

التصدي للجرائم الإلكترونية المنتهكة لخصوصية الأفراد في ظل قانون العقوبات رقم 24-06
The legal framework for cybercrimes violating individuals' privacy
under Penal Code N° 06-24

♦ سي مرابط شهرزاد

جامعة عين تموشنت / الجزائر

chahrazed.simerabet@univ-temouchent.edu.dz

تاريخ النشر: 2025/12/25

تاريخ القبول: 2025/10/19

تاريخ الإرسال: 2025/03/15

الملخص:

يعتبر موضوع الأمن السيبراني معضلة العصر، باعتباره السلاح الاستراتيجي الحالي، نظرا لما يفرزه الواقع التكنولوجي الذي يفرض نفسه على المجتمعات ومتطلباته، من تهديدات سيبرانية غير معروفة وهجمات غير متوقعة تثير ذعر الجميع، تساهم في زيادة حدة مخاطرها كل من الرقمنة والذكاء الاصطناعي، وبما أن الجزائر تتجه بشكل متسارع نحو رقمنة قطاعاتها، فقد بات من الضروري مناقشة اهتمامها بقضية تأمين منظومتها الإلكترونية ومدى قدرتها على توفير الأمن والحماية الكافية لأفرادها وخصوصيتهم، وبالأخص التصدي لمركبي الجرائم الرقمية المنتهكة لخصوصية الافراد بما أنهم أحد أركان قيام الدولة، وهو ما يسعى إليه المشرع من خلال قانون العقوبات رقم 06-24 الذي يسعى إلى تأطير منظومة الجرائم الإلكترونية مواكبة منه للتطورات الرهيبة في العالم الرقمي وضمان الامن والأمان.

الكلمات المفتاحية: الأمن السيبراني، الجريمة الإلكترونية، الخصوصية، الرقمنة

Abstract:

The topic of cybersecurity is considered the dilemma of the era, as it is the current strategic weapon, given what the technological reality that imposes itself on societies and its requirements produces, from unknown cyber threats and unexpected attacks that cause everyone to panic, and digitization and artificial intelligence contribute to increasing the severity of their risks, and since Algeria is rapidly moving towards digitizing its sectors, it has become necessary to discuss its interest in the issue of securing its electronic system and the extent of its ability to provide adequate security and protection for its individuals and their privacy, they

are one of the pillars of the establishment of the state, which is what the legislator seeks through Penal Code No. 06-24, which seeks to frame the system of cybercrimes in keeping pace with the terrible developments in the digital world and ensuring security and safety

Keywords: Cybersecurity, Cybercrime, Privacy, Digitization

مقدمة:

يشهد العالم اليوم عصر جديد تطغى فيه تكنولوجيا المعلومات واستخدام التقنيات العصرية في مختلف القطاعات، لاسيما استخداماتها في قطاعات الامن الداخلي والخارجي، مما زاد من فرص ارتكاب الجرائم الالكترونية والمخاطر التي يمكن ان تتسبب فيها على الاستقرار والامن الاجتماعي والاقتصادي للدولة، الى حد تهديد كيان الدولة وأمنها القومي بارتكاب بعض الجرائم مثل التجسس الالكتروني والابتزاز والتهديد، مما يقتضي- إيجاد وخلق آليات عصرية لمكافحة هذا النوع من الجرائم سواء من الناحية التشريعية العقابية والاجرائية، الكفيلة بقمع هذه الجرائم، وضبطها وتحقيقها أو من الناحية التقنية بإعداد الكوادر الفنية المؤهلة والمدرية على استخدام أحدث الوسائل والأجهزة المعلوماتية لكشف وضبط هذه الجرائم.

تعيش الدولة وافراده في زمن صعب ومكشوف كانت المعلوماتية أو ثورة المعلومات سببا فيه، التي ترتكز على آلية المعلومات وطفرة الاتصالات، حيث ظهر مصطلح الجريمة المعلوماتية أو الالكترونية أو السيبرانية لوصف فكرة جزء من الحاسب الآلي أو عصر- المعلومات، أما بخصوص الجريمة فهي السلوكيات والأفعال الممنوعة والمجرمة قانونا، والجرائم الالكترونية هي المخالفات التي ترتكب ضد الدولة أو الأفراد او المجموعات من الأفراد بدافع الجريمة وبقصد إيذاء سمعة الضحية أو اذى مادي أو معنوي للضحية مباشر أو غير مباشر باستخدام شبكات الاتصالات مثل الانترنت عن طريق مواقع التواصل الاجتماعي والردشة والبريد الالكتروني والهاتف النقال.

فالمعلوماتية أصبحت قضية الجميع ولم تعد ظاهرة محدودة النطاق مقصورة على قطاع تقني محدد، بل ترتب عن ذلك تزايد عدد المعنيين بها، وعليه أصبح لزاما تدخل القانون في الاهتمام بهذه الظاهرة الخطيرة وسريعة التطور والتفاعل معها، وعليه سعى المشرع الجزائري الجزائي إلى إصدار قانون العقوبات الجديد رقم 06-24¹ الذي عدل وحين وأضاف جرائم إلكترونية جديدة حسب حجم الشكاوى والقضايا التي سجلت بخصوصها سواء على مستوى مصالح الشرطة أو تكررت على رفوف العدالة.

لا شك ان الجريمة الالكترونية هي ظواهر إجرامية تفرع أجراس الخطر لتنبه مجتمعا عن حجم المخاطر والخسائر التي يمكن أن تنجم عنها، خاصة انها جرائم ذكية تنشأ وتحدث في بيئة الكترونية رقمية، يقترفها اشخاص مرتفعي

¹ القانون رقم 06-24 المؤرخ في 28 أبريل 2024 المتعلق بقانون العقوبات، يعدل ويجم الأمر رقم 66-156 المؤرخ في 8 جويلية 1966 والمتضمن قانون العقوبات.

التصدي للجرائم الإلكترونية المنتهكة لخصوصية الأفراد في ظل قانون العقوبات رقم 06-24

الذكاء ويمتلكون أدوات المعرفة التقنية، مما يسبب خسائر للمجتمع ككل على المستويات الاقتصادية والاجتماعية والثقافية والأمنية.

من هنا يظهر دور السلطة التشريعية الهام والخطير في مواجهة الإجرام المعلوماتي والتصدي له ، لأنه لا جدال في ان الجرائم المعلوماتية أضحت من اخطر واعقد الجرائم باعتبارها عابرة للحدود، حيث تستخدم فيها احدث التقنيات، بحيث فقدت الحدود الجغرافية كل أثر في الفضاء الشبكي المتشعب العلاقات، وأصبحنا بالتالي أمام جرائم عابرة للحدود تتم في فضاء الكتروني معقد عبارة عن شبكة اتصال لا متناهية غير محسدة وغير مرئية متاحة لأي شخص حول العالم وغير تابعة لأي سلطة حكومية، يتجاوز فيها السلوك المرتكب المكان بمعناه التقليدي، فقد يكون الكمبيوتر أداة للجريمة مثل جريمة السرقة والنصب والابتزاز وتشويه السمعة، وقد يكون معبرا للجريمة أو محلا لها مثل جريمة تدمير المعلومات، ومن هنا يظهر جليا دور النظام القانوني في مواكبة الأحداث التكنولوجية والمعلوماتية في شقها السلبي المتمثل في الجرائم المعلوماتية والتصدي لها ووضع حد للتجاوزات الإلكترونية سواء تعلق الامر بالأفراد أو المؤسسات أو حتى أجهزة الدولة من عدمه.

وعليه نطرح الإشكالية التالية: كيف تصدى المشرع الجزائري للتهديدات الرقمية التي تشكل خطرا على خصوصية الأفراد في قانون العقوبات؟

من خلال هاته الورقة البحثية سنجيب على الإشكالية المطروحة من خلال المحورين التاليين:

العنوان الرئيسي الأول: ماهية الجريمة الإلكترونية

العنوان الرئيسي الثاني: الجرائم الإلكترونية المنتهكة لخصوصية الأفراد في ظل قانون العقوبات رقم 06-24

1- العنوان الرئيسي الأول: ماهية الجريمة الإلكترونية

الجريمة الإلكترونية هي إحدى الجرائم المعاصرة التي أصبحت تمثل خطرا على الفرد والمجتمع وعلى أمن الدولة¹ ، نتيجة للتقدم والتطور الرهيب في مجال تقنيات وسائل التكنولوجيا والمعلومات ،فمصطلح الجريمة الإلكترونية اصبح شائع ومتكرر على مسامعنا وعلى رفوف العدالة، فهو إحدى المصطلحات الحديثة المستخدمة التي تمثل افعال غير مشروعة تستند بالإنترنت لتنفيذها، الأمر الذي جعل مصطلحات الجريمة الإلكترونية متعددة من سببية او معلوماتية وغيرها، وذلك لنشأة وتطور ظاهرة الإجرام المرتبط والمتصل بتقنية تكنولوجيا المعلومات.

¹عبد العال الديري، محمد صادق إسماعيل، الجرائم الإلكترونية، دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والانترنت، ط1: المركز القومي للإصدارات القانونية، القاهرة، 2012، ص: 41

1.1- العنوان الفرعي الأول: مفهوم الجريمة الإلكترونية

يشكل مصطلح الجريمة السيبرانية أو الإلكترونية أو المعلوماتية إحدى المصطلحات الحديثة والمستخدمه عن جرائم الإنترنت الذي تعددت مصطلحاته وذلك لنشأة وتطور ظاهرة الإجرام المرتبط والمتصل بتقنية المعلومات، فمنهم من عرفها على أنها هي الجريمة التي تتم بواسطة الكمبيوتر أو أحد وسائل التقنية الحديثة على كمبيوتر آخر أو أحد وسائل أو أحد وسائل التقنية الحديثة، مع ضرورة توفر شبكة اتصال فيما بينهما.

والبعض الآخر عرفها على أساس أنها نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود، أو هي سلوك غير مشروع أو منافي للأخلاق الذي يكون مرتبط بالشبكات المعلوماتية العالمية، ومنه تعتبر جرائم العصر- الرقمي التي تطل بالمال والمعرفة والثقة والسمة وهي كلها تنفذ عن طريق التقنية.

ويمكن تعريف جرائم الانترنت بأنها مجمل الجرائم المرتكبة باستعمال المعلوماتية أو الشبكات المعلوماتية، وتكون هذه الجرائم ذات طبيعة متعددة، ويمكن أن تأخذ شكل الإجرام التقليدي باستعمال الوسائل التقنية للشبكات¹.

كذلك يمكن تعريف الجريمة الإلكترونية بأنها: "كل سلوك إجرامي يأتيه الجاني عن عمد، وسواء تم هذا السلوك باستخدام الحاسب الآلي أو شبكة الانترنت أو أي وسيط تقني آخر يكون هدفه الاعتداء على معطيات الحاسب الآلي أو شبكاته، وسواء نتج عن ذلك السلوك إلحاق خسارة أو فقدان حيازة أو ضياع ملكية للمجني عليه أم لا وسواء حصل الجاني على منفعة لنفسه أو لغيره أم لا، ويقرر له المشرع عقوبة جنائية أو تدبيرا احترازيا"².

فقهاء القانون لم يستقروا على تعريف واحد، وهذا أمر عادي يرجع لحداثة الجريمة الإلكترونية واختلافات الثقافات والقوانين بين الدول، وأيضا خشية في أن يحضروا المصطلح في نطاق ضيق أو محدد.

وبالتالي نستنتج أن الجريمة الإلكترونية أو المعلوماتية أو الافتراضية، هي أفعال غير مشروعة تستهدف إيذاء الآخر وتشويه سمعته أو إفشاء سر من الأسرار المهنية وغيرها من الأفعال المهددة لخصوصيات الأفراد، مما يؤدي إلى حصول المجرم الإلكتروني على فوائد مالية أو خدماتية أو معنوية انتقامية مقابل تحميل الضحية خسائر وتدميره، كل ذلك عن طريق استخدام والاستنجا بوسائل الاتصال والإعلام التكنولوجية في واقع افتراضي عابر للمسافات وللحدود.

¹ حامد علي، المعلوماتية وإجرام الانترنت، دار الفكر الجامعي، الإسكندرية، 2007، ص: 17

² حفوطة الأمير عبد القادر، الجريمة الإلكترونية وآليات التصدي لها، الملتقى الوطني: آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، الجزائر 2017، ص: 92.

2.1- العنوان الفرعي الثاني: الخصوصية والأمن في العالم الرقمي: التكامل والاختلاف

يعتبر الأمن والخصوصية تحدي ومفهوم معقد في العالم الرقمي، إذ تشير الخصوصية إلى حق الشخص في التحكم في كيفية الوصول إلى معلوماته واستخدامها، بينما يشير الأمن إلى الحماية من التهديدات أو المخاطر في العالم الرقمي، حيث يهدف بشكل عام إلى منع الوصول غير المصرح به إلى البيانات، على سبيل المثال من قبل المتسللين أو مجرمي الإنترنت. إذا كانت الخصوصية تتعلق بحق الفرد في إدارة معلوماته الشخصية، فإن الأمان يتعلق بحماية تلك المعلومات. كلاهما يمثل جوانب مهمة للأمن السيبراني¹.

يشير مفهوم خصوصية المعلومات الإلكترونية أو البيانات الرقمية كمفهوم مستقل على باقي مفاهيم الخصوصية إلى المؤلفين الأمريكيين WESTIN ALAN و MILAR في مؤلفهما الخصوصية والحرية، ان مفهومي الخصوصية المعلوماتية أو الرقمية مترادفان وما يفرقهما هو فقط أن الخصوصية المعلوماتية برزت في ظل ظهور الانترنت وتقنيات الاتصال الحديثة والفضاءات الرقمية، بينما الخصوصية عامة موجودة منذ القدم².

بالرغم من وجود نقاط مشتركة بين الأمن والسرية، إلا أن المفهومين يظلمان مختلفين. تتعلق السرية بمعلومات الفرد الشخصية بالإضافة إلى طرق الوصول إليها واستخدامها. ومن ناحية أخرى، يشير الأمن إلى حماية هذه البيانات والمعلومات. عند تنزيل تطبيق جديد على الهاتف الذكي، غالباً ما يُطلب منا الموافقة على سياسة الخصوصية. وهذا يشرح بالتفصيل المعلومات التي سيجتمعها التطبيق ولأي غرض سيتم استخدامه. الأمر متروك للفرد لتقرر ما إذا كان يقبل هذه الشروط أم لا. يتعلق الأمان بحماية البيانات والمعلومات، غالباً من خلال منتجات وتدابير الأمن السيبراني. الذي يستخدم تقنيات وأدوات الأمان لمنع الوصول غير المصرح به إلى بيانات الأفراد من خلال تسرب البيانات أو اختراقها³.

كما أنه يوجد فرق كبير بين الخصوصية والأمن: الأول يتعلق بكيفية التحكم في البيانات واستخدامها، في حين يهدف الأخير إلى حماية تلك البيانات. يمكن أن يوجد الأمن دون الخصوصية، ولكن العكس ليس صحيحاً. عندما يتعلق الأمر بإدارة المعلومات والبيانات الحساسة والشخصية، يعد الأمان والخصوصية ضروريين. بشكل عام، تشير الخصوصية إلى التفاصيل التي تهم الفرد بشكل مباشر وكيف يرغب في مشاركتها. الأمن يحمي الفرد من التهديدات المحتملة⁴. ولذلك، فإن الأمن السيبراني يتعلق بتأمين البيانات ضد الوصول أو الاستخدام غير المصرح به. عندما يتعلق الأمر بالبيانات، تتعلق الخصوصية بشكل مباشر بكيفية قيام الشركات بجمع وإدارة وتخزين ومراقبة استخدام البيانات التي تقدمها لهم. غالباً ما كانت الخصوصية تُعتبر ترفاً متاحاً لقلّة محظوظة فقط، في حين يعتبر الأمان منذ فترة طويلة أمراً ضرورياً. وكثيراً ما يحدث أن تكون السلامة العامة

¹ عدنان السيد، انتهاك حرمة الحياة الخاصة عبر الانترنت، مجلة دمشق للعلوم الاقتصادية، 2013، ص: 422.

² ليلى بن برغوث، الأمن السيبراني وحماية خصوصية البيانات الرقمية، المجلة الدولية للاتصال الاجتماعي، جامعة مستغافم، 2023، ص: 447

³ الشمري صلاح الدين، الأمن السيبراني كمرتكز جديد في الاستراتيجية العراقية، دار النشر العراق، 2020، ص: 62.

⁴ سعيداني نعم، آليات البحث والتحرّي عن الجريمة الإلكترونية، رسالة ماجستير في العلوم القانونية، جامعة الحاج لخضر باتنة، 2013، ص: 75.

سي مرابط شهرزاد

الأولية على فكرة حماية الحياة الخاصة؛ ومع ذلك، يمكن أن يصبح الافتقار إلى الخصوصية مشكلة تتعلق بالسلامة العامة لكن على الرغم من اختلافها، إلا أنه يجب الحفاظ على الأمن والسرية¹.

3.1- العنوان الفرعي الثالث: التقنيات المستخدمة في الجرائم الإلكترونية

أضحى من السهل الآن ارتكاب جريمة بمجرد التمكن واكتساب الخبرة من وسائل المعلوماتية التكنولوجية، حتى وإن هذه الأفعال تعتبر غير مشروعة ومتبكة للقانون والحقوق سواء الفردية أو الجماعية².

تتركز الجريمة الإلكترونية على مجموعة من التقنيات لتنفيذها وتحقيق أغراض المجرم المعلوماتي، وعلى أساسها الانترنت التي تجعل الاتصال سهل بين الأفراد والمختربين لنشر المعلومات الغير مشروعة وتشويه وتشهير الفضائح والأسرار الشخصية أو المهنية، كذلك هناك برامج خاصة لنسخ المعلومات المخزنة في جهاز الحاسوب للوصول الى بيانات سرية، استخدام تقنيات مدمرة لاختراق الأجهزة الحاسوبية تتركز الجريمة الإلكترونية على مجموعة من التقنيات لتنفيذها وتحقيق أغراض المجرم المعلوماتي، وعلى أساسها الانترنت التي تجعل الاتصال سهل بين الأفراد والمختربين لنشر المعلومات الغير مشروعة وتشويه وتشهير الفضائح والأسرار الشخصية أو المهنية، كذلك هناك برامج خاصة لنسخ المعلومات المخزنة في جهاز الحاسوب للوصول الى بيانات سرية، استخدام تقنيات مدمرة لاختراق الأجهزة الحاسوبية كبرامج حصان طروادة والدودة³.

تعتبر كذلك برامج التجسس من أخطر التقنيات التي يستخدمها المجرم المعلوماتي من خلال ربط الكاميرات بخطوط الاتصال الهاتفي للمراقبة عن بعد سواء بالنسبة للفرد بمحد ذاته أو بالنسبة للمؤسسات أو أجهزة الدولة، مما يشكل خطر ورعب حالي لدى مختلف دول العالم الذي أعلنت دخولها في عصر حرب المعلومات.

كل ذلك ولا زالت هناك تقنيات هائلة باتت توظف في مجال الهجمات السيبرانية يطلق عليها تسمية الأسلحة السيبرانية من أهمها: انترنت الأشياء- التزييف العميق- تقنية البلوك تشين- الحوسبة السحابية والتعلم العميق- التعلم الآلي... وغيرها، كل هذا سببه التقدم المتسارع الذي يشهده العالم في مجال الذكاء الاصطناعي والتطور التكنولوجي خلق تحديات كبيرة على صعيد تحقيق الأمن السيبراني وتعزيز الدفاعات السيبرانية للدول والمجتمعات مؤكدا على مجموعة من التكنولوجيات الحديثة التي ترتبط خاصة بالذكاء الاصطناعي.

2- العنوان الرئيسي الثاني: الجرائم الإلكترونية المستحدثة في قانون العقوبات رقم 24-06

نظرا لتزايد حجم التهديدات الرقمية وكثرة القضايا بخصوص الجريمة الإلكترونية وتطورها شيئا فشيئا، أصبح لزاما على المشرع مواكبة التطورات الرقمية وتعديل القوانين الخاصة بحماية الأفراد والمؤسسات والدولة من

¹ عدنان السيد، المرجع السابق، ص: 450

² ليلى برغوث، المرجع السابق، ص: 448

³ بن مرزوق عنتر، البعد الإلكتروني للسياسة الأمنية الجزائرية في مكافحة الإرهاب، مجلة العلوم الإنسانية والاجتماعية، 2018، ص: 38.

التصدي للجرائم الإلكترونية المنتهكة لخصوصية الأفراد في ظل قانون العقوبات رقم 24-06

هاجس التهديد الإلكتروني، وبالتالي أدخل المشرع على قانون العقوبات جرائم إلكترونية جديدة تمس بالحريات الفردية¹.

1.2- العنوان الفرعي الأول: تصنيفات الجرائم الإلكترونية

يعد الأمن السبراني أحد المداخل النظرية والتطبيقية الحديثة في صيانة الأمن الإلكتروني سواء للمؤسسات والحكومات أو خصوصيات الأفراد، فهو أداة فعالة تضمن حماية امن المعلومات وخصوصية البيانات الرقمية². إن الأمن السبراني يعد مجموعة من الأدوات التنظيمية والتقنية والإجرائية، والممارسات الهادفة إلى حماية أنظمة المعلومات والحواسيب والشبكات وما بداخلها من بيانات من الاختراقات أو تعطل الوصول للمعلومات أو الخدمات وحتى التهديدات الرقمية التي أصبحت في إطار الجريمة الإلكترونية.

أ- جرائم إلكترونية ماسة بالأفراد

اضحى عدد القضايا الإلكترونية الماسة بالأفراد بشكل عدد رهيب على رفوف العدالة، لكون ان أغلب الضحايا ليس لديهم فطنة الكترونية ودراية كافية حول تقنيات تكنولوجيا المعلومات، ومن اهم هذه الجرائم تهديد الافراد وابتزازهم لغاية مالية او خدمة غير مشروعة او شيء آخر يسبب الازى، وذلك من خلال استعمال التجسس وقرصنة الحسابات الإلكترونية والدخول في جهاز حاسوب الضحية الذي يحمل في طياته معلومات سرية وأشياء خاصة تجعله يهرب ويعيش مخاوف بمجرد كبسة زر من المجرم الإلكتروني.

كذلك من بين الجرائم الإلكترونية التي تمس فئة الافراد نجد انتحال المجرم الإلكتروني شخصية ما بهدف التوصل الى أسرار او معلومات مهمة قصد التشهير وتحقيق مكاسب مالية وافساد العلاقات الاجتماعية.

دخل في تصنيف الجرائم الماسة بالأفراد تشويه سمعة الضحية وتخطيها من خلال تزييف المعلومات وإخراج دعايات ونشرها على المواقع الإلكترونية سواء بنية الانتقام او لمرض نفسي في المجرم الإلكتروني.

كما يوجد نوع آخر من الجرائم الإلكترونية التي تمس بالأفراد وهي ابتزاز الضحايا بالقيام بأعمال غير مشروعة تتمثل في ترويج المخدرات أو الاختلاس أو الدعارة وغيرها من الأفعال التي يعاقب عليها القانون³.

ب- جرائم إلكترونية ماسة بالمؤسسات

يدخل العالم اليوم في مرحلة جد حساسة وهي حرب المعلومات، مما يعني ان أقوى الدول وأقوى الشركات والمؤسسات يجب ان يكون لديها جدار أمن محكم ضد الاختراقات والقرصنة من طرف مجرمي المعلوماتية، بحيث يتصيد هؤلاء المجرمون المؤسسات المالية من اجل سرقة الأموال، والشركات من اجل سرقة

¹ بن مرزوق عنتر، نفس المرجع السابق، ص: 42.

² ليلى برغوث، المرجع السابق، ص: 453.

³ حامد علي، المرجع السابق، ص: 38.

سي مرابط شهرزاد

منتوج أو معلومات سواء تفيد المجرم في مجالته أو لغرض تخطيم الشركة بدافع الانتقام، مما يكلف هاته المؤسسات والشركات خسائر سواء على الصعيد المهني أو المالي¹.

عندما نقول المؤسسات والشركات يعني عجلة الاقتصاد، فالدولة سواء بمؤسساتها عامة كانت أو خاصة، إذا تم اختراقها وقرصنتها من طرف مجرمي المعلوماتية ستتأثر بشكل كبير سواء من حيث الاقتصاد أو من حيث زعزعة الأمن والسرية والاستقرار، مما يستوجب من القائمين على مصلحة الاعلام الآلي تكوين وتعزيز قدراتهم في مجال تكنولوجيات الاعلام والاتصال ومواجهة المستجدات الرقمية والمعلوماتية الأمنية لمواجهة أخطار ومحاولات الاختراق اليومية، فدورهم اليوم يكتسي أهمية بالغة لدى الدولة بصفة عامة والمؤسسات بصفة خاصة².

ت- الجرائم الإلكترونية الماسة بالأموال

عندما نقول جريمة الكترونية ماسة بالأموال يأتي على بالنا مباشرة اختراق وسرقة الحسابات البنكية، سواء تعلق الامر ببطاقة ائتمان الأفراد أو حسابات المؤسسات البنكية عامة كانت أو خاصة،

لكن الأمر الذي لربما يخفى على الأغلبية أنه حتى التعدي على الملكية الفكرية والأدبية يعتبر جريمة الكترونية متعلقة بالأموال، سواء تعلق الامر بسرقة محتوى أو سيناريوهات أو مشروع منتج، وكلها تسبب أذى وضرر للضحية أو مؤسسة الإنتاج وصناعة البرامج وحتى يمكن أن تسبب له خسائر مالية فادحة³.

ث- الجرائم الإلكترونية الماسة بأمن الدولة

أصبحت الجرائم التي تهدد أمن وسلامة الدولة منتشرة وسهلة المنال وأحدثها الجرائم السيبرانية الإلكترونية القائمة على الجوسسة، وذلك من خلال انتشار العديد من برامج وتقنيات التجسس التي تستهدف الأغراض الاقتصادية والأمنية والاستراتيجية للبلاد، والتي يشغلها في أغلب الأحيان فرد يدخل للقطاع بشكل سلس أو يعمل فيها، يضع جهاز التجسس لخدمة أعداء الدولة والأطراف الخارجية بمقابل مالي أو خدمة أخرى، ليعمل هذا العدو على معرفة كل مستجدات القطاع الأمني أو اقتصادي أو الرئاسي، لغرض تخطيم وتدمير خطط و استراتيجيات النجاح والتقدم للدولة ومؤسساتها⁴.

كما يوجد نوع آخر يدخل في مطاف الجريمة السيبرانية الماسة بأمن الدولة وهي الموجهة من طرف الإرهاب لخلق الفوضى وزعزعة النظام العام والاستقرار في الدولة، من خلال الارتكاز على التضليل ونشر دعايات

¹ الامن السيبراني، وزارة البريد والمواصلات السلكية واللاسلكية من الموقع الإلكتروني: <https://fs.mpt.gov.dz/cybercriminalite>

² بن مرزوق عنزة، المرجع السابق، ص: 42.

³ محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الاسكندرية، 2007، ص: 153.

⁴ بوزيدي مختارية، ماهية الجريمة الإلكترونية، ملتقى وطني "آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، الجزائر، 2017، ص: 11.

التصدي للجرائم الإلكترونية المنتهكة لخصوصية الأفراد في ظل قانون العقوبات رقم 06-24

ومعلومات لا صحة لها¹، وللأسف نجد أغلب ضحاياهم الشباب الغير واعى والافراد الذي يكاد ينعدم فيهم الايمان والمواطنة الحقيقية، والنتيجة هي نزاعات دائمة وصراعات ولربما حرب أهلية، كل هذا بمجرد كبسة زر وبالأخص مع التطور السريع الذي يكتسح وسائل الإعلام والاتصال.

2.2 العنوان الفرعي الثاني: الجرائم الإلكترونية ضد الأفراد المستحدثة بموجب قانون العقوبات رقم 06-24

تسعى الجزائر جاهدة في مكافحة التهديدات الرقمية التي تمس خصوصية أفرادها وكذا مؤسساتها، وخير دليل على ذلك المرسوم الرئاسي الخاص بالأمن السيبراني لسنة 2020 الذي يقضي- بإرساء استراتيجية للأمن السيبراني وانشاء مجلس ووكالة للأمن السيبراني وكذا اعتماد نظام يقضه شامل يهدف التصدي للتهديدات الجديدة، وفي 2021 تم استحداث قطب جزائي جديد مكلف بمتابعة الجرائم السيبرانية ومكافحتها²، وفي 2024 تم تعديل قانون العقوبات وازافة جرائم الكترونية تواكب التطور الرقمي وتتصدى لكثرة القضايا بخصوص التهديدات الرقمية المنتهكة لخصوصية الأفراد.

أولا: جريمة النشر الإلكتروني أو التهديد به دون إذن صاحبه:

يعتبر هذا العنصر الإجرامي الجديد في قانون العقوبات بمثابة مواكبة للتطورات التكنولوجية الإلكترونية التي أصبحت حديث الساعة والمعاملات، والواقع الملموس التي شهدته التبليغات لدى مصالح الشرطة وعدد القضايا المرفوعة لدى المحاكم القضائية، للانتشار الواسع في مشاركة خصوصيات المرء لدى مواقع التواصل الإلكتروني وبالأخص بدون إذن أو رخصة من صاحبها، مما دفع بالمشروع الجزائي بتجريم هذا النوع من الاعمال حفاظا على النظام العام وكيان الدولة بحماية رعاياها وتوفير الأمن السيبراني في ظل التهديدات والمخاطر الإلكترونية العديدة، وتطبيقا لمبدأ مكافحة الجريمة السيبرانية وحماية الخصوصية الفردية في ظل حقوق الإنسان جاء المشروع بنص المادة 333 مكرر³ الذي يتمحور فحواها على كل شخص ينشر- محتوى فيه صور او رسائل الكترونية او فيديوهات لشخص آخر دون اذنه ويقصد الإضرار به يعاقب بالحبس من ثلاث سنوات الى 7 سبع سنوات.

كما تضعف العقوبة في حال ما إذا تم تهديد الضحية بالنشر وتشويه السمعة بغرض الحصول على فائدة مادية أو خدمة أو شيء آخر.

¹ حفظة الأمير عبد القادر، الجريمة الإلكترونية وآليات التصدي لها، الملتقى الوطني: آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، الجزائر 2017، ص: 94.

² مجلة الجيش، ديسمبر 2022.

³ -المادة 333 مكرر 4 من قانون العقوبات سالف الذكر.

سي مرابط شهرزاد

مما نستنتج أن إطار التلاعب بخصوصيات المرء في مواقع التواصل الاجتماعي تم التصدي له بقوة حتى وإن جاء متأخرا نوعا ما إلا أنه اليوم نقف امام مجرمي الإلكترونيات أحسن من الغد المتأزم الذي يحمل الدولة تبعات حفظ النظام العام وجرائم جديدة معقدة ومستعصية لربما تؤدي إلى عصيان وانفلات الشباب.

ثانيا: جريمة النشر الإلكتروني أو التهديد به اثناء قيام الرابطة الزوجية او الخطوبة:

بدا بالبدا تعرف الخطوبة على أنها طلب الخاطب ليد مخطوبته لإنشاء مشروع زواج ، فإذا تمت الامور حسب رضا وتفاهم الطرفين قامت الرابطة الزوجية بالزواج، أما إذا اختلف الطرفان تنتهي هاته الخطوبة في شكلها العادي حسب ما هو متعارف عليه، وفي بعض الأحيان أحد أطراف العلاقة يصبح يهدد الطرف الاول بنشر خصوصيات الطرف الثاني أو ينشرها بالفعل مما يأزم الحال ويدفعه لباب القضاء لإيقاض سمعته وشرفه وغيرها من الأمور الشخصية، لكن قبل صدور القانون رقم 06-24 المتعلق بقانون العقوبات¹ لم يكن هناك إطار قانوني خاص بتجريم هاذ النوع من الأفعال مما زاد الطين بلة وأصبح النشر- والتهديد بالنشر على مواقع التواصل الاجتماعي من الأمور الرائجة والتي تحصل على مشاهدات عالية هدفها سواء كان الانتقام المعنوي أو الربح المالي نتيجة المشاهدات التي تحصل عليها الفيديو او الصور.

هذا ما دفع المشرع الجزائي لوضع إطار قانوني خاص بالجرائم الإلكترونية في بندها الثاني الخاص بالعلاقات سواء الخطوبة او الرابطة الزوجية للحد من هاته التطاولات والمساس بالخصوصيات وبالتالي انتهاك الحرمات، جاءت المادة 333 مكرر 05² واضحة بهذا الخصوص وعاقبت بالحبس كل من ينشر صور تمس بحياء وشرف الزوج أو الخاطب سواء أثناء الخطوبة أو عند قيام الرابطة الزوجية بخمس سنوات5 إلى عشر- سنوات 10 وغرامة مالية من 500.000دج إلى 1.000.000دج.

ثالثا: جريمة منصوص عليها قانونيا ترتكب او يسهل ارتكابها تكنولوجيات الإعلام والاتصال:

كآخر جديد بخصوص ضبط الإطار القانوني الخاص بالتجريم الإلكتروني وضبط النظام العام وحفظ عدالة وكيان الدولة، زاد المشرع الجزائي بتوسيع دائرة الجرائم الإلكترونية، وأفاد في نص المادة 333 مكرر 6³ على مضاعفة العقوبة في الجرائم التي يتم فيها استعمال تكنولوجيات الاعلام والاتصال وبالأخص جرائم التهديد وافشاء السر المهني والسب وغيرها من الجرائم الماسة بالأفراد.

مما يعني أن كل ما هو مجرم ومعاقب عليه في القانون يضاعف العقوبة عليه في حال ما تم الاستعانة بالوسائل التكنولوجية الخاصة بالإعلام والاتصال، وهذا يعتبر نقطة جيدة انتبه إليها المشرع لمنع التجاوزات والنشر- على نطاق واسع بممارسة الجريمة علنا.

¹ القانون رقم 06-24 المتعلق بقانون العقوبات، المرجع السابق.

² القانون رقم 06-24 المتعلق بقانون العقوبات، المرجع السابق.

³ المادة 333 مكرر 6 من القانون رقم 06-24 المتضمن قانون العقوبات، نفس المرجع السابق.

التصدي للجرائم الإلكترونية المنتهكة لخصوصية الأفراد في ظل قانون العقوبات رقم 24-06

وبطبيعة الحال يخطو المشرع خطوة أخرى موفقة من خلال الردع لمرتكي الجرائم الإلكترونية من خلال مصادر الأموال المتحصل عليها وكل الأجهزة والحسابات والمحلات التي سهلت من عمل ارتكاب الجريمة طبقاً للمواد 333 مكرر 4 ومكرر 5 ومكرر 6¹.

هذا ما يجعلنا نستنتج ان حجم العقوبة لا يقتصر بالحبس والغرامة على الشخص فقط، وإنما الأمر أبعد بكثير، بما أن الجرائم الإلكترونية هي جريمة من نوع خاص يجب كذلك التصدي للوسائل الإلكترونية المستعملة، مواقع التواصل الاجتماعي والمواقع الإلكترونية بصفة عامة التي تم استغلالها أثناء الجريمة حتى يتم القضاء على عنصر- التجريم من أساسه وحماية خصوصية الأفراد وسريتهم والتحكم في زمام الامور.

خاتمة:

نتيجة للتطور العلمي الهائل، فإن الإيجائيات التي جلبتها المعلوماتية قد جلبت الى جانبها أيضاً مخاطر عدة ناجمة عن إساءة استخدام شبكة الانترنت وتطويعها لصالح المجرم المعلوماتي لممارسة نشاطاته الإجرامية، وعليه أحيانا ارتفاع مستوى التعليم يؤدي الى رفع مستوى الأداء الإجرامي للمجرمين المحترفين، أي مستوى الاحتراف، ومن ثم تؤدي الى ارتكاب أفعال إجرامية أكثر دقة وتخطيط، وأكثر براعة في التنفيذ وهذا من شأنه أن يصعب إمكانية اكتشافها، فالتقنية الحديثة سهلت ظهور طائفة جديدة من الجرائم المستحدثة، والتي تعجز النصوص العقابية التقليدية مواجعتها، وعليه لابد من تحيين النصوص القانونية بشكل مستمر وفق المستجدات الرقمية وكذا رسم استراتيجية شاملة للجهاز الامني من خلال التدريب والتكوين الرقمي .

هذه اهم التوصيات التي نقترحها:

- تحيين القانون الجزائي والاجرائي بشكل مستمر لمواكبة التطورات الرقمية والتقنية.
- إنشاء أجهزة أمنية وقضائية متخصصة في الجرائم المعلوماتية.
- إنشاء أكاديميات تقنية قضائية لإعداد وتأهيل الخبراء القضائيين في مجال الجرائم الإلكترونية.
- حجب المواقع الإلكترونية المشبوهة التي تسعى الى نشر الارهاب والرذيلة والافكار المتطرفة.
- تعزيز التعاون الدولي من خلال مراقبة كل دولة للأعمال الاجرامية التخريبية الإلكترونية.
- توعية مستخدمي الانترنت والحاسب الآلي حول خطورة الجرائم الإلكترونية، واعلامهم بإجراءات التصرف في حال وجود تهديد او ابتزاز الكتروني بوقوع جريمة.

¹ القانون رقم 24-06 المتعلق بقانون العقوبات السالف الذكر.

سي مرابط شهرزاد

- ضرورة تخصيص شرطة خاصة لمكافحة الجريمة الإلكترونية وذلك لأننا دخلنا عصر- أو حرب المعلومات.
- تنسيق وتوحيد الجهود بين الجهات القضائية والتشريعية والضبطية والفنية، وذلك من أجل سد منافذ الجريمة الإلكترونية قد المستطاع والعمل على ضبطها وإثباتها بالطرق الفنية والقانونية.
- تفعيل الدور الوقائي الذي يسبق وقوع الجريمة الإلكترونية، وذلك من خلال تفعيل دور المؤسسات التربوية والدعوية كالمسجد والمدارس والجامعات وأجهزة الاعلام والصحافة، وذلك بالتوعية بخطورة هذه الجرائم على الأسرة والمجتمع والسعي في تقوية الوازع الديني.
- تعزيز التعاون والتنسيق مع المؤسسات الدولية المعنية بمكافحة الجرائم المعلوماتية، وخصوصا الانترنت.

قائمة المراجع:

الكتب:

- (1) الشمري صلاح الدين، الأمن السيبراني كمرکز جديد في الاستراتيجية العراقية، دار النشر العراق، 2020.
- (2) حامد علي، المعلوماتية وإجرام الانترنت، دار الفكر الجامعي، الإسكندرية، 2007.
- (3) عبد العال الديري، محمد صادق إساعيل، الجرائم الإلكترونية، دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والانترنت، ط1: المركز القومي للإصدارات القانونية، القاهرة، 2012.
- (4) محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الاسكندرية، 2007.
- (5) محمود مدين: الجريمة الإلكترونية وتحديات الأمن القومي، ط2، المصرية للنشر والتوزيع.

الرسائل الجامعية:

- (1) سعيداني نعيم، آليات البحث والتحري عن الجريمة الإلكترونية، رسالة ماجستير في العلوم القانونية، جامعة الحاج لخضر باتنة، 2013.

المجلات والمقتنيات:

- (1) بن مرزوق عنتر، البعد الإلكتروني للسياسة الأمنية الجزائرية في مكافحة الإرهاب، مجلة العلوم الإنسانية والاجتماعية، 2018.
- (1) بوزيدي مختارية، ماهية الجريمة الإلكترونية، ملتقى وطني "آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري"، الجزائر، 2017.

التصدي للجرائم الإلكترونية المنتهكة لخصوصية الأفراد في ظل قانون العقوبات رقم 24-06

- (2) حفوظة الأمير عبد القادر، الجريمة الإلكترونية وآليات التصدي لها، الملتقى الوطني: آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، الجزائر 2017.
- (3) ذياب موسى البداينة، ورقة علمية بعنوان: الجرائم الإلكترونية المفهوم والأسباب، الملتقى العلمي: الجرائم المستحدثة في ظل المتغيرات والتحول الإقليمي والدولية، عمان، المملكة الأردنية الهاشمية، 2013.
- (4) عدنان السيد، انتهاك حرمة الحياة الخاصة عبر الانترنت، مجلة دمشق للعلوم الاقتصادية، 2013.
- (5) ليلي بن برغوث، الأمن السيبراني وحماية خصوصية البيانات الرقمية، المجلة الدولية للاتصال الاجتماعي، جامعة مستغافم، 2023
- (6) مجلة الجيش، ديسمبر 2022.

النصوص القانونية:

- (1) القانون رقم 06-24 المؤرخ في 28 أبريل 2024 المتعلق بقانون العقوبات، يعدل ويتم الأمر رقم 66-156 المؤرخ في 8 جويلية 1966 والمتضمن قانون العقوبات.

المواقع الإلكترونية:

¹ - الإنترنت: الجريمة السيبرانية عبر الموقع الإلكتروني: <https://www.interpol.int/ar>

¹ - الأمن السيبراني، وزارة البريد والمواصلات السلكية واللاسلكية من الموقع الإلكتروني:

<https://fs.mpt.gov.dz/cybercriminalite/>