استمارة المشاركة:

الاسم واللقب: هرندي كريمة

الرتبة: أستاذة محاضرة أ

مؤسسة الانتماء: جامعة محمد بن أحمد وهران2. الجزائر.

البريد الالكتروني:harendikarima@gmail.com

المحور03: جهود الدولة الجزائرية في مواجهة تهديدات الأمن السيبراني.

عنوان المداخلة: التشريع القانوني وهندسة التأثير للجريمة السيبرانية في ظل التطور التكنولوجي.

الملخص:

لقد أصبح العالم والمجتمعات البشرية عبارة عن بوابة تطل علة كل مجريات أحداث العالم في أي نقطة من نقاطه، مع تكنولوجيات الاتصالات المتنوعة، في تجربة لا تعترف بحدود أو إقليم، تكتسح تلك المعالم لتصنع عالما خاصا بها، في دورة انتشار واستعمال لها من قبل أفراد ابتكروا فنيات وتطبيقات تصنع من المخفي ظاهر في عالم الكتروني، تسيرها أفعال أفراد بوجهات وأهداف متعددة قد يكون فيها المنطلق معروف لكن أبعادها وتجلياتها تتخذ منحنيات ومسارات لا يمكن التمكن من رصدها بشكل مستمر، ليصبح الفعل الاجتماعي هذا ممارسة فعلية متمرسة لأفراد معينون، فتصنع من الفعل العادي فعل إجرامي ينتهك كل الحدود القانونية والجغرافية في هندسة تخطيطية مسبقة. إنّها الجريمة الالكترونية وما تحمله من توظيف لاستراتيجيات وتقنيات وحيل متنوعة وفقا لإطار زماني يعتمد على السرعة والدقة في التنفيذ في سياقات تجعل من هذا الفعل الالكتروني جريمة حقيقة إذ ما ألحقت الأضرار بالأفراد، فالمجتمعات، في مداخلتنا سوف نركز على ثنائية الجريمة الالكترونية والإجراءات، خاصة في ظل ما أصبحنا نعيشه من تدابير مراقباتية صارمة في هذا المجال بالتحديد، وعليه **ما المقصود بالجريمة الالكترونية؟ وما هي أهم الخصائص المنوط بها، وأين يكمن تأثيرها؟**

الكلمات المفتاحية: جريمة الكترونية، مجتمع، عابرة حدود، تأثير، تكنولوجية الاتصال.

The world and human societies have become a portal overlooking all the events of the world at any of its points, with various communication technologies, in an experiment that does not recognize borders or territory, sweeps those landmarks to create a world of its own, in a cycle of spread and use by individuals who have created techniques and applications that are made criminal violates all legal and geographical boundaries in engineering Pre-Schematic. It is a cyber crime and the use of various strategies, techniques and tricks in accordance with a time frame based on speed and accuracy in implementation in contexts that make this electronic act a real crime if it has caused damage to individuals, societies, in our intervention we will focus on the duality of cyber crime and procedures, especially in light of what are its most important characteristics, and where does its impact lie

Keywords: cyber crime, society, cross-border, Influence, Communication Technology.

" التشريع القانوني وهندسة التأثير للجريمة السيبرانية في ظل التطور التكنولوجي "

د.هرندي كريمة[1]

1. مقدمة:

إنّ مصطلح الجريمة الالكترونية ليس بالمصطلح الجديد، إذ أن وجوده اقترن بذيوع تكنولوجيات الاتصال، والاستخدام الواسع لها لاسيما بالآونة الأخيرة، وفي ظل ما أصبحت تعيشه المجتمعات البشرية قاطبة دونما استثناء من انتشار الوباء بات الاستخدام والإقبال على هذه التكنولوجيات كبيرا إلى درجة الإدمان، لتتعدد صيغ هذا النوع من الجرائم بتعدد وتنوع مستخدميها.

اختراع وسائل وتكنولوجيات الاتصال كانت بمثابة حدث عالمي مذهل، ونتيجة عصارة بحث العقل البشري لسنوات طوال، فمع ظهور الحاسب الآلي بدأت البشرية تتجه نحو مسار جديد من مسارات الاختراعات الاتصالية، لخدمة الفرد والمجتمع معا في مجالات متعددة، ليعرف بعدها هذا الاستخدام زيغ فعلي عن المسار الذي أوجدت من أجله والهدف الذي اخترعت له، لتتحول من مسار النفع العام إلى خدمة مسار الجريمة الالكترونية. فأضحت بذلك هذه الوسيلة السبيل الأمثل والأبسط لتحقيق المشروع الإجرامي التكنولوجي لممارسي هذا الفعل الإجرامي، من دون أن يعرف هذا الفعل الركود أو الثبات من حيث الابتداع والتنويع فيه، الأمر مقترن في حقيقته بتنوع الوسائل التكنولوجية، وتعدد النسخ الابتكارية فيها، فمع كل ابتكار جديد تفنن وتطوير لهذه الجريمة، مع ابتكار رموز وخطط خاص بهؤلاء الفاعلون، لا تقف عملية حلها عند رجالات القانون فقط بل كل المختصين في مجالات المجتمع بشكل عام؛ كون أنّ هذه العملية القائم بها والمتضرر من ورائها هو القاسم المشترك بين كل العلوم الإنسانية والاجتماعية قاطبة "**الإنسان**" اللغز الذي لا تزال العلوم تبحث في تفسير أفعاله المتنوعة والمتداخلة مع أفعال تتسم بطابعها المتعدد، في ترجمة نوعية لها من خلال ممارساته المتنوعة وعلى مستويات مختلفة في كل المجالات.

---

[1]- أستاذة محاضرة صنف أ، كلية العلوم الاجتماعية، جامعة محمد بن أحمد وهران2-الجزائر.

إنّ غالبية الدول سعت إلى إيجاد قاعدة قانونية جد صارمة بحق مثل هكذا ممارسات تهدد أمن المجتمعات، مع السعي على مضض تحديث هذه القاعدة تماشيا مع تطور واستحداث آليات هذا الفعل المقترن مع التطور المستمر لتكنولوجيات الاتصال، لذلك تسعى إلى إتباع أسلوب التجديد في هذه التشريعات المتعلقة بمثل هذا النوع من الممارسات. لكن بالرغم من هذه القاعدة التشريعية القانونية التحديثية لمواجهة الجريمة الالكترونية إلاّ أنّ هذا الأمر وحده غير كاف بل يحتاج إلى نشر سياسة الوعي الاجتماعي والثقافي لمعرفة حيثيات وعناصر وأساليب وتبعات هذه الجريمة لخلق رد فعل وقائي يساهم في التقليل من أخطار وتبعات هذه الجريمة على الأفراد والمجتمعات؛ خاصة وأنّ ممارسة فعل الجريمة الالكترونية لم يعد فعل نادر الوقوع بل يحدث بوتيرة مستمرة وفي أي وقت وحين.

هذه المداخلة تسعى إلى إبراز أهمية الوعي الاجتماعي والتشريعات القانونية في الوقوف بوجه هذه الجريمة للحد من تبعاتها وأضرارها الوخيمة والجسيمة.

2. **تعريف الجريمة الإلكترونية:**

لقد خلقت الثورة المعلوماتية العديد من الممارسات الإيجابية والسلبية، ومن بين هذه الأخيرة الجريمة الإلكترونية التي تعد"كل سلوك إجرامي ترتكبه مجموعة من الأشخاص يحترفون الإجرام بشكل مستمر لتحقيق أهدافهم ضمن نطاق أكثر من دولة" (الجنيبي خالد علي، 2015، صفحة 82). تعرف الجريمة الإلكترونية بعدة تسميات منها الجريمة المعلوماتية، جرائم إساءة استخدام لتكنولوجيات المعلومات والاتصال، الجريمة الناعمة، إساءة استخدام الكمبيوتر، الجريمة المرتبطة بالكمبيوتر، احتيال الكمبيوتر، جرائم الإنترنيت...، كلها تسميات لمثل هذا النوع من الجرائم والممارسات المنافية لنظام الدول الداخلي وكذا الخارجي على حد سواء.

يعرِّف القانون الأمريكي الجريمة الالكترونية بأنّها " الاستخدام الغير مصرح به لأنظمة الكمبيوتر المحمية أو ملف البيانات أو الاستخدام المتعمد الضار لأجهزة الكمبيوتر أو ملفات البيانات وتتراوح خطورة تلك الجريمة ما بين جنحة من الدرجة الثانية إلى جناية من الدرجة الثالثة" (يوسف خليل يوسف العفيفي، 2013، صفحة 07)

بالنسبة لمؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد في فينا 2000 فقد عرّف الجريمة الالكترونية بأنّها "أيّة جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب، والجريمة تلك التي تشمل من الناحية المبدئية

جميع الجرائم التي ارتكابها في بيئة الكترونية" (حوالف حليمة، 2021، الصفحات 142-143). أي أنّ أصل ممارسة هذه الجريمة هو الحاسوب مع شبكة الانترنيت كثنائيين وعاملين فاعلين في حدوثها، في وسط الكتروني يكون فيه الضحية أي فرد له علاقة بهذين العاملين. وتعرّف كذلك الجريمة الإلكترونية بأنّها "أيّ فعل يرتكب متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام" (يوسف خليل يوسف العفيفي، 2013، صفحة 07)، من خلال هذين التعريفين للجريمة الإلكترونية نلاحظ بأنّ هذا النوع من الأفعال يقوم على فكرة المخالفة الفعلية لنظام معلومات أي مجتمع من المجتمعات واستخدام غير مصرح به، لم يلحقه من ضرر للمجتمعات التي اخترق نظام معلوماتها، فهذا الفعل ليس لصيق في تأثيره بالفرد بل المجتمع ككل حسب ما أشار إليه هذان التعريفين.

تعرف الجريمة الالكترونية بأنّها " فعل غير شرعي يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازم لارتكابه من ناحية لملاحقته وتحقيقه من ناحية أخرى... وتعد كذلك كل نشاط غير مشروع موجه لنسخ أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو تغييرها أو حذفها أو التي تحول عن طريقه" (عائشة نايري، 2017/2016، الصفحات 06-07)، من خلال هذا التعريف يتضح لنا بأنّ الجريمة الالكترونية هو فعل غير شرعي ونشاط غير مشروع مدام الأصل فيه إلحاق الضرر من خلال محاولة الاطلاع على معلومات ليست بالمعلومات المتعلقة بالشخص ذاته بل بحواسيب أشخاص آخرين دون علمه. تتوقف تعريفات "الجريمة السيبرانية" "في المقام الأول على الغرض من استخدام المصطلح. فالجريمة السيبرانية الأساسية تتمثل في عدد محدود من الأعمال التي تمس بسرية البيانات أو النظم الحاسوبية وسلامتها وتوافرها. أمّا الأعمال المنفذة بواسطة الحواسيب والرامية إلى تحقيق مكاسب شخصية أو مالية أو إحداث أضرار، بما في ذلك أشكال الجريمة المتصلة بالهوية وبمحتوى الحواسيب والتي تندرج كلها ضمن نطاق أوسع من معنى مصطلح الجريمة السيبرانية، فلا يمكن تطويعها بسهولة لتنضوي ضمن تعريفات قانونية لمصطلح جامع.

ويلزم تعريف الأعمال الأساسية التي تُشكِّل جريمة سيبرانية، وإن كان تعريف الجريمة السيبرانية لا يتسم بنفس القدر من الأهمية فيما يخص الأغراض الأخرى، كتحديد نطاق صلاحيات الهيئات المختصة بالتحريات والتعاون الدولي، حيث يفضل التركيز على الأدلة الإلكترونية فيما يخصّ أي جريمة، بدلا من التركيز على تركيبة واسعة واصطناعية لـ" الجريمة السيبرانية" (مكتب الأمم المتحدة ، فبراير2013، صفحة 23)، من خلال هذا

التعريف الذي أقرته هيئة الأمم المتحدة حول الجريمة السيبرانية فإنّها ركّزت في تعريفها على النقاط الآتية:

- عدد محدود من الأعمال التي تمس بسرية البيانات أو النظم الحاسوبية وسلامتها وتوافرها.
- أشكال الجريمة المتصلة بالهوية وبمحتوى الحواسيب.

ولإدانة هذه الجريمة حسب ذات التعريف لابد من ضرورة وجود أدلة إلكترونية تثبت الفعل الإجرامي.

وتعرّف كذلك الجريمة السيبرانية بأنّها "نشاط إجرامي تستخدم فيه التقنية الالكترونية الحاسوب الآلي الرقمي وشبكة الإنترنيت بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الفعل الإجرامي المستهدف... وهي جرائم الشبكة العالمية التي يستخدم الحاسب وشبكاته العالمية كوسيلة مساعدة لارتكاب جريمة مثل استخدامه في النصب والاحتيار وغسل الأموال وتشويه السمعة والسب" (صغير يوسف، 2013، صفحة 8).

إذن إنّ مسألة وضع تعريف جامع لـ"**الجريمة السيبرانية**" غير وارد نظرا لتعدد أبعاد تحليل هذا الفعل كمفهوم وممارسة بالآن ذاته، ولتعدد زوايا تناول هذا الموضوع كتقنية وفنية تكنولوجية من زاوية قانونية، أو كفعل اجتماعي إجرامي من الناحية الاجتماعية، لذلك تعددت واختلفت الرؤى التحليلية لهذا المفهوم من منطلق ما تم ذكره سالفا، ولكن معظم التعريفات التي تضمنتها مداخلتنا ركّزت على النقاط الآتي ذكرها:

- الجريمة السيبرانية فعل غير مشروع ونشاط إجرامي.
- الجريمة السيبرانية تعتمد على استغلال المعلومات دون إذن.
- الجريمة السيبرانية اختراق لأنظمة الحواسيب.
- الجريمة السيبرانية ظاهرة عابرة للحدود.
- الجريمة السيبرانية تمس سرية البيانات والمعلومات التي يمتلكها الأفراد أو المؤسسات.
- الجريمة السيبرانية تتنوع أغراضها وتتعدد تقنياتها بتعدد تكنولوجيات المعلومات.
- الجريمة السيبرانية استخدام غير مصرح للمعلومات والبيانات لذا تعد قانونيا جنحة.

هناك العديد من المجالس الدولية والعالمية والاتفاقيات التي استنكرت لشرعية هذا الفعل الإجرامي في دوراتها من بينها:

-الجماعة الاقتصادية لدول غرب إفريقيا (ايكواس)، 2009، مشروع توجيهي بشأن مكافحة الجريمة السيبرانية داخل دول غرب إفريقيا.

-الاتحاد الأوروبي 2010، المشروع 517 النهائي التوجيهي للبرلمان الأوروبي ومجلس أوروبا بشأن الهجمات ضد نظم المعلومات واستبدال القرار لإطاري للمجلس.

-الاتحاد الدولي للاتصالات/جماعة الكاريبيه/الاتحاد الكاريبي للاتصالات،2010. النصوص التشريعية النموذجية بشأن السيبرانية/ الجرائم الالكترونية والأدلة الالكترونية (الاتحاد الدولي للاتصالات/ الجماعة الكاريبية/ النصوص التشريعية النموذجية للاتحاد الكاريبي للاتصالات.

-جامعة الدول العربية 2004، القانون العربي النموذجي لمكافحة الجرائم المتعلقة بنظم تكنولوجيا المعلومات.

-جامعة الدول العربية، 2010، الاتفاقية العربية بشأن مكافحة جرائم تقنية المعلومات (اتفاقية جامعة الدول العربية).

- منظمة شنغهاي للتعاون 2010، اتفاقية التعاون في مجال أمنت المعلومات الدولية.

3. **خصائص الجريمة السيبرانية:**

تتميز الجريمة السيبرانية بمجموعة من السمات والخصائص من بينها:

-أنّها مستترة وتتم في كامل السرية، لذلك من الصعوبة اكتشافها وإثباته.

-أنّها ظاهرة عالمية لها مخاطر وأضرار متنوعة.

-تقوم على اختراق نظام الحواسيب من أجل المعلومات التي تحتويها لاستغلالها في أغراض معينة.

-نشاط إجرامي يستخدم فيه الحاسب الآلي بطريقة مباشرة أو مباشرة لتحقيق هدف معين.

-تتسم هذه الجريمة بالسرعة والتطور في رسائل ارتكابها.

-أقل عنف في التنفيذ من الجرائم التقليدية.

-هي جريمة عابرة للحدود.

-صعوبة إثباتها لعدم وجود أدلة مادية عنها نظرا لسهولة إتلافها.

4. **القاعدة القانونية في مواجهة الجريمة الالكترونية:** تقوم قاعدة الدول والمجتمعات قاطبة على العديد من السياسات في محاولة مواجهتها للجريمة السيبرانية وتدابير إستراتيجية تسعى كلها إلى التقليل من احتمالات حدوث مثل هذا النوع من الجرائم ومحاولة التقليل من أضرارها، فحسب الدراسة التي قامت بها الأمم المتحدة في مشروع مواجهة مثل هذا النوع هو أنّ الممارسات الجيدة في مجال منع الجريمة السيبرانية يتمثل في كل من:

- ❖ نشر التشريعات.
- ❖ القيادة الفعالة.
- ❖ تنمية القدرات على صعيد العدالة الجنائية وإنقاذ القانون والتعليم والتوعية.
- ❖ إنشاء قاعدة معرفية قوية.
- ❖ التعاون بين الحكومات والمجتمعات المحلية والقطاع الخاص.

هناك تحد كبير في مواجهة مثل هذا النوع من الجرائم، ومرد ذلك إلى أنّ الجريمة السيبرانية في تطور مستمر مقترن بشكل أساسي بالتطور المستمر لتكنولوجيات المعلومات، وهذا التحد والصعوبة الحقيقية راجع إلى كل من (إبراهيم رمضان إبراهيم عطايا، 2015، الصفحات 374-375):

- ✓ عدم وجود اتفاق عام بين الدول على مفهوم الجرائم الإلكترونية، وبالتالي عدم وجود توافق في القوانين.
- ✓ النقص الظاهر في مجال الخبرة لدى رجال الشرطة.
- ✓ الاعتداء على برامج ومعلومات الحاسب يجعلنا أمام مشكلة قانونية ذات طبيعة خاصة.
- ✓ ظهور وتنامي الأنشطة الإجرامية الالكترونية وتوصل مرتكبيها بتقنيات جديدة غير مسبوقة في مجال تكنولوجيا المعلومات والاتصالات.
- ✓ الأنماط الجديدة للجريمة السيبرانية.

إنّ العالم ككل يسعى إلى وضع حد من استفحال هذه الظاهرة، في محاولة منها العمل في وجود ترسانة قانونية متجددة بتجدد وبتطور تكنولوجيا الاتصال من أجل التخفيف من تبعات هذه الجريمة، والتقليل من الأضرار الناجمة عنها، والجزائر واحدة من بين هذه الدول تحاول بصورة مستمرة في إنشاء خلية تقصي الكترونية تعمل على تتبع مثل هذا النوع من الجرائم، إضافة إلى تخصيص مواد في القانون الجزائري خاصة بهذا النوع من الجرائم من مثل: "المادة 13 من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وحسب نص المادة الثانية من المرسوم الرئاسي 19-127، هذه المادة نصت على إنشاء هيئة التي تعد مؤسسة عمومية ذات الطابع الإداري تتمتع بالشخصية المعنوية والاستقلالية المادية توضع تحت سلطة وزارة الدفاع" (حوالف حليمة، 2021، صفحة 151). إذن توجد هيئة تسيرها شخصية معنوية تشرف على عملية ترصد ممارسة الجرائم الالكترونية تشرف عليها وزارة الدفاع الوطني؛ كون أنّ الجريمة السيبرانية جريمة عابرة للحدود وليس فقط متمركزة داخل المجتمع الواحد فقط.

لقد عرّف المشرع الجزائري واصطلح على تعريف الجريمة الالكترونية بالجريمة المتصلة بتكنولوجيا الإعلام والاتصال، من خلال "التعريف الذي جاءت به الاتفاقية الدولية للإجرام المعلوماتي، بموجب المادة الثانية من القانون04/09... فعرّفها على أنّها جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية" (ونوغي نبيل، 2019، صفحة 132)، من خلال هذا التعريف يتضح بأنّ المشرع الجزائري قد أورد نص قانوني للوقوف بوجه هذا النوع من الجرائم، المتصل بنظامي المعلومات والاتصالات، وأي اختراق لهما يترتب عنها عقوبة قانونية الهدف الأساسي منها الحد من هذه الجريمة.

إنّ القاعدة القانونية تختلف في الجريمة الالكترونية عنها في الجريمة التقليدية نظرا لخصائص كل واحدة منهما على حدا، ما يوضحه الجدول الآتي (ذياب موسى البداينة، 2014، صفحة 05):

الجريمة التقليدية	الجريمة الالكترونية
الاحتيال	الاحتيال على الشبكة ، الاحتيال بالمزاد الالكتروني...
السطو	القرصنة على الإنترنيت، الحرمان من الخدمة، الفيروسات.
جرائم الأطفال الجنسية	استمالة الأطفال على النات، المواقع الإباحية.
غسيل الأموال	أنظمة الدفع على الشبكة
السرقة	جرائم الهوية، وسرقة الملكية

لقد جرّم المشرع الجزائري كل اعتداء على معطيات النظام؛ كونه جرما ليس بالهين، لما له من تبعات جد خطيرة على الفرد والمجتمع فالمجتمعات فيما بينها قاطبة، حيث أنّ هذا الاعتداء يتخذ صورتين أو شكلين ألا وهما:

1-**الاعتداء على المعطيات الداخلية للنظام** (براهيمي جمال، /، الصفحات 133-134):

فقد جرّم المشرع الجزائري أي اعتداء يقع على المعطيات الموجودة داخل نظام المعالجة الآلية من خلال المادة 394 مكرر1 قانون العقوبات التي تنص على أنّه **يعاقب بالحبس من 6 أشهر إلى 3 سنوات، وبالغرامة المالية من 50.000 دج إلى 2000000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدّل بطريق الغش المعطيات التي يتضمنها".** فمن خلال هذه المادة نلاحظ بأنّ المشرع الجزائري كان وضحا كل الوضوح في مسألة الجزاء القانوني، هذا الجزاء الذي كان مادي

ومعنوي معا: السجن مع الغرامة المالية، والقصد من ذلك هو التحذير الفعلي من هذا الاعتداء في صوره الثلاث: الغش في إدخال المعلومات، أو الإزالة، أو تعديل المعطيات.

2-**الاعتداء على المعطيات الخارجية للنظام** (براهيمي جمال، /، صفحة 135):

يقصد بالمعطيات الخارجية لنظام المعالجة تلك المعطيات التي لها دور في تحقيق نتيجة معينة تمثل في المعالجة الآلية للمعطيات، وقد نص عليها المشرّع الجزائري في المادة 394 مكرّر 2 من قانون العقوبات على النحو الآتي: "**يعاقب بالحبس من شهرين إلى 3 سنوات وبغرامة مالية من 1000000دج إلى 5000000 دج كل من يقوم عمدا أو عن طريق الغش بـ:**

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

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

يتضح لنا من نص هذه المادة بأنّ ركزت بشكل عام على الحماية الفعلية لمختلف المعطيات سواء الداخلية أو الخارجية المتعلقة بنظام معلوماتي معين، وهذه المادة هي تصريح علني لأهم التدابير والإجراءات القانونية المطبق على كل مرتكب هذا الجرم في شكليه اللذين كنا قد أشرنا إليهما سالفا، وفقا للصور الثلاث التي حددتها المادة القانونية في المكرر1. ولقد سعى المشرع الجزائري كذلك في قانون العقوبات "رقم 04-05 المؤرخ في تاريخ10 نوفمبر 2004 في القسم السابع مكرر من الفصل الثالث الخاص بجرائم الجنايات والجنح ضد الأموال تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، في المادة 394 مكرر يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من خمسين ألف إلى مائة ألف دينار كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من المنظومة للمعالجة الآلية للمعطيات أو يحاول ذلك... وتضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظمة، وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام أشغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين وغرامة من خمسين ألف إلى مائة وخمسون ألف دينار. المادة 394 مكرر1" (زعيطي أمينة، برناوي راضية، 2019، الصفحات 233-234) ، إنّ الملاحظ من هذه المادة أنّ شكل العقوبة يتحدد وفقا لطبيعة الجرم المرتكب، والعقوبة تتضاعف حسب طبيعة الجريمة الالكترونية، سواء أكانت هذه العقوبة مادية (غرامة مالية) أو معنوية (السجن)، ليبقى الغرض الأساسي من هذه العقوبة هو اعتبار بأنّ الجريمة الالكترونية جنحة يعاقب عليها القانون أولا، وفي كل مرة تتخذ شكلا مغايرا معنويا أو ماديا الغرض منه ثانيا، ولكون

مرتكب هذه الجريمة تجده بشكل أو بآخر يلجأ إلى إعادة ممارسة فعله الإجرامي في حال لم يجد رادع لفعله.

إنّ ما نصّت عليه المادة 394 مكرر فيما يتعلّق بتخريب النظام من خلال الاعتداء عليه من شأنه التأثير على المعطيات الداخلية والخارجية لهذا النظام المعلوماتي، باستعمال الكثير من البرامج الفيروسية وبرامج معلوماتية أخرى تعمل على التأثير وسير النظام المعلوماتي لأي جهة من الجهات، سواء أكانت هذه الجهة أفراد عاديين أو أصحاب شركات أو نظام معلوماتي لمجتمعات معينة. يمكن أن تتخذ الأفعال الماسة بسير النظام عدّة صور نذكر منها (ونوغي نبيل، 2019، صفحة 136):

1.**التعطيل:** يمكن أن يصيب التعطيل الأجهزة المادية للنظام، كتحطيم الاسطوانات أو قطع شبكة الاتصال أو يصيب الكيانات المنطقية للنظام: كالبرامج أو المعطيات باستخدام برنامج فيروسي أو قنبلة منطقية مما يؤدي إلى عرقلة سير النظام .

2.**الإفساد:** هو جعل نظام غير صالح للاستعمال بإحداث خلل في نظام سيره، وفقدان توازن في أداء وظائفه، كان يعطي نتائج غير تلك التي كان من الواجب الحصول عليها، ومثل هذا الفعل إن لم يؤدي إلى تعطيل نظام المعالجة كلية فإنّه يحول دون تحقيقه لوظائفه بشكل صحيح.

خطورة الجريمة الالكترونية يكمن في كونها عابرة للحدود، بفضل ربط أي نقطة من نقاط هذا العالم الواسع والشاسع بشبكة الاتصالات العالمية والأقمار الصناعية، الأمر الذي من شأنه تعزيز بعض الممارسات الناتجة بالدرجة الأولى عن عملية الانتشار والغزو الثقافي في إطار ما يسمى بالعولمة الثقافية؛ هذه الأخيرة التي باتت أخطارها تظهر تجلياتها بصورة واضحة للعيان من خلال ممارسات الأفراد التي باتت تتخذ في كل مرة شكلا جديدا يتطلب إعادة الدراسة وفقا للمعطيات الجديدة، ووفقا للظروف المجتمعية المتعددة، مع الأخذ بالاعتبار التطور السريع لتكنولوجيات الإعلام والاتصال، والإقبال الواسع على استخدام هذه الوسائل، لاسيما في ظل ما أصبح يعيشه المجتمع البشري من مخاطر خاصة الوباء العالمي، فبظهوره ظهرت العديد من الظواهر والمشكلات الاجتماعية، ناهيك عن الإقبال الواسع لكل شرائح وفئات المجتمعة على هذه التكنولوجية بشكل مخيف وداع للقلق، إقبال في كثير من الأحايين يفتقر إلى المراقبة المستمرة خاصة لفئات الأطفال، خاصة وأنّ هذه التكنولوجيات لا تعترف بأي حدود إقليمية أو دولية أو محلية، ولا تتقيد لا بزمان ولا بمكان محدد، والجريمة الالكترونية لعبة اجتماعية ذات أبعاد متعددة مسرحها العالم ككل وممثلوها أفراد من مختلف المجتمعات.

إنّ المشرع الجزائري من خلال تشريعاته القانونية ومساعيه المتعددة تجاه الحد من الجريمة الالكترونية، لم يتوقف عند حدود النصوص المتعلقة بالاعتداءات المادية، بل تجاوزه إلى نصوص

الملكية الفكرية؛ هذه الأخيرة التي تندرج ضمنها كل من: حقوق المؤلف الأدبية، حقوق الملكية التجارية، في هذا السياق اشترط و"اعتمد المشرع الجزائري من أجل حماية المصنفات الفكرية شروطا عامة، تتمثل في وجود المصنف أوّلا ثم عدم مخالفته للنظام العام ثانيا، وأخرى خاصة وهي وجود ابتكار جديد في المصنف أوّلا ثم القيام بإيداعه القانوني ثانيا" (عائشة نايري، 2017/2016، صفحة 33). وهناك العديد من الجرائم الالكترونية التي يعاقب فاعلوها ويترتب عنها عقوبة قانونية منها:

-الجريمة الالكترونية الواقعة على نظام المعلومات.

-جريمة الدخول إلى نظم معلوماتية أخرى والبقاء غير المشروع في هذا النظام.

-الجريمة الالكترونية المتعلقة بأسرار الأفراد أو المجتمعات والدول معا، خاصة ما تعلق بها بالأمن القومي.

-جريمة المساس بمنظومة معلوماتية معينة.

-جريمة الغش الالكتروني.

-جريمة البرامج المتعلقة بالقرصنة واستخدامها للولوج إلى أي قاعدة معلوماتية دون إذن الجهات القائمة عليها.

إذن المشرع الجزائري في سنه للمواد القانونية المتعلقة بالجريمة الالكترونية، تعامل معها مثلما يتعامل مع الجريمة العادية، بالرغم من تعدد أشكالها وتنوع صورها، وبالرغم من اختلاف المواد والأجهزة والبرامج المستعملة فيها، وبالرغم من الفئة الاجتماعية التي ارتكبتها، لتبقى في الأول والأخير جريمة حقيقية، كرّس لها القانون والمشرّع الجزائري نص قانوني يُدين بشاعتها، سواء بالسجن أو بغرامة مالية. وتحت طائل التطور التكنولوجي والاتصال الجماهيري أصبح الفرد والمجتمع معا أكثر عرضة لمختلف التهديدات الالكترونية على نطاقات متعددة، ومن جهات مختلفة، لذا فتعامل المجتمع الجزائري مع الثورة التكنولوجية قائم بالدراسة الأولية على منهج فهم وتفهم واقعية هذه الظاهرة الجديدة، ثم العمل على إنشاء جهاز قانوني لكن هذا الجهاز يتخذ سحنة افتراضية الكترونية؛ لأنّ حقيقة وقوع هذا الجريمة هو العالم الالكتروني، لذلك هنالك آليات متعددة لمواجهة مختلف التهديدات الناجمة عن لجريمة الالكترونية في مقدِّمتها:

-استغلال الطاقات الشابة، خاصة خريجي الجامعات أصحاب الشهادات في طور التكوين الخاص بالبرمجيات أو حتى الإعلام الآلي في مواجهة هذه المشكلة، كعناصر فاعلة في طاقم الجهاز الالكتروني القانوني.

-محاولة التنويع في الدورات التكوينية الخاصة بمختلف التقنيات الحديثة المتعلقة بالدرجة الأولى بتكنولوجيات الإعلام والاتصال، ومختلف تقنياتها وبرمجياتها.

-تفعيل أهمية المورد البشري كطاقة حيوية في تسيير أسس فهم نظام مختلف الاعتداءات الالكترونية.

-النزوح نحو رقمنة قطاع الشرطة، والجهاز القانوني، وخلق آليات حماية ضد مختلف الجرائم الالكترونية.

تنشيط دور الجمعيات والمجتمع المدني في نشر الوعي الالكتروني عبر منصات الكترونية متعددة للتعريف بخطورة هذا الجرم.

-إبرام اتفاقية دولية وشراكة تعاملية للاستفادة منهم في تجاربهم بهذا المجال.

إنّ التهديدات المتربص بالمجتمع الجزائري، لاسيما وأنّ هذا النوع من الجرائم في تطور مستمر، مرتبط بالأساس بتطور النظم المعلوماتية وتكنولوجيات الاتصال والإعلام يستدعي دائما من القائمين على التشريع الجاهزية الالكترونية لمواجهة هذه الظاهرة، على الأقل بأقل خسائر. لن تكون فعالية هذه الجاهزية إلاّ من خلال مجتمع المعرفة المدرك لحقيقة مجتمع المخاطر التي بات يتميز بها المجتمع الحديث في مجالات المجتمع الحيوية، ودونما أدنى أو أي استثناء.

5. **التأثير الاجتماعي للجريمة الإلكترونية:**

إنّ المجتمع بكل مؤسساته ورأس ماله التفاعلي بين أفراده يسعى دائما إلى المحافظة على بقاءه واستمراره من خلال وجود جهاز قانوني يحاول تحقيق هذا المبتغى، إضافة إلى قواعد العرف الاجتماعي والضمير الجمعي الذي يقف دائما على حافة ممارسات الأفراد، لكن هناك ملامح اضطراب وخلل تحول دون تحقيق هذا التوازن، في سياقات عديدة تزيغ بعض الممارسات عن مسارها الطبيعي، فتخلق نوع من اللا اتزان، والجريمة السيبرانية هي جريمة متعددة التأثير، لأنّ الموضوع الرئيسي فيها هو الإنسان (الأفراد)، لتظهر بصورة جلية تلك الانعكاسات والتأثيرات الاجتماعية يمكن إيجازها باختصار في الآتي:

- تهديد الأمن الاجتماعي للخطر.
- اتساع نطاق التخوف من الإقبال على استعمال تكنولوجيات الاتصال.
- خلق توتر بين الفرد والمجتمع من خلال تعزيز فكرة اللا ثقة.
- كثرة الاعتداءات الالكترونية قد يؤثر على هوية الانتماء الاجتماعي لدى الفرد تجاه مجتمعه.

- تفشي ظاهرة السرقة الالكترونية يؤثر على نسيج العلاقات الاجتماعية بين الأفراد حتى ولو كانت هذه العلاقات افتراضية.

- كثرة جرائم السب والقذف يؤدي إلى اتساع نطاق الوصم داخل المجتمع، مما يؤثر على طبيعة التواصل الاجتماعي بين أفراد المجتمع الواحد.

- الاعتداء المباشر أو غير المباشر على الحياة الشخصية للأفراد.

- الغياب النسبي للخصوصية الفردية داخل نظام هدف هذا النوع من الجرائم.

- خلخلة الرأس مال العلائقي الاجتماعي بين الدول والمجتمعات.

- كثرة انتشار جرائم القذف والسب يخلق نزاع ونفور مستمر بين الأفراد.

- التجسس وإمكانية ممارسة فعل القرصنة على معلومات أي فرد إن لم يكن على قدر كبير من الوعي بهذه الجريمة، خاصة في ظل النزوع نحو تكنولوجيا المعلومات وتطور وسائلها بشكل رهيب.

- الهلع النفسي الدائم الذي تثيره هذه الجريمة على ضحاياه بعد عيش هذه التجربة.

5. **خاتمة:**

إذن تعتبر مسألة الحماية من الجريمة الالكترونية أمرا بات محتما على كل المجتمعات دونما خلق قاعدة استثناء؛ لأنّ الأمر متعلق بمصير دول وأفرادها، ناتج عنها العديد من الأضرار الوخيمة والأخطار التي تهدد الصالح العام قبل الصالح الخاص. في ظل وجود مجموعة مسببات متداخلة فيما بينها، وظروف متنوعة صنعت من العادي في بدايته جريمة تحاك بصورة مباشرة أو غير مباشر، سواء أكان الأمر في بدءه مجرد تجربة أو تعمد، مرنة في حدوثها لكن معقدة في حل تفاصيلها، لذا لم يتساهل المشرع الجزائري والدولي في محاولاته الحثيثة وعلى مضض في محاربة هذه الجريمة المتصلة بشكل أساسي ومباشر بتكنولوجيات الاتصال والإعلام؛ هذه الأخيرة التي باتت تصنع في كل ثانية تحدي جديد وتطور سريع ومتجدد، وتزامنا معه فلا بد من تجديد المنظومة القانونية فيما يخص مسألة التكفل المستمر بمراقبة وتيرة تطور وصيغ ممارسة هذه الجريمة، وفقا لتجديد النصوص والإجراءات القانونية المرتبطة بالجريمة الالكترونية للتخفيف من آثار جريمة عابرة للحدود لا تعرف فرد ولا مجتمع، لا تعرف قوي ولا ضعيف، لا تعرف بمشروع أو غير مشروع... همها الوحيد خلق عالم قائم سواء على الانتفاع الشخص أو كممارسة جاءت من منطلق تجريبي لتتحول فيما بعد إلى تمرس فعلي.

7.**التوصيات:**

-إنشاء شرطة الإنترنيت لإلقاء القبض على مرتكبي هذه الجريمة.

-محاولة تجنب استقبال أو إدخال أي ملفات من أشخاص غير معروفين وغير موثوق فيهم إلى الكمبيوتر الشخصي أو في مكان العمل.

-التواصل مع ضحايا هذه الجريمة للتكفل بهم، نظرا لما لهذه الظاهرة من تأثير مستقبلي على الجهاز النفسي للفرد.

-استخدام نظام تشفير الملفات الموجودة بالكمبيوتر لصعوبة اختراقها.

-تجنب فتح الرسائل الإلكترونية من أشخاص مجهولين الهوية.

-المراقبة الأسرية للأطفال خاصة أثناء ولوجهم لعالم الإنترنيت.

-توعية الأفراد بخطورة ووجود مثل هذا النوع من الجرائم وبشكل مستمر.

-تشديد العقوبات القانونية على مرتكبي هذه الجريمة ليكون عبرة للآخرين.

-إنشاء محاكم قضائية افتراضية مختصة في مثل هذه الجرائم.

-تطبيق أقصى العقوبات على مرتكبي هذه الجريمة، وإخضاعه للمتابعة النفسية والقانونية بشكل مستمر.

-عرض نماذج مختلفة للجريمة السيبرانية لكل شرائح المجتمع، من خلال الحملات الإعلامية للتعريف بهذا النوع الجديد من الجرائم عبر وسائل الإعلام والاتصال المختلفة للاحتراز أكثر منها.

-غرس ثقافة الوعي التكنولوجي للوقاية من الجرائم الناتجة عنها.

-تعزيز الجسر التواصلي بين الجهاز القانوني والمواطن، خاصة مع الشرطة الالكترونية، للتخفيف من التخوف الكبير من هذا الجهاز أو عدم معرفته جيدا من قبل بعض المواطنين لتقديم شكواهم في حالة تعرضهم لمثل هذا الاعتداء، وعدم الاكتفاء بالصمت.

8.قائمة المراجع:

-إبـراهيم رمضـان إبـراهيم عطايـا (2015)، الجريمـة الإلكترونيـة وسـبل مواجهتهـا في الشـريعة الإسلامية والأنظمة الدولية: مصر.

-الجنيبي خالد علي (2015)، الجريمة الالكترونية بين تحديات الواقع واستشراف المستقبل، دار المنظومة: الرياض.

-حوالـف حليمـة(2021)، معـالم الجريمـة المعلوماتيـة في القـانون الجزائـري، **مجلـة البحـوث القانونية والسياسية**، المجلد الثالث، العدد 16، (140-155).

-زعيطي أمينة(2019)، مكافحة الجرائم الإلكترونية في ضوء قانون العقوبات الجزائري: دراسة مقارنة، **مجلة حقوق الإنسان والحريات العامة**، مجلد الرابع، العدد السابع، (220-238).

-صـغير يوسـف(2013)، **الجريمـة المرتكبـة عبر الإنترنيـت**، رسـالة ماجسـتير في القـانون، كليـة الحقوق والعلوم الإنسانية: الجزائر.

-عائشـة نـايري (2016-2017)، الجريمـة الإلكترونيـة في التشـريع الجزائـري، مـذكرة ماسـتر في القانون الإداري، كلية الحقوق والعلوم السياسية: أدرار-الجزائر.

-مكتـب الأمـم المتحـدة (فبرايـر2013)، دراسـة شـاملة عـن الجريمـة السـيبرانية، الأمـم المتحـدة: نيويورك.

-نيـاب موسى البداينـة (2014)، الجرائم الالكترونيـة: المفهـوم والأسـباب، الملتقى العلمي الجـرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، كلية العلوم الإستراتيجية، عمان.

-ونـوغي نبيـل، زيـوش عبـد الـرؤوف(2019)، الجريمـة المعلوماتيـة في التشـريع الجزائـري، مجلـة العلوم القانونية والاجتماعية، المجلد الرابع، العدد الثالث، (127-139).

-يوسـف خليل يوسـف العفيفي (2013)، **الجرائم الإلكترونية في التشـريع الفلسـطيني: دراسـة تحليلية مقارنة**، رسالة ماجستير في القانون العام، كلية الشريعة والقانون، فلسطين.