الأطر القانونية للجريمة السيبرانية في التشريع الجزائري بين الوقاية والمكافحة

LEGAL FRAMEWORKS FOR CYBERCRIME IN ALGERIAN LEGISLATION BETWEEN PREVENTION AND CONTROL FIGHTING

أمينة بصافة[1]

[1] كلية علوم الإعلام والاتصال/جامعة الجزائر3 (الجزائر)، bessafa.amina@univ-alger3.dz

تاريخ الإرسال: 2022/03/24 تاريخ القبول:2023/02/22 تاريخ النشر: مارس/2023

الملخص:

تهدف هذه الورقة البحثية إلى مناقشة الأطر القانونية للجريمة السيبرانية في التشريع الجزائري بداية من سنة 2004 إلى يومنا خاصة أمام بلوغ هذه الظاهرة مستويات عالية نتيجة الاستخدام اليومي المتزايد للأنترنت، حيث أصبحت تمثل مصدر قلق متزايد للجزائر على جميع مستويات التطورات، ويمثل المشهد المتطور لهذه الجرائم والفجوات الناتجة عن ذلك في المهارات تحديًا كبيرًا لوكالات إنفاذ القانون والمشرعين.

وعليه، وضمن هذا السياق، سعت الجزائر عبر تشريعاتها إلى سن قوانين للوقاية من الجرائم السيبرانية قبل وقوعها، ومن بين المساعي تعديل لقانون الإجراءات الجزائية، حيث ثم إنشاء القطب الوطني المتخصص في محاربة الجريمة الإلكترونية وتشديد العقوبات على مرتكبيها، دون المساس بالمنشورات الفردية وكبح حريات المواطن، وهو ما استدعى وضع قانون موضوعي وإجرائي ووقائي، سنقوم بتوصيفه اضافة الى التعريج على واقع هذه الجرائم في الجزائر، وهذا للاجابة عن سؤال الاشكالية الجوهري: ما هي الأطر القانونية الوقائية والمكافحة للجرائم السيبرانية في التشريع الجزائري؟

الكلمات المفتاحية: الجريمة الالكترونية، القانون الموضوعي، القانون الإجرائي، القانون الوقائي، الحماية.

Abstract:

Our study seeks to discuss cybercrime laws in Algerian legislation from 2004 to today, especially in view of its rise, which made it a growing source of concern for Algeria at all levels of developments, and the evolving scene of these crimes represents a major challenge for law enforcers and legislators.

Accordingly, and within this context, Algeria has sought, through its legislation, to enact laws to prevent cyber crimes before they occur, which necessitated the development of an objective, procedural and preventive law, which we will describe in addition to clarifying the reality of these crimes, and this is to answer our problems: What are the preventive legal frameworks and the fight against crimes Cyber in Algerian legislation?

Key words: Cybercrime, substantive law, procedural law, preventive law, protection.

المؤلف المرسل: أمينة بصافة، الإيميل المهني: bessafa.amina@univ-alger3.dz

مقدمة:

تعود جذور الأحداث التاريخية الأولى المتعلقة بالجرائم الإلكترونية عندما تم إنشاء شبكات الكمبيوتر الأولية وفي نفس الوقت بسبب نمو الحوسبة الشخصية، كانت هذه الأحداث بمثابة توسع في الجريمة الإلكترونية، وعلى الرغم من أن المصطلح كان يهدف إلى وصف الاستخدام الخيالي للتلاعب بأجهزة الكمبيوتر في البداية، إلا أنه مع مرور الوقت اكتسب دلالة مختلفة مرتبطة بإحداث أضرار لأنظمة المعلومات وأجهزة الكمبيوتر، وكانت السويد أول دولة تسن قانونًا لحماية البيانات يسمى "قانون البيانات السويدية لعام 1973" ، وينص على أنه يجب حماية البيانات ضد أي وصول غير مصرح به ثم كانت الولايات المتحدة الأمريكية ثاني دولة تسن قانونًا لمعاقبة الجرائم الإلكترونية حيث تم تقديم هذا القانون من قبل السناتور أبي ريبيكوف وتم التصديق عليه كـ "قانون حماية أنظمة الكمبيوتر الفيدرالي لعام 1977"، كان روبرت موريس جونيور أول مجرم إلكتروني يخضع للمحاكمة وحكم عليه في 26 يوليو 1989 بموجب "قانون الاحتيال وإساءة استخدام الكمبيوتر لعام 1986"[1].

وضمن هذا السياق تعتبر الجريمة سببا رئيسيا في تخلف المجتمعات باعتبار أنها تخلف عواقب مادية ملموسة سلبية اجتماعيا واقتصاديا وثقافيا وسياسيا وأمنيا، مهما كان نوعها سواء كانت تقليدية أو سيبرانية، فالجرائم السيبرانية تُرتكب على الإنترنت باستخدام الكمبيوتر كأداة تستهدف الأشخاص الذين يقفون خلفه كضحايا، كالقرصنة ومهاجمة معلومات الكمبيوتر والموارد الأخرى التي تتطلب خبرة فنية عالية، وقد أصبح التوسع والتنويع المتزايد في استراتيجيات وممارسات الجريمة السيبرانية عقبة صعبة من أجل فهم مدى المخاطر الكامنة وتحديد سياسات الوقاية الفعالة للشركات والمؤسسات والوكالات. وعليه تمثل هذه الدراسة مراجعة للأطر القانونية للجريمة الالكترونية وكيفية مكافحتها والوقاية منها في التشريع الجزائري، حيث تناقش هذه الورقة أولاً مدخل مفاهيمي للجريمة السيبرانية، وثانياً، قراءة في الأطر القانونية لمكافحة الجريمة الالكترونية في التشريع الجزائري، ثم تقديم ومناقشة الأطر القانونية للوقاية من الجريمة الالكترونية في ذات التشريع الذي تتجه جهوده نحو حماية ثالوث الأمن السيبراني الذي يحيط بالسرية والنزاهة والتوافر، خاصة وأن المخاطر المرتبطة بضعف تدابير الحماية من الجرائم الالكترونية في الواقع تؤثر على البلدان النامية أكثر بشكل مكثف وتقف في وجه التنمية، لذلك حرصت الجزائر منذ 2004 على وضع تدابير تقنية لتعزيز الأمن السيبراني من خلال سن التشريعات المناسبة لها بالاستعانة باستراتيجيات تتماشى مع المعايير الدولية .

1- مدخل مفاهيمي للجريمة الالكترونية وتصنيفاتها:

قبل أن نقدم مفهوم الجريمة الالكترونية نود أن نوضح أننا قمنا باستخدام مصطلح الجريمة الالكترونية كمرادف للجريمة السيبرانية استنادا إلى ما استخدمه مكتب الأمم المتحدة الإقليمي المعني بالمخدرات والجريمة للشرق الأوسط وشمال افريقيا، حيث استخدمهما كمترادفين[2]، ومع هذا سنقدم الفرق بين المصطلحين من خلال الجدول التالي:

الجدول 1: يبين الفرق بين الجريمة الإلكترونية والجريمة السيبرانية

الجريمة الإلكترونية Computer Crime	الجريمة السيبرانية Cybercrime
تشير جرائم الكمبيوتر المعروفة أيضًا باسم الجريمة الإلكترونية أو الجريمة الإلكترونية أو الجريمة الإلكترونية أو جرائم التكنولوجيا الفائقة إلى أي جريمة يرتكبها مستخدم الكمبيوتر المتمرس .يُعرف هذا النوع من مستخدمي الكمبيوتر الذين يمكنهم القيام بهذه الأنواع من الجرائم باسم الهاكرز .مصطلح المتسلل، على الرغم من أنه في الأصل كلمة تكميلية لعشاق الكمبيوتر، أصبح الآن له معنى مهين ويشير إلى شخص يصل إلى جهاز كمبيوتر أو شبكة بشكل غير قانوني .يمكنهم حتى إتلاف الملفات الضرورية لمنظمة من جهاز كمبيوتر الجريمة الالكترونية لا تستلزم توصيل الأجهزة الالكترونية كالحاسوب والهاتف الذكية واللوحة الالكترونية بالأنترنت، يمكن ارتكابها بمعزل عنها عكس الجريمة السيبرانية التي لا تتم إلا بربط الجهاز الالكترونية بشبكة الأنترنت في الفضاء السيبراني. الجريمة الالكترونية أكثر تكلفة وأكثر تعقيد من الجريمة السيبرانية.	هي الجرائم التي تتم عبر أجهزة الكمبيوتر المتصلة بشبكة الانترنت لإنشاء المعلومات الهامة وتخزينها وإدارتها وبالتالي، وتشير إلى أي حدث أو إجراء قد يتسبب في فقدان أو تلف أجهزة الكمبيوتر أو البرامج أو البيانات أو المعلومات أو القدرة على المعالجة، وتكون في الغالب مقصودة عن طريق ترك رسالة أو عن طريق تغيير البيانات أو إتلافها عن عمد، وأحيانا عرضية حيث لا يتسبب مرتكبوها في أي ضرر ويقومون فقط بالوصول إلى البيانات أو المعلومات أو البرامج الموجودة على شبكة الأنترنت. وبالتالي هي كل فعل متعمد مخالف للقانون يشمل جهاز الكمبيوتر المتصل بالشبكة وغير المتصل وبهذا الجريمة السيبرانية أشمل من الجريمة الالكترونية فهي الأعمال غير القانونية عبر الإنترنت أو القائمة على الإنترنت.

المصدر: JESSICA BREGANT and ROBERT BREGANT, Cybercrime and Computer Crime, The Encyclopedia of Criminology and Criminal Justice, First Edition. Edited by Jay S. Albanese, 2014, p1-5.

1.1- مفهوم الجريمة الالكترونية قانونيا:

صاغ سوسمان وهاستون مصطلح الجرائم الإلكترونية في عام 1995. حيث يرى أنه لا يمكن وصف الجريمة الإلكترونية على أنها تعريف واحد، فمن الأفضل اعتبارها مجموعة من الأفعال أو السلوكيات – تستند هذه الأفعال إلى كائن الجريمة المادية وطريقة العمل التي تؤثر على بيانات الكمبيوتر أو الأنظمة، ويشكل هذا مصطلح أفعالًا غير قانونية حيث يكون الجهاز الرقمي أو نظام المعلومات إما أداة أو هدفًا أو مجرد مزيج من الاثنين، يمكن استخدام تعبير الجرائم الإلكترونية بالتبادل إما كجرائم الكمبيوتر أو الجرائم الإلكترونية أو جرائم التكنولوجيا العالية أو جرائم عصر المعلومات أو الجرائم المرتبطة بالحاسوب أو الجرائم الرقمية، كلها مرادفات لمصطلح واحد[3].

ويُنظر إلى مرتكبي الجرائم الالكترونية في الغالب على أنهم فئة مظلمة وشريرة وتعمل في بيئات تحت الأرض وخاصة بهدف إلحاق الضرر بأنظمة معلومات المجتمع، ويمكن أن تكون دوافعهم من مجرد الاستمتاع الشخصي – مثل أطفال البرامج النصية الذين يقومون بتشويه مواقع الويب وكسر كلمات مرور الوصول، إلى ما يرضي الاعتراف بهم على أنهم مجرمون الكترونيون من النخبة من خلال كسر الأمن السيبراني والسرقة من شركات[4].

وعليه، فإن الجريمة الالكترونية من الناحية القانونية تعرف بأنها: " كل فعل من شأنه التعدي على الآخرين وعلى الممتلكات العامة والأنظمة بواسطة استخدام الوسائل التقنية الالكترونية في الفضاء السيبراني أو خارجه، ويعتبر جريمة يعاقب عليها القانون، لما في ذلك من إخلال بالأمن بمختلف مستوياته، من أمن الفرد وأمن المجتمع وأمن الدولة والأمن العالمي باعتبارها عابرة للحدود، وقد أصدرت الولايات المتحدة تشريعات لمكافحة الجريمة الإلكترونية عام 1973 مفادها أن النظام يسمح للأشخاص أو المؤسسات التي تم الاعتداء على حواسبهم بتفويض السلطات لمراقبة تحرك المعتدين وبالتالي تتولى السلطة متابعة اتصالات المعتدي التي يبثها إلى تلك الأجهزة المحمية، وسنت أستراليا قوانين لمكافحة الجريمة الإلكترونية لحماية تدفق المعلومات عبر الشبكة العالمية وحددت الجرائم الإلكترونية بواسطة المشرع ومنها أن الشخص الذي يدخل لأنظمة الحاسب الآلي من غير إذن شرعي ويتمكن من الوصول إلى البيانات الموجودة في الحاسبات أو البيانات الخاصة بدول الكومنولث ومخزنه في حاسبات أخرى لا تنتمي لهذه الدول يعتبر هذا الشخص متهما ومنتهكا للقوانين ويستحق عقوبة السجن لمدة ستة أشهر إلى جانب مواد أخرى، وينص نظام مكافحة الجريمة المعلوماتية الكندي على أن أي فرد يحتال وبدون وجه حق على الحصول على خدمات الحاسب الآلي بواسطة أدوات إلكترومغناطيسية أو سمعية أو ميكانيكية أو أي أدوات تعترض أو تسبب خللا لوظائف نظام الحاسب أو استخدام رقم سري لشخص آخر، فإنه يعتبر مدانا ويستحق عقوبة السجن لمدة لا تتعدى عشر سنوات[5]، وسنتطرق لمفهومها في التشريع الجزائري لاحقا.

وعليه، فإن مفهوم الجريمة السيبرانية غير متفق عليه، ولكن يمكن القول أنها تغطي أي سلوك غير قانوني موجه من خلال العمليات الإلكترونية التي تستهدف أمن أنظمة الكمبيوتر والبيانات التي تتم معالجتها وتبث عبر الشبكة، وبهذا فالجريمة الإلكترونية هي أي نشاط تكون فيه أجهزة الكمبيوتر أو الشبكات أداة، والتي تحتاج إلى تشريعات تعزيز الحماية من جرائم الإنترنت والإرهاب، وفي المقابل يمثل إيجاد استراتيجيات الاستجابة والحلول لتهديد الجرائم الإلكترونية تحديًا كبيرًا، لا سيما بالنسبة إلى الدول النامية، حيث تحتوي الإستراتيجية الشاملة لمكافحة الجرائم الإلكترونية بشكل عام على حماية التقنية وتطويرها وهو ما يحتاج وقت كبير وتكلفة عالية لا تمتلكها هذه الدول[6]، ومع هذا سعت جاهدة إلى سن قوانين تحد من انتشارها وتعاقب مرتكبيها، ومن بين هذه الدول الجزائر، ونبغي معرفة تصنيفات هذه الجرائم الالكترونية وهو ما سنوضحه أدناه:

2.1- تصنيفات الجريمة الالكترونية:

من خلال أدبيات الجرائم الالكترونية يتبين أن المجرمين الالكترونيين ينقسمون إلى فئات تتمثل في[7]:

- **القبعات البيضاء:** يعمل هؤلاء الأفراد ضمن قوانين أخلاقيات الهاكر أو القراصنة (عدم الإضرار) أو كخبراء أمنيين، وعليه هم الأفراد ذوو مهارات القرصنة الذين يعملون لحماية الشبكات بطريقة دفاعية، إنهم يعملون في بيئات الشركات كمحللين أمنيين.
- **القبعات الرمادية:** من أشهر مجموعات القراصنة وهم المستشارين الأمنيين، فهم قراصنة يعملون بشكل هجومي ودفاعي في مواقف مختلفة.
- **القبعات السوداء:** هؤلاء الفئة الأكثر خطورة كونهم مدفوعون بالقوة أو الغضب أو الكراهية، ليس لديهم أي مخاوف لسرقة أو ويقومون بتدمير بيانات الشبكة التي يخترقونها، وهم قراصنة يتمتعون بمهارات حوسبة ممتازة ينجذبون إلى الأنشطة الخبيثة، دوافعهم هي إحداث الضرر وسرقة المعلومات وتدمير البيانات وكسب المال.
- **النخبة:** لديهم المعرفة والمهارات على أعلى مستوى. يمكن اكتساب هذه المكانة من خلال استغلال مشهور بشكل خاص أو اختراق أو لديهم خبرة اكتسبوها نتيجة الاستخدام الكستمر للشبكة لفترات زمنية طويلة.
- **المقلدين:** المجموعة الفرعية الأكثر ازدراءًا داخل مجتمع الهاكرز الأكبر، هؤلاء هم عادة الأعضاء الأقل مهارة والأصغر سناً الذين يستخدمون الأدوات التي أنشأها فئة النخبة، فهم ليسوا على دراية بأساليب القرصنة، إنهم يميلون إلى التركيز في الحصول على كميات كبيرة من الهجمات بدلاً من تنفيذ هجمات عالية الجودة.
- **الإرهابيون السيبرانيون:** يستخدمون علم الاختزال والتشفير لتـبادل المعلومات ومشاركة المؤامرات

عبر الإنترنت، ويعتبر هؤلاء من أخطر المجرمين الالكترونيين، قراصنة يهدفون إلى تدمير البنية التحتية الحيوية لأسباب جذرية ولا يخشون الذهاب إلى السجن. إنهم مرتبطون بالمفجرين الانتحاريين وعضو نشط في مجموعات الإرهاب السيبراني.

- **الموظفون الساخطون (السابقون):** أحد أخطر المجموعات وأقلها شهرة، اعتقد هؤلاء الأشخاص أنهم مدينون بتقدير – خاص لعملهم في الشركة وسوف ينتقمون من عدمه.
- **مؤلفو الفيروسات:** تميل هذه المجموعة إلى استغلال نقاط الضعف التي اكتشفها المجرمون الالكترونيون من مختلف الفئات، ثم طرق البرمجة لتنفيذ عيوب الكمبيوتر.
- **هاكتيفيزم Hacktivist:** هذا الاسم مشتق من الجمع بين الكلمتين "النشاط" و"القرصنة". وهي واحدة من المجموعات الفرعية للقراصنة الأسرع نموًا، والتي يتم تحفيزها لتشويه مواقع الويب وشن هجمات رفض الخدمة (DOS) لتلبية الأجندات السياسية والدينية والاجتماعية.
- **قراصنة التجسس:** هؤلاء المتسللون متعاقدون لاختراق الأسرار التجارية لمنافسيهم وكسبها.
- **قراصنة ترعاهم الدولة:** قراصنة ترعاهم الدولة ويتم توظيفهم لإلحاق الضرر بشبكات وأنظمة المعلومات في البلدان الأخرى.

وهذه التصنيفات عالمية وموجودة في كل البلدان والجزائر كمثيلاتها فيها هذه التصنيفات حسب ما يبرزه واقع الجريمة الاكترونية بها، وهو ما سنوضحه فيمايلي:

2- الأطر القانونية وواقع الجريمة الالكترونية في التشريع الجزائري:

1.2- واقع الجريمة الالكترونية في الجزائر:

فى الجزائر تم تسجيل أكثر من 500 جريمة إلكترونية في الجزائر خلال سنة 2016، علما أن هذا يخص عدد الحالات التي قامت بعملية التبليغ فقط، والأكيد أن البعض يرفض إيداع شكوى لاعتبارات اجتماعية وثقافية، وهو الأمر الذي جعل مصالح الدرك الوطني تتجند لحماية مستعملي الانترنت مثل مستخدمي مواقع التواصل الاجتماعي الذين يشكلون حيزا كبيرا من طبيعة استعمال هذه التكنولوجيا، كما تمت معالجة 385 جريمة الكترونية من قبل الفرق المتخصصة في مكافحة الجريمة الالكترونية التابعة للأمن الوطني، إلى جانب تسجيل 57 قضية في مجال جرائم الاعتداء على سلامة الأنظمة المعلوماتية[8]

إذ سجلت مصالح الدرك والشرطة الجزائريتين قرابة 2500 جريمة إلكترونية خلال سنة 2017 بما فيها جرائم القرصنة والابتزاز والتشهير والتحرش الإلكتروني والاحتيال. وثقت الشرطة الجزائرية حوالي 2500 جريمة إلكترونية خلال العام المنصرم.

وتشير أرقام المصالح الأمنية المكلفة بمكافحة الجرائم الإلكترونية، إلى أن 80 بالمائة من الجرائم المرتكبة تمت عن طريق موقع التواصل الاجتماعي "الفايسبوك" تعرض من خلالها عدد الأشخاص إلى عمليات ابتزاز وتهديد بنشر الصور أغلبها مفبركة. يقول رئيس الرابطة الجزائرية للدفاع عن حقوق

الإنسان، هواري قدور، في حديث خاص بـ DW عربية بأن منظمته تقوم بدورها يومياً في التصدي للابتزاز الإلكتروني بكافة أشكاله والعمل على مجابهته في الميدان حفاظاً على المجتمع الجزائري"، مشيراً إلى أن الرابطة تدعو إلى إيقاع أقصى العقوبات بالفاعلين، في ظل تسجيل ما معدله ثلاث إلى أربعة جرائم إلكترونية كل يوم. ويؤكد أن الرابطة لم ولن تقف مكتوفة الأيدي في مواجهة من يبتز المواطنين[9].

كما شهدت الجزائر مؤخرا ارتفاعا كبيرا في نسبة الجريمة الالكترونية وهو ما حذرت المصالح الأمنية منه، حيث سجلت مصالح الدرك والشرطة ما يتجاوز 8 آلاف جريمة إلكترونية خلال 2020، مما جعلها تنافس الجريمة التقليدية، حيث سجلت المديرية العامة للأمن الوطني، ارتفاعا قياسيا، أي من 500 جريمة سنة 2015، إلى 5200 قضية، خاصة بالجرائم الإلكترونية سنة 2020، في حين سجلت قيادة الدرك الوطني 1362 جريمة سيبرانية تورط فيها 1028 شخص خلال سنة 2020. وبينت عملية تحليل المعطيات للجرائم المسجلة أن القذف والسب عبر الفضاء الافتراضي احتل الصدارة بنسبة تفوق 55 بالمائة، تليها الجرائم ضد الأمن العمومي، ثم الأفعال الماسة بالحياة الخاصة وإفشاء الأسرار، وأخيرا الابتزاز والنصب والاحتيال والاستغلال الجنسي والأفعال المخالفة للآداب العامة وقضايا مشابهة، وأكد المختصون في مكافحة الجريمة السيبرانية أنه وفقا لآخر تقرير للموقع الإلكتروني "داتاريبورتال "DATAREPORTAL"" المختص في الإحصائيات المتعلقة بأنترنت الهاتف الثابت والنقال في العالم، فإن عدد مستخدمي الانترنت في الجزائر ارتفع بـ3.6 مليون في ظرف سنة، منتقلا بذلك إلى 26.35 مليون مستخدم. وأبرز التقرير أن الجزائر أحصت إلى غاية 31 جانفي الفارط 26.35 مليون مستخدم ما يمثل زيادة تقدر بـ3.6 مليون مستخدم منذ جانفي2020.

كما تضمن التقرير ذاته إحصائيات متعلقة بوسائل التواصل الاجتماعي والتجارة الإلكترونية، إضافة إلى توجهات ومعلومات تخص وضع الرقمنة في العالم، كما عرف عدد مستخدمي مواقع التواصل الاجتماعي "فايسبوك، تويتر، يوتيوب، انستاغرام" ارتفاعا في الجزائر إلى غاية 31 جانفي 2021، حيث تم تسجيل نحو 3 ملايين مستخدم جديد لمواقع التواصل الاجتماعي أي بزيادة 13.6 بالمائة خلال سنة واحدة وهو ما جعل العدد الإجمالي لمستخدمي هذه التطبيقات يقفز إلى 25 مليونا أي بنسبة 56.5 بالمائة من عدد السكان الإجمالي، حيث تستعمل أغلبية مستخدمي مواقع التواصل الاجتماعي الهاتف الذكي واللوحات الإلكترونية للاتصال بهذه الشبكات. ومن جهتها، فإن شركة "كسبرسكي"، المختصة في محاربة الجريمة السيبرانية، أحبطت 95 ألف هجمة إلكترونية ضد الجزائر، خلال سنة 2020، حيث صنفت سنة 2018 الأولى عربيا والـ14 عالميا من حيث البلدان أكثر تعرضا للهجمات الإلكترونية[10]. ومن بين الجرائم الالكترونية التي عرفتها الجزائر مؤخر في 2021 قضية النصب على الطلبة باستخدام المؤثرين (يوتيوبرز) والتي لايزال التحقيق جاريا مع حبس المتورطين الذين بلغ عددهم 11 متهما ووضع الباقي تحت الرقابة. وعلاوة على ذلك، سجلت مصالح المديرية العامة للأمن الوطني، المختصة في

مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال خلال الـ 08 أشهر الأولى من السنة الجارية،567 قضية تتعلق بجرائم الأنترنت، تورّط فيها 543 شخصا، حيث تمكنت الفرق المتخصصة في مكافحة الجرائم الإلكترونية للأمن الوطني ومن خلال معالجة كافة المعطيات التقنية والأدلة المادية المرتبطة بالقضايا السالفة الذكر، من معالجة 385 جريمة إلكترونية من أصل 567 قضية مسجلة ومحل متابعة لفك خيوطها، وهذا وفق ما توضحه المعطيات الواردة في الجدول التالي[11]:

الجدول 2: يمثل أنواع الجرائم الالكترونية في الجزائر ونسبها

نوع الجريمة	القضايا المسجلة	القضايا المعالجة	عدد المتورطين	النسبة المئوية للقضايا المعالجة
جرائم المساس بالأشخاص عبر الأنترنت	430	289	365	%68
جرائم الإعتداء على سلامة الأنظمة المعلوماتية	57	31	39	%55
جرائم الإحتيال عبر الأنترنت	25	17	32	%68
جرائم التحريض والتطرف عبر الأنترنت	14	14	31	%100
الجرائم المخلة بالحياء	12	08	22	%67
جرائم بيع السلع المحظورة عبر الأنترنت	06	05	15	%84
جرائم مختلفة (نسخ البرامج دون حق، القرصنة)	23	21	39	%92
المجموع	**567**	**385**	**543**	**%68**

المصدر: المديرية العامة للأمن الوطني، مصالح شرطة مكافحة الجرائم الإلكترونية تسجل 567 قضية تتعلّق بجرائم الأنترنت، 2021.

واستنادا على ما سبق، وبعد التعرض إلى واقع الجريمة الالكترونية في الجزائر الذي هو في تزايد مستمر نظرا لسهولتها واختلاف فئات المجرمين شرع المشرع الجزائر قوانين موضوعية واجرائية ووقائية بداية من 2004 لاحتواء الجريمة الالكترونية والتصدي لها وهذا ما يتضح في تعريفه لها هي 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[12] سنوضحه فيما يلي:

2.2– قوانين الجريمة الالكترونية الموضوعية والاجرائية والوقائية في التشريع الجزائري

1. القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون العقوبات،ج.ر، عدد 71:

لقد جرم المشرع الجزائري الأفعال الماسة بأنظمة الحاسب الآلي (الحاسوب والشبكة) في قانون العقوبات بموجب القانون 15/04 تحت عنوان : "المساس بأنظمة المعالجة الآلية للمعطيات " ويتضمن هذا القسم الـسابع ستة مواد من المادة 394 مكرر إلى 394 مـكرر 6[13]، وباعـتباره القانون الأول في مجال الجريمة الالكترونية سنعرض مواده بالتفصيل، وجاء فيه:

المادة 394 مكرر: "يعاقب بالحبس من ثلاث أشهر وبغامة من 50.000 دينار جزائري إلى 100.000 دينار جزائري كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك، تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة. إذا ترتب على الأفعال المذكورة تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50.000 دج إلى 150.000 دج"، ويقصد بهذا الجرائم المرتبطة بالحاسوب وبيانات شبكة الأنترنت.

المادة 394 مكرر1: "يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها" وهنا تم تشديد اللهجة العقابية لتكون أكثر حدة في المادة الموالية، يرجع سبب تجريم المشرع الجزائري للأفعال المذكورة أعلاه بنص مستقل عن جريمتي الدخول و البقاء غير المرخص بهما في نظام المعالجة، واللتان تمثلان الطريق العادي للوصول إلى المعطيات الموجودة داخل النظام وارتكاب جريمة محو أو إدخال أو تعديل ضدها، إلى وجود طرق أخرى لاقتراف هذه الأفعال عن بعد أي دون الدخول أو البقاء في النظام، كاستخدام مثلا القنابل المعلوماتية الخاصة بالمعطيات أو برامج الفيروسات[14].

المادة 394 مكررة 2: "يعاقب بالحبس من شهرين إلى ثلاث سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج كل من يقوم عمدا بطريق الغش بما يأتي:

- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات خزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.
- حيازة أو افشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها في احدى الجرائم المنصوص عليها في هذا القسم" وهنا تم تشديد لهجة العقاب في الجرائم الالكترونية المتعلقة بالقرصنة وتصميم الفيروسات.

المادة 394 مكرر 3: "تضاعف العقوبات المنصوص عليها في هذا القسم إذا استهدفت الجريمة الدفاع الوطني او الهيئات والمؤسسات الخاضعة للقانون العام دون الاخلال بتطبيق عقوبات أشد" وهنا كان المشرع حازما باعتبار هذه الجرائم الالكترونية تمس الأمن القومي للبلاد، وشدد العقوبات لزعزعتها استقرار البلاد.

المادة 394 مكرر4: "يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي" ويقصد هنا بالشخص المعنوي المؤسسات والمنظمات بينما الشخص الطبيعي هو الفرد.

المادة 394 مكرر5: "كل من شارك في مجـموعة أو اتفاق تالف بغرض الاعداد لـجريمة أو أكثر

من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها"، وهنا حدد المشرع فاعلين آخرين ليس فقط مرتكب الجريمة ولكن أيضا من شارك فيها.

المادة 394 مكرر6: "مع الاحتفاظ بحقوق الغير حسن النية يحكم مصادرة الأجهزة والبرامج والوسائل المستخدمة مع اغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم علاوة على اغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها" ويقصد هنا في حال ارتكاب جريمة الكترونية بمقاهي الأنترنت فالذي يعاقب هو صاحب المقهى.

واستنتاجا لما سبق يعتبر هذا القانون من القوانين الموضوعية التي تركز على جوهر الجريمة، مثل عناصر الجريمة التي تشمل السلوك المحظور (الفعل الإجرامي – "الفعل المذنب") والعنصر العقلي (النية الجرمية – "العقل المذنب")، كما أنه يتضمن القوانين التي تحظر أنواعًا معينة من الجرائم الإلكترونية المذكورة أعلاه وتعاقب على عدم الامتثال لهذه القوانين بالسجن أو بغرامات مالية، أو بهما معا، تشمل الجرائم الإلكترونية الجرائم التقليدية الواقعية (غير المتصلة بالإنترنت) (مثل الاحتيال والتزوير والجريمة المنظمة وغسل الأموال والسرقة) التي تُرتكب في الفضاء السيبراني وهي جرائم "مختلطة" أو "ممكّنة عبر الإنترنت"، بالإضافة إلى جرائم "جديدة" أو الجرائم "المعتمدة على الإنترنت" وهو ما قامت به العديد من البلدان قبل الجزائر بهذا الخصوص، فألمانيا واليابان والصين قامت بتعديل الأحكام ذات الصلة من قانونها الجنائي لمكافحة الجرائم الإلكترونية. استخدمت البلدان أيضًا القوانين الحالية المصممة للجرائم الكلاسيكية لاستهداف بعض الجرائم الإلكترونية ففي العراق، يتم استخدام القانون المدني الحالي (القانون المدني العراقي رقم 40 لعام 1951) وقانون العقوبات (قانون العقوبات العراقي رقم 111 لعام 1969) لمقاضاة جرائم العالم الحقيقي المرتكبة عبر الإنترنت والتكنولوجيا الرقمية.[15]

وفي المقابل يعتبر هذا القانون من القوانين الاجرائية التي تحدد العمليات والإجراءات الواجب اتباعها لتطبيق القانون الموضوعي والقواعد لتمكين إنفاذه، والذي يتضمن قواعد ومبادئ توجيهية شاملة حول الطريقة التي يتم بها التعامل مع الأشخاص المشتبه بهم والمتهمين والمدانين ومعالجتهم من قبل نظام العدالة، ويتضمن قانون الجرائم الإلكترونية الإجرائي أحكامًا بشأن الاختصاص القضائي وسلطات التحقيق، وقواعد الإثبات والإجراءات الجنائية التي تتعلق بجمع البيانات، والتنصت على المكالمات الهاتفية، والبحث والمصادرة، وحفظ البيانات والاحتفاظ بها، حيث حرص المشرع الجزائري في بداية الأمر إلى وضع قانون موضوعي اجرائي وقام بتعديله كما حدث في القانون الاجرائي رقم 06- 22 الصادر سنة 2006 في المادة 12 في الجزئية المتعلقة بالجرائم الالكترونية التي مفادها "...، وإذا قامت ضد الشخص دلائل قوية ومتماسكة من شأنها التدليل على اتهامه فيتعين على ضابط الشرطة القضائية أن يقتاده إلى وكيل الجمهورية دون أن يوقفه للنظر أكثر من ثمان وأربعين

(48) ساعة. يمكن تمديد آجال التوقيف للنظر بإذن مكتوب من وكيل الجمهورية المختص :

– مرة واحدة (1) عندما يتعلق الأمر بجرائم لاعتداء على أنظمة المعالجة الآلية للمعطيات"، وفي المادة 65 من الفصل الرابع التي مفادها " المادة 65 مكرر 5 : "إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد يجوز لوكيل الجمهورية المختص أن يأذن بما يأتي :

– اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية...[16]، وبعد هذه القوانين المعدلة والمتممة قام المشرع الجزائري بإصدار قانون وقائي سنة 2009 وهو ما سنناقشه أدناه.

2. القانون الوقائي رقم 04/09 المؤرخ في 05 أوت 2009 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها،ج.ر .عدد 47:

حدد المشرع الجزائري الهدف من هذا القانون في المادة 1:" يهدف هذا القانون إلى وضع قواعد خاصة بالوقاية من الجرائم المتعلقة بتكنولوجيات الاعلام والاتصال ومكافحتها"[17]، وهنا نجد المشرع الجزائري قد حدد نوعية هذا القانون كما أنه استبدل مصطلح جرائم منظومة المعالجة الآلية للمعطيات بمصطلح الجرائم المتعلقة بتكنولوجيات الاعلام والاتصال واللذان حسب المشرع الجزائري مرادفان لمصطلح الجريمة الالكترونية ولهما نفس مفهومها الذي ذكرناه سابقا، وقد تم تعريفها في المادة 2 ومست هذه الجرائم الالكترونية المنظومة المعلوماتية، معطيات معلوماتية، مقدمو الخدمات، المعطيات المتعلقة بحركة السير، الاتصالات الالكترونية.

وجاء الفصل الثالث من هذا القانون بعنوان مراقبة الاتصالات الإلكترونية، وحدد فيها المشرع الجزائري الحالات التي تسمح باللجوء إلى المراقبة الالكترونية وذلك في المادة 4 كإجراء وقائي من الأفعال الارهابية والاعتداءات على أمن الدولة ومكافحتها، وحماية الحياة الخاصة للأفراد.

وفضلا عن ذلك كان عنوان الفصل الرابع من هذا القانون القواعد الاجرائية تفتيش المنظومات المعلوماتية ويحدد كيفية تعامل ضباط الشرطة القضائية مع المجرمين الالكترونيين من تفتيش ودخول الى أنظمة التخزين وحساباتهم في حالة معلوماتهم تقع داخل اقليم الدولة، وإن كانت خارجها يتم اللجوء على السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية، ويتم حجز أو نسخ البيانات الالكترونية كدليل للاتهام وهذا ما ورد في المادة في المادتين 5 و6 بينما نصت المادة 7 على منع الوصول إلى بيانات المجرمين في حالة استحالة الحجز أو النسخ، ونصت المادة 8 على منح الصلاحية للهيئات المختصة بمنع الاطلاع على المعطيات التي يشكل محتواها جريمة الالكترونية، كما أن المادة 9 من نفس الباب

أكدت على عدم استعمال تلك البيانات إلا في الحدود الضرورية.

وفي المقابل ورد الفصل الرابع بعنوان التزامات مقدمي الخدمات/ مساعدة السلطات وفي المادة 10 منه تم التأكيد بحكم القانون على تقديم المساعدة للسلطان من طرف مقدمي الخدمات من خلال جمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها، كما يلزمهم بكتمان السرية وإلا يتعرضون للعقوبات، كما ورد في المادة 11 كيفية حفظ المعطيات المتعلقة بحركة السير سواء تعلق الأمر بزمن ومدة الاتصال، أو بالخدمات المطلوبة، أو التعرف على المرسل والمتلقي وعناوين المواقع الالكترونية المطلع عليها، وتم في هذه المادة أيضا تحديد نشاطات الهاتف التي تسمح بالتعرف على مصدر الاتصال، وتحديد مكانه، وتم تحديد عقوبات للمعرقلين لحسن سير التحريات القضائية بدفع غرامات مالية والسجن لمدة خمس سنوات، وعلاوة على ذلك ورد في هذا الباب الالتزامات الخاصة بمقدمي خدمة الأنترنت وذلك بالتدخل الفوري لسحب المحتويات الرقمية الاجرامية وتخزينها ومنع الدخول اليها، وحصر امكانية الدخول إلى الموزعات التي تحمل بيانات اجرامية.

والأمر الأساسي الذي نص عليه هذا القانون في الباب الخامس منه ما قبل الأخير انشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها في المادة 13، وحددت المادة 14 مهامها والمتمثلة في:

- تنشيط وتنسيق عمليات الوقاية من الجرائم الالكترونية.
- مساعدة الهيئات المختصة في التحريات وتجميع المعلومات وانجاز الخبرات القضائية.
- تبادل المعلومات مع النظراء الأجانب قصد جمع المعلومات اللازمة للتعرف على المجرمين الالكترونيين.

وفي الباب السادس والأخير خطت الدولة الجزائرية خطو مهمة في مجال الوقاية ومكافحة الجريمة الالكترونية في مجال التعاون الدولي وذلك في المادة 15 التي نصت على أن السلطات الجزائرية لديها الحق في النظر بالنظر في الجرائم الالكترونية المرتكبة خارج الاقليم عندما يستهدف مرتكبوها الأجانب مؤسسات الدولة أو الدفاع الوطني ...، بينما المادة 16 نصت على امكانية تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الالكترونية، وهنا وفي هذه المادة بالضبط في هذه الجزئية استخدم المشرع الجزائري مصطلح الجريمة في الشكل الالكتروني، وفي المادة 17 تم تحديد مجال تبادل المعلومات واتخاذ الاجراءات التحفظية، أما في المادة 18 الأخيرة في هذا القانون تم توضيح القيود الواردة على طلبات المساعدة القضائية الدولية حيث يرفض تنفيذ طلبات المساعدة في مجال مكافحة الجريمة الالكترونية التي من شأنها المساس بالسيادة الوطنية، وان كانت الاستجابة لطلبات المساعدة مفيدة يشترط الالـــتزام بالسرية التامة، ويبقى هذا القانون ساري المفعول إلى غاية يومنا ومرجـــعية قانونية للفصل في الجرائم الالكترونية بالجزائر.

وعليه، وفي سياق الجرائم الإلكترونية يركز القانون الوقائي الجزائري على التنظيم وتخفيف المخاطر، حيث تسعى التشريعات الوقائية إما إلى منع الجرائم الإلكترونية أو على الأقل التخفيف من الضرر الناتج عن ارتكابها، كقوانين حماية البيانات (على سبيل المثال، اللائحة العامة لحماية البيانات في الاتحاد الأوروبي لعام 2016، واتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية لعام 2014، وقوانين الأمن السيبراني (على سبيل المثال، قانون أوكرانيا بشأن المبادئ الأساسية لضمان الأمن السيبراني لأوكرانيا لعام 2017) لتقليل الأضرار المادية الناتجة عن الانتهاكات الجنائية للبيانات الخاصة في حالة حدوث جريمة إلكترونية و / أو تقليل تعرض القطاع الخاص، وبهذا تمكّن القوانين الأخرى من تحديد الجرائم الإلكترونية والتحقيق فيها ومقاضاة مرتكبيها من خلال ضمان وجود الأدوات والتدابير والعمليات اللازمة لتسهيل هذه الإجراءات (البنية التحتية لمزودي خدمات الاتصالات الإلكترونية تتيح التنصت على المكالمات الهاتفية والبيانات. الحفاظ)[18].

وبعد صدور القانون **رقم 04/09، والقانون رقم 20-06** وضمن القانون الوقائي ومكافحة الجريمة الالكترونية بالجزائر، صدر الأمر الذي يقضي بانشاء القطب الجزائي الوطني في محاربة الجريمة الإلكترونية وتشديد العقوبات على الجرائم السيبرانية، وهو ما سنناقشه أدناه.

3. الأمر رقم 21-11 المؤرخ في 16 محرم عام 1443 الموافق 25 غشت سنة 2021، المتعلق بانشاء القطب الجزائي الوطني المتخصص في محاربة الجريمة الالكترونية:

وكتثمين للقوانين السابقة الذكر الموضوعية والاجرائية والوقائية عمد المشرع الجزائري إلى اتمام الكتاب الأول من الأمر رقم 66-155 المؤرخ سنة 1966 بباب سادس عنوانه "القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ويتضمن المواد من 211 مكرر 22 إلى غاية 211 مكرر 29، حيث تنص:

المادة 211 مكرر 22: على انشاء القطب على مستوى محكمة مقر مجلس قضاء الجزائر، وهو متخصص في المتابعة والتحقيق في الجرائم الالكترونية، كما يختص في الحكم عليها إذا كانت تشكل جنحا.

المادة 211 مكرر 23: يمارس وكيل الجمهورية القطب لدى القطب وكذا قاضي التحقيق ورئيس القطب صلاحيتهم في كامل الاقليم الوطني، وحسب المادة 211 مكرر 24 يختصون حصريا بالمتابعة والتحقيق والحكم في الجرائم الالكترونية التي تمس أمن الدولة ودفاعها الوطني، وجرائم نشر وترويج أخبار كاذبة بين الجمهور التي من شأنها المساس بالأمن والسكينة والاستقرار في المجتمع، وتلك الجرائم الالكترونية المرتبطة بالإدارات والمؤسسات العمومية، وجرائم نشر وترويج الأنباء التي تمس بالأمن والنظام العمومي ذات الطابع المنظم والعابر للحدود الوطنية، جرائم التمييز وخطاب الكراهية، وجرائم الاتجار بالأشخاص أو بالأعضاء أو تهريب المهاجرين، كما يختصون حسب المادة 211 مكرر 25

بالجرائم الالكترونية الأكثر تعقيدا والمقصود بها النظر إلى تعدد الفاعلين أو الشركاء أو المتضررين او بسبب اتساع الرقعة الجغرافية لمكان ارتكاب الجريمة أو جسامة الأضرار المترتبة عليها كما حدث في جريمة قتل الشاب جمال بن اسماعيل خلال عملية حرق الغابات بمنطقة تيزي وزو بالقبائل وما نتج عنها من الفاعلين والمتضررين والأضرار الجسيمة التي كادت تفتك بالوحدة الوطنية نتيجة خطاب التمييز والكراهية الذي انتشر في مواقع شبكات التواصل الاجتماعي، وباللجوء إلى هذه المادة تم الحكم على أكثر من 44 متورط، وهذه الجرائم تتطلب استعمال كل وسائل التحري الخاصة والخبرة الفنية المتخصصة أو اللجوء إلى تعاون قضائي دولي، وقد أكدت المادة 211 مكرر 26 على تطبيق هذا الاختصاص للقطب، لتأتي المادتين 211 مكرر 27 و211 مكرر 28 لتأكد على صلاحيات الهيئات المختصة في تخصصهم في كل الاختصاصات وزوالها وجوبا في حالة علاقتها بالجريمة الالكترونية، وتم تدعيمها بالمادة الأخير من هذا الباب لهذا الأمر، بوجوب زوال كل اختصاص مرتبط بالجريمة الالكترونية ليكلف به القطب حتى لو كان اختصاص محكمة مقر مجلس قضاء الجزائر.

واستنادا لما تم ذكره يعتبر هذا القطب آلية من آليات المشرع الجزائري للقضاء على كل أنواع الجرائم الالكترونية مع احترام حرية الرأي والتعبير والنشر عب مختلف المواقع مادامت لا تحدث ضررا، ويمثل بهذا مكسبا لقطاع العدالة، كما يسعى المشرع الجزائري إلى استحداث قطب وطني متخصص لمكافحة الجريمة الالكترونية.

خاتمة:

وختاما، ومن خلال قراءة متأنية في القوانين السالفة الذكر نستنتج أن الأطر القانونية الوقائية والمكافحة للجرائم السيبرانية في التشريع الجزائري تتمثل في قانون القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون العقوبات، والذي يعتبر قانونا وضعيا اجرائيا جاء لسد الفراغ الذي كان سابقا في مجال الجرائم الالكترونية، ليتمم بالقانون الوقائي رقم 04/09 المتضمن للقواعد الخاصة للوقاية من الجرائم الالكترونية ومكافحتها، كما حرص القانون رقم 20-06 المؤرخ في 28 أفريل 2020 المعدل والمتمم لقانون العقوبات على تشديد العقوبات على مرتكبي الجريمة الالكترونية في مجال المساس بنزاهة الامتحانات والمسابقات في المواد من 253 مكرر6 إلى 253 مكرر 12^{19}، وبهذا تكون الجزائر قد حددت موقفها الحاسم من الجريمة الالكترونية سواء بالمكافحة أو الوقاية وكل هذه القوانين صادرة في الجريدة الرسمية، وهي جريدة تصدر باللغة العربية، وتندرج فيها القوانين والنصوص التنظيمية والقرارات والوثائق التي تفرض النصوص القانونية والتنظيمية الجاري بها العمل، بمصادقة رئيس الجمهورية، وتم تتويج هذه القوانين بالأمر رقم 21-11 الذي يقضي بانشاء القطب الجزائي الوطني المتخصص في محاربة الجريمة الالكترونية، وتسعى الآن إلى انشاء قطب آخر متخصص في هذا الشأن، فالمشرع الجزائري لم يترك أي فراغ قانوني لهؤلاء المجرمين في الفضاء السيبراني.

وعليه تقــترح هذه الدراسة مجـــموعة من الاقتراحات للحد من الجريمة الـــسيبرانية والوقاية منها وتتمثل في:

- اتخاذ تدابير لحماية أجهزة الكمبيوتر والبيانات الخاصة بالأفراد والمؤســـسات من الضياع والتلف وسوء الاستخدام.
- الاستعانة بتقنيين من أعلى المستويات مثل عبد القادر معز مكتشف الثغرات الأمنية في زظام عمل أجهزة آبل، وذلك لتشفير الحسابات المهمة وحمايتها من الاختراق.
- تدريب المواطنين واعطائهم التدابير الوقائية لحماية حساباتهم من الاختراق.
- تشديد العقوبات على مرتكبي الجرائم السيبرانية باعتبارها أهم استراتيجية من استراتيجيات الاتصال الاقناعي للتأثير من خلال تخويف المجرمين.
- تشجيع الضحايا على الإبلاغ عن مرتكبي هذه الجرائم فالعديد من الجرائم الالكترونية لا يتم معاقبة مرتكبيها بسبب خوف الضحايا من التبليغ.
- التعجيل في انشاء القطب الجزائري لمحاربة الجريمة الالكترونية، وتكوين قوات أمنية خاصة في هذا المجال.
- تكييف قوانين جنائية لمواكبة التقنيات الاجرامية المتطورة.

الهوامش:

1- REGNER SABILLON, J. C. Cybercrime and Cybercriminals: A Comprehensive Study. *International Journal of Computer Networks and Communications Security* , 2016. p165-176.

2-مكتب الأمم المتحدة الإقليمي، الجريمة السيبرانية، تاريخ الاسترداد 2022/02/10 من:
https://www.unodc.org/romena/ar/cybercrime.html

3 -Gercke, M. UNDERSTANDING CYBERCRIME:P H E N O M E N A , C H A L L E N G E S A N D L E G A L R E S P O N S E. New York : Telecommunicat ion Development Sector, 2 0 1 2. p11.

4 -REGNER SABILLON, J. C. Op. Cit, p165-176.

5-حسن بن أحمد الشهري، نحو قانون دولي موحد لمكافحة الجرائم المعلوماتية، ص 513-526، تاريخ الاسترداد 2022/01/12 من: https://www.asjp.cerist.dz/en/downArticle/20/1/1/4439

6 -Gercke, M, Op. Cit, p4.

7- REGNER SABILLON, J. C. Op. Cit, p165-176.

8- سعيدة بوزنون، مكافحة الجريمة الالكترونية في التشريع الجزائري. *مجلة العلوم الانسانية*، 2019، ص 55.

9-خديجة بودومي، الجريمة الإلكترونية بالجزائر. *DW عربية*، 2018، تاريخ الاسترداد/12/01/2022 من:
https://www.dw.com/ar

10-نوارة باشوش، الإجرام الإلكتروني.. أرقام مرعبة، الشروق أولاين، 2020، تاريخ الاسترداد 22/01/2022 من: https://www.echoroukonline.com

11-المديرية العامة للأمن الوطني. مصالح شرطة مكافحة الجرائم الإلكترونية تسجل 567 قضية تتعلّق بجرائم الأنترنت . تاريخ الاسترداد 19 فيفري, 2022، من
La Police Algérienne - Algeriepolice.dz: https://www.algeriepolice.dz

12-قانون رقم 09 -04 المؤرخ في 2009. *الجريدة الرسمية* ،2009، ص 1-4.

13-القسم السابع مكرر: المساس بأنظمة المعالجة الآلية للمعطيات. *الجريدة الرسمية*، 2004، ص 11-12.

14- ونوغي نبيل، زيوش عبد الرؤوف. الجريمة المعلوماتية في التشريع الجزائري. *مجلة العلوم القانونية والاجتماعية*، 2019، ص 127-139.

15 -Maras, M.-H. *Cybercriminology*. Oxford : University Press. 2016. P 132

16- قانون رقم 22 - 06 المعدل والمتمم للأمر 66- 155 المتضمن قانون الاجراءات الجزائية. *الجريدة الرسمية* ، ص 7- 8.

17-قانون رقم 09- 04 المتضمن للقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها. *الجريدة الرسمية*، 2009، ص 5- 8.

18 -Maras, M.-H. Op. Cit, p165

19-القانون رقم 20-06 المعدل والمتمم لقانون العقوبات. *الجريدة الرسمية*، 2020، ص 3-4.