

الجرائم السيبرانية: مفهوما وآليات مكافحتها

Cyber crimes: its concept and mechanisms to combat it

السبتي آسيا^{1*}، بوقريط عمر²¹جامعة الإخوة منتوري قسنطينة 1 sebti.assia@doc.umc.edu.dz

مخبر الدراسات القانونية التطبيقية

²جامعة الإخوة منتوري قسنطينة 1 bougrit.omar@gmail.com

تاريخ النشر: 2025/04/20

تاريخ القبول: 2025/04/11

تاريخ الاستلام: 2024/12/15

ملخص:

تعتبر الجريمة السيبرانية من أهم الجرائم المستحدثة التي تحدث أضرارا كبيرة في اقتصاد الدول تفوق في حدتها تلك الناتجة عن الجرائم التقليدية، مما دفعها إلى الإسراع في إيجاد حلول تشريعية للحد من هذه الظاهرة التي لا تزال تنتشر بسرعة نظرا للتطور الهائل في مجال تكنولوجيات الإعلام والاتصال في كافة أنحاء العالم، إن الهدف من دراسة هذا الموضوع يكمن بالدرجة الأولى في التحسيس بالمخاطر السيبرانية وسبل مواجهتها على المستويين الدولي والمحلي، والوقوف على موقف المشرع الجزائري من هذه المخاطر والتحديات، وفي الأخير، نتطرق إلى مدى فعالية التشريعات الدولية والوطنية في التقليل من آثار الجريمة السيبرانية.

وتكمن أهمية هذا الموضوع في أن الجرائم السيبرانية اليوم أصبحت تمثل نمط جديد من أنماط الجرائم عابر للحدود الوطنية للدول، مم استدعى مضاعفة الجهود بهدف مكافحتها من خلال إبرام اتفاقيات ومواثيق ووضع تشريعات وقوانين سننتطرق إليها في هذه الورقة البحثية..

كلمات مفتاحية: الجريمة السيبرانية، الجرائم التقليدية، التشريعات الوطنية، المخاطر، الجهود.

Abstract:

Cybercrime is considered one of the major crimes of the time, causing massive damage to the economy of countries that exceeds the damage caused by traditional crimes, which has prompted them to accelerate finding legislative solutions to reduce this phenomenon, which continues to worsen because of the enormous development in the field of information and communications technologies around the world.

The aim of this study lies primarily in sensitizing cyber risks and ways to confront them at the international and local levels, and identifying the position of the Algerian legislator towards these risks and threats, and finally, we address the effectiveness of international and national legislation in curbing cyber crime.

This issue is important because cybercrime today has become a new type of crime that transcends the regional borders of countries, which necessitated intensified efforts to address it through the conclusion of agreements and charters and the development of legislation and laws which we are going to address in this research paper.

Keywords: cybercrime, traditional crime, national legislation, risks, efforts.

مقدمة

إن الجريمة السيبرانية تعد واحدة من التحديات الجديدة التي نشأت مع التطور الرقمي وزيادة الاعتماد على استخدام هذه التقنيات عبر الانترنت، تتنوع هذه الجرائم بين سرقة المعلومات والاختراق إلى قضايا أخلاقية مثل الابتزاز والتهديد والاختطاف مما يجعلها تتخطى الحدود الجغرافية وتهدد الأمن الاجتماعي والدولي،

لقد أصبح موضوع الجريمة السيبرانية الشغل الشاغل للمجتمعات والدول بسبب التسارع في تطور هذه الجرائم وازدياد العديد من المشكلات وانعكاساتها السلبية على كيانات الدول، مما دفعهم إلى اتخاذ تدابير أمنية ووضع استراتيجيات وسن تشريعات لمكافحة هذه الجرائم أو على الأقل التقليل من آثارها الوخيمة على المجتمع،

يهدف هذا الموضوع إلى التطرق إلى مفهوم الجريمة السيبرانية والآليات القانونية الموضوعية لمكافحتها على المستويين الوطني والدولي،

ولعل أهمية هذا الموضوع تبرز في أنه في ظل التطور التكنولوجي واندماجه في مختلف المجالات السياسية والاقتصادية والاجتماعية، أصبح توفير الحماية لمستخدمي الانترنت ضرورة يجب أخذها بعين الاعتبار لتفادي ارتكاب جرائم سيبرانية،

وتأسيسا على ما سبق، فإن الإشكالية المطروحة في هذا البحث هي:

ماهي الجريمة السيبرانية؟ وماهي الآليات القانونية الموضوعية التي وضعتها الدول والحكومات لمكافحتها على المستويين الوطني والدولي؟

وقد اعتمدنا في هذه الدراسة على المنهج الوصفي التحليلي لوصف متغيرات الدراسة وتحليلها ، واقترحنا الخطة المبينة أدناه.

المبحث الأول: مفهوم الجريمة السيبرانية

المطلب الأول: تعريف الجريمة السيبرانية وخصائصها

المطلب الثاني: أنواع الجريمة السيبرانية وأسباب انتشارها

المبحث الثاني: الآليات القانونية الدولية والإقليمية والوطنية لمكافحة الجريمة السيبرانية

المطلب الأول: الآليات القانونية الدولية لمكافحة الجريمة السيبرانية

المطلب الثاني: الآليات القانونية الإقليمية لمكافحة الجريمة السيبرانية

المطلب الثالث: الآليات القانونية الوطنية لمكافحة الجريمة السيبرانية

المبحث الأول: مفهوم الجريمة السيبرانية

في هذا المبحث، سوف نتطرق إلى التعريف بالجريمة السيبرانية وخصائصها في مطلب أول، وفي المطلب الثاني، نتطرق إلى أنواعها وأسباب انتشارها ،

المطلب الأول: تعريف الجريمة السيبرانية وخصائصها

نتناول في الفرع الأول تعريف الجريمة السيبرانية وفي الفرع الثاني نتطرق إلى خصائصها

الفرع الأول: تعريف الجريمة السيبرانية

مصطلح الجريمة السيبرانية يستخدم حديثا للإشارة إلى جرائم الانترنت التي نشأت وتطورت كظاهرة الإجرام المرتبط بتكنولوجيا المعلومات،

تشمل هذه الجرائم أي فعل أو امتناع متعمد يتعلق بالاستخدام غير المشروع لتكنولوجيا المعلومات بهدف الاعتداء على الممتلكات المادية أو المعنوية أو انتهاك خصوصية الأفراد *

وتعود صياغة هذا المصطلح إلى ويليام جيبسون Willam Gibson في عام 1982، ومنذ ذلك الوقت توسع مفهوم الجريمة السيبرانية بشكل كبير،

وخلال السنوات الأولى من نشأتها، فضل العلماء والمؤسسات في البداية استخدام مصطلح جرائم الكمبيوتر بمعناه الضيق عوضا عن الجريمة السيبرانية بمفهومها الأوسع ،[†]

ومع تطور المصطلحات، بذلت جهود أكاديمية لتعريف الجريمة السيبرانية كمرجع شامل لمجموعة من الأفعال التي تستهدف البيانات أو الأنظمة حاسوبية أو تستخدم فيها، بالإضافة إلى جهود أخرى شملت الجرائم التي تتعلق بانتهاك المعلومات الحاسوبية أو استغلال موارد المعلومات لأغراض غير قانونية،

تتضمن الجرائم السيبرانية أيضا الاعتداء على الأنظمة المعلوماتية مثل الدخول غير المشروع إلى نظام معلوماتي أو البقاء فيه بهدف الوصول إلى البيانات الحساسة، كما تشمل تعطيل العمل المعلوماتي بشكل متعمد ‡

من ناحية أخرى، تعتبر الجرائم السيبرانية تلك الجرائم التي يستخدم فيها النظام المعلوماتي كوسيلة لارتكاب جرائم تقليدية سواء أكانت ضد الممتلكات مثل التحويل غير المشروع للأموال إلكترونيا، أو ضد الأفراد مثل التشهير أو السب أو القذف عبر الأنترنت،

* - نبيل دريس: الجريمة السيبرانية بين المفاهيم والنصوص التشريعية - الجزائر نموذجاً - مجلة القانون والمجتمع، المجلد 05، العدد 02، 2017، ص 30.

† - مانيو جيلالي، عروس كوثر: الجريمة السيبرانية في صورها المستحدثة، مجلة القانون والتنمية، المجلد 04، العدد 01، جويلية 2022، ص 53.

‡ - الطيب عيساوي، هشام شكاردة: التربية الإعلامية كآلية للحد من الجريمة السيبرانية على شبكة الانترنت بين إلزامية التأطير وضرورة الاستخدام، المجلة الجزائرية للأبحاث والدراسات، المجلد 03، العدد 04، سبتمبر 2020، ص 76.

تعتبر الجريمة السيبرانية فعلا مخلا بالقانون يستخدم تكنولوجيا المعلومات والاتصالات بهدف الإطاحة بالشبكات والأنظمة والبيانات والمواقع الالكترونية أو لتسهيل ارتكاب جرائم أخرى،

وتزداد خطورة هذه الجريمة مع ظهور اتجاهات جديدة بشكل مستمر مما يجعل مرتكبيها أكثر مهارة وقدرة على التكيف، فهم يستغلون التقنيات الحديثة بسرعة ملحوظة ويخططون لهجماتهم بدقة مستخدمين أساليب مبتكرة، ويتعاونون بطرق جديدة غير تقليدية، وتنشط الشبكات الإجرامية المنتشرة حول العالم وتنفذ هجمات متطورة في وقت قصير جدا.

الفرع الثاني: خصائص الجريمة السيبرانية

تختلف الجرائم السيبرانية عن الجرائم التقليدية بالوسط الذي ترتكب فيه، حيث تتطلب من الجاني أدوات تقنية لارتكاب فعله غير القانوني وحدا أدنى من المعرفة التقنية، وهي سلوك إجرامي ناشئ عن ارتكاب فعل حرمه القانون أو الامتناع عن فعل يفرضه القانون،

ويمكن إجمال خصائص هذه الجرائم في عدة نقاط: **

- 1- تتم باستخدام الحاسب الآلي والأنترنت كأداة لارتكاب الجريمة،
- 2- سرية لا يتم في اغلب الأحيان التبليغ عنها، خاصة إذا تعلق الأمر بالمؤسسات والشركات التجارية، تجنباً للإساءة للسمعة أو اهتزاز ثقة العملاء.
- 3- صعوبة الاكتشاف لعدم تركها لآثار مادية يمكن من خلالها التحقيق في القضية ويطلق على هذه الآثار بالآثار المعلوماتية الرقمية.
- 4- جرائم غامضة لصعوبة إثباتها وذلك بسبب غياب الدليل المادي ولأن أغلب البيانات عبارة عن رموز لا يمكن قراءتها.
- 5- جرائم عابرة للحدود الوطنية للدول وتلحق أضرارا جسيمة تمس عدة أقاليم.
- 6- جرائم تستدعي إلمام مرتكبيها بالمعرفة التقنية والخبرة الفائقة في مجال الإعلام الآلي.
- 7- جرائم لا تمتاز بالعنف، لا تستوجب استخدام مرتكبيها للقوة الجسدية أو العضلية للقيام بالجريمة

المطلب الثاني: أنواع الجريمة السيبرانية وأسباب انتشارها

الفرع الأول: أنواع الجريمة السيبرانية

تعددت أنواع وأشكال الجرائم السيبرانية لعل من أبرزها يمكن أن نذكر:

1- الجريمة المادية:

§ - مانيو جيلالي، عروس كوثر: المرجع السابق، ص 54.

** - مهدي رضا: الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري، مجلة ايليزا للبحوث والدراسات، المجلد 06، العدد 02، 2021، ص 114.

† - نفس المرجع ونفس الصفحة.

تتضمن هذه الجرائم التسبب في أضرار مالية للضحايا مثل السرقة الالكترونية التي تشمل الاستيلاء على أجهزة الصرف الآلي والبنوك، إنشاء مواقع أنترنت شديدة التشابه مع مواقع البنوك الكبرى، تلقي رسائل بريدية من مصادر مجهولة تطلب الاشتراك في تحرير أموال من الخارج مع وعد بنسب مئوية من المبالغ .

2- الجريمة الثقافية:

تتمثل في اعتداء الجاني على الملكية الفكرية ونسب الأعمال لنفسه دون موافقة من صاحب الحق، ويشمل ذلك قرصنة البرمجيات عبر نسخ برامج لشركة عالمية وبيعها بأسعار منخفضة، وكذلك الاعتداء على القنوات الفضائية بالإضافة ونسخ الكتب العلمية والأدبية .

3- الجريمة السياسية الاقتصادية:

تشمل استخدام الجماعات الإرهابية للاتصالات وبث الأخبار الكاذبة وتحويل الأموال بشكل غير مشروع إضافة إلى السيطرة على مواقع حساسة وسرقة المعلومات ونشر الفيروسات والأفكار السلبية بين الشباب مثل تشجيع الإرهاب والإدمان لتحقيق أهداف سياسية واقتصادية.

4- الجريمة الجنسية:

تشمل الابتزاز والتغريب والاستدراج .

فيما سبق استعرضنا أهم أنواع الجرائم التي انتشرت بشكل كبير في البيئة الرقمية التي كانت نتيجة انتشار التطبيقات التكنولوجية المختلفة بالإضافة للبعد الإنساني، فتفاعل الإنسان مع هذه الآليات الجديدة خلق مشكلات وجرائم لم تكن معروفة من قبل مع الإشارة إلى أن الانتشار الكبير والإقبال الكبير على استخدام التكنولوجيات الحديثة بشكل عام والانترنت بشكل خاص أدى لبروز مظاهر تميز البيئة الرقمية تختلف باختلاف ردود الأفعال في هذا المجال منها:

- التحديات الفكرية والاجتماعية والإعلامية والسياسية والاقتصادية بفعل تأثير التكنولوجيا التي أوجدت بيئة اجتماعية ووظيفية صعبة.
- ترافق تلك التحديات تناقضات وتعقيدات سلبية وإيجابية.
- الاندفاع والحماس نحو التكنولوجيا من طرف البعض ومقاومة شديدة أو متوسطة من طرف البعض الآخر، كما يظهر آخرون إعجابا شديدا أو متوسطا مقابل خوف وتراجع من الجانب الآخر. بشكل عام هذه هي سمات البيئة الرقمية وجرائم الأنترنت .^{***}

‡ - حكيمة جاب الله: انعكاسات الجريمة السيبرانية على البيئة الرقمية: دراسة في آليات واستراتيجيات مكافحتها، **حوليات جامعة الجزائر 1**، المجلد 35، العدد 03، 2021، ص 653.

§ - نفس المرجع ونفس الصفحة.

*** - نفس المرجع، ص 654.

ويرى وول Wall أن الفضاء الرقمي من خلال خصائصه المتميزة مقارنة بالبيئة الواقعية قد أتاح فرصا جديدة لارتكاب الجرائم من أهمها نذكر:

- العولمة التي تمكن الجناة من تجاوز الحدود الجغرافية التقليدية وحتى الزمنية.
- الإجمالية والشمولية التي مكنت الجناة من إذلال ضحاياهم عن بعد دون التنقل والتواجد في مسرح الجريمة.
- شبكات التوزيع التي ولدت فرصا جديدة لتكوين الضحايا عبر الدول دون حدود.
- مسارات البيانات التي خلقت فرصا جديدة للجاني لارتكاب سرقة الهوية.

فالبينة الرقمية وخصائصها ساهمت في نمو الجريمة السيبرانية سواء أكانت تهديدا أو تخريبا مع توفر الأمن والفرار نتيجة غياب الأثر وصعوبة المتابعة في ظل غياب الرقابة الأمنية، فهذه الجريمة أكثر أمنا مقارنة بالجريمة التقليدية .

الفرع الثاني: أسباب انتشار الجريمة السيبرانية

يمكن أن نلخص أسباب انتشارها في النقاط التالية:

- الرغبة في التعلم بهدف الحصول على معلومات وسر أغوار هذه التقنية المتسارعة التطور، ويفضل هؤلاء البقاء في الظل أكبر وقت ممكن حتى يتمكنوا من مواصلة عملهم داخل الأنظمة وتعلم كيفية اختراق المواقع الممنوعة والتقنيات الأمنية الحاسوبية.
- الرغبة في تحقيق مكاسب مادية في زمن قياسي (الدوافع المادية).
- التحدي والرغبة في قهر النظام المعلوماتي وإثبات الذات: أن اختراق الأنظمة الإلكترونية واختراق الحواجز الأمنية التي تحيط بهذه الأنظمة يمكن أن يكون مصدرا للمتعة والتسلية كبيرة لأولئك الذين يرتكبونها لسد أوقات فراغهم ... وإظهار تفوقهم والشعور بالقوة وجنون العظمة، بالإضافة لعوامل أخرى مثل:
- الرغبة في الانتقام من شخص مثلا أو من رب العمل أو من مؤسسة أو حتى من بعض الأنظمة السياسية في بعض الدول.
- الافتقار إلى ثقافة التعامل الآمن مع شبكة الانترنت
- عوامل اجتماعية أسرية تتعلق بطبيعة الحياة الاجتماعية المعاصرة مما زاد من العزلة وأدى لغياب المشاعر والأحاسيس الأسرية.
- إهمال تطبيق إجراءات التأمين والحماية اللازمين لجهاز الحاسوب، بالإضافة للكثير من الأسباب التي تختلف من بيئة لأخرى .

ومن الأسباب أيضا:

- مرونة بنية الشبكات المعلوماتية مما يسهل عملية اختراقها

† - نفس المرجع ونفس الصفحة.

‡ - نفس المرجع ونفس الصفحة.

- مرافقة العمليات العسكرية الميدانية
- تزايد اعتماد الدول على الفضاء السيبراني
- سهولة الوصول إلى المعدات المساعدة على الهجمات السيبرانية
- صعوبة الوصول إلى هوية المهاجم مما يساعد على توسع نطاق الهجمات

§

بالإضافة إلى ذلك، للجريمة السيبرانية أركان هي:

- الركن المادي ويتمثل في الفعل إيجاباً أو سلباً،
- الركن المعنوي ويتمثل في قصد المكلف،
- الركن الشرعي ويتمثل في وجود النص المجرم المعاقب على الجريمة****

المبحث الثاني: الآليات القانونية الدولية والإقليمية والوطنية لمكافحة الجريمة السيبرانية

توجد الكثير من الهيئات والمنظمات والمجالس الدولية التي تلعب دوراً بارزاً في إبرام الاتفاقيات بهدف تعزيز التعاون الدولي لمكافحة الجريمة السيبرانية، تأتي هيئة الأمم المتحدة والمجلس الأوروبي وبعض الجهات الأخرى في طليعة هذه الجهود.

المطلب الأول: الآليات القانونية الدولية لمكافحة الجريمة السيبرانية

سنطرق في هذا المطلب إلى جهود الأمم المتحدة في مجال مكافحة الجريمة السيبرانية وبعض المنظمات الدولية كمنظمة التعاون الاقتصادي والتنمية والاتحاد الدولي للاتصالات.

الفرع الأول: دور الأمم المتحدة في مكافحة الجريمة السيبرانية

أوصى المجلس الاقتصادي والاجتماعي التابع للأمم المتحدة بأن تتولى المنظمة دوراً رئيسياً في صياغة سياسة منع الجريمة وإرساء العدالة الجنائية الدولية، وقد تحقق ذلك عندما وافقت الجمعية العامة للأمم المتحدة على هذه التوصية في عام 1950 مما أدى إلى إنشاء اللجنة الاستشارية لمنع الجريمة ومعاملة المجرمين التي تضطلع بمكافحة الجريمة وتقديم المشورة للأمين العام بالإضافة إلى وضع برامج ورسم سياسات للتدابير الدولية في هذا المجال .⁺

كما تجدر الإشارة إلى أن مؤتمر الأمم المتحدة السابع لمنع الجريمة ومعاملة المجرمين الذي عقد في ميلانو بإيطاليا عام 1985 أسفر عن مجموعة من القواعد التوجيهية والتي صيغت في الجلسات الإقليمية التحضيرية للمؤتمر الثامن الذي تبنى هذه المبادئ وعقد في هافانا بكوبا عام 1990.

§ - دراغو عز الدين: الآثار الاقتصادية والمالية للهجمات السيبرانية في ظل التحول الرقمي: النتائج، التجارب والحلول - مع الإشارة لحالة الجزائر، مجلة التكامل الاقتصادي، المجلد 10، العدد 02، 2022، ص 115.

**** - عبد العزيز بن فهد بن محمد بن داود: الجرائم السيبرانية- دراسة تأصيلية مقارنة، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد 09، العدد 03، 2020، ص 149.

† - قطاف سليمان، بوقرين عبد الحليم: مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية، مجلة البحوث القانونية والاقتصادية، المجلد 05، العدد 02، 2022، ص 73

كما أكد المؤتمر على ضرورة تطبيق التطورات الجديدة في العلم والتكنولوجيا في جميع الأماكن لصالح الجمهور وبالتالي منع الجريمة بفعالية، كما أكد على أن التكنولوجيا بما أنها سلاح ذو حدين ، فانه من المهم اتخاذ تدابير مناسبة لمنع إساءة استخدامها، وإقرار نظم كفيلة بوصول الأفراد إلى البيانات وتصحيح الأخطاء فيها،

ويمكن إجمال توصيات مؤتمر هافانا 1990 في المبادئ التالية:

- تحديث القوانين الجنائية الوطنية بما في ذلك التدابير المؤسسية،
- تعزيز أمن الكمبيوتر والضوابط الوقائية،
- توفير تدريب كافي للموظفين والهيئات المسؤولة عن منع الجرائم الاقتصادية وجرائم الحاسب الآلي والتجسس والادعاء فيها ، ‡ ‡ ‡
- تضمين آداب الحاسب الآلي ضمن مقررات الاتصال والمعلومات وتبني سياسات لمعالجة القضايا المتعلقة بالضحايا في هذه الجرائم،
- تعزيز التعاون الدولي لمكافحة هذه الجرائم بشكل فعال.

كما عقد المؤتمر التاسع لمنع الجريمة ومعاملة المجرمين بإشراف الأمم المتحدة في القاهرة عام 1990، حيث شدد على ضرورة حماية خصوصية الإنسان وحقوقه الفكرية من المخاطر المتزايدة للتكنولوجيا وأكد على أهمية التنسيق والتعاون المثمر بين مؤسسات وأفراد المجتمع الدولي لاتخاذ التدابير المناسبة للحد من هذه المخاطر.

ضف إلى ذلك أن أفضل إستراتيجية طويلة الأجل لمكافحة الجريمة السيبرانية هي من خلال الاتفاقيات الدولية أي التعاون في تقديم مرتكبي جرائم الكمبيوتر إلى العدالة نظرا للانتشار العالمي للانترنت . §

الفرع الثاني: دور المنظمات الدولية في مكافحة الجريمة السيبرانية

اتخذت العديد من المبادرات بواسطة منظمات متعددة مثل الاتحاد الدولي للاتصالات، منظمة التعاون الاقتصادي والتنمية، مؤسسة الأنترنت للأسماء والأرقام المخصصة، المنظمة الدولية لتوحيد المقاييس، اللجنة الكهروتقنية الدولية، بالإضافة إلى فرق عمل هندسة الأنترنت ومنظمة التعاون الاقتصادي للمحيط الهادئ وآسيا ومنظمة الدول الأمريكية ورابطة دول جنوب شرق آسيا وجامعة الدول العربية والاتحاد الإفريقي، وفي دراستنا هذه سوف نركز على عمل منطمتين كمثال.

الفقرة الأولى: منظمة التعاون الاقتصادي والتنمية (OECD)

تركز هذه المنظمة على تحقيق أعلى مستويات النمو الاقتصادي وتحقيق التوازن بين التطور الاقتصادي والتنمية الاجتماعية، منذ عام 1978، بدأت المنظمة في التركيز على الجريمة السيبرانية من خلال وضع أدلة وقواعد توجيهية تتعلق بتقنية المعلومات،

‡ - نفس المرجع، ص 74.

§ - نفس المرجع، ص 75.

كان من أوائل الأدلة التي اعتمدها مجلس المنظمة في عام 1980 هو الدليل المتعلق بحماية الخصوصية وقواعد نقل البيانات مع توصية الأعضاء بالالتزام به،

في عام 1983 أصدرت المنظمة تقريراً بعنوان الجرائم المرتبطة بالحاسوب وتحليل السياسة القانونية الجنائية استعرض السياسة الجنائية الحالية وقدم مقترحات خاصة بعدة دول أعضاء، وتضمن التقرير الحد الأدنى من الأفعال المتعلقة بإساءة استخدام الحاسوب التي على الدول تجريمها وتشمل هذه الأفعال:

- الاستخدام أو الدخول غير المصرح به إلى أنظمة وموارد الحاسوب.
- الإفشاء غير المصرح به للمعلومات المعالجة آلياً والنسخ والإتلاف أو التخريب وما يتعلق بذلك من بيانات وبرامج والتعطيل غير المشروع لموارد الحاسوب بهدف منع استخدام برامجه أو البيانات المخزنة فيه . ****

الفقرة الثانية: الاتحاد الدولي للاتصالات (ITU)

أصدر المؤتمر العالمي لتنمية الاتصالات عام 2006 القرار رقم 45 الذي دعا فيه مدير مكتب تنمية الاتصالات إلى تنظيم اجتماع حول الأمن المعلوماتي ومكافحة الرسائل غير المرغوب فيها وتقديم تقرير يتضمن نتائج الاجتماع إلى مؤتمر المندوبين المفوضين التي عقدت في نفس السنة، وتمخض عنه تبني مجموعة من التوصيات في مجالي الأمن المعلوماتي والرسائل الاقتحامية،

في عام 2007 أطلق الأمين العام جدول أعمال الأمن المعلوماتي العالمي الذي يهدف إلى وضع إطار كفيل بمواجهة الخطورة المتزايدة لأمن الانترنت، والبحث عن حلول لتعزيز الأمن في مجتمع المعلومات، وفي أكتوبر 2007 أنشأ فريق من الخبراء رفيع المستوى يتكون من أكثر من مائة خبير قدموا تقاريرهم وتوصياتهم عام 2008، حيث نشرت الإستراتيجية العالمية في 2008/11/12 واشتملت على عدة مجالات: التدابير القانونية والإجرائية، الهياكل التنظيمية وبناء القدرات والتعاون الدولي .

المطلب الثاني: الآليات القانونية الإقليمية لمكافحة الجريمة السيبرانية

سنتطرق في هذا المطلب إلى توصيات المجلس الأوروبي بشأن المشاكل الجنائية المتعلقة بتكنولوجيا المعلومات، كذلك جهود اتفاقية بودابست لمكافحة جرائم الانترنت واتفاقية الجامعة العربية لمكافحة الجريمة السيبرانية.

الفرع الأول: توصيات المجلس الأوروبي

جاءت هذه التوصيات نتيجة التطور السريع في مجال الحاسب وتقنية الانترنت وشعور الدول بأهمية إعادة النظر في الإجراءات الجنائية ، حيث أصدر المجلس الأوروبي التوصية رقم 13/95 بتاريخ 1995/09/11 بخصوص مشاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات، ومن بين ما تضمنته هذه التوصية:

**** - نفس المرجع، ص 76.

† - نفس المرجع، ص 77.

- على القوانين أن توضح إجراءات تفتيش أجهزة الكمبيوتر وضبط المعلومات المتواجدة عليها بالإضافة إلى مراقبة البيانات أثناء انتقالها،
- أن تتيح الإجراءات الجزائية الوطنية للجهات المؤهلة صلاحية ضبط برامج الكمبيوتر والمعلومات على الأجهزة وفقا للشروط المتبعة في عمليات التفتيش التقليدية، ويجب إبلاغ الشخص المعني بأن الأجهزة كانت موضوعا للتفتيش مع توضيح المعلومات التي تم ضبطها.
- يجب السماح للجهات المختصة بتمديد نطاق التفتيش ليشمل أنظمة الكمبيوتر الأخرى المرتبطة بالنظام الجاري تفتيشه شريطة أن يكون ذلك ضروريا ومع مراعاة الضمانات الأساسية[‡]
- كما ينبغي على قانون الإجراءات الجزائية أن يوضح بأن الإجراءات المستخدمة مع الوثائق التقليدية تنطبق أيضا على المعلومات المحفوظة على أجهزة الكمبيوتر،
- إصدار أوامر للعاملين في المؤسسات الحكومية والخاصة التي تقدم خدمات الاتصال بالتعاون مع السلطات المختصة لأغراض المراقبة والتسجيل،
- تعديل القوانين الإجرائية لتشمل إصدار أوامر لمن يملك معلومات مثل البرامج أو قواعد البيانات المتعلقة بأجهزة الكمبيوتر لتسليمها بغرض الكشف عن الحقائق،
- يتطلب الاعتراف الدولي تطوير وتوحيد أنظمة التعامل مع الأدلة الالكترونية وتطبيق القواعد الإجرائية المختلفة على الأدلة التقليدية والالكترونية،
- ينبغي تشكيل وحدات متخصصة لمكافحة جرائم الكمبيوتر وتطوير برامج تدريب خاصة للعاملين في نظام العدالة الجنائية لتحديث مهاراتهم في مجال تكنولوجيا المعلومات،
- استحداث إجراءات سريعة وفعالة ونظام اتصالات يسمح للجهات التحقيقية بالتواصل مع جهات خارجية لجمع أدلة معينة مع التأكيد على موافقة هذه الجهات على عمليات التفتيش والضبط اللازمة .

الفرع الثاني: اتفاقية بودابست لمكافحة الجرائم السيبرانية 2001

في أواخر عام 2001 شهدت العاصمة المجرية بودابست توقيع أولى الاتفاقيات الدولية التي تهدف إلى مكافحة جرائم الأنترنت وهي اتفاقية بودابست التي أبرمت في 2001/11/08 ووضعت للمصادقة في 2001/11/23 والتي تضمنت التعريف بأهدافها ووضعت قائمة للجرائم التي يجب على الدولة أن تجرمها في قوانينها الداخلية منها: الإرهاب، تزوير بطاقات الائتمان، دعاية الأطفال،

كما تعد الاتفاقية الوحيدة المتعددة الأطراف المعنية بمكافحة الجرائم التي تتم باستخدام أو ضد الكمبيوتر وباستخدام شبكة الأنترنت، وقد تضمنت هذه الاتفاقية الأقسام التالية:

- القسم الأول: تحديد المصطلحات،

[‡] - نفس المرجع، ص 78.

[§] - نفس المرجع، 78-79.

- القسم الثاني: الخطوات الواجب إتباعها في إطار التشريع الوطني،
- القسم الثالث: التعاون الدولي،
- القسم الرابع: الشروط النهائية حول الانضمام إلى الاتفاقية.

***** كما عددت الجرائم التي يجب أن تتضمنها التشريعات الوطنية للدول الأعضاء وذلك كما يلي:

- الجرائم المتعلقة بأمن الشبكات كالدخول والمراقبة غير المشروعة والعدوان على الثقة في البيانات أو على النظام والإساءة إليه ،
- الجرائم المعلوماتية مثل الاختراق والانتحال والنصب والاحتيال المعلوماتي،
- جرائم الأخلاق مثل إنتاج أو بث أو حيازة ما يتعلق بدعارة الأطفال،
- جرائم العدوان على حقوق الملكية الأدبية والفكرية كاستنساخ المصنفات المشمولة بالحماية،
- المسؤولية الجنائية للأشخاص المعنوية وكذلك الاهتمام بالإجراءات الجنائية لاسيما في مرحلة التحقيق والملاحقة القضائية مثل التحفظ على الأدلة والتفتيش والضبط وما إلى ذلك،

كما تضمنت الاتفاقية باب آخر من التعاون حول إكساب أعوان الأمن خبرات عملية كما جاء في توصية اللجنة الفنية المتخصصة بدراسة طرق مكافحة الجرائم السيبرانية، وتعتبر الولايات المتحدة الأمريكية واحدة من الدول المتقدمة تقنيا في هذا المجال مكافحة الجرائم المعلوماتية والشبكات، فهي تلعب دورا مهما في تدريب أجهزة الشرطة والقضاة من دول أخرى لتعزيز قدراتهم على التعامل مع الجرائم السيبرانية قبل تفاقمها، وقد أنشأت وزارة العدل الأمريكية مكتب يختص بالمساعدة والتدريب لتطوير أجهزة الادعاء العام في دول أخرى، ويعمل بالتوازي معه برنامج دولي لتقديم المساعدة والتدريب لأجهزة الشرطة في الدول النامية.

كما شددت اتفاقية بودابست على أهمية الربط بين مكافحة الجرائم الالكترونية واحترام حقوق الإنسان، إذ تلزم الدول الأعضاء في الاتفاقية بتقديم أكبر قدر ممكن من المساعدة المتبادلة فيما بينها

الفرع الثالث: اتفاقية الجامعة العربية لمكافحة الجريمة السيبرانية

صدر عن جامعة الدول العربية دليل استرشادي لمكافحة جرائم تقنية تكنولوجيا السيبراني، حيث سعت الدول العربية لتقنين وتجريم الأعمال غير المشروعة المرتكبة من خلال استخدام الفضاء السيبراني ووقعت على الاتفاقية العربية الخاصة بمكافحة جرائم تقنية المعلومات في 2010/12/21 بهدف تعزيز التعاون بين الدول العربية في محاربة الجرائم السيبرانية والحفاظ على أمنها وسلامة مجتمعاتها.

***** - نفس المرجع، ص 80.

† - نفس المرجع، ص 81.

‡ - عمار مراد العيسوي: الإطار القانوني للجريمة السيبرانية، المجلة الشاملة للحقوق، المجلد 02، العدد 04، 2022، ص 202.

ودعا المجلس الدول العربية المصدقة على الاتفاقية إلى إبلاغ الأمانة الفنية للمجلس بالإجراءات التي اتخذتها من أجل موازنة تشريعاتها مع أحكام الاتفاقية وتجرى أشكال الجرائم الالكترونية المستحدثة لمنع الإرهابيين من استخدام الانترنت، كما دعا إلى تعزيز التعاون مع لمنظمات الدولية والإقليمية المعنية بمحاربة كافة أشكال جرائم الإرهاب الالكتروني،

كما شجع المجلس الدول العربية على التعاون لمنع الإرهابيين من استغلال تكنولوجيا المعلومات والاتصالات والانترنت بهدف التحريض على دعم أنشطتهم الإرهابية وتمويلها والتخطيط والإعداد لها،

بالرغم من كل هذه الجهود الدولية سواء على مستوى الأمم المتحدة والمنظمات الدولية أو على المستوى الإقليمي وخاصة اتفاقية بودابست التي تعتبر بمثابة دعوة للدول لإعادة النظر في تشريعاتها الداخلية والدعوة إلى التعاون الدولي لأجل مكافحة الجرائم السيبرانية التي لا تعترف بالحدود الجغرافية، إلا أن هناك صعوبات تواجه هذه الجهود تتمثل في:

- غياب نموذج موحد فيما يتعلق بالنشاط الإجرامي بالإضافة إلى افتقاد تعريف متفق عليه للأفعال التي ينبغي اعتبارها جرائم،
- عدم وجود معاهدات ثنائية أو جماعية بين الدول يساهم في تعطيل التعاون المثمر في مكافحة هذه الجرائم، وحتى المعاهدات القائمة فإنها لاتزال غير قادرة على توفير الحماية المطلوبة بسبب التطور السريع في أنظمة وبرامج الحاسب الآلي وشبكة الانترنت،
- تفتقر الدول فيما بينها إلى التنسيق في الإجراءات الجنائية المتعلقة بالجريمة المعلوماتية خاصة فيما يتعلق بالتحقيق وجمع الأدلة
- مشكلة الاختصاص في الجرائم الالكترونية تشكل عقبة كبيرة أمام الحصول على الأدلة نتيجة التداخل والترابط بين شبكات المعلومات، حيث يمكن أن تقع الجريمة في مكان معين وتنتج آثارها في مكان آخر *****

المطلب الثالث: الآليات القانونية الوطنية لمكافحة الجريمة السيبرانية

وضعت العديد من دول العالم قوانين للتصدي للتهديدات السيبرانية بعدما تبين بوضوح مدى سرعة انتشارها وحجم الخسائر التي تسببها، ومن بين هذه الدول، سنقوم بدراسة حالة الجزائر

الفرع الأول: سبل مكافحة الجرائم السيبرانية قبل صدور القانون 04-09

اعتبر المشرع الجزائري برامج الحاسب الآلي من المصنفات الأدبية والفنية، وذلك في المادة 04 من الأمر رقم 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة، فالحقوق المادية أو المالية هي الإطار الذي يمكن صاحب الحق من استغلال برنامجه

§ - قطاف سليمان، بوقرين عبد الحليم، المرجع السابق، ص 82.

***** - نفس المرجع، ص 82-83.

† - لامية طالة: التهديدات والجرائم السيبرانية: تأثيرها على الأمن القومي للدول واستراتيجيات مكافحتها، مجلة معالم للدراسات القانونية والسياسية، المجلد 04، العدد 02، 2020، ص 66.

بشقي الطرق دون غيره، ويترتب على ذلك حقوق مادية للمؤلف صاحب البرنامج بالاستغلال التجاري له ولورثته بمختلف الطرق.

وقد حدد هذا الأمر أحكام جزائية تنص على جنحة التقليد والعقوبات المقررة لها بموجب المواد من 151 إلى 160 من هذا الأمر، ومع هذه البداية دخلت مجموعة تعديلات أخرى على قانون العقوبات والإجراءات الجزائية

الفقرة الأولى: تعديل قانون العقوبات

واكب المشرع الجزائري التطورات التكنولوجية من خلال إدخاله مجموعة تعديلات على قانون العقوبات بإدراج قسم خاص يتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات بموجب القانون 04-15 المؤرخ في 10 نوفمبر 2004،

بعده ذلك، جرت تعديلات شاملة وتم إدراج سلوكيات إجرامية معينة ضمن القانون 06-23 المؤرخ في 20 ديسمبر 2006 تشمل هذه السلوكيات الدخول أو التواجد بطريقة غير قانونية في جزء أو كامل منظومة المعالجة الآلية للبيانات، إدخال معطيات غير قانونية في النظام أو القيام بحذفها أو تعديلها دون إذن، كما يشمل القانون تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار بالبيانات المخزنة أو التي تتم معالجتها أو إرسالها عبر نظام معلوماتي بالإضافة إلى حيازة أو إفشاء أو استخدام تلك البيانات بشكل غير مشروع، وتشدّد العقوبات بشكل أكبر في حالات حذف أو تغيير البيانات أو تخريب عمل النظام.

وبالرغم من نص المشرع الجزائري على هذه المواد، إلا أنه لم يتطرق إلى جرائم القذف والسب الإلكتروني أو المطاردة عبر الانترنت أو الغش المعلوماتي، وإنما اكتفى بالنصوص العقابية التقليدية التي لا تتوافق مع طبيعة الجرائم السيبرانية ولا تتماشى مع مبدأ شرعية الجرائم والعقوبات وحظر القياس،

كما جرم المشرع الجزائري ضمن هذا القانون المساس بجرمة الحياة الخاصة، غير أنه لم يضع الآليات القانونية المعتمدة للتصدي لهذه الجرائم

الفقرة الثانية: تعديل قانون الإجراءات الجزائية

اتخذ المشرع الجزائري مجموعة من الإجراءات الخاصة المتعلقة بالعالم الرقمي استحدثها المشرع الجزائري بموجب قانون الإجراءات الجزائية مثل اعتراض المراسلات والتقاط الصور وتسجيل الأصوات وإجراء التسرب، حيث تستخدم هذه التدابير للتحري والتحقيق في جرائم معينة خاصة تلك التي تهدد أنظمة المعالجة الآلية للبيانات، وذلك وفق شروط محددة قانونا مثل الحصول على إذن مسبق والتأكد من طبيعة الجريمة، الحفاظ على السر المهني وإعداد تقرير من قبل ضابط الشرطة القضائية المخول،

كما أجاز المشرع اللجوء إلى التسرب وفق المادة 65 مكرر 11 من قانون الإجراءات الجزائية، حيث سمح لوكيل الجمهورية أو لقاضي التحقيق بعد إبلاغ وكيل الجمهورية أن يأذن بتنفيذ عملية التسرب تحت إشرافهم للتحقيق في الجرائم المحددة مع

‡ - مهدي رضا: المرجع السابق، ص 116.

§ - نفس المرجع، ص 117.

احترام الضمانات والشروط المقررة قانونا والمتمثلة في احترام شرط الإذن المكتوب والمسبب، ومن ثم، يمكن استخدام هوية مستعارة للقيام بالتسرب في مدة زمنية محددة تقدر بأربعة أشهر قابلة للتجديد، ويجرر تقريراً يتضمن أهم العناصر الضرورية لمعينة الجريمة *****

الفرع الثاني: سبل مكافحة الجريمة السيبرانية على ضوء القانون 04-09

قام المشرع الجزائري بإصدار القانون 04-09 كمبادرة جديدة للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال ومكافحتها، رغم ذلك يبقى تطبيق نصوصه على أرض الواقع لا يزال محدوداً حالياً بسبب عدم التركيز على الجوانب التقنية الضرورية لتصنيف هذه الجرائم وتحديد العقوبات المناسبة لمرتكبيها، ومع ذلك يشمل القانون مجموعة من التدابير الوقائية والإجرائية لمكافحة هذه الجرائم:

الفقرة الأولى: التدابير الوقائية

من بينها:

1- المراقبة الالكترونية: في حالات محدودة وفق إذن كتابي من السلطات القضائية المختصة، يلجأ إلى هذا الإجراء للوقاية من الأعمال الإرهابية أو التخريبية أو الجرائم التي تمس بأمن الدولة، أو في حالة وجود معلومات تدل على اعتداء محتمل على نظام معلوماتي يهدد النظام العام أو الأمن العام أو المؤسسات الوطنية أو الاقتصاد الوطني

2- الاستعانة بمزودي الخدمات للوقاية من الجرائم السيبرانية: ويكون ذلك من خلال قيام مزودي الخدمات بتقديم المساعدة للجهات المسؤولة على التحريات القضائية بهدف جمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات بشكل فوري، كما يتم وضع هذه المعطيات تحت تصرف السلطات المختصة:

- المعطيات التي تتيح التعرف على مستعملي الخدمة
- البيانات المتعلقة بالأجهزة الطرفية المستخدمة في الاتصالات
- المواصفات التقنية بالإضافة إلى تاريخ ووقت ومدة كل اتصال
- بيانات عن الخدمات التكميلية المطلوبة أو المستخدمة ومقدميها
- المعلومات التي تتيح التعرف على المرسل إليهم وعناوين المواقع التي تمت زيارتها.

الفقرة الثانية: التدابير الإجرائية

من بينها:

1- تفتيش وحجز المنظومة المعلوماتية:

***** - نفس المرجع، ص 118.

† - نفس المرجع، ص 119.

وذلك لمتطلبات حفظ النظام العام أو لمقتضيات التحريات القضائية الجارية، غير أن إجراء الحجز قد تعترضه عدة صعوبات لأسباب تقنية مما يستوجب على السلطات التي تقوم بالتفتيش استعمال تقنيات مناسبة لمنع الوصول إلى البيانات المتواجدة في النظام المعلوماتي وإلى النسخ المتاحة للأشخاص المصرح لهم باستخدام هذا النظام.

2- تمديد الاختصاص بنظر هذه الجرائم:

تتولى المحاكم الجزائرية اختصاص النظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج البلاد بشرط أن يكون مرتكب الجريمة أجنبيا وأن تمس الجريمة تمس مؤسسات الدولة الجزائرية أو دفاعها الوطني أو مصالحها الإستراتيجية.

3- تبادل المساعدة القضائية الدولية:

فيما يتعلق بتبادل المساعدة القضائية الدولية، سمح المشرع الجزائري بإجراءات تهدف إلى جمع الأدلة المتصلة بالجريمة الالكترونية، كما يمكن للمحاكم الاستجابة لطلبات المساعدة المتعلقة بتبادل المعلومات أو اتخاذ إجراءات احترازية وفقا للاتفاقيات الدولية أو مبدأ المعاملة بالمثل .

4- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

أنشأت هذه الهيئة بموجب القانون 04-09 وبقيت تشكيلتها وتنظيمها وكيفية سيرها لتحديد عن طريق التنظيم والذي شهد تغييرات عديدة ابتداء من المرسوم الرئاسي لسنة 2015 ثم سنة 2019 إلى غاية المرسوم الرئاسي لسنة 2020 الذي أعاد تنظيم الهيئة .

الفرع الثالث: القوانين اللاحقة المدعمة للقانون 04-09 في مجال الحد من الإجرام السيبراني

الفقرة الأولى: القانون 04-18 المتعلق بالقواعد العامة المتعلقة بالبريد والاتصالات الالكترونية

تضمن هذا القانون مجموعة من الآليات بهدف التصدي للجرائم المتعلقة بالعالم الافتراضي منها:

- إنشاء هيئة تنظيمية تتولى ضمان التزام مقدمي خدمات البريد والاتصالات الالكترونية بالقوانين والأنظمة ذات العلاقة.
- تجريم انتهاك سرية المراسلات المرسلة عن طريق البريد أو الاتصالات الالكترونية أو إفشاء مضمونها أو نشرها أو استعمالها دون ترخيص من المرسل أو المرسل إليه أو الإخبار بوجودها، وتجريم محاولة فتح أو تخريب أو تحويل البريد أو المساعدة في ارتكاب هذه الجريمة .

الفقرة الثانية: القانون 07-18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي

قام المشرع الجزائري بتطوير مجموعة من الآليات المتعلقة بالعالم الافتراضي والتي يمكن تلخيصها في عدة نقاط:

‡ - نفس المرجع، ص 121.

§ - نفس المرجع ونفس الصفحة.

- إنشاء سلطة وطنية متخصصة لحماية البيانات ذات الطابع الشخصي،
- وضع مجموعة التزامات ملقاة على عاتق المسؤول عن المعالجة الآلية للمعطيات ذات الطابع الشخصي،
- اتخاذ مجموعة من الإجراءات الإدارية من طرف السلطة الوطنية في حالة خرق أحكام القانون من طرف المسؤول عن المعالجة،
- تقوم السلطة الوطنية بإجراء تحريات ومعاينات للمحلات والأماكن التي تتم فيها المعالجة مع استثناء المحلات السكنية، كما تتمتع السلطة بصلاحيات الوصول إلى المعطيات المعالجة وكافة المعلومات والوثائق بغض النظر عن الوسيلة التي تم تخزينها بها،
- تأهيل أعوان رقابة للقيام ببحث ومعاينة الجرائم المتعلقة بالمعطيات ذات الطابع الشخصي تحت إشراف وكيل الجمهورية،

- يمكن للمدعي في حالة المساس بحق من حقوقه المتضمنة في هذا القانون أن يلجأ إلى القضاء ويطلب اتخاذ أي إجراءات تحفظية للحد من التعدي أو للحصول على تعويض،
- تجريم الاعتداء على المعطيات ذات الطابع الشخصي بإفراد عقوبات مالية أو أخرى سالبة للحرية وفقا للمواد من 54 إلى 74 من هذا القانون.

بالرغم من الجهود التي تبذلها الدولة، يرى المختصون أن البنية التنظيمية والتشريعية لا تزال غير محكمة بالقدر الكافي، فمع أن هناك قوانين تحتوي على قواعد ملزمة وراعية، إلا أن العديد من الجوانب لم تتطور لتناسب مع البيئة الوطنية ك معايير الحماية الدولية، المواصفات التقنية للمعلومات، البيانات، الأنظمة، البرامج والأجهزة التي وردت في اتفاقية بودابست الدولية لعام 2001

خاتمة:

لقد سهلت تكنولوجيا المعلومات والاتصالات الكثير من الإجراءات العملية، لكنها في المقابل أدت الى انتشار الكثير من المشكلات والجرائم التي باتت تهدد البيئة الرقمية، خاصة في المجتمعات النامية التي مازالت تعاني من الفجوة

- نفس المرجع، ص 122.

† - قطاف سليمان، بوقرين عبد الحليم: الآليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل اتفاقية بودابست والتشريع الجزائري،
المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد 06، العدد 01، 2022، ص 354.

الرقمية نتيجة انتشار الأمية الرقمية وعدم التحكم في استخدام هذه التقنيات الحديثة، مما يستوجب اتخاذ إجراءات مشتركة بين الدول بهدف التصدي لهذه التهديدات أو للتقليل من آثارها الوخيمة.

إن مواجهة انعكاسات الجريمة السيبرانية أضحت من أصعب التحديات التي تتطلب تضافر الجهود، خاصة وان استخدام هذه التكنولوجيات في تزايد مستمر في إدارة مختلف الشؤون الأمنية والاقتصادية والعسكرية، مما يتطلب التعاون بين الدول في مجال امن المعلومات ومواجهة الجريمة السيبرانية على المستويين الدولي والوطني.

ومن أهم التوصيات التي يمكن أن نقدمها في نهاية هذا البحث:

- ضرورة مواكبة تطورات الجريمة السيبرانية من خلال إجراء بحوث ودراسات لمعرفة الأسباب الكامنة وراء انتشار مثل هذه المشكلات ومحاولة إيجاد الآليات التي يمكن أن تقلص من آثارها الوخيمة.
- العمل على نشر ثقافة الوعي في استخدام هذه التكنولوجيات التي يعد غيابها سبب رئيسي في انتشار الجريمة.
- تكثيف وتعزيز التعاون على المستوى الوطني والدولي على حد سواء.
- توفير الآليات الخاصة بالاستخبارات التي تساهم في استشعار التهديدات قبل وقوعها من خلال كشف المبكر.

قائمة المراجع:

1. المقال المنشور:

- نبيل دريس: الجريمة السيبرانية بين المفاهيم والنصوص التشريعية - الجزائر نموذجاً - مجلة القانون والمجتمع، المجلد 05، العدد 02، 2017.
- مائنو جيلالي، عروس كوثر: الجريمة السيبرانية في صورها المستحدثة، مجلة القانون والتنمية، المجلد 04، العدد 01، جويلية 2022.
- الطيب عيساوي، هشام شكاردة: التربية الإعلامية كآلية للحد من الجريمة السيبرانية على شبكة الانترنت بين إلزامية التأطير وضرورة الاستخدام، المجلة الجزائرية للأبحاث والدراسات، المجلد 03، العدد 04، سبتمبر 2020.
- مهدي رضا: الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري، مجلة ايليزا للبحوث والدراسات، المجلد 06، العدد 02، 2021.
- حكيمة جاب الله: انعكاسات الجريمة السيبرانية على البيئة الرقمية: دراسة في آليات واستراتيجيات مكافحتها، حوليات جامعة الجزائر 1، المجلد 35، العدد 03، 2021.
- قطاف سليمان، بوقرين عبد الحليم: مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية، مجلة البحوث القانونية والاقتصادية، المجلد 05، العدد 02، 2022.
- عمار مراد العيساوي: الإطار القانوني للجريمة السيبرانية، المجلة الشاملة للحقوق، المجلد 02، العدد 04، 2022.
- لامية طالة: التهديدات والجرائم السيبرانية: تأثيرها على الأمن القومي للدول واستراتيجيات مكافحتها، مجلة معالم للدراسات القانونية والسياسية، المجلد 04، العدد 02، 2020.
- قطاف سليمان، بوقرين عبد الحليم: الآليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل اتفاقية بودابست والتشريع الجزائري، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد 06، العدد 01، 2022.
- دراغو عز الدين: الآثار الاقتصادية والمالية للهجمات السيبرانية في ظل التحول الرقمي: النتائج، التجارب والحلول مع الإشارة لحالة الجزائر، مجلة التكامل الاقتصادي، المجلد 10، العدد 02، 2022.
- عبد العزيز بن فهد بن محمد بن داود: الجرائم السيبرانية: دراسة تأصيلية مقارنة، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد 09، العدد 03، 2020.