار القانوني الذي ينظمها وكيفية إضفاء التكييف القانوني الصحيح للوقائع التي تكتسي طابع الجريمة المعلوماتية. كما يهدف هذا المقال إلى مناقشة أهم الإشكالات العملية المطروحة في مجال الجرائم المعلوماتية والتي تواجه القاضي الجزائي وقضاة النيابة على ضوء الممارسة القضائية، ومحاولة إيجاد حلول لها قصد المساهمة في توحيد العمل القضائي. وتكمن أهمية دراسة الموضوع لحدائته من جهة، وخطورته من جهة أخرى، وللوقوف على مدى مواكبة المشرع الجزائري للتطورات الحاصلة في مجال مواجهة جرائم تكنولوجيا الإعلام والاتصال باعتبارها من أكثر أنواع الجرائم تعقيدا لارتباطها بالنظام المعلوماتي.

الكلمات المفتاحية: المجرم المعلوماتي، الإجرام السيبراني، الدليل الإلكتروني، الحق في الخصوصية، التعاون الدولي.

Abstract

The rapid technological development, driven by the widespread use of modern information and communication technologies in all fields, has led to the emergence of a new type of crime known as cybercrime or electronic crime. This type of crime, in all its forms and variations, represents one of the biggest challenges faced by countries due to its large spread and its transnational nature. It has now started to threaten the cyber security of individuals and institutions, making it necessary to address this type of crime.

This article involves a discussion of one of the most significant and highly serious crimes brought before the judiciary, namely: cybercrimes. This will be achieved by shedding light on the legal framework regulating these crimes and exploring how to apply the correct legal characterization to facts that constitute cybercrime. This article also aims to discuss the most significant issues in the field of cybercrimes, which penal judges and public prosecutors face in light of judicial practice. Moreover, this study seeks to identify solutions that contribute to the unification of judicial work. The importance of studying this topic lies in its novelty on the one hand and its severity on the other hand. Additionally, it seeks to assess the extent to which the Algerian legislator has kept pace with developments in addressing crimes related to information and communication technologies, which are among the most complex types of crimes due to their connection with information systems.

Keywords: Cybercriminal, Cybercrime, Electronic Evidence, Right to Privacy, International Cooperation.

مقدمة:

وبمجرد القراءة الأولية لهذه الإحصائيات الحديثة

فإن الارتفاع الحاد في استخدام الأنترنت راجع أساسا إلى عدة عوامل من بينها الآثار الناجمة عن انتشار وباء كورونا في العالم والتدابير المتخذة من طرف الدول وزيادة الحاجة للجوء إلى الخدمات الإلكترونية من خلال التحول الرقمي مثل: الخدمات المصرفية عبر الأنترنت، التعليم عن بعد، العمل عن بعد، التجارة الإلكترونية... الخ.

كما أن هذه الأرقام لها مدلول إيجابي حول واقع الأنترنت في الجزائر، إذ تعتبر خطوة مهمة نحو بناء مجتمع معلوماتي أكثر شمولاً لكنها من جهة أخرى، تبرز الحاجة الملحة لزيادة الحماية الإلكترونية على المستوى الوطني قصد تعزيز الأمن السيبراني في الجزائر.

وتجدر الإشارة إلى أن حق الأشخاص في الاتصال وتبادل المعلومات يتطلب الحماية القانونية بما يضمن ممارسة هذا الحق، والتي تعتبر من الضمانات الدستورية حيث يترتب على سهولة الاتصال والحصول على المعلومات عبر شبكة الأنترنت وبواسطة الأنظمة المعلوماتية سهولة حدوث بعض الأفعال الإجرامية قد تتعدى آثارها الحدود الوطنية باعتبار أن الجريمة المعلوماتية من الجرائم العابرة للحدود، إلا أن مكافحة الجريمة المعلوماتية والتصدي لها لا يتأتى دون تسليط الضوء على الإشكالات التي تثيرها من خلال الممارسة

إن التطورات السريعة في مجال التكنولوجيا الرقمية نتيجة استخدام الشبكة العالمية الأنترنت أدت إلى بروز نمط جديد من الإجرام وهو الإجرام الإلكتروني أو ما يسمى بالجريمة المعلوماتية، نظرا لتوفر الوسائط المستحدثة لتكنولوجيات الإعلام والاتصال، والتي ساهمت بشكل كبير في انتشار الجريمة المعلوماتية وتطورها، فحسب آخر الإحصائيات لسنة 2021 الصادرة عن الاتحاد الدولي للاتصالات وهي وكالة تابعة للأمم المتحدة متخصصة في مجال تكنولوجيا المعلومات والاتصالات (ITU) أشارت إلى وجود نمو عالمي قوي في استخدام الأنترنت حيث ارتفع مستخدميها عبر العالم إلى 4.9 مليار شخص خلال سنة 2021 وفي المقابل يبقى 2.9 مليار شخص عبر العالم غير موصول بشبكة الأنترنت، أي ما يعادل نسبة 37 بالمائة من مجموع سكان العالم.¹

أما بالنسبة للجزائر وحسب نفس المصدر، فقد بلغ عدد مستخدمي الأنترنت في جانفي 2021 حوالي 26.35 مليون شخص أي بنسبة 59.6 بالمائة من مجموع السكان، كما تزايد عدد مستخدمي مواقع التواصل الاجتماعي في الجزائر وبلغ 25 مليون شخص أي بنسبة 56,5 بالمائة من مجموع السكان.²

¹ - الموقع الرسمي للاتحاد الدولي للاتصالات www.itu.int

² - المرجع نفسه.

القضائية لكون ذلك من شأنه أن يساعد في فهم ماهيتها مما يسهل محاربتها من خلال سد الثغرات. وللوقوف على مدى مواكبة المشرع الجزائري للتطورات الحاصلة في مجال مواجهة جرائم تكنولوجيات الإعلام والاتصال باعتبارها من أكثر أنواع الجرائم تعقيدا لارتباطها بالنظام المعلوماتي.

المحور الأول: الإطار المفاهيمي للجرائم المعلوماتية

أولاً- نشأة الجريمة المعلوماتية وتطورها ضمن التشريعات الدولية:

خلال سنة 1966 سجلت أول قضية في الولايات المتحدة الأمريكية تتعلق بارتكاب أفعال إساءة استعمال الحاسوب أين تمت محاكمة مهندس يعمل في البنك من أجل قيامه بالتحايل على برنامج الإعلام الآلي لاختلاس مبلغ مالي، كما تم تسجيل عدة قضايا مماثلة تتعلق بالدخول خلسة إلى الأنظمة المعلوماتية للاطلاع على محتواها وكان القضاء يتعامل مع هذه القضايا على أساس قضية سرقة بالإكراه وأحيانا يعتبرها إخلال بالتزامات المسؤولية العقدية.

وفي اليابان، سجلت أول قضية خلال سنة 1970 تتعلق بالمساس بالأنظمة المعلوماتية على إثر اكتشاف عملية سرقة ونشر معطيات شخصية لزيائن شركة تجارية.¹

ونظرا لصعوبة التعامل مع هذا النوع من الجرائم بسبب خصائص البيئة المعلوماتية الافتراضية، تبلورت

ولمعالجة هذه المسائل يمكن طرح الإشكالية التالية: ما مدى نجاعة الترسانة القانونية التي وضعها المشرع الجزائري لمكافحة الجريمة المعلوماتية والوقاية منها؟

وتتفرع عن هذه الإشكالية عدة تساؤلات فرعية تتمثل فيما يلي:

- كيف يمكن مباشرة إجراءات التحقيق في الجريمة المعلوماتية دون أن يتعارض مع الحق في الخصوصية؟
- ما مدى مساهمة المشرع الجزائري لتطور الإجرام المعلوماتي بالموازاة مع سرعة التكنولوجيات الحديثة؟
- ماهي الإشكالات العملية التي تثيرها الجرائم المعلوماتية على ضوء الممارسة القضائية؟
- ماهي الحلول المقترحة لمعالجة هذه الإشكالات؟

ولمعالجة هذه الإشكالية، تم تقسيم المداخلة إلى ثلاث محاور أساسية:

¹ - عبد الله دغش العجوي، المشكلات العملية والقانونية للجرائم الإلكترونية: دراسة مقارنة، مذكرة ماجستير، جامعة الشرق الأوسط كلية الحقوق، عمان، الأردن، 2014، ص. 43.

إلى ضرورة التعاون الدولي في هذا المجال أين صدرت عدة اتفاقيات إقليمية ودولية من بينها اتفاقية بودابست والمتعلقة بمكافحة الجرائم الإلكترونية التي أدها مجلس أوروبا سنة 2001 ودخلت حيز التنفيذ في 2004 وتلاها بروتوكولين إضافيين سنة 2006 والثاني في سنة 2021.³ وصادقت على هذه الاتفاقية عدة دول، إذ تعتبر الإطار الدولي الوحيد إلى غاية اليوم في مجال مكافحة الجرائم المعلوماتية، التي تهدف أساسا لتوحيد الجهود الدولية وتوطيد التعاون الدولي للتصدي لهذا النوع من الإجرام.

ثانياً- تعريف الجريمة المعلوماتية:

في الواقع لا يوجد أي تعريف موحد أو متفق عليه للجريمة المعلوماتية لأن ذلك يتطلب إسقاط مفاهيم مادية في عالم لامادي (IMMATERIEL) أي افتراضي وهذا ما زاد في الأمر تعقيدا، بالرغم من أن العنصر الوحيد الذي لا يتغير هو (ID IDENTIFIANT) (المعرف الرقمي).

وتجدر الإشارة إلى أن كل من اتفاقية بودابست، والقانون الاسترشادي العربي، والاتفاقية العربية

فكرة ضرورة وضع نصوص قانونية خاصة وبادرت عدة دول إلى إصدار تشريعات تجرم إساءة استعمال الكمبيوتر ونذكر على سبيل المثال:

- الولايات المتحدة الأمريكية في سنة 1970 صدر أول قانون خاص بحماية البيانات وحق الوصول إليها ثم في سنة 1977 أصدرت أول تشريع فدرالي خاص بجرائم الحاسوب.

- السويد، سنة 1973 أصدرت قانون المعطيات المعلوماتية.

- فرنسا، سنة 1978 أصدرت قانون يتعلق بالمعلوماتية والحريات.

وفي سنة 1988 أصدرت قانون يتعلق بجرائم المساس بأنظمة المعالجة الآلية للمعطيات (GODFRAIN)¹.

وفي مطلع الثمانينات تبني مجلس أوروبا اتفاقية حماية المعطيات الشخصية والمعالجة الآلية لها.²

واستمر التطور التشريعي لمعالجة هذا النوع من الجرائم في العديد من الدول عبر العالم، وبرزت الحاجة

¹ مختار الاخضري، الإطار القانوني لمواجهة جرائم المعلوماتية في الفضاء الافتراضي، مداخلة أقيمت خلال أعمال الملتقى الدولي بالجزائر بعنوان "مكافحة الجريمة المعلوماتية"، يومي 5-6 ماي 2010، مركز البحوث القانونية والقضائية، طبعة 2011، ص.54.

² الاتفاقية رقم 108 المؤرخة في 1981/01/28 لمجلس أوروبا المتعلقة بحماية الأشخاص اتجاه المعالجة الآلية للمعطيات ذات الطابع الشخصي، والبروتوكول الإضافي رقم 181 لسنة 2001 الخاص بسلطات المراقبة وانسياب وتدقيق المعطيات عبر الحدود، للاطلاع على الاتفاقية والبروتوكول الإضافي من خلال رابط الموقع الرسمي لمجلس أوروبا. www.int.coe

³ الاتفاقية الأوروبية لمكافحة الجرائم الإلكترونية، الموقعة ببودابست بتاريخ 23 نوفمبر 2001، وبروتوكولها الإضافي الأول الموقع بستراسبورغ بتاريخ 28 جانفي 2003، بشأن تجريم الأفعال المرتبطة بالتمييز العنصري وكراهية الأجانب التي ترتكب عن طريق أنظمة الكمبيوتر، والبروتوكول الإضافي الثاني المؤرخ في 2021/11/17 بشأن تعزيز التعاون والكشف عن الأدلة الإلكترونية.

لكفاحه جرائم تقنية المعلومات، لم يتضمنوا أي تعريف للجريمة المعلوماتية، فمسألة وضع تعريف لهذه الجريمة تم تناولها من طرف الفقهاء وبعض التشريعات والهيئات من عدة زوايا سواء من الجانب الفقهي، أو من الجانب التقني أو من الجانب التشريعي وهذا ما سنتناوله من خلال عرض بعض التعاريف:

أ-التعريف الفقهي:

حسب الفقيه الألماني تاديمان: "هي كل أشكال السلوك غير المشروع أو الضار بالمجتمع والذي يرتكب باستعمال الحاسب الآلي".¹

ب-التعريف التقني:

حسب مكتب تقييم التقنية في الولايات المتحدة الأمريكية: "هي الجرائم التي تلعب فيها بيانات الكمبيوتر والبرامج المعلوماتية دورا رئيسيا".²

تعريف منظمة التعاون الاقتصادي والتنمية التابعة للأمم المتحدة (OCDE): "كل سلوك غير مشروع أو مناف للأخلاق أو غير مرخص به يرتبط بالمعالجة الآلية للبيانات أو نقلها".³

تعريف منظمة الأمم المتحدة المؤتمر العاشر لمنع الجريمة ومعاينة المجرمين المنعقد بفيينا سنة 2000:

ج-التعريف القانوني حسب المشرع الجزائري:

أدرج المشرع الجزائري الجريمة المعلوماتية لأول مرة بموجب قانون العقوبات رقم 04-15 المعدل في 2004، استنادا إلى الالتزامات الدولية للجزائر من بينها الإعلان العالمي لحقوق الانسان والعهدين الدوليين، اتفاقية الأمم المتحدة الخاصة بالجريمة المنظمة العابرة للحدود الوطنية لتاريخ 2000/11/15، المصادق عليها بموجب المرسوم الرئاسي رقم 55/02، المؤرخ في 2002/02/05. ثم التعديل الذي شمل قانون العقوبات سنة 2006 أين قام المشرع بتشديد العقوبات، إلا أن الملاحظ أن المشرع الجزائري لم يضع أي تعريف لهذه الجريمة وإنما جرم إحدى صورها بموجب القسم السابع مكرر تحت عنوان: المساس بأنظمة المعالجة الآلية للمعطيات.

ثم تدارك الأمر سنة 2009، بموجب القانون رقم 04-09 المؤرخ في 5 غشت سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، أين استعمل مصطلح

¹ - إسماعيل جابو ربي، دور الأمن السيبراني في مواجهة التهديدات الإلكترونية دراسة حالة الجزائر، مجلة تحولات جامعة ورقلة، المجلد الثالث: العدد الثاني ديسمبر 2020، ص 68.

² - نفس المرجع السابق، ص 67.

³ - Myriam QUÉMÉNER, Yves CHARPENEL: Cybercriminalité, droit pénal appliqué, Edition ECONIMICA, 2010, 8P.

⁴ - نفس المرجع السابق.

التقليدية المادية، وعليه سنعرض أهم هذه الخصائص والمتمثلة فيما يلي:

أ- الجريمة المعلوماتية جريمة مستحدثة وعدم وجود تعريف مشترك لها:

تعتبر من أبرز أنواع الجرائم الجديدة التي أفرزتها ثورة التكنولوجيا كما أنه لا يوجد أي مفهوم أو تعريف أو مصطلح قانوني موحد للدلالة على هذا النوع من الجرائم، إذ اختلفت التسميات بشأنها كما سبق ذكره أعلاه وهذا راجع أساسا إلى تطور هذه الجريمة تزامنا مع التطور التكنولوجي.

الملاحظ هو وجود اختلاف في التسميات التي أطلقت على الجريمة الإلكترونية نظرا لتطور هذا النوع من الإجرام المتصل بتقنية المعلوماتية إلا أن معظم المصطلحات المستعملة تحمل نفس الدلالة فمنهم من يطلق عليها مصطلح:

-الجرائم المعلوماتية،

-الجرائم الإلكترونية، الجرائم السيبرانية، جرائم الكمبيوتر أو جرائم الحاسوب - جرائم الانترنت،

-جرائم الفضاء السيبران (La criminalité dans le cyber espace)

الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وعرفها ضمن أحكام المادة الثانية على أنها: "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"، ومن خلال أحكام هذا القانون حرص المشرع الجزائري على الموازنة بين الحق في الخصوصية وبين تنظيم القواعد الإجرائية للوقاية من الجرائم المعلوماتية ومواجهتها.¹

وبموجب الأمر رقم 11/21 المتضمن تعديل قانون الإجراءات الجزائية واستحداث القطب الجزائي الوطني المتخصص في هذه الجرائم،² عرّف المشرع الجزائري بموجب المادة 211 مكرر 22 الفقرة الثالثة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال على أنها: "أي جريمة ترتكب أو يسهل ارتكابها استعمال منظومة معلوماتية أو نظام للاتصالات الإلكترونية أو أي وسيلة أخرى أو آلية ذات صلة بتكنولوجيات الإعلام والاتصال".

ثالثاً- خصائص الجريمة المعلوماتية:

نظرا للطابع الخاص لجرائم المعلوماتية فإنها تمتاز بخصائص متنوعة مما جعلها تختلف عن الجرائم

¹ - تجدر الإشارة إلى أن أغلب قواعد القانون رقم 09-04 مستوحاة من أحكام اتفاقية بودابست لمكافحة الجرائم الإلكترونية، لسنة 2001.

² - الأمر رقم 21-11 المؤرخ في 25/08/2021 المنتم للأمر رقم 66-155 المؤرخ في 8 يونيو سنة 1966 المتضمن قانون الإجراءات الجزائية الجديدة الرسمية عدد 65 المؤرخة في 26 غشت 2021. والذي بموجبه قام المشرع الجزائري باستحداث القطب الجزائي الوطني المتخصص لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، المادة 211 مكرر 22 وما بعدها.

د- جريمة تتطلب خبرة فنية وتحكّم في تكنولوجيا المعلوماتية أثناء التحقيق والمتابعة:

نظرا للطبيعة التقنية للجريمة المعلوماتية لابد، أن يكون المحققين أو عناصر الضبطية القضائية متخصصين في هذا النوع من الجرائم والتعامل باحترافية ومهارة أثناء مرحلة البحث والتحري، كما تتطلب المتابعة المستمرة للتطورات التكنولوجية ومعرفة الوسائل التقنية والإجرائية لمواجهة الجرائم المعلوماتية، وكذلك ضرورة التدريب المستمر وتبادل الخبرات بين المتخصصين في هذا المجال سواء على المستوى الدولي أو الوطني وكذا تفعيل دور التعاون الدولي لاكتساب المهارات والخبرات من الدول المتقدمة. كما تساعد الخبرة العلمية والتقنية في الكشف عن الدليل الإلكتروني وتحديد خصائصه كالمستند الرقمي، البرامج، التطبيقات، الاتصالات، الصور،... الخ.

هـ- جريمة تتسم بخطورة بالغة من شأنها المساس بالاقتصاد الوطني والدولي وتسبب في خسائر مالية كبيرة:

فحسب دراسة حديثة أصدرها مركز الدراسات الاستراتيجية والدولية CSIS تم التوصل إلى أن الجرائم الإلكترونية تكلف الاقتصاد العالمي نحو 445 مليار دولار سنويا.¹

-الإجرام السيبراني (Cybercriminalité - cyber crime)

-جرائم التقنية العالية او جرائم التكنولوجيا المتقدمة (Les crimes de la haute technologie)

-جرائم الهاكرز (HACKERS CRIMES)

-الجرائم المتصلة بتكنولوجيات الإعلام والاتصال (Infractions liées aux technologies d'information et communication)

ب- صعوبة الكشف عن الجريمة المعلوماتية وإثباتها:

تكمن صعوبة إثبات هذا النوع من الجرائم لأنها لا تترك أي آثار مادية ظاهرة وكذلك لسهولة محو الدليل الإلكتروني كما أنه من الصعب اكتشافها لكونها ترتكب في بيئة رقمية افتراضية وهي مسرح الجريمة، كما تمتاز بسرعة تنفيذها وبدون أي عنف أو إكراه.

ج- غالبا هي جريمة عابرة للحدود الوطنية:

أي أنها ذات طابع دولي وهذه الخاصية ناجمة من أن المجتمع المعلوماتي (société de l'informations) لا يعترف بالحدود الجغرافية أو المكانية أو الزمانية مما طرح مشكلة الاختصاص القضائي وهنا ظهرت الحاجة لضرورة صياغة تشريع قانوني دولي ومكافحة هذا النوع من الجرائم.

¹ مقال منشور في الموقع الرسمي لمركز الدراسات الاستراتيجية والدولية CSIS بعنوان: "الجرائم الإلكترونية تكبد الاقتصاد العالمي خسائر باهضة"، <https://www.csis.org>

رابعاً- تصنيفات الجريمة المعلوماتية حسب اتفاقية بودابست لسنة 2001:

صنفت الاتفاقية الأوروبية المتعلقة بالجريمة الإلكترونية (بودابست 2001) الجرائم المعلوماتية إلى عدة أصناف تتمثل في:

-الصنف الأول/ الجرائم الماسة بخصوصية وسلامة الأنظمة والبيانات: وتشمل جرائم النفاذ غير المشروع، جرائم الاعتراض والالتقاط غير المشروع، التدخل في البيانات، التدخل في الشبكات والأنظمة المعلوماتية، إساءة استخدام الأجهزة.

-الصنف الثاني/ الجرائم المتصلة بالكمبيوتر: وتشمل التزوير والاحتيال بواسطة الحاسوب.

-الصنف الثالث/ الجرائم المتصلة بالمحتوى: وتشمل إنتاج، توزيع، حيازة مواد إباحية يستخدم فيها الأطفال.

-الصنف الرابع/ الجرائم المتعلقة بانتهاكات حقوق النشر والتأليف، والحقوق المجاورة.

خامساً- أطراف الجريمة المعلوماتية:

أ- **المجرم المعلوماتي:** إن التطور التكنولوجي أفرز صنفاً جديداً من المجرمين وهم المجرمون المعلوماتيون (cyber criminels)، يتمتعون بقدرات عالية من الذكاء والتحكم في الوسائل والاتصالات الإلكترونية ويحرص المجرم المعلوماتي على إخفاء هويته باستمرار من خلال استعمال أفضل التقنيات والبرامج لذا من

الصعب الكشف عنه وتحديد هويته الحقيقية وينقسم المجرمون المعلوماتيون إلى عدة أصناف من بينهم: القراصنة، الهاكرز، الهواة، المتطفلون، الكراكر (CRACKERS)...الخ

ب- **الضحية:** قد يكون ضحية الإجرام المعلوماتي أشخاصاً طبيعيين أو معنوية إذ أن المجرم المعلوماتي يقوم مباشرة بقرصنة الحواسيب أو الهواتف أو اختراق البريد الإلكتروني أو حسابات الأفراد على منصات مواقع التواصل الاجتماعي، كما تشكل الجرائم الإلكترونية التي تستهدف الأشخاص المعنوية خطراً كبيراً سواء في القطاع العام أو القطاع الخاص كالشركات التجارية والبنوك، الوزارات، المستشفيات...إلخ.

وتزداد الخطورة إذا أدى للمساس بقطاعات حساسة في الدولة والمتعلقة بالدفاع والأمن الوطني والوزارات لكونها فيها مساساً بالسيادة الوطنية.

ج- الشاهد المعلوماتي:

تختلف الشهادة في الجريمة المعلوماتية عن تلك المعتاد الأخذ بها في الجريمة التقليدية، نظراً للبيئة الافتراضية التي ترتكب فيها هذا النوع من الجرائم وبالتالي فإن الشهود غالباً ما يكونوا من الأشخاص المحيطون بهذه البيئة اللامادية، وهم الأشخاص الذين لهم دراية وخبرة في مجال تكنولوجيا المعلومات والاتصال ونذكر على سبيل المثال: المبرمجون، القائمين على تشغيل الحاسوب،

مهندسو الصيانة والاتصالات مزودو خدمات الأنترنت والاستضافة، وللإشارة فقد ألزم المشرع الجزائري بموجب المادة 10 الفقرة الأولى من القانون رقم 04/09 مقدمي الخدمات بتقديم المساعدة للسلطات المكلفة بالتحريات القضائية وإمدادهم بكل المعلومات المتعلقة بمحتوى الاتصالات.

سادساً- الإطار القانوني للجريمة المعلوماتية في التشريع الجزائري:

أ- الدستور: (لاسيما المواد 41، 43، 47، 50، 51، 52، 54، 55، المتعلقة أساسا بحماية الحريات الفردية، حماية الحياة الخاصة، الحق في سرية المراسلات والاتصالات الخاصة، حماية الأشخاص الطبيعيين عند معالجة المعطيات ذات الطابع الشخصي).¹

ب- الاتفاقيات الدولية والإقليمية:

✓ تعديل قانون العقوبات بموجب كل من:

- ❖ القانون رقم 01-09، المؤرخ في 26 جوان 2001.
- ❖ القانون رقم 04-15، المؤرخ في 10 نوفمبر 2004.

إضافة القسم السابع مكرر يتضمن مواد جديدة تعاقب على المساس بأنظمة المعالجة الآلية للبيانات.

- ❖ القانون رقم 14-01، المؤرخ في 14 فيفري 2014، المعدل والمتمم لقانون العقوبات.

- الإعلان العالمي لحقوق الإنسان 1948،

- العهد الدولي الخاص بالحقوق المدنية والسياسية 1966،

- العهد الدولي الخاص بالحقوق الاقتصادية والاجتماعية والثقافية 1966،

- اتفاقية الأمم المتحدة الخاصة بالجريمة المنظمة العابرة للحدود الوطنية المؤرخة في 15/11/2000،

¹ - لقد تم تكريس هذه المبادئ الدستورية ضمن كافة الدساتير الجزائرية لاسيما التعديل الدستوري لسنة 2020 الصادر بموجب المرسوم الرئاسي رقم 20-442 المؤرخ في 2020/12/30 المتعلق بإصدار التعديل الدستوري، الجريدة الرسمية عدد 82 المؤرخة في 2020/12/30.

❖ القانون رقم 02-16، المؤرخ في 10 يونيو 2016،
المتمم لقانون العقوبات.

❖ القانون رقم 06-20 مؤرخ في 28 أبريل 2020،
المتعلق بالوقاية من التمييز وخطاب الكراهية
ومكافحتهم، أين تم إضافة مواد جديدة تعاقب على
نشر وترويج أخبار أو أنباء تمس بالنظام والأمن
العموميين لاسيما عبر وسائل الاتصال الحديثة.

✓ القوانين الخاصة ذات الصلة:

✓ القواعد الإجرائية المقررة لمكافحة الجرائم الإلكترونية:

❖ القانون رقم 01-08، المؤرخ في 23 جانفي 2008،
يتم القانون رقم 83-11 المؤرخ في 2 جويلية 1983،
المتعلق بالتأمينات الاجتماعية، تم بموجبه تحديد
الجرائم الواقعة على البطاقة الإلكترونية الشفاء.

❖ القانون رقم 14-04، المؤرخ في 10 نوفمبر 2004،
المعدل والمتمم لقانون الإجراءات الجزائية.

❖ القانون العضوي رقم 05-12، المؤرخ في 12 جانفي
2012، المتعلق بالإعلام.

❖ القانون رقم 22-06، المؤرخ في 20/11/2006
المعدل لقانون الإجراءات الجزائية: يهدف إلى وضع
قواعد إجرائية أكثر تكيفًا مع بعض أنواع معينة من
الجرائم الجديدة أو الأكثر انتشارًا، بما في ذلك
الهجمات على أنظمة المعالجة الآلية للبيانات، ومن بين
المستجدات التي تم إدراجها: اعتراض المراسلات،
تسجيل الصوت وأخذ الصورة.

❖ القانون رقم 12-15، المؤرخ في 15 جويلية 2015،
يتعلق بحماية الطفل.

❖ القانون رقم 13-15، المؤرخ في 15 جويلية 2015،
يتعلق بأنشطة وسوق الكتاب.

❖ القانون رقم 01-06، المؤرخ في 20 فبراير 2006،
يتعلق بالوقاية من الفساد ومكافحته.

❖ الأمر رقم 03-05، المؤرخ في 19 جويلية 2005،
المتعلق بحقوق المؤلف والحقوق المجاورة.

❖ القانون رقم 03-16 المؤرخ في 19 جوان 2016
المتعلق باستعمال البصمة الوراثية في الإجراءات
القضائية.

❖ القانون رقم 04-09، المؤرخ في 05 أوت 2009،
المتضمن القواعد الخاصة بالوقاية من الجرائم
المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها:
هذا القانون يعكس السياسة الجديدة للجزائر في

- ❖ القانون رقم 04-08، المؤرخ في 14 أوت 2004، المتعلق بشروط ممارسة الأنشطة التجارية، المعدل والمتمم.
- ❖ القانون رقم 04-18، المؤرخ في 10 ماي 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية.
- ❖ القانون رقم 05-18، المؤرخ في 10 ماي 2018، يتعلق بالتجارة الإلكترونية.
- ❖ القانون رقم 07-18، المؤرخ في 10 جوان 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.
- ❖ القانون رقم 03-09، المؤرخ في 25 فيفري 2009، المتعلق بحماية المستهلك وقمع الغش.
- ❖ المرسوم التنفيذي رقم 06-348، المؤرخ في 05 أكتوبر 2006، المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق.
- ❖ المرسوم التنفيذي رقم 09-410، المؤرخ في 10 ديسمبر 2009، المحدد لقواعد الأمن المطبقة على النشاطات المنصبة على التجهيزات الحساسة.
- ❖ القانون رقم 04-15 الذي يضع القواعد العامة للتوقيع والتصديق الإلكترونيين.
- ❖ المرسوم التنفيذي رقم 16-134، المؤرخ في 25 أبريل 2016، الذي يحدد تنظيم المصالح التقنية والإدارية للسلطة الوطنية للتصديق الإلكتروني وسيرها ومهامها.
- سابعاً- الإطار المؤسسي لمكافحة الجريمة المعلوماتية:**
- أ- الهيئات الوطنية المتخصصة:**
- 1- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال:**
- المرسوم الرئاسي رقم 21-439 المؤرخ في 07/11/2021. يتضمن إعادة تنظيم هذه الهيئة.
- استحدثت هذه الهيئة بموجب القانون رقم 04-09 المؤرخ في 05/08/2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- لتحدد تشكيلة هذه الهيئة بصدور المرسوم الرئاسي رقم 19-172 المؤرخ في 06/06/2019 الذي يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفية سيرها.
- ثم تم إعادة تنظيم هذه الهيئة بمقتضى المرسوم الرئاسي رقم 21-439 المؤرخ في 07/11/2021.

2- القطب الجزائري الوطني المتخصص لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها:

استُحدث بموجب الأمر رقم 21-11 المؤرخ في 26 أوت 2021 المتضمن تعديل قانون الإجراءات الجزائية وطبقا للمادة 211 مكرر 22 يختص هذا القطب بالمتابعة والتحقيق في الجرائم المتصلة بتكنولوجيات الاعلام والاتصال والجرائم المرتبطة بها، ويمارس وكيل الجمهورية وقاضي التحقيق ورئيس القطب صلاحياتهم عبر كامل الإقليم الوطني كما حددت المادة 211 مكرر 24 الجرائم المرتبطة بتكنولوجيات الاعلام والاتصال وهي: الجرائم الماسة بأمن الدولة أو الدفاع الوطني، جرائم نشر وترويج أخبار كاذبة ماسة بالأمن العام، جرائم نشر وترويج أخبار مغرضة ماسة بالنظام والأمن العموميين ذات الطابع المنظم والدولي، جرائم المساس بأنظمة المعالجة الآلية للمعطيات المتعلقة بالإدارات والمؤسسات العمومية، جرائم الإتجار بالأشخاص أو الأعضاء البشرية أو تهريب المهاجرين، جرائم التمييز وخطاب الكراهية.

3- استحداث القطب الجزائري المالي والاقتصادي:

إذ تشير المادة 211 مكرر 11 الفقرة الثانية على أنه يؤول الاختصاص للقطب الاقتصادي والمالي في حالة الاختصاص المتزامن للقطب الجزائري الاقتصادي والمالي مع القطب الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ويؤول الاختصاص وجوبا لوكيل الجمهورية التابع للقطب الجزائري

الاقتصادي والمالي لدى محكمة سيدي أمحمد بالجزائر العاصمة.

4- المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني:

أنشأ بموجب المرسوم الرئاسي رقم 04/183 المؤرخ في 26/06/2004، ويعتبر مكسب مؤسساتي كبير للجزائر بفضل التقنيات الحديثة والمتطورة المستخدمة في مجال التحقيقات ومكافحة الجريمة وتبنيه نظام إدارة الجودة مما مكّنه من الحصول على شهادة اعتماد على الصعيدين الوطني والدولي، ومن بين المهام المسندة للمعهد:

-إنجاز الخبرات والتحليل بناء على طلبات القضاة، المحققين والسلطات المؤهلة.

-الدعم التقني للوحدات أثناء التحقيقات المعقدة.

-تصميم بنوك معطيات وإنجازها وفقا للقانون.

-المشاركة في الدراسات والبحوث المتعلقة بالوقاية والتقليل من كل أشكال الإجرام.

- المساهمة في تحديد سياسة جنائية مثلى لمكافحة الإجرام.

-المبادرة بالبحوث المتعلقة بالإجرام وإجرائها باللجوء إلى التكنولوجيات الدقيقة.

- العمل على ترقية البحث التطبيقي وأساليب التحريات
- مخبر الفيديو،
- المشاركة في ميدان علم الإجرام والأدلة الجنائية على
- مخبر الصوت لتحديد شرعية التسجيلات
- الصوتية مثلا.²
- المشاركة في تنظيم دورات تحسين المستوى والتكوين.
- 5- المصلحة المركزية لمكافحة الجرائم المتصلة
- بتكنولوجيات الإعلام والاتصال التابعة للمديرية
- العامة للأمن الوطني: التي تتمثل مهامها في:
- دائرة الإعلام الآلي والإلكتروني:
- المساعدة ومعالجة كل دليل الكتروني لفائدة
- أجهزة العدالة.
- تقديم مساعدة تقنية للمحققين في التحقيقات
- المعقدة.
- السهر على تأمين اليقظة التكنولوجية من أجل تحيين
- المعارف والتقنيات والطرق المستعملة في الخبرات
- العلمية.¹
- وتنقسم دائرة الإعلام الآلي والإلكتروني إلى (03)
- مخابر وكل مخبر مزود بفصيلة تسند لها مهمة اقتناء
- المعطيات من دعائم المعلومات وضمان نزاهة
- وشرعية الدليل الإلكتروني
- وتتمثل هذه المخابر الثلاثة فيما يلي:
- مخبر الإعلام الآلي،

¹ - أنظر الموقع الرسمي لوزارة الدفاع الوطني www.mdn.dz.

² - أومدور نجا، خصوصية التحقيق في مواجهة الجرائم المعلوماتية، رسالة دكتوراه في القانون الخاص، كلية الحقوق، جامعة محمد البشير الإبراهيمي، برج بوعريج، 2021، ص. 101.

- استقبال شكاوي المواطنين وإجراء التحقيقات الجنائية بالتنسيق مع الجهات القضائية
 - المشاركة في البحث والتحري في الجرائم المعلوماتية.
 - المشاركة في حملات التوعية والتحسيس.
 - متابعة شبكة الأنترنت لرصد أي محتوى مجرم.
 - تحليل الوضع السياسي، الاقتصادي والاجتماعي المتداول في مواقع التواصل الاجتماعي من أجل العمل على وضع استراتيجية وقائية للحفاظ على النظام والامن العموميين.
- 7- المنظومة الوطنية لأمن الأنظمة المعلوماتية التابعة لوزارة الدفاع الوطني:**

- ✓ إنشاء أقسام مختصة في تحليل الأدلة الرقمية على مستوى المخابر الثلاثة المتواجدة بكل من العاصمة، وهران وقسنطينة، تكمن مهامها في:
- وضع بروتوكولات العمل المتعلقة باستخلاص الأدلة الرقمية.

- تقديم الدعم التقني في ميدان مكافحة الجريمة المعلوماتية.
- إجراء الأعمال التقنية الجنائية بناء على طلبات ضباط الشرطة القضائية.

- إنجاز خبرات لفائدة الأجهزة القضائية في ميدان الأدلة الرقمية.

- المنظمة العربية لتكنولوجيات الاتصال والمعلومات تم تأسيسها من طرف جامعة الدول العربية بتاريخ 10/09/2001 ودورها في التصدي لهذا
- 6-السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي: تحت وصاية رئاسة الجمهورية أنشأت بموجب القانون رقم 07-18، المؤرخ في 10 ماي 2018،

النوع من الإجرام، وتعتبر الجزائر من ضمن الدول الأعضاء. يتحقق هذا الركن بتوفر السلوك الإجرامي، والنتيجة والعلاقة السببية بينهما.

- هيئة الأمم المتحدة لاسيما الاتحاد الدولي للاتصالات وهي وكالة متخصصة في التكنولوجيات والاتصالات، وتعتبر الجزائر عضوا فيها.
- المنظمة العالمية للملكية الفكرية.

المحور الثاني: التكييف القانوني للجرائم المعلوماتية

إن مسألة التكييف القانوني تتمثل في إعطاء الوصف القانوني الصحيح للوقائع بما يتطابق مع النص القانوني المناسب، إلا أن الأمر أكثر تعقيدا فيما يتعلق بالتكييف القانوني للجرائم المعلوماتية نظرا لخصائصها إذ يتطلب الأمر إسقاط وقائع مادية في عالم افتراضي أي في بيئة رقمية وهي مسرح الجريمة. ومن هذا المنطلق يتعين التطرق لأركان الجريمة المعلوماتية (أولاً)، والأحكام الخاصة المتعلقة بإحدى صورها وهي جرائم المساس بنظام المعالجة الآلية للمعطيات (ثانياً).

أولاً- أركان الجريمة المعلوماتية:

أ-الركن المادي: الركن المادي في الجرائم المعلوماتية يتطلب وجود بيئة رقمية وهي مسرح الجريمة ويتطلب كذلك معرفة بداية النشاط والشروع فيه وبالتالي

ب-الركن المعنوي: اشترط المشرع الجزائري لقيام بعض الجرائم قصدا عاما فقط وفي بعض الحالات اشترط وجوب توافر القصد الخاص ونذكر على سبيل المثال المادة 394 مكرر 2 كل من يقوم عمدا وعن طريق الغش. وللإشارة قد ترتكب الجريمة المعلوماتية في إطار جماعة إجرامية منظمة لاسيما تلك التي تنطوي على دوافع مالية لغرض الربح مثلا إذ تتطلب درجة عالية من التنظيم وهي الصورة الغالبة في الوضع الحالي حسب الإحصائيات الحديثة.

ثانياً- الأحكام الخاصة المتعلقة بجرائم المساس بنظام المعالجة الآلية للمعطيات:

لقد خصص المشرع الجزائري منذ تعديل قانون العقوبات سنة 2004 ثم التعديل اللاحق في سنة 2006 القسم السابع مكرر من قانون العقوبات تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، والذي يندرج ضمن الباب الثاني: الجنايات والجنح ضد الأفراد، الفصل الثالث الجنايات والجنح ضد الأموال (المواد من 394 مكرر إلى 394 مكرر 7 قانون العقوبات).

وتجدر الإشارة إلى أن المشرع الجزائري من خلال أحكام هذه المواد لم يضع أي تعريف لمصطلح نظام المعالجة الآلية للمعطيات،¹ إلا أنه تدارك الأمر من

¹ - الدكتور مناصرة يوسف، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، دار الخلدونية، طبعة 2018، ص 125.

طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

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

وشدد المشرع الجزائري العقوبة إذا استهدفت الجريمة مصالح الدفاع الوطني أو الهيئات والمؤسسات العمومية، كما طبق المشرع أحكام قانونية تتعلق بالشخص المعنوي في حالة إذا ارتكب إحدى هذه الجرائم.

وفي نفس السياق أكدت محكمة النقض الفرنسية بموجب القرار الصادر بتاريخ 2021/06/08 تحت رقم 00699 على أنه تعتبر التعديلات أو حذف المعطيات الواردة في نظام معالجة آلية احتيالية بالضرورة بالمفهوم الوارد ضمن أحكام المادة 323-3 من قانون العقوبات عندما يتم إخفاؤها عن قصد عن مستخدم آخر على الأقل لهذا النظام حتى ولم تكن لديه حقوق التعديل، وبرر قضاة الاستئناف قرارهم لما أدانوا المتهم لارتكابه جريمة المساس بنظام المعالجة الآلية للمعطيات، وأنه قام بحذف أصل الحكم في نسخته الرقمية والبيانات الهامشية مع علمه التام بالأفعال المنسوبة إليه دون علم المستخدم الآخر لهذا النظام. وللتوضيح أكثر للقرار تتلخص وقائع القضية أنه تمت إدانة المتهم وهو أمين ضبط بجنحة الحذف عن طريق الغش لمعطيات داخل نظام معالجة آلية للمعطيات

خلال القانون رقم 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وقام بإدراج تعريف لهذا المصطلح ضمن أحكام المادة الثانية فقرة ب كما يلي: "المنظومة المعلوماتية هو نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذًا لبرنامج معين".

ومن خلال أحكام مواد قانون العقوبات فقد حددت المادة 394 مكرر صور المساس بأنظمة المعالجة الآلية للمعطيات وتشمل ما يلي:

- الدخول والبقاء بالغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو محاولة ذلك.

- حذف أو تغيير لمعطيات المنظومة إذا ترتب عن الدخول أو البقاء غير المشروع بغرض تحريف نظام اشتغال المنظومة.

أما المادة 394 مكرر 1 أشارت إلى:

- إدخال بطريق الغش معطيات في نظام المعالجة الآلية أو إزالة أو تعديل بطريق الغش المعطيات التي يتضمنه.

أما المادة 394 مكرر 2 فقد بينت المساس بأنظمة المعالجة الآلية للمعطيات كما يلي:

- تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مرسلّة عن

أحكام المادة 394 مكرر 2 إذ وردت بعض العبارات غامضة في تبيان السلوك المادي للجريمة والمتمثلة في عبارة: بحث، تصميم، توفير، تجميع، مما يثير صعوبة في تصور الجريمة وتحديد الفعل المجرم.

ب- استبدال مصطلح "المعطيات" (DONNEES) الواردة في تعريف الجرائم المدرجة ضمن أحكام المواد من 394 إلى 394 مكرر 1، بمصطلح "معطيات معلوماتية"، تماشيا مع أحكام القانون رقم 04/09.

وذلك حتى نضمن معايير الصياغة القانونية للنصوص التي تتطلب الدقة، الوضوح، وتفادي التأويل من جهة، ومن جهة أخرى فإن اختلاف المصطلحات يؤدي إلى انعدام الأمن القانوني مما يشكل عائقا أمام التعاون الدولي.

ج- يوجد إشكال قانوني آخر يتعلق بعدم توحيد المصطلحات المستعملة فأحيانا يستعمل المشرع الجزائري عبارة "نظام" في المادة 394 مكرر 1، وتارة يستعمل عبارة "منظومة" في المادة 394 مكرر، ثم أدرج عبارة "حذف أو تغيير في المادة" 394 مكرر، أما في المادة 394 مكررا 1 فقد استعمل عبارة "إزالة أو تعديل"، وهو اختلاف في المفردات وعليه كان من الأجدر على المشرع الجزائري شرح وتعريف هذه المصطلحات واستبدال مصطلح "نظام معالجة آلية للمعطيات" (المادة 394 وما يليها من قانون العقوبات) بالمصطلح الذي ورد ضمن

بعد إعادة تكييف الوقائع، وذلك على إثر اكتشاف اختفاء أصل حكم قضائي على مستوى أمانة ضبط المحكمة التجارية وحذف النسخة الرقمية للحكم على مستوى النظام المعلوماتي لتسيير الملفات القضائية، وبعد إجراء التحقيق تم اكتشاف قيام أمين الضبط بارتكاب جنحة حذف معطيات ومضمون الحكم القضائي بالدخول عن طريق الغش لنظام المعالجة الآلية للمعطيات على مستوى المحكمة.¹

المحور الثالث: الإشكالات الموضوعية والإجرائية التي

تثيرها الجريمة المعلوماتية

أولاً- الإشكالات الموضوعية: يمكن حصر أهمها فيما يلي:

أ- إشكال يتعلق بالمصطلحات المستعملة، نظرا للطابع التقني والحديث للجريمة المعلوماتية فإنها تطرح إشكالا عمليا عند تطبيق النصوص القانونية يتعلق بالمصطلحات التقنية إذ تتضمن بعض النصوص القانونية المجرمة مصطلحات غامضة المفهوم مما يجعلها عائقا أمام فهم هذه النصوص، إذ لم يقم المشرع الجزائري بشرح وتعريف المصطلحات الواردة في المواد القانونية المتعلقة بتجريم أفعال المساس بأنظمة المعالجة الآلية للمعطيات لاسيما أنها تعتبر مصطلحات حديثة وذات طابع تقني، مما يؤدي إلى عدم تحقيق الأمن القانوني والقضائي، وعلى سبيل المثال نذكر

¹ - موقع دالوز www.dalloz.fr

وفي هذا الصدد يتعين الإشارة إلى مسألة هامة وهي التصيد الإلكتروني أو ما يسمى بـ (PHISHING) وهي تقنية حديثة لسرقة بيانات الهوية الرقمية مثل بيانات بطاقة الائتمان البنكية والتي أصبحت ظاهرة خطيرة في عالم الإجرام السبيري، إذ تشير آخر الإحصائيات لسنة 2020 الصادرة عن الإنترنت أنها بلغت نسبة 59 بالمائة خاصة مع انتشار وباء كورونا.²

كما أكدت الإحصائيات الصادرة سنة 2021 عن مجموعة العمل لمكافحة التصيد الاحتيالي (APWG) زيادة في معدلات التصيد الاحتيالي.³

ثانياً- الإشكالات الإجرائية: يمكن حصر أهمها فيما يلي:
أ- إشكال يتعلق بصعوبة التعرف على مرتكب الجريمة المعلوماتية وتحديد هويته الحقيقة وأن الاعتماد على عنوان البروتوكول (Internet protocole/ IP) لا يؤدي حتماً بجهات التحقيق إلى التوصل إلى الفاعل الحقيقي لأنه يمكن اختراق أجهزة كمبيوتر تابعة لأشخاص آخرين.

ب- إشكال يتعلق بامتناع الضحايا سواء أشخاص طبيعية أو معنوية عن التبليغ عن الجرائم المعلوماتية بسبب الحفاظ على سمعتهم الشخصية أو التجارية في حالة الشركات مثلاً أو اكتشافهم للجريمة في وقت

أحكام القانون رقم 04/09، ليصبح "نظام معلوماتي" لكونه مصطلح أدق وأشمل وذلك حتى نضمن معايير الصياغة القانونية للنصوص التي تتطلب الدقة، الوضوح، وتفادي التأويل.

د- إشكال يتعلق بالمادة 12 من القانون رقم 04/09 التي تجعل الالتزام بالتدخل الفوري يقع على عاتق مقدم الخدمة، ونقترح إعادة تغيير عنوان المادة 12 السالفة الذكر بجعل الالتزام بالتدخل الفوري يقع على عاتق مقدم الخدمة وإيواء الخدمة معاً.

هـ- إشكال عملي يتعلق بالفراغ القانوني: عدم تجريم بعض الأفعال التي تتسم بطابع الجريمة المعلوماتية (مبدأ الشرعية).

و- إشكال قانوني يتعلق أساساً بوجود فراغ تشريعي في القانون الجزائري فالعديد من صور الإجرام الإلكتروني غير مجرمة ونذكر على سبيل المثال: جريمة انتحال الهوية الرقمية إذ أن المشرع الفرنسي جرم هذه الصورة في سنة 2011 بموجب قانون (LOPPSI2)، ضمن أحكام المادة 2 أين تم إدراج المادة 1-4-226 في قانون العقوبات الفرنسي في إطار الاستعمال عن طريق الغش لمعطيات ذات طابع شخصي.¹

¹-Loi n 2011-267 publié au journal officiel du 14 mars 2011 d'Orientation et de Programmation pour la Performance de la Sécurité Intérieure dite LOPPSI2. <http://www.legifrance.gouv.fr/>.

²- أنظر الموقع الرسمي للإنترپول www.Intrepol.int

³- أنظر موقع مجموعة العمل لمكافحة التصيد الاحتيالي APGW : WWW.APGW.ORG

و- إشكال ناجم عن التعاون الدولي يتعلق باختلاف التشريعات والنظم القانونية الإجرائية للدول مما نتج عنه عدم وجود نموذج موحد للتعامل مع النشاط الإجرامي، وهو ما يؤثر مباشرة على إجراءات جمع الدليل الإلكتروني، فمثلا الاجراء الذي يعتبر مشروعا في دولة ما قد تعتبره دولة أخرى خارج إطار الشرعية الإجرائية وهو ما يترتب عنه لاحقا عدم مشروعية الدليل الإلكتروني.

وفي هذا الإطار أصدرت محكمة النقض الفرنسية قرار بتاريخ 2020/11/25 تحت رقم 17-19.523 الغرفة الاجتماعية، أكدت من خلاله على مسألة مشروعية الحصول على الدليل الإلكتروني والتي تعتبر من أهم شروط قبول الدليل الإلكتروني أمام القضاء، إذ اعتبرت محكمة النقض لأول مرة أن عنوان بروتوكول الانترنت (Internet protocole/ IP) والملفات اليومية تعتبر بمثابة معطيات ذات طابع شخصي وأن معالجتها تخضع وجوبا لترخيص سابق من طرف اللجنة الوطنية للمعلوماتية والحريات (CNIL)، وأكدت محكمة النقض على أنه يتعين على القضاة مناقشة مشروعية الدليل في إطار مبدأ تناسب الإجراء إذا كان فيه مساس بالحياة الخاصة للعامل¹

ونشير في هذا الصدد إلى أنه لا توجد معايير خاصة محددة نص عليها المشرع الجزائري فيما يتعلق بإنشاء أي تكوين أو قبول الدليل الإلكتروني في قواعد الإثبات

متأخر، أو عدم علمهم أصلا بأنهم وقعوا ضحايا جريمة معلوماتية.

ج- إشكال يتعلق بعدم تجاوب الضحايا أحيانا مع مصالح الضبطية القضائية المختصة في حالة إنذارهم بوجود هجوم سببراني محتمل على النظام المعلوماتي التابع للشركة أو المؤسسة لوجود ثغرة في النظام المعلوماتي (faible de sécurité) إلا أن صاحب الشركة التجارية لا يتخذ أي إجراءات لتعزيز تأمين النظام المعلوماتي للشركة، مما يؤدي لوقوع الهجوم السببراني بصفة فعلية.

د- عدم تمتع المحققين أحيانا بالخبرة الكافية أو نقص الاحترافية في التعامل مع الوسائل التقنية الحديثة مقارنة بالإجرام الإلكتروني الذي يتمتع به المجرمون أحيانا بمستوى عال من الاحترافية والذكاء، وهو ما يترتب عليه خرق قواعد إجراءات التعامل مع الدليل الإلكتروني أثناء التفتيش أو الضبط وبالتالي المساس بالشرعية الإجرائية مما يؤثر على مصداقية الدليل الإلكتروني المستخلص.

هـ- صعوبات تتعلق بالدليل الإلكتروني في حد ذاته لكونه دليل غير مادي وقد يتطلب الوصول إليه المساس ببيانات أخرى محاطة بالخصوصية المعلوماتية، بالإضافة إلى سهولة إتلاف الدليل الإلكتروني أو تعديله أو نقله بعد تنفيذ الجريمة في مدة وجيزة.

¹ - موقع الدوز، مرجع سابق.

الجزائي أمام القاضي الجزائي (production et admissibilité)، وإنما يخضع إنشاء الدليل الإلكتروني وقبوله من طرف القاضي إلى معيارين وهما:

✓ معيار شرعية الدليل الجنائي (légalité)

✓ معيار مشروعية الدليل الجنائي (loyauté) (légitimité).

ز- إشكال يتعلق بالمساعدة القضائية الدولية التي تعتبر من أشكال التعاون الدولي في مجال التحقيق الجنائي في الجرائم الإلكترونية ومن صورها الإنابة القضائية الدولية بين جهات التحقيق إلا أن بطء الإجراءات التي يتوجب على الدولة طالبة الإنابة القضائية أن تسلكها بعد تقديمها الطلب إلى البلد الآخر وانتظار الرد تشكل معوقات لجهات التحقيق في الجريمة الإلكترونية من شأنه أن يؤدي إلى إتلاف وضياح الدليل الإلكتروني، وفي هذا الإطار وبموجب اتفاقية بودابست تم إنشاء مراكز اتصال لتأمين عملية المتابعة، وجمع واعتراض بيانات الحركة في الوقت الحقيقي ((en temps réel وتبادل المعلومات بين الدول الأطراف دون انقطاع أي على مدار الساعة 24/24 وطيلة أيام الأسبوع 7/7 وتعتبر مراكز الاتصال أساس فعالية التحقيق وتبادل المعلومات من خلال هذه الاتفاقية.

كذلك من بين التعقيدات التي أفرزتها الجريمة المعلوماتية هي تلك الصعوبات التي تواجه التعاون الدولي في مجال التحقيق ومن بينها مسألة تنازع الاختصاص القضائي على المستوى الدولي، فالسلوك الإجرامي في الجريمة الإلكترونية قد يرتكب في دولة معينة ولكن آثاره ونتيجته تتحقق في دولة أخرى، فالتحقيق يتطلب امتداد الاختصاص القضائي إلى الخارج وأن عملية جمع الأدلة الإلكترونية مثلا يتطلب الولوج إلى أنظمة معلوماتية متواجدة خارج إقليم الدولة المعنية وهو ما يتعارض مع السيادة الوطنية.¹ (وتجدر الإشارة إلى أن اتفاقية بودابست عالجت هذه المسألة من خلال المواد 31-32).

ج- إشكال يتعلق بالاصطدام بالحق في الخصوصية المعلوماتية وتنعكس في الإجراءات التالية:

✓ مسألة التسرب الإلكتروني والتفتيش الإلكتروني كإجراء فعال من إجراءات جمع الأدلة في الجريمة الإلكترونية طبقا للمواد 65 مكرر 5 و65 مكرر 11 ق 1 ج.

✓ الإجراءات المتعلقة برقابة الاتصالات الإلكترونية من أجل اعتراض أشكال المراسلات التي تتم عبر وسائل الاتصال السلكية واللاسلكية وكذا عبر البريد الإلكتروني، والتي قد يشكل محتواها دليلا لإثبات

¹ - أومدور نجا، مرجع سابق، ص 43.

وللإشارة فإن التهديدات السيبرانية في تزايد مستمر حسب الاتحاد الدولي للاتصالات أين تم إطلاق مبادرة الرقم القياسي العالمي للأمن السيبراني في إطار البرنامج العالمي للأمن السيبراني والذي يقوم على خمسة (5) ركائز أساسية وهي:

- التدابير القانونية،
- التدابير التقنية والإجرائية،
- الهياكل التنظيمية،
- بناء القدرات،
- التعاون الدولي،

وبالتالي الهدف من هذا البرنامج هو بناء الثقة الرقمية والأمن في استعمال تكنولوجيا المعلومات والاتصالات، وحماية الفضاء السيبراني وتعزيز القدرات الفنية الوطنية في الدفاع ضد التهديدات السيبرانية¹.

وخلال سنة 2018 صُنّفت الجزائر ضمن البلدان العربية التي بدأت في تنفيذ التزامات في مجال الأمن السيبراني، بينما سجلت خمسة بلدان عربية مستويات عالية من الالتزام إزاء جميع ركائز الرقم القياسي العالمي للأمن السيبراني الخمس، بينما طورت ثلاثة بلدان عربية أخرى - الكويت والأردن وتونس - التزامات معقدة وانخرطت في برامج ومبادرات للأمن السيبراني، وحصلت السعودية وعمان وقطر على المراتب الثلاث الأولى في

الجريمة الإلكترونية إلا أن هذا الإجراء من شأنه أن يشكل تهديدا ومساسا بالخصوصية المعلوماتية مما يتطلب تقييد اللجوء لهذا الإجراء بشروط صارمة حفاظا على حرمة الحياة الخاصة للأفراد.

ط- إشكال يتعلق بعدم الالتزام بحفظ المعطيات المتعلقة بحركة السير من طرف مزودي الخدمات عبر الانترنت المحددة بمدة سنة في التشريع الجزائري بموجب القانون رقم 04/09 مما يعرقل حسن سير إجراءات التحريات الأولية والتحقيق القضائي.

ي- إشكال يتعلق أساسا بنقص تفعيل دور الأمن السيبراني في مواجهة التهديدات الإلكترونية والهدف منه حماية الأنظمة المعلوماتية والشبكات والبرامج الحكومية من الهجمات الرقمية ويتم ذلك بوضع استراتيجية وطنية شاملة من أجل ضمان أمن المعلومات في الفضاء السيبراني.

كما أن المسألة تزداد تعقيدا في حالة لجوء بعض الإدارات العمومية وشركات كبرى في الجزائر إلى استخدام البرامج المقرصنة (الكراك)، أو استعمال أنظمة تشغيل مقرصنة (نظام التشغيل وينداوز مقرصن)، استعمال برامج مدفوعة عن طريق استخدام برامج قرصنة بها فيروسات، استعمال برامج مجانية تحتوي على برامج جوسسة، دون الأخذ بعين الاعتبار لمخاطرها الأمنية في المجال الإلكتروني.

¹ - الموقع الرسمي للاتحاد الدولي للاتصالات، مرجع سابق.

الفايسبوك المرتبة الأولى ثم اليوتوب في المرتبة الثانية ثم الواتساب في المرتبة الثالثة وهو ما أدى لزيادة المخاطر السببرانية كما هو موضح في الشكل البياني.²

خاتمة

في الختام وعلى ضوء ما سبق تفصيله، نؤكد أن الرصيد التشريعي الجزائري الحالي غير كاف لمكافحة كل صور الجرائم المعلوماتية، بل لابد من تحيين القوانين حتى تشمل جرائم أخرى لم تشملها القوانين الحالية مثل قرصنة أسماء المواقع المجالات على شبكة الأنترنت أو انتحال الهوية الرقمية، كما أن أحكام التشريع الجزائري وآليات التعاون القضائي الدولي لازالت غير كافية لمواجهة الإجرام المعلوماتي الذي يصعب فيه إثبات الفعل المجرم أو ضبط الجاني بسبب طبيعة الدليل الإلكتروني ولكون الجريمة المعلوماتية في أغلب الأحوال عابرة للحدود لارتكابها عبر شبكات الاتصال الحديثة.

لذلك أصبح من الضروري السعي لوضع اتفاقية عالمية تحت إشراف هيئة الأمم المتحدة قصد سنّ إطار دولي للإجرام الإلكتروني وضمان تعزيز التعاون الدولي لتوحيد الجهود الدولية لمكافحة هذا النوع من الإجرام الخطير ولمواجهة الهجمات السببرانية، لكون أن الجريمة المعلوماتية في أغلب الأحوال عابرة للحدود

منطقة الدول العربية إزاء جميع ركائز الرقم القياسي العالمي للأمن السببراني الخمس السالفة الذكر.¹

وفي نفس السياق نشير إلى زيادة التهديدات الإلكترونية عبر العالم باستعمال تقنيات أخرى مستحدثة في مجال الإجرام السببراني ومن بينها:

- تقنية برامج الفدية الخبيثة/ (RANSOMWARE)
- تقنية التصيد الإلكتروني/ (PHISHING)
- تقنية ارسال بريد الكتروني غير مرغوب فيه (SPAMMING)/
- تقنية انتحال IP عنوان بروتوكول الأنترنت/ (SPOOLING)
- تقنية حجب الخدمة/ (DENIAL OF SERVICES)
- برمجة خبيثة/ (MALWARE)

- تقنية برامج الجوسسة/ (SPYWARE)
- تقنية قرصنة خادم (Pharming /DNS)

كما يتعين لفت الانتباه أيضا إلى تفاقم الجرائم السببرانية عبر مواقع التواصل الاجتماعي في سنة 2021 نظرا لزيادة المستخدمين عبر العالم، واحتل موقع

¹ - تقرير مؤرخ في 2021/03/22، حول الاجتماع الإقليمي الافتراضي التحضيري للدول العربية للمؤتمر العالمي لتنمية الاتصالات لعام 2021 المنعقد بتاريخ 7-8 أبريل 2021، الاتجاهات الرقمية في الدول العربية في عام 2021. متوفر على الموقع الرسمي للاتحاد الدولي للاتصالات www.itu.int.

² - أنظر الموقع الإلكتروني www.datareportal.com

لارتكائها عبر شبكات الاتصال الحديثة، وبالتالي من الضروري مواكبة التطورات التكنولوجية واستحداث إجراءات خاصة تتناسب مع خصوصية التعامل مع البيئة الرقمية نظرا للتعقيدات والصعوبات التي تواجه السلطات المختصة أثناء استخلاص الأدلة الإلكترونية والكشف عن الجناة، إلا أنه من جهة أخرى فإن استحداث هذه الإجراءات والقواعد الخاصة يجب أن يكون مراعيًا لإقامة توازن بين الحق في استخدام الوسائل الحديثة للكشف عن الجريمة وجمع الأدلة فيها، وبين الحرية الشخصية للأفراد واحترام خصوصياتهم من خلال الالتزام بالضوابط القانونية الملائمة في ذلك.

قائمة المصادر والمراجع

I- قائمة المصادر

أولاً: باللغة العربية

1- المرسوم الرئاسي رقم 442-20 المؤرخ في 2020/12/30 المتعلق بإصدار التعديل الدستوري، الجريدة الرسمية عدد 82 المؤرخة في 2020/12/30.

2- الاتفاقية رقم 108 المؤرخة في 1981/01/28 لمجلس أوروبا المتعلقة بحماية الأشخاص اتجاه المعالجة الآلية للمعطيات ذات الطابع الشخصي، والبروتوكول الإضافي رقم 181 لسنة 2001 الخاص بسلطات المراقبة وانسياب وتدفق المعطيات عبر الحدود.

3- الاتفاقية الأوروبية لمكافحة الجرائم الإلكترونية، الموقعة ببودابست بتاريخ 23 نوفمبر 2001، وبروتوكولها الإضافي الأول الموقع بستراسبورغ بتاريخ 28 جانفي 2003، بشأن تجريم الأفعال المرتبطة بالتمييز العنصري وكراهية الأجانب التي ترتكب عن طريق أنظمة الكمبيوتر، والبروتوكول الإضافي الثاني المؤرخ في 2021/11/17 بشأن تعزيز التعاون والكشف عن الأدلة الإلكترونية.

4- الأمر رقم 11-21 المؤرخ في 2021/08/25 المتمم للأمر رقم 66-155 المؤرخ في 8 يونيو سنة 1966 المتضمن قانون الإجراءات الجزائية الجريدة الرسمية عدد 65 المؤرخة في 26 غشت 2021.

ثانيا- باللغة الأجنبية:

1-Loi n 2011-267 publié au journal officiel du 14 mars 2011 d'Orientation et de Programmation pour la Performance de la Sécurité Intérieure dite LOPPSI2. <http://www.legifrance.gouv.fr/>

II- قائمة المراجع

أولاً: باللغة العربية

1- الكتب:

1- مختار الأخضر، الإطار القانوني لمواجهة جرائم المعلوماتية في الفضاء الافتراضي، مداخلة أُلقيت خلال أعمال الملتقى الدولي بالجزائر بعنوان "مكافحة الجريمة المعلوماتية"، يومي 5-6 ماي 2010، مركز البحوث القانونية والقضائية، طبعة 2011.

2- الدكتور مناصرة يوسف، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، دار الخلدونية، طبعة 2018

2- مذكرات ورسائل جامعية:

1- أومدور نجاة، خصوصية التحقيق في مواجهة الجرائم المعلوماتية، رسالة دكتوراه في القانون الخاص، كلية الحقوق، جامعة محمد البشير الإبراهيمي، برج بوعريج، 2021

- 2- عبد الله دغش العجني، المشكلات العملية والقانونية للجرائم الإلكترونية: دراسة مقارنة، مذكرة ماجستير، جامعة الشرق الاوسط كلية الحقوق، عمان، الأردن، 2014.
- 5- أنظر موقع مجموعة العمل لمكافحة التصيد الاحتيالي APGW: WWW.APGW.ORG
- 6- تقرير مؤرخ في 2021/03/22، حول الاجتماع الإقليمي الافتراضي التحضيري للدول العربية للمؤتمر العالمي لتنمية الاتصالات لعام 2021 المنعقد بتاريخ 7-8 أفريل 2021، الاتجاهات الرقمية في الدول العربية في عام 2021. متوفر على الموقع الرسمي للاتحاد الدولي للاتصالات www.itu.int

3- المقالات

- إسماعيل جابو ربي، دور الأمن السبراني في مواجهة التهديدات الإلكترونية دراسة حالة الجزائر، مجلة تحولات جامعة ورقلة، المجلد الثالث: العدد الثاني ديسمبر 2020
- 7- أنظر الموقع الإلكتروني www.datarep

ثانياً- باللغة الأجنبية:

-Myriam QUÉMÉNER, Yves CHARPENEL : Cybercriminalité, droit pénal appliqué, Edition Economica, 2010.

III- المواقع الإلكترونية:

- 1- مقال منشور في الموقع الرسمي لمركز الدراسات الاستراتيجية والدولية CSIS بعنوان: "الجرائم الإلكترونية تكبد الاقتصاد العالمي خسائر باهضة"، <https://www.csis.org>
- 2- أنظر الموقع الرسمي لوزارة الدفاع الوطني www.mdn.dz
- 3- موقع دالوز www.dalloz.fr
- 4- أنظر الموقع الرسمي للانترپول www.Intrepol.int