الجمهورية الجزائرية الديموقراطية الشعبية

وزارة التعليم العالي و البحث العلمي

جامعة محمد البشير الابراهيمي –برج بوعريريج–

كلية الحقوق و العلوم السياسية

مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر اكاديمي في الحقوق

تخصص: قانون إعلام آلي و انترنت

الموسومة ب:

مقتضيات التعامل مع الجرائم السيبيرانية في الجزائر

إعداد الطالبين:

ميهوبي هشام

حسام جلاد

إشراف:

الدكتور هدفي العيد

لجنة المناقشة

داود حسين	أستاذ محاضر قسم –أ–	رئيسا
هدفي العيد	أستاذ التعليم العالي	مشرفا و مقررا
بلعقون محمد الصالح	أستاذ مساعد قسم –ب–	ممتحنا

السنة الجامعية: 2025/2024.

2020 ماي 27

ملحق بالقرار رقم ...1082.... المؤرخ في ....

الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي

الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

(الطالب الثاني)

أنا الممضي أسفله،

السيد(ة): جلاد حسام .... الصفة: طالب، أستاذ، باحث ..... طالب

الحامل(ة) لبطاقة التعريف الوطنية رقم: .... والصادرة بتاريخ ....

المسجل(ة) بكلية / معهد الحقوق ..... قسم القانون العام

والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج، مذكرة ماستر، مذكرة ماجستير، أطروحة دكتوراه).

عنوانها: مقتضيات التعامل مع الجرائم

السيبرانية في الجزائر

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في انجاز البحث المذكور أعلاه .

2025 ماي 22

التاريخ: ....

توقيع المعني (ة)

... د للمصادقة على التوقيع أو البصم

... (ة) جلاد حسام

... 108611401

... 2018 04 ...

2025 ماي 22

ملحق بالقرار رقم ....1082.... المؤرخ في ..... 27 ديسمبر 2020 .....
الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي

الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

(الطالب الأول)

أنا الممضي أسفله،

السيد(ة): سهيلي هشام ..... الصفة: طالب، أستاذ، باحث طالب

الحامل(ة) لبطاقة التعريف الوطنية رقم: 100838316 والصادرة بتاريخ 09 ديسمبر 2016

المسجل(ة) بكلية / معهد الحقوق قسم القانون العام

والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج، مذكرة ماستر، مذكرة ماجستير، أطروحة دكتوراه)،

عنوانها: مقتضيات التعامل مع الجرائم المستحدثة في التشريع الجزائري

أصرح بشرفي أنني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه .

التاريخ: 22 ماي 2025

توقيع المعني (ة)

شهد للمصادقة على التوقيع أو البصمة
للسيد (ة) سهيلي هشام
رقم 100838316
صادر بتاريخ 09 ديسمبر 2016
22 ماي 2025
رئيس المجلس الشعبي البلدي
بالنيابة
نائب الرئيس المفوض
خوخ احميدة

الاهداء

اهدي هذا العمل الى الوالد الكريم اطال الله في عمره،

والى رح الوالدة العزيزة التي لم يكتب لنا الله ان تسجل حضورها في اي من النجاحات طوال المشوار الدراسي رحمها الله واسكنها الجنان،

الى الاخوات و ابنائهن جوزاف باشا شفاء و طاوس ..

الى الطبيب ..

كما لا ننسى من كان سببا وصاحب الفضل بعد الله في هذا المشوار " azihed " ،

والى جميع الاصدقاء ومن كان سند لنا في هذا المشوار الدراسي اليكم جميعا.

هشام

الاهداء

بكل امتنان وتقدير، أهدي هذا العمل إلى عائلتي العزيزة،

السند الأول والداعم الدائم في كل مراحل حياتي،

وإلى أصدقائي الذين كانوا لي عونًا بالكلمة والتشجيع.

كما أخصّ بالشكر كل من ساهم من قريب أو بعيد في إنجاح هذا العمل،

فبفضل دعمهم وتوجيههم،

أصبح لهذا الجهد معنى وقيمة.

حسام

الفهرس

مقدمة

مقدمة:

يشهد العالم اليوم تطورًا غير مسبوق في مجال التكنولوجيا، حيث باتت التقنيات الرقمية تسيطر على مختلف جوانب الحياة اليومية، محولةً العالم إلى قرية مترابطة من خلال شبكات الاتصال الإلكترونية. هذا التطور ساهم في تسهيل حياة الإنسان، إذ أصبح بإمكانه إدارة الأعمال وتنظيم حياته اليومية عبر المنصات الرقمية، لا سيما شبكة الإنترنت، مما وفر مستوىً عاليًا من الراحة والرفاهية. ومع ذلك، لم يخلُ هذا التقدم من تحديات ومخاطر تهدد الأفراد والمؤسسات والدول، إذ تزايدت الجرائم السيبرانية مثل الاختراقات الإلكترونية، الاحتيال المالي، التجسس، والإرهاب الإلكتروني، مؤثرةً بشكل مباشر على الأمن والاستقرار الدولي و الوطني.

في هذا الإطار، لم تكن الجزائر بمنأى عن هذه التهديدات السيبرانية، حيث تعرضت العديد من مؤسساتها الوطنية لهجمات إلكترونية، كان من أبرزها اختراق برنامج "بيقاسوس" الإسرائيلي، إلى جانب ازدياد جرائم الاحتيال والنصب التي تستهدف الأفراد والمؤسسات عبر شبكات التواصل الاجتماعي. وموقع الجزائر الاستراتيجي جعلها هدفًا رئيسيًا للهجمات الإلكترونية سواء من جهات دولية أو أفراد، مما دفعها إلى تبني سياسات أمنية لتعزيز أمنها السيبراني ومواجهة هذه المخاطر المتزايدة.

مع انتهاء الحرب الباردة، شهد النظام الدولي تحولات جوهرية أثرت على مفهوم الأمن القومي، حيث أدى التطور التكنولوجي إلى ظهور تهديدات غير تقليدية وعابرة للحدود، على رأسها الحروب الإلكترونية والسيبرانية التي أصبحت تمثل تحديًا استراتيجيًا للدول. وقد أدركت الجزائر، مثل باقي الدول، أهمية تعزيز أمنها السيبراني لمواجهة هذه التحديات، لا سيما بعد تصنيف الفضاء السيبراني كميدان خامس في الحروب، إلى جانب البر والبحر والجو والفضاء.في هذا الإطار، تهدف هذه الدراسة إلى تسليط الضوء

على متطلبات مواجهة الجرائم السيبرانية في الجزائر، من خلال تحليل الإطار التشريعي الوطني والدولي، واستكشاف الآليات الفعالة لمكافحة هذه الجرائم. كما تسعى إلى استعراض التحديات التي تواجه الجزائر في هذا المجال، وتقديم مقترحات لتعزيز الأمن السيبراني عبر التدابير الوقائية والتشريعات الملائمة.

إشكالية الدراسة:

على ضوء ما سبق نطرح الاشكالية التالية:

"إلى أي مدى تُعد الأطر القانونية والمؤسساتية في الجزائر فعالة في التصدي للجرائم السيبرانية في ظل التحديات التقنية والقانونية الراهنة؟ وما هي السبل الكفيلة لتعزيز الأمن السيبراني؟"

أهمية الموضوع:

تكتسب هذه الدراسة أهميتها من دورها في تعزيز الفهم العميق لطبيعة الجرائم السيبرانية والتحديات المرتبطة بمكافحتها في الجزائر، كما تشكل مرجعًا قيّمًا للباحثين وصناع القرار في مجال الأمن السيبراني.

أهداف الدراسة:

تسعى الدراسة إلى تقديم رؤية متكاملة حول التحديات التي تفرضها الجرائم السيبرانية، وآليات مواجهتها، مع التركيز بشكل خاص على السياق الجزائري في ظل التحولات الرقمية المتسارعة التي يشهدها العالم.

منهج الدراسة:

طبيعة هذا الموضوع فرضت علينا منهجين هما المنهج الوصفي والمنهج التحليلي.

خطة الدراسة:

من خلال تتبع تفاصيل و طبيعة هذا الموضوع وجدنا انه من اللازم تقسيم دراستنا الى فصلين لكل فصل ثلاث مباحث مع مجموعة من التفرعات بمقدمة و خاتمة.

الفصل الاول:

الجريمة السيبرانية (المفاهيم والأسس)

الفصل الاول: الجريمة السيبرانية (المفاهيم والأسس)

يمثل هذا الفصل مدخلًا تمهيديًا لفهم ظاهرة آخذة في التصاعد والتعقيد، تتمثل في الجريمة السيبرانية، التي باتت تُعد من أبرز التحديات التي تواجه المجتمعات المعاصرة في ظل الثورة الرقمية. فمع التطور المتسارع في تقنيات الاتصال والاعتماد الواسع على الفضاء السيبراني في مختلف مناحي الحياة، أضحى من الضروري التعمق في دراسة طبيعة هذه الجرائم وأساليبها وأطرها القانونية والأمنية من أجل التصدي لها بفعالية.

يهدف هذا الفصل إلى تأسيس قاعدة معرفية شاملة حول الجريمة السيبرانية، من خلال تناول الأسس النظرية التي تُسهم في توضيح معالمها وفهم بنيتها القانونية والأمنية. وقد تم تقسيمه إلى ثلاثة مباحث رئيسية، من خلال هذا البناء، يهدف الفصل الأول إلى تزويد القارئ بفهم معمق للأسس النظرية للجريمة السيبرانية، ليكون بمثابة قاعدة تمهيدية للانتقال لاحقًا إلى دراسة الجوانب التطبيقية والتحديات الواقعية المرتبطة بها.

المبحث الأول: الإطار المفاهيمي للجريمة السيبرانية

يهدف هذا المبحث إلى تقديم تصور واضح لمفهوم الجريمة السيبرانية، من خلال استعراض التعريفات المتداولة في الفقه القانوني والأدبيات الأمنية، مع تسليط الضوء على التحديات المرتبطة بتأطيرها القانوني نتيجة تباين الأنظمة التشريعية الوطنية والدولية. كما يتناول الخصائص الجوهرية التي تميز هذا النمط من الجرائم عن الأشكال التقليدية، سواء من حيث طبيعة الوسائل المستخدمة، أو خصائص الجناة والضحايا، أو من حيث صعوبة الكشف عنها وملاحقة مرتكبيها قانونيًا.

المطلب الاول: تعريف الجريمة السيبرانية.

1. التعريف اللغوي للجريمة السيبرانية:

يتكوّن مصطلح "الجريمة السيبرانية" من كلمتين: "الجريمة" و"السيبرانية". لذا، سنبدأ أولًا بتعريف "الجريمة" من الناحية اللغوية، ثم ننتقل إلى تعريف "السيبرانية" من حيث المعنى اللغوي.

- التعريف اللغوي للجريمة:

تُستخدم كلمة "الجريمة" في اللغة للدلالة على معنيين:

أ. الذنب: حيث يُقال "جرم" و"أجرم" و"اجترم" بمعنى واحد، أي ارتكب ذنبًا.

ب. الجناية: كما يُقال "جرم إليهم" و"عليهم جريمة"، و"أجرم"، أي اقترف جناية. ويُقال أيضًا "جرم" إذا كان جرمه عظيمًا، أي ارتكب إثمًا جسيمًا.[1]

- التعريف اللغوي للسيبرانية:

كلمة Cyber هي مصطلح إنجليزي. وقد عرّف قاموس أكسفورد مصطلح "سيبراني" أو Cyber على أنه صفة تُطلق على أي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو العالم الافتراضي.[2]

---

[1] لطفي، خالد حسن أحمد. الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية. الإسكندرية: دار الفكر الجامعي، الطبعة الأولى، 2222، ص 13.

[2] الروضان، وليد أحمد. "ما الفرق بين أمن المعلومات والأمن السيبراني". صحيفة الجزيرة الإلكترونية، مؤسسة الجزيرة للصحافة والنشر، العدد 16631، 1431هـ. متاح على: https://www.al-jazirah.com/2018/20180411/rj3.htm.

2. التعريف الشرعي للجريمة:

تُعرَّف الجريمة شرعًا بأنها ارتكاب فعل محرَّم يستوجب العقوبة، أو الامتناع عن فعل واجب يُعاقَب على تركه. كما يمكن تعريفها بأنها أي فعل أو ترك حرَّمته الشريعة الإسلامية ورتَّبت عليه عقوبة.[1]

3. مفهوم الجرائم السيبرانية في التشريع الجزائري:

تُعرف الجريمة السيبرانية بأنها أي فعل ضار يرتكبه شخص يمتلك معرفة بتقنيات الحاسوب، مستخدمًا نظامًا حاسوبيًا أو شبكة حاسوبية، بهدف الوصول إلى البيانات أو البرامج، وذلك بغرض نسخها أو تعديلها أو حذفها أو تزويرها أو تخريبها أو تعطيلها، أو حتى حيازتها وتوزيعها بطرق غير قانونية.[2]

حدد المشرع الجزائري مفهوم هذا النوع من الجرائم في الفقرة الأولى من المادة الثانية من القانون رقم 04-09 الصادر في 5 أغسطس 2009، والمتعلق بوضع قواعد خاصة للوقاية من الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال ومكافحتها.[3]

وقد استخدم المشرع مصطلح "الجرائم المتصلة بتكنولوجيات الإعلام والاتصال"، موضحًا أنها تشمل الجرائم التي تستهدف أنظمة المعالجة الآلية للمعطيات، كما هو

---

[1] عياد، سامي علي حامد. الجريمة المعلوماتية وإجرام الإنترنت. الإسكندرية: دار الفكر الجامعي، بدون طبعة، 2007، ص 12.

[2] السالك، كامل فريد. الجريمة الإلكترونية. محاضرة ألقيت في ندوة التنمية ومجتمع المعلوماتية، 21-23 أكتوبر 2000، الجمعية السورية للمعلوماتية، حلب، سورية.

[3] القانون رقم 04-09 المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، الصادر بتاريخ 16 أوت 2009.

منصوص عليه في قانون العقوبات، إضافةً إلى أي جريمة أخرى تُرتكب أو يُسهَّل ارتكابها عبر منظومة معلوماتية أو نظام اتصالات إلكتروني.[1]

يتضح أن المشرع الجزائري تبنّى مفهومًا واسعًا لهذا النوع من الجرائم، فبالرغم من تقييدها بالجرائم المرتبطة بتكنولوجيات الإعلام والاتصال، إلا أنه ترك المجال مفتوحًا ليشمل أي جريمة قد تنشأ بفعل التطور التكنولوجي. ويتجلى ذلك بوضوح في نص المادة، التي نصت على: "أو أي جريمة أخرى تُرتكب أو يُسهَّل ارتكابها عبر منظومة معلوماتية أو نظام للاتصالات الإلكترونية". وهذا يدل على إدراك المشرع للتطور السريع في هذا المجال، وحاجته إلى تشريعات مرنة تواكب هذه المستجدات.[2]

المطلب الثاني: خصائص الجريمة السيبرانية.

تتميز الجرائم السيبرانية بخصائص فريدة تميزها عن الجرائم التقليدية، وذلك بسبب طبيعتها الخاصة والعناصر التي تتكون منها، بالإضافة إلى الأدوات والتقنيات المستخدمة في ارتكابها. وتتمثل هذه الخصائص في:

- تُرتكب الجرائم السيبرانية عبر التقنيات التكنولوجية الحديثة، وعلى رأسها شبكة الإنترنت، التي تُستخدم كأداة رئيسية لتنفيذها.
- **<u>من حيث الهدف:</u>** تهدف هذه الجرائم إلى اختراق الأنظمة المعلوماتية بغرض التلاعب بالبيانات أو تشويه المعلومات الخاصة بمستخدمي الفضاء الرقمي، بما يشابه بعض الجرائم التقليدية.

[1] المادة 2 من القانون 04-09، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[2] زناتي، محمد السعيد. الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية، مقال منشور في مجلة إليزا للبحوث والدراسات، الصادرة عن المركز الجامعي بإليزي – الجزائر، العدد 02، سنة 2017، ص 33-34.

- تُعد الجريمة السيبرانية من الجرائم الناعمة نظرًا لسهولة تنفيذها وصعوبة اكتشافها، حيث قد لا يلاحظ الضحية وقوعها أثناء تصفحه للشبكة. ويتمتع مرتكبها بمهارات تقنية متقدمة تتيح له ارتكابها دون ترك أدلة واضحة، مثل سرقة الأموال أو إرسال فيروسات خبيثة تستهدف البرامج وأجهزة الكمبيوتر.[1]
- **صعوبة اكتشافها:** تتميز الجريمة السيبرانية بصعوبة تعقب مرتكبيها، نظرًا لعدم وجود آثار مادية ملموسة يمكن أن تستعين بها سلطات الأمن وأجهزة التحقيق لتحديد الجاني. إذ تعتمد البيئة الرقمية على بيانات ومعلومات مخزنة في صورة نبضات إلكترونية غير مرئية، مما يسهل على الفاعل إخفاء الأدلة الرقمية أو محوها بالكامل بسرعة ودقة، مما يزيد من تعقيد عملية الكشف عنها.[2]
- **جريمة ذات بعد دولي:** تتسم الجريمة السيبرانية بطابعها العابر للحدود، إذ لا تخضع لقيود الزمان أو المكان، حيث يمكن أن يكون الجاني والمجني عليه في مواقع جغرافية متباعدة وفي مناطق زمنية مختلفة. ويعود ذلك إلى طبيعة الفضاء الرقمي، الذي يتجاوز الحدود الجغرافية، مما يتيح تنفيذ هذه الجرائم عبر شبكات مفتوحة دون أي رقابة أو قيود تقليدية.[3]
- **جرائم يصعب إثباتها:** تُعد الجرائم السيبرانية من أكثر الجرائم تعقيدًا من حيث الإثبات، حيث غالبًا ما يتم اكتشافها بمحض الصدفة، ويصعب تتبعها أو تحديد موقع حدوثها بسبب عدم تركها أي آثار مادية ملموسة. فهي تتجسد في شكل بيانات وأرقام تتنقل

[1] الصغير، يوسف. الجريمة المرتكبة عبر الإنترنت. رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013/2012، ص 14-15.

[2] الصغير، عبد المؤمن. الطبيعة الخاصة للجريمة الإلكترونية المرتكبة عبر الإنترنت في التشريع الجزائري والتشريع المقارن. مجلة الحقوق والحريات، جامعة محمد خيضر، بسكرة، المجلد 02، ص 08.

[3] التميمي، تميم عبد الله سيف. الجرائم المعلوماتية في الاعتداء على الأشخاص. مكتبة القانون والاقتصاد، الرياض، الطبعة الأولى، 2016، ص 16.

داخل الأنظمة الرقمية والمواقع الإلكترونية، مما يجعل عدد الجرائم غير المكتشفة يفوق بكثير تلك التي يتم الكشف عنها. وتعود هذه الصعوبة إلى عدة أسباب، منها:

أ. عدم ترك أي أثر ملموس بعد ارتكاب الجريمة.

ب. صعوبة الاحتفاظ بالأدلة الرقمية وإمكانية محوها بسرعة.

ت. الحاجة إلى خبرة فنية متخصصة يصعب على المحقق التقليدي امتلاكها.

ث. اعتماد مرتكبيها على تقنيات التمويه والخداع لإخفاء هوياتهم.

ج. تتطلب مستوى عالٍ من الذكاء واستخدام أدوات تقنية متطورة لتنفيذها.[1]

المبحث الثاني: دوافع وتصنيفات الجريمة السيبرانية

و ينقسم الى مطلبين:

المطلب الاول: أسباب الجريمة السيبرانية.

مع الانتشار الواسع لشبكة الإنترنت وتعقيد السيطرة على الفضاء السيبراني في بعض الدول، أصبحت أجهزة الاستخبارات تستغل هذه الشبكات في النزاعات الدولية، وذلك من خلال اختراق الأنظمة الرقمية، والسيطرة عليها، أو تعطيلها، أو حذف البيانات، أو إتلافها، أو حتى استخدامها كوسيلة للضغط على الدول المستهدفة. بالإضافة إلى ذلك، تسهم الدوافع الفردية، مثل السعي للتشهير بالآخرين أو تحقيق مكاسب غير مشروعة، في تفاقم هذه الجرائم وانتشارها.

[1] محمود أحمد القرعان، الجرائم الإلكترونية، دار وائل للنشر والتوزيع، عمان، الطبعة الأولى، 2017، ص 40.

1. الاسباب السياسية:

يصعب تحديد هوية مرتكبي الجرائم السيبرانية، لا سيما في الهجمات الإلكترونية المعقدة والمتطورة، حيث كلما ازداد تعقيد الهجوم، أصبحت عملية التعرف على الفاعل ودوافعه أكثر صعوبة. لهذا السبب، غالبًا ما تنكر الدول المتهمة بتنفيذ هذه الهجمات أي صلة لها بها، كما حدث مع روسيا في استهداف إستونيا وجورجيا، ومع الولايات المتحدة وإسرائيل في قضية فيروس "ستاكنست". ويعود ذلك إلى عدم قدرة الدول المستهدفة على تقديم أدلة دامغة تثبت تورط جهة معينة أو تحميلها المسؤولية المباشرة. ونتيجة لذلك، بات بإمكان الدول تحقيق أهدافها السياسية من خلال الهجمات الإلكترونية، بدلًا من استخدام القوة العسكرية التقليدية.[1]

2. الأسباب الفكرية والمادية:

تنشأ هذه الأسباب من رغبة بعض الأفراد في تحقيق المتعة وإثبات الذات، حيث قد تُمارَس القرصنة كوسيلة للتسلية وملء وقت الفراغ، خاصة لدى الشباب الذين يسعون إلى استعراض مهاراتهم في التكنولوجيا وإبراز تفوقهم فيها.[2]

وفي المقابل، قد يكون السبب ماديًا بحتًا، إذ يلجأ البعض إلى الجرائم السيبرانية سعياً لتحقيق مكاسب مالية سريعة، من خلال الوصول غير المشروع إلى معلومات حساسة وذات قيمة عالية بالنسبة لأطراف معينة.[3]

---

[1] بهاء، عدنان. "انتقال التهديدات من الواقع إلى العالم الافتراضي." مجلة بابل للعلوم الإنسانية، المجلد 27، العدد 4، العراق، 2019، ص 476.

[2] وفاء، محمد علي. "الأبعاد الاجتماعية للجرائم الإلكترونية: دراسة تحليلية لمضمون عينة من القضايا في محكمة سوهاج". مجلة كلية التربية في العلوم الإنسانية والأدبية، المجلد 27، العدد 3، 2021، ص 454.

[3] طعبة، سعاد. "الجريمة الإلكترونية: تفعيل لآليات القانون من أجل تحقيق العدالة". مجلة الحقوق والعلوم الإنسانية، العدد 15، 2022، ص 229.

3. الأسباب الاجتماعية والاقتصادية:

يعد الانحراف الإجرامي نتيجة طبيعية للصراعات النفسية والاجتماعية التي تنشأ عن مشاعر الفشل والإحباط وعدم تحقيق الأهداف الحياتية. وتتفاعل هذه العوامل مع البيئة الاجتماعية التي ينتمي إليها الأفراد، مما قد يؤدي إلى اضطرابات نفسية واجتماعية تدفع بعضهم إلى ارتكاب الجرائم.[1]

ومن أبرز العوامل المؤثرة في ذلك: البطالة، والفقر، والتهميش السياسي والاجتماعي، حيث يشعر الأفراد بعدم الأمان في ظل غياب دخل ثابت يوفر لهم مستوى معيشيًا كريمًا. كما أن الأزمات الاقتصادية والتحولات التي يشهدها المجتمع تؤثر بشكل مباشر على سلوك الأفراد وتوجهاتهم.

إضافة إلى ذلك، يسهم تفكك الروابط الأسرية وضعف الرقابة الأبوية في زيادة احتمالية انخراط الأفراد في سلوكيات إجرامية. وفي هذا السياق، برزت الجرائم الإلكترونية العابرة للحدود، التي تعتمد على تكنولوجيا الشبكات، كإحدى الأشكال الحديثة للجريمة في العصر الرقمي.[2]

المطلب الثاني: أنواع الجرائم السيبرانية.

تُصنَّف الجرائم السيبرانية إلى عدة أنواع بناءً على طبيعتها والأهداف التي تسعى إلى تحقيقها. ورغم التمييز بين جرائم الحاسب الآلي، التي تستهدف أنظمته وبرامجه وبياناته

---

[1] العطيان، تركي بن محمد. "البطالة وعلاقتها بالسلوك الإجرامي: دراسة نظرية على المجتمع السعودي". المجلة العربية للدراسات الأمنية، المجلد 21، العدد 41، 2006، ص 341-403.

[2] Chareonwongsak, K. "Globalization and Technology: How Will They Change Society?" Technology in Society, vol. 24, no. 3, 2002, p. 191.

المخزنة، وجرائم الإنترنت، التي تتعلق بنقل المعلومات والبيانات عبر الشبكات، إلا أن التطورات التقنية دمجت هذين المجالين تحت مصطلح "CYBERCRIME". وبناءً على ذلك، يمكن تصنيف الجرائم السيبرانية إلى أربعة أنواع رئيسية وفقًا للمنهجية المعتمدة.

1. جرائم الحاسب الآلي:

تشير جرائم الحاسب الآلي إلى الأفعال التي تستهدف أجهزة الحاسوب، سواء من حيث المكونات المادية (HARDWARE)، مثل وحدات الإدخال والإخراج، ووسائل التخزين المرنة والصلبة، والشاشات والطابعات، أو من حيث المكونات المعنوية (SOFTWARE & DATA BASES)، مثل البيانات والمعلومات المخزنة داخله. وتتفاوت هذه الجرائم وفقًا لطبيعة العنصر المستهدف، فقد يكون الاعتداء موجّهًا نحو الأجهزة والمعدات، أو نحو البرامج والبيانات المخزنة داخل الحاسب. وفي كلتا الحالتين، يظل الحاسب الآلي ومحتوياته الهدف الأساسي للنشاط الإجرامي.[1]

2. جرائم الإنترنت:

تشمل جرائم الإنترنت جميع الأفعال غير المشروعة التي تستهدف المواقع الإلكترونية، سواء من خلال تعطيلها أو تشويهها أو التعديل عليها دون إذن، أو الاختراق غير المشروع لمواقع غير مصرح بالدخول إليها. كما تشمل استخدام عناوين مزيفة للوصول إلى شبكات المعلومات، واقتحام الشبكات، ونقل الفيروسات لإلحاق الضرر بالأنظمة. بالإضافة إلى ذلك، تندرج تحتها إرسال رسائل مسيئة عبر البريد الإلكتروني، سواء كانت تمس كرامة الأفراد أو تهدف إلى الترويج لمحتويات وأفعال غير قانونية.[2]

---

[1] زناتي، محمد السعيد. "الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية ".**مجلة إليزا للبحوث والدراسات**، المركز الجامعي بإليزي، الجزائر، العدد 02، 2017، ص33.

[2] نفس المرجع السابق، ص33.

3. جرائم شبكة المعلومات:

تشمل جرائم شبكة المعلومات جميع الأفعال غير المشروعة التي تستهدف الوثائق أو النصوص المخزنة على الشبكة. ومن أبرز صورها انتهاك حقوق الملكية الفكرية للمحتويات الرقمية، مثل البرامج، والإنتاج الفني والأدبي، والأعمال العلمية. وتتطلب هذه الجرائم الاتصال بالإنترنت واستخدام الحاسب الآلي للوصول إلى قواعد البيانات بهدف الاطلاع غير المصرح به أو التعديل عليها دون إذن.[1]

4. الجرائم المرتبطة باستخدام الحاسب الآلي:

تشمل هذه الجرائم الأفعال غير المشروعة التي يُستخدم فيها الحاسب الآلي كأداة رئيسية لارتكابها، مثل الاحتيال والتزوير الإلكتروني. في السابق، كانت هذه الجرائم تُصنَّف ضمن جرائم الحاسب الآلي بشكل عام، حيث كان المصطلح يشمل كافة الجرائم التي يكون فيها الحاسب إما هدفًا أو وسيلة للجريمة. ولكن مع تطور التقنية وظهور جرائم الإنترنت، أصبح من الضروري التمييز بين الجرائم التي يكون الحاسب هدفًا لها، وتلك التي يُستخدم كوسيلة لارتكابها، مما أدى إلى تصنيف الجرائم المرتبطة باستخدام الحاسب الآلي كفئة مستقلة ضمن الجرائم السيبرانية.[2]

---

[1] زناتي، محمد السعيد. "الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية ".**مجلة إليزا للبحوث والدراسات**، المركز الجامعي بإليزي، الجزائر، العدد 02، 2017، ص 34.

[2] زناتي، محمد السعيد، مرجع سابق، ص 33-34.

المبحث الثالث: البنية القانونية والأمنية للجريمة السيبرانية

ينقسم الى اركان الجريمة السيبيرانية و ابعاد الامن السيبيراني:

المطلب الاول: أركان الجريمة السيبرانية.

تشترك الجرائم السيبرانية مع الجرائم التقليدية في كونها تتطلب توافر أركان محددة لاعتبار الفعل جريمة وفقًا لقانون العقوبات. وتعتمد هذه الجرائم، كسائر الجرائم الأخرى، على ركنين أساسيين: الركن المادي والركن المعنوي، حيث لا يمكن اعتبار السلوك جريمة دون تحقق هذين العنصرين.

إلى جانب ذلك، هناك عنصر مفترض يقرّه المشرّع مسبقًا في جرائم المعلوماتية، ويُعد جزءًا من الركن المادي للجريمة، ويتمثل في:

1. <u>الركن المادي للجريمة السيبرانية:</u>

يتطلب الركن المادي في الجرائم السيبرانية تحقق الشروط التي يحددها المشرّع، سواء من خلال توافر عناصره الثلاثة: النشاط أو السلوك المادي، العلاقة السببية، والنتيجة الإجرامية، أو بالاكتفاء بعنصر واحد فقط، وهو النشاط أو السلوك المادي.[1]

في هذه الحالة، تُعتبر الجريمة محققة دون الحاجة لإثبات تحقق النتيجة أو وجود العلاقة السببية، حتى وإن وجدت فعليًا، حيث تُصنف ضمن الجرائم الشكلية، والتي يسميها بعض الفقهاء في القانون الجنائي بـ "جريمة السلوك أو النشاط"[2].

يقصد بالنشاط أو السلوك المادي الفعل الذي يرتكبه الجاني مخالفًا لإرادة المشرّع، ويجب أن يكون لهذا الفعل مظهر خارجي واضح يمكن ملاحظته. يُعد هذا الركن عنصرًا

[1] إبراهيم، خالد ممدوح. جرائم المعلوماتية على شبكة الإنترنت، دار الفكر الجامعي، ص 98.

[2] المري، بهاء. شرح جرائم تقنية المعلومات، منشأة المعارف، ص 33.

جوهريًا في تكوين الجريمة، سواء كانت مادية أو شكلية، إذ لا يمكن وقوع أي جريمة دون وجود سلوك إجرامي. وهو النشاط الظاهر الذي يقوم به الجاني ويشكّل الجانب المادي للجريمة، وقد يتسبب في ضرر أو خطر.

كما أنه ليس بالضرورة أن يكون الهدف من هذا السلوك تحقيق نتيجة إجرامية محددة، فقد تتحقق النتيجة حتى دون أن تتجه إرادة الجاني إليها[1].

يختلف السلوك الإجرامي باختلاف نوع الجريمة، وفي الجرائم السيبرانية يختلف عن السلوك في الجرائم التقليدية، حيث يتطلب وجود بيئة رقمية خاصة. وتشمل هذه البيئة مجموعة من المواد الرقمية مثل النصوص، الصور، والفيديوهات المخزنة بصيغة رقمية، والتي يمكن الوصول إليها عبر وسائل متعددة كالكمبيوترات، الهواتف الذكية، وشبكة الإنترنت.

علاوة على ذلك، فإن السلوك المادي في الجرائم السيبرانية يستلزم تحديد بداية النشاط الإجرامي، مراحل الشروع فيه، ونتيجته. على سبيل المثال، قد يقوم الجاني بتجهيز جهازه لارتكاب الجريمة، مثل تحميل برنامج اختراق أو تطويره بنفسه، أو إعداد صفحات إلكترونية تحتوي على محتويات غير قانونية وتحميلها على الخوادم المستضيفة (Server Hosting). كما قد تتضمن هذه الجرائم تصميم ونشر الفيروسات كمرحلة أولى لتنفيذ هجوم إلكتروني.[2]

مع ذلك، ليست كل جريمة سيبرانية تتطلب تحضيرات مسبقة، إذ يرتبط السلوك الإجرامي في هذا النوع من الجرائم مباشرةً بالمعلومات المخزنة على الحاسوب. وتكمن

[1] الحجازي، عبد الفتاح بيومي. الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، بهجان للطباعة والتجليد، ص 119.

[2] إبراهيم، خالد ممدوح. جرائم المعلوماتية على شبكة الإنترنت، دار الفكر الجامعي، ص 98.

خطورتها في إمكانية تنفيذها بمجرد ضغطة زر واحدة، مما قد يؤدي إلى تدمير أنظمة مالية، مثل حذف أرصدة العملاء في أحد البنوك أو إساءة استخدام بطاقات الائتمان[1].

- النتيجة الإجرامية:

بناءً على ما سبق، تُصنّف الجريمة السيبرانية ضمن الجرائم التي تعتمد على السلوك المجرد، إذ لا يشترط تحقق نتيجة محددة لاعتبارها جريمة، بل يكفي وقوع الفعل الإجرامي ذاته.

على سبيل المثال، يُعد مجرد الإبلاغ الكاذب عن جريمة سيبرانية فعلًا مجرمًا بذاته، دون الحاجة إلى انتظار تحقق نتيجة محددة. وكذلك، فإن إنشاء موقع إلكتروني بقصد التشهير بشخص معين يُعتبر جريمة، حتى لو لم يتم نشر الموقع على الإنترنت، ومع ذلك، لا يُعفى الفاعل من المسؤولية القانونية[2].

- علاقة السببية:

تشير علاقة السببية إلى الارتباط بين السلوك الإجرامي والنتيجة الإجرامية، بحيث يثبت أن الفعل المرتكب هو السبب المباشر في وقوع النتيجة[3].

وتكمن أهمية علاقة السببية في دورها في توحيد عناصر الركن المادي للجريمة وإثبات تكاملها. فإذا لم تثبت هذه العلاقة، فإن مسؤولية الفاعل تقتصر على الشروع فقط، في حال كانت الجريمة عمدية وتوافرت عناصر الشروع. أما في الجرائم غير

[1] عبد المطلب، ممدوح عبد الحميد. جرائم استخدام الكمبيوتر وشبكة المعلومات العالمية، دار الفتح للطباعة والنشر، الإمارات (الشارقة)، 2000، ص 56.

[2] مرابط، حياة. الجريمة الإلكترونية في التشريع الجزائري، رسالة لنيل درجة ماجستير، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم – الجزائر، 2018، ص 13.

[3] حسني، محمود نجيب. الفقه الجنائي الإسلامي، دار النهضة العربية، ص 279.

العمدية، فلا يُسأل الفاعل قانونيًا، نظرًا لعدم إمكانية تصور الشروع في الجرائم غير العمدية.

تُبحث علاقة السببية بشكل عام في الجرائم المادية، وليس في الجرائم الشكلية، حيث تُعد الجريمة قائمة بمجرد وقوع السلوك الإجرامي في الجرائم الشكلية، دون الحاجة إلى تحقق نتيجة ملموسة[1].

وباعتبار أن الجرائم السيبرانية تندرج ضمن الجرائم ذات السلوك المجرد، فإن المشرّع يفرض العقوبة بمجرد وقوع الفعل، دون الحاجة إلى إثبات العلاقة السببية أو تحقق نتيجة جنائية محددة. بمعنى آخر، لا يُشترط في هذا النوع من الجرائم وجود النتيجة الجنائية أو علاقة السببية لقيام الجريمة.

مع ذلك، تتطلب الجريمة دائمًا إسنادًا ماديًا ومعنويًا، حيث يشير الإسناد المادي إلى نسبة الجريمة إلى فاعل معين وربطها بالفعل المرتكب، بينما يتعلق الإسناد المعنوي بنسبة الجريمة إلى شخص يتمتع بالأهلية القانونية لتحمل المسؤولية الجنائية، أي أن يكون قادرًا على الإدراك وحرية الاختيار[2]. ويعد كل من الإسناد المادي والمعنوي عنصرين أساسيين في المسؤولية الجنائية، إذ لا يمكن إثباتها دونهما.

ولا يختلف مفهوم علاقة السببية في الجرائم السيبرانية عن نظيره في الجرائم التقليدية، حيث تعني ارتباط الفعل التقني غير المشروع بالنتيجة الإجرامية على نحو يجعل الفعل سببًا مباشرًا في وقوع النتيجة. ومع ذلك، فإن هذه العلاقة تمتد إلى الواقع الافتراضي،

[1] الأطرقجي، هدى سالم محمد. التكييف القانوني للجرائم في القانون العقوبات العراقي، رسالة لنيل درجة دكتوراه، كلية القانون، جامعة الموصل، ص 101.

[2] عبيد، رؤوف. السببية في القانون الجنائي، مطبعة الاستقلال، ص 3.

حيث يتم ارتكاب الجريمة عبر الإنترنت، بينما تظهر آثارها في الواقع المادي. وبالتالي، تتحقق الجريمة متى ما أدى السلوك التقني غير المشروع إلى نتيجة مؤثّمة قانونًا[1].

- العنصر المفترض:

يشير العنصر المفترض إلى المركز القانوني أو الواقعي الذي يجب أن يكون متحققًا قبل وقوع الجريمة، أو هو الشرط الذي يشترطه القانون مسبقًا لقيام الجريمة، بحيث لا يمكن الحديث عن الجريمة في حال عدم وجوده[2]. وقد يرتبط هذا العنصر بالجاني، أو المجني عليه، أو محل الجريمة.

وفي سياق الجرائم السيبرانية، حيث أصبحت المعلومات والبيانات ذات قيمة تستحق حماية قانونية خاصة، فإن المحل الإجرامي يصبح عنصرًا مفترضًا لا غنى عنه في بعض الجرائم. فعلى سبيل المثال، في جريمة خيانة الأمانة السيبرانية، التي تُصنّف ضمن الجرائم العمدية وتتطلب توافر القصد الجنائي، يتحقق العنصر المفترض عندما يقوم الجاني بتسليم وسائط إلكترونية (مثل الأسطوانات التي تحتوي على برامج أو بيانات)، ثم يقوم بنسخها وإعادتها مع الاحتفاظ بنسخة لنفسه، ما يؤدي إلى تحوّل الحيازة المؤقتة إلى حيازة كاملة، على الرغم من أن الهدف الأساسي من تسليمها كان لاستخدامها في نطاق محدد وبما يخدم مصلحة صاحب الحق.

وينطبق الأمر ذاته على الجاني الذي يدرك مسبقًا الضرر الناجم عن تلاعبه بالبرامج أو البيانات التي يملك حق الوصول إليها بحكم عمله أو صلاحياته الوظيفية، لا سيما

[1] بن يونس، عمر محمد أبو بكر. الجرائم الناشئة عن الإنترنت، بدون ذكر دار النشر، ص 321.

[2] عبد المجيد، محمود سعد. الجرائم السيبرانية وانعكاسات ثورة تكنولوجيا المعلومات والاتصال على النظرية العامة للجريمة من حيث أسباب التكوين والأركان والعناصر وأساسيات المكافحة الجنائية، دار المطبوعات الجامعية، الإسكندرية، 2023، ص 201.

في حالات إفشاء المعلومات السرية أو الاستيلاء على أموال الغير [1]. ومن الجدير بالذكر أن الجريمة السيبرانية تنصب بشكل أساسي على المعلومات نفسها، بغض النظر عن الوسيط المادي الذي يحملها.

2. الركن المعنوي للجريمة السيبرانية:

يشير الركن المعنوي إلى الحالة النفسية للجاني ومدى ارتباطه بالسلوك الإجرامي الذي يرتكبه. ويُعد هذا الركن عنصرًا أساسيًا في تحديد المسؤولية الجنائية، حيث لا يمكن قيام الجريمة بدونه، إذ يمكّن المشرّع من تقييم نية الفاعل واتجاه إرادته نحو ارتكاب الفعل المحظور.

وعلى الرغم من أن الجرائم السيبرانية تُرتكب في بيئة افتراضية، فإن الركن المعنوي يظل ضروريًا لإثبات الجريمة. فيجب أن يكون الجاني على علم بأن فعله غير مشروع، ومع ذلك، يقدم عليه بإرادة حرة تهدف إلى تحقيق نتيجة معينة. وتتمثل أهمية هذا الركن في كونه يعكس مدى وعي الجاني بسلوكه الإجرامي ومدى سيطرته النفسية عليه.

لا يقتصر الركن المعنوي على مجرد توافر الإرادة، بل يجب أن تكون هذه الإرادة موجهة نحو ارتكاب الفعل الذي يجرّمه القانون. فالجاني قد يُقدم على ارتكاب الجريمة عن وعي وإدراك كاملين لنتائجها، أو قد يرتكب الفعل دون قصد مباشر لتحقيق النتيجة الإجرامية، لكنه يظل مسؤولًا عن عواقب فعله متى توافرت الظروف التي حددها القانون.[2]

- الجريمة السيبرانية كجريمة عمدية:

[1] الصغير، جميل عبد الباقي. القانون الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، 1992، ص 117.

[2] عبد المجيد، محمود سعد. الجرائم السيبرانية وانعكاسات ثورة تكنولوجيا المعلومات والاتصال على النظرية العامة للجريمة من حيث أسباب التكوين والأركان والعناصر وأساسيات المكافحة الجنائية، دار المطبوعات الجامعية، الإسكندرية، 2023، ص 206.

استنادًا إلى ما تم ذكره سابقًا حول عناصر الجريمة، فإن القصد الجنائي يُشير إلى توافر الإرادة الموجهة نحو تحقيق تلك العناصر والرضا بنتائجها. يمكن تطبيق هذا التعريف على مختلف أشكال القصد الجنائي، سواء كان مباشرًا أو احتماليًا. ويعتمد القصد الجنائي على عنصرين رئيسيين هما: العلم والإرادة، إلا أن الإرادة تُعد العنصر الأهم، حيث تمثل جوهر القصد الجنائي، بينما يُعتبر العلم مجرد شرط ضروري لتكوين الإرادة وتوجيهها بالشكل الصحيح. ويتحقق القصد الجنائي عندما تتوافر لدى الجاني الإرادة الواعية لارتكاب الفعل الإجرامي إلى جانب الإدراك الكامل لحقيقة هذا الفعل من حيث طبيعته القانونية ونتائجه المحتملة.[1]

يُعد القصد الجنائي أحد أخطر صور الركن المعنوي، إذ تنصرف إرادة الجاني إلى ارتكاب السلوك الإجرامي وما يترتب عليه من آثار جنائية. ويكمن الفرق الجوهري بين الجريمة العمدية وغير العمدية في النتيجة الإجرامية؛ فإذا كانت النية متجهة نحو تحقيق تلك النتيجة، وكان الجاني يسعى إلى وقوعها، تُعتبر الجريمة عمدية. أما إذا لم يكن الجاني يقصد النتيجة أو لم يتوقعها، أو أخطأ في تقدير آثارها دون اتخاذ الاحتياطات اللازمة لتجنبها، فإن الجريمة تُصنف عادة على أنها غير عمدية.

فيما يتعلق بالجرائم السيبرانية، يمكن أن تأخذ الاعتداءات على أنظمة الحاسب الآلي صورة الجرائم العمدية، مثل السرقة الإلكترونية، النصب، خيانة الأمانة، التزوير السيبراني، أو إتلاف المكونات المادية والبرمجية للحواسيب. وقد يترتب على هذه الأفعال

[1] عبد المجيد، محمود سعد. الجرائم السيبرانية وانعكاسات ثورة تكنولوجيا المعلومات والاتصال على النظرية العامة للجريمة من حيث أسباب التكوين والأركان والعناصر وأساسيات المكافحة الجنائية، دار المطبوعات الجامعية، الإسكندرية، 2023، ص 206.

خسائر كبيرة، كما حدث في أحد البنوك الفرنسية عندما تعرض نظامه الشبكي للتخريب، مما أدى إلى تأخير العمليات المالية، وأسفر عن خسائر قُدرت بمليوني فرنك فرنسي[1].

غالبًا ما تكون الجرائم السيبرانية نتيجة لتخطيط مسبق، حيث يتم اختراق الشبكات الحاسوبية عمدًا بهدف الحصول على معلومات أو تحقيق مكاسب شخصية. ومن الأمثلة على ذلك قيام قراصنة إلكترونيين بنسخ برامج من مواقع الإنترنت، أو تعطيل أنظمة الحماية الخاصة بها، مما يؤدي إلى الإضرار بالشركات والجهات المالكة لهذه البرامج.

- الجريمة السيبرانية كجريمة غير عمدية:

تُعد الجريمة غير العمدية تلك التي يرتكبها الجاني عندما تتجه إرادته فقط إلى السلوك الإجرامي، دون أن يقصد تحقيق النتيجة الجرمية المحددة في النص القانوني. وبمعنى آخر، تنشأ الجريمة غير العمدية عن خطأ غير مقصود، شريطة أن يكون القانون قد نص عليها. ويلاحظ أن قانون العقوبات المصري لم يورد تعريفًا دقيقًا للخطأ غير العمدي، بل اكتفى بتحديد صوره المختلفة، لا سيما في الجرائم غير العمدية مثل القتل والإصابة الخطأ. ويعود ذلك إلى التحديات التي تواجه المشرّع في وضع تعريف شامل للخطأ، بحيث يشمل جميع الحالات الحالية والمستقبلية، دون أن يقيد القاضي في تقدير الوقائع المتغيرة والمعقدة التي قد تُعرض عليه[2].

عند محاولة تطبيق هذا المفهوم على الجرائم السيبرانية، يمكننا تصوّر أن بعض الجرائم الإلكترونية قد تحدث نتيجة لأخطاء غير متعمدة. فعلى سبيل المثال، قد يقوم موظف في مؤسسة ما بإلحاق ضرر بالأجهزة أو البيانات دون قصد، استنادًا إلى

[1] زين الدين، بلال أمين. جرائم نظم المعالجة الآلية للبيانات، دار الفكر الجامعي، 2008، ص 31.

[2] عبد المجيد، محمود سعد. الجرائم السيبرانية وانعكاسات ثورة تكنولوجيا المعلومات والاتصال على النظرية العامة للجريمة من حيث أسباب التكوين والأركان والعناصر وأساسيات المكافحة الجنائية، دار المطبوعات الجامعية، الإسكندرية، 2023، ص 215.

افتراضات خاطئة. فقد يستخدم جهاز الحاسوب الخاص به في إجراءات غير مشروعة دون إدراك العواقب، أو يقوم بإدخال قرص مرن أو ملف مصاب بفيروس إلى نظام المؤسسة، مما يؤدي إلى تلفه جزئيًا أو كليًا. وتبقى هذه الاحتمالات قائمة طالما أن العنصر البشري يظل مشاركًا في عمليات معالجة البيانات.

أ. محل الجريمة السيبرانية:

يُعد الحاسوب عنصرًا أساسيًا في الحياة الحديثة، حيث يحقق فوائد كبيرة لكنه في الوقت نفسه يثير تحديات أمنية. فهو مجرد أداة تُنفذ الأوامر دون تمييز بين الاستخدام المشروع وغير المشروع. ومع انتشار الإنترنت، زادت احتمالات استغلاله في الجرائم السيبرانية. فالجريمة السيبرانية تشمل أي تصرفات تستهدف الإضرار بأنظمة الحواسيب أو مكوناتها، سواء كانت مادية أو غير مادية، من قِبل أفراد ذوي خبرة تقنية[1].

محل الجريمة السيبرانية يتمثل في المعطيات والمصالح المنتهكة، حيث تُستهدف المعلومات باعتبارها أصولًا أو أسرارًا أو بيانات شخصية ذات قيمة. وتُعد المعلومات الإلكترونية أكثر عرضة للخطر مقارنة بالمعلومات الورقية، مما دفع المشرعين إلى إصدار قوانين خاصة لحمايتها من الاختراق والاطلاع غير المشروع، وهو ما لا ينطبق بنفس الدرجة على المعلومات الورقية.[2]

المطلب الثاني: أبعاد الأمن السيبراني.

[1] عزيزة، رابحي. الأسرار المعلوماتية وحمايتها الجزائية، رسالة لنيل درجة دكتوراه في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد – تلمسان، ص 184.

[2] عطا الله، شيماء عبد الغني محمد. الحماية الجنائية للمعاملات الإلكترونية، دار الجامعة الجديدة، 2007، ص 94.

يُعد الأمن السيبراني عنصرًا أساسيًا في حماية الأنظمة الرقمية من التهديدات السيبرانية المتزايدة، والتي باتت تشكّل خطرًا مستمرًا. ولهذا المجال أبعاد متعددة تتداخل مع مختلف جوانب الحياة، حيث يمكن تصنيفها إلى خمسة أبعاد رئيسية، وهي: البُعد القانوني، البُعد المجتمعي، البُعد السياسي، البُعد العسكري، والبُعد الاقتصادي، حيث تلعب جميعها دورًا مهمًا في تعزيز الأمن الرقمي والتصدي للهجمات السيبرانية.

1. البعد القانوني:

يترتب على الأنشطة الفردية، المؤسسية، والحكومية في الفضاء السيبراني آثار قانونية تتطلب اهتمامًا خاصًا بالمسائل الناتجة عن التطورات الرقمية. لذا، أصبح من الضروري مواكبة التحولات المرتبطة بمجتمع المعلومات، مما أدى إلى ظهور حقوق رقمية جديدة، مثل حق الوصول إلى شبكة المعلومات العالمية، وتوسّع بعض المفاهيم القانونية لتشمل أساليب الممارسة الحديثة باستخدام تقنيات المعلومات والاتصالات. ومن أبرز هذه الحقوق: حق إنشاء المدونات الإلكترونية، حق تكوين التجمعات عبر الإنترنت، وحق حماية الملكية الفكرية للبرمجيات.

2. البعد السياسي:

يكتسب البعد السياسي للأمن السيبراني أهمية متزايدة، نظرًا لتأثيره المباشر على الاستقرار الداخلي والدولي. فمن أبرز التحديات الاختراقات الإلكترونية للوثائق الحساسة، والتي قد تؤدي إلى أزمات معقدة. كما لا يمكن إنكار الدور المتعاظم لشبكات التواصل الاجتماعي في التأثير السياسي، سواء من خلال تنظيم الحملات الانتخابية، التظاهرات

الافتراضية، أو الحركات الاحتجاجية الإلكترونية. إضافةً إلى ذلك، تستخدم بعض الحكومات هذه المنصات كوسيلة لتبرير سياساتها أو توجيه الرأي العام.[1]

3. البعد العسكري:

تمنح القوة السيبرانية ميزة استراتيجية للجيوش، حيث تتيح ربط الوحدات العسكرية عبر الشبكات الإلكترونية، مما يسهل تبادل المعلومات، سرعة إصدار الأوامر، وتنفيذ العمليات عن بُعد. ومع ذلك، قد تتحول هذه الميزة إلى نقطة ضعف خطيرة في حال تعرض الشبكات العسكرية للاختراق، مما قد يؤدي إلى هجمات إلكترونية مضادة تستهدف البنية التحتية للقوات المسلحة، أجهزة الاستخبارات، وأنظمة الدفاع الجوي. كما يمكن لهذه الهجمات أن تعطل الاتصالات بين الوحدات العسكرية، تشل أنظمة الدفاع، أو حتى تفقد القيادة السيطرة على عملياتها، مما يشكل تهديدًا حقيقيًا للأمن العسكري للدول.[2]

4. البعد الاجتماعي:

تلعب شبكات التواصل الاجتماعي دورًا بارزًا في تمكين الأفراد من التعبير عن تطلعاتهم السياسية وطموحاتهم الاجتماعية بمختلف أشكالها. كما تسهم في إشراك جميع فئات المجتمع وتوفير وسيلة فعالة لتطوير المعرفة وتبادل المعلومات، مما يساعد في تعزيز الاستقرار الاجتماعي والرقمي. إضافةً إلى ذلك، فإن انفتاح المجتمعات على

[1] سميرة بارة. الأمن السيبراني في الجزائر: السياسات والمؤسسات، المجلة الجزائرية للأمن الإنساني، المجلد 02، العدد 04، 2017، ص 263.

[2] ميرة بارة. الأمن السيبراني في الجزائر: السياسات والمؤسسات، المجلة الجزائرية للأمن الإنساني، المجلد 02، العدد 04، 2017، ص 263.

بعضها البعض عبر الفضاء الإلكتروني يتيح فرصة لتبادل الخبرات والأفكار، ويعزز آفاق التعاون والتكامل بين الثقافات.

5. البعد الاقتصادي:

يرتبط الأمن السيبراني ارتباطًا وثيقًا بالاقتصاد، حيث يُعدّ اقتصاد المعرفة واستخدام تقنيات المعلومات والاتصالات من الركائز الأساسية للنمو الاقتصادي. تلعب البيانات والمعلومات المتداولة والمخزنة دورًا محوريًا في مختلف القطاعات، كما تسهم التكنولوجيا في تعزيز التنمية الاقتصادية للعديد من الدول عبر الاستفادة من الفرص التي توفرها الشركات الدولية والمؤسسات الكبرى لتحسين إدارة تكاليف الإنتاج.

إضافةً إلى ذلك، شهد العالم تطورًا كبيرًا في التمويل الإلكتروني مع إطلاق الخدمات الرقمية، حيث تزايدت استثمارات البنوك والمؤسسات المالية في الأنظمة المصرفية الرقمية، مع تنافس الشركات على تطوير تطبيقات تقدم آليات دفع إلكترونية آمنة. وقد دفعت هذه التحولات بعض الدول إلى سنّ تشريعات خاصة لحماية أموالها ومواجهة التحديات الاقتصادية والمالية، مثل غسل الأموال والتهرب الضريبي، مما يُبرز أهمية الأمن السيبراني في تأمين المعاملات المالية والحد من الجرائم الاقتصادية العابرة للحدود.[1]

[1] عطية، إدريس. مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، مجلة مصداقية، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي – تبسة، الجزائر، المجلد 01، العدد 01، 2019، ص 105.

الفصل الثاني:

الأمن السيبراني وآليات مكافحة الجرائم السيبرانية

الفصل الثاني: الأمن السيبراني وآليات مكافحة الجرائم السيبرانية

يمثل هذا الفصل امتدادًا منطقيًا للفصل الأول الذي تناول الأسس المفاهيمية والنظرية للجريمة السيبرانية، حيث ينتقل بالبحث من الطابع النظري إلى البعد العملي والتطبيقي، مسلطًا الضوء على سبل حماية الفضاء السيبراني والآليات المعتمدة لمكافحة الجرائم المرتكبة ضمنه.

في ظل التوسع الهائل في استخدام التكنولوجيا وازدياد التهديدات السيبرانية من حيث العدد والتعقيد، تبرز الحاجة إلى منظومة أمنية متكاملة ترتكز على تدابير تقنية متطورة وأطر قانونية وتشريعية فعالة على الصعيدين الوطني والدولي. ويهدف هذا الفصل إلى تحليل هذه المنظومة وبيان مرتكزاتها الأساسية التي تقوم عليها مواجهة الجريمة السيبرانية.

وقد تم تقسيم هذا الفصل إلى ثلاثة مباحث رئيسية مترابطة تغطي الأبعاد الأمنية والقانونية والتنظيمية للموضوع.

من خلال هذا التناول المتكامل، يسعى الفصل الثاني إلى تقديم رؤية واضحة وشاملة حول آليات التصدي للجريمة السيبرانية، بما يدعم فهمًا معمقًا لمجالات الوقاية والحماية في الفضاء الرقمي، استنادًا إلى القاعدة النظرية التي بُنيت في الفصل الأول.

المبحث الأول: الأبعاد والتدابير الأمنية السيبرانية

تفطّن المشرع الجزائري إلى تنامي الإجرام الإلكتروني، فسارع إلى تدارك الوضع من خلال سنّ مجموعة من القوانين، بدأها بتعديل قانون العقوبات بموجب القانون رقم 04-15، والذي أدرج فيه الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات. ثم تبعه بالقانون رقم 06-22 المعدل لقانون الإجراءات الجزائية، وكذا القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال. وقد اتخذ المشرع عدة تدابير يمكن تقسيمها إلى مطلبين: الأبعاد والتدابير الأمنية السيبرانية (المطلب الأول)، والتدابير الموضوعية والتقنية للأمن السيبراني (المطلب الثاني).

المطلب الاول: التدابير القانونية للأمن السيبراني:

سار المشرع الجزائري على نهج الدول المتقدمة، وخاصة فرنسا، في سنّ قوانين تُجرّم السلوكيات التي تمسّ بأنظمة المعالجة الآلية للمعطيات، وذلك عبر إدراج إجراءات حديثة ضمن القانون رقم 06-22،[1] ويمكن تبيانها في النقاط التالية:

عمل المشرع الجزائري، على غرار عدد من التشريعات المقارنة، على تجريم الأفعال الماسة بأنظمة الحاسب الآلي، مدفوعاً بالتطور التكنولوجي الكبير الذي أفرز أنماطاً جديدة من الجرائم غير المسبوقة. وقد تم تعديل قانون العقوبات بموجب القانون رقم 04-15، المتمم للأمر رقم 66-156، حيث خُصص القسم السابع مكرر منه

[1] القانون رقم 06-22، المؤرخ في 29 ذي القعدة عام 1427 الموافق لـ 20 ديسمبر سنة 2006، يعدل ويتمم الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق لـ 8 يونيو سنة 1966، والمتضمن قانون الإجراءات الجزائية، الصادر في الجريدة الرسمية عدد 84، المنشور بالجريدة الرسمية بتاريخ 24 ديسمبر سنة 2006، ص. 4.

لجرائم "المساس بأنظمة المعالجة الآلية للمعطيات"، ونُص فيه على عدة جرائم تتعلق بهذا المجال.

وفي سنة 2006، تم تعديل قانون العقوبات مرة أخرى بموجب القانون رقم 06-23، [1]حيث تم الإبقاء على النصوص التجريمية نفسها الواردة في القسم السابع مكرر، مع تشديد العقوبات المقررة لها. ويُعزى هذا التعديل إلى تزايد الوعي بخطورة هذه الجرائم الجديدة، خاصة لما لها من تأثير سلبي على الاقتصاد الوطني.

كما أضاف المشرع بموجب القانون رقم 16-02 [2] المعدل والمتمم لقانون العقوبات مادتين جديدتين، هما المادة 87 مكرر 11، التي استُعملت فيها عبارة "تكنولوجيات الإعلام والاتصال"، والمادة 394 مكرر 8 التي تضمنت مصطلح "مقدّم خدمات الإنترنت[3]."

المطلب الثاني: التدابير التقنية والإجرائية للأمن السيبراني:

أدرك المشرع الجزائري جيداً أن المواجهة الفعالة للإجرام الإلكتروني لا تتحقق فقط من خلال سن قواعد قانونية موضوعية ذات طابع ردعي، بل لا بد من دعمها بإجراءات وقائية وتحفظية ذات طبيعة إجرائية، من شأنها تفادي وقوع الجريمة الإلكترونية أو على الأقل الكشف عنها في مرحلة مبكرة، بما يسمح بتدارك مخاطرها.

---

[1]القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006، الذي يعدل ويتمم قانون العقوبات المعدل والمتمم (الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق لـ 8 يونيو سنة 1966)، الصادر في الجريدة الرسمية رقم 84، المنشور بالجريدة الرسمية عدد 49 المؤرخة في 11 يونيو 1966، ص. 702، والمنشور بالجريدة الرسمية بتاريخ 24 ديسمبر سنة 2006

[2]القانون رقم 16-02، المتضمن تعديل قانون العقوبات.

[3]مراد مشوش، *الجريمة المعلوماتية في ظل قانون العقوبات وقانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال*، مجلة القانون، المجلد 09، العدد 01، 2020، ص. 112.

وقد استدرك المشرع هذا الأمر من خلال إدراج تدابير إجرائية مستحدثة ضمن القانون رقم 06-22 [1]المعدل والمتمم لقانون الإجراءات الجزائية، والتي تتعلق بآليات التحقيق في الجرائم الإلكترونية. وتتمثل أبرز هذه التدابير في :مراقبة الاتصالات الإلكترونية وتسجيلها، والتسرب المعلوماتي.(infiltration)

ويقصد بـ «اعتراض المراسلات" كل عملية اعتراض أو تسجيل أو نسخ للمراسلات التي تكون في شكل بيانات قابلة للإنتاج، أو التوزيع، أو التخزين، أو الاستقبال، أو العرض، والتي تتم عبر قنوات الاتصال السلكية أو اللاسلكية، وذلك في إطار البحث والتحري عن الجرائم الإلكترونية وجمع الأدلة بشأنها.

وقد بيّن المشرع ظروف وكيفية اللجوء إلى هذا الإجراء في المادة 65 مكرر 5 من قانون الإجراءات الجزائية. حيث أجاز لسلطات التحقيق والاستدلال، عند الضرورة، في حالة التلبس بجريمة أو في سياق التحقيق في الجرائم الإلكترونية، اللجوء إلى إجراءات اعتراض المراسلات السلكية واللاسلكية، وتسجيل المحادثات والأصوات، والتقاط الصور، مع الاستعانة بكافة الترتيبات التقنية اللازمة لذلك. ويتم ذلك بهدف الوصول إلى الكشف عن ملابسات الجريمة الإلكترونية وإثباتها، دون التقيد بقواعد التفتيش والضبط التقليدية.

ومع ذلك، لم يُطلق المشرع الجزائري يد سلطات التحري في استخدام هذه الوسائل التقنية، بل أحاطها بجملة من الضمانات القانونية، التي تهدف إلى منع أي تعسف في

[1]القانون رقم 06-22، المؤرخ في 29 ذي القعدة عام 1427 الموافق لـ 20 ديسمبر سنة 2006، يعدل ويتمم الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق لـ 8 يونيو سنة 1966، والمتضمن قانون الإجراءات الجزائية، الصادر في الجريدة الرسمية عدد 84، المنشور بالجريدة الرسمية بتاريخ 24 ديسمبر سنة 2006، ص. 4.

استعمال هذه الصلاحيات، وحماية الحقوق والحريات الأساسية، وخاصة ما يتعلق بخصوصية الأفراد وحياتهم الخاصة[1].

المبحث الثاني: الآليات المحلية و الدولية لمكافحة الجرائم السيبرانية

نظرًا للتطور السريع لتكنولوجيا المعلومات والاتصال، أصبحت الجرائم السيبرانية تمثل تهديدًا حقيقيًا للأمن العام والاقتصاد العالمي، وهو ما دفع المجتمع الدولي والدول بشكل منفرد إلى سن تشريعات واعتماد آليات خاصة لمكافحتها. وفي هذا السياق، يهدف هذا المبحث إلى استعراض الجهود الدولية والجهود الوطنية الجزائرية في مواجهة الجريمة السيبرانية، من خلال مطلبين أساسيين: المطلب الأول يتحدث عن الآليات الإجرائية لمكافحة الجرائم السيبرانية على المستوى الدولي (اتفاقية بودابست 2001)، والمطلب الثاني وهو الأخير يتحدث عن آليات مكافحة الجرائم السيبرانية على ضوء القانون 04-09.

المطلب الأول: الآليات القانونية المحلية في التشريع الجزائري لمكافحة الجرائم السيبرانية على ضوء القانون 04-09

كخطوة جديدة، قام المشرع الجزائري بسنّ القانون 09-04 المتعلق بالوقاية من تكنولوجيات الإعلام والاتصال ومكافحتها، وإن كان تجسيد بنوده على أرض الواقع لا يزال ضعيفًا إلى حد الساعة، نتيجة إهمال الجوانب التقنية الكفيلة بتصنيف هذه الجرائم

[1] أسمهان بوضياف، *الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر*، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 03، العدد 03، 2018، ص. 364.

وتحديد العقوبة المناسبة في حق مرتكبيها، حيث تقتصر العقوبات في غالبية الأحيان على الغرامة المالية فقط.[1]

غير أنه وضع مجموعة من التدابير الوقائية والإجرائية للوقاية من هذه الجرائم ومكافحتها، وأهمها :

1. التدابير الوقائية

أ. المراقبة الإلكترونية:

سمح القانون باللجوء إلى هذا الإجراء في حالات محددة حصراً[2]، ويكون ذلك بموجب إذن مكتوب من السلطات القضائية المختصة، وذلك للوقاية من الأفعال الإرهابية أو التخريبية أو الجرائم الماسة بأمن الدولة، أو في حالة توفر معلومات حول احتمال اعتداء على منظومة معلوماتية بطريقة تهدد النظام العام، أو الدفاع الوطني، أو مؤسسات الدولة، أو الاقتصاد الوطني. كما يمكن اللجوء إلى هذا الإجراء لأغراض التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتائج مهمة في الأبحاث الجارية دون استخدامه. ويمكن أيضًا الاستعانة بالمراقبة الإلكترونية في إطار تنفيذ المساعدة القضائية الدولية المتبادلة.

ب. الاستعانة بمزودي الخدمات للوقاية من الجرائم السيبرانية.

ويكون ذلك من خلال تقديم مزودي الخدمات المساعدة للسلطات المكلفة بالتحريات القضائية، من خلال جمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها، ووضع هذه المعطيات تحت تصرف السلطات المختصة.

---

[1] أحمد بن خليفة، حفوظة الأمير عبد القادر 2017، الجريمة الالكترونية وآليات التصدي لها العدد 01، ص 165.

[2] المادة 04 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، ص 06.

وتشمل هذه المعطيات:[1]

- المعطيات التي تسمح بالتعرف على مستعملي الخدمة،
- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال،
- الخصائص التقنية، بالإضافة إلى تاريخ ووقت ومدة كل اتصال،
- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدّميها،
- المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسَل إليهم في الاتصال، وكذا عناوين المواقع التي تم الاطلاع عليها.

ويُشترط على مقدمي الخدمات الالتزام بحفظ هذه المعطيات، والتي أُطلق عليها اسم "المعطيات المتعلقة بحركة السير". وقد عرّفها القانون في مادته الأولى بأنها أي معطيات متعلقة بالاتصال عبر منظومة معلوماتية، تنتجها هذه الأخيرة باعتبارها جزءًا من حلقة الاتصالات، وتشمل مصدر الاتصال، والوجهة المرسل إليها، والطريق الذي يسلكه، وتاريخ ووقت وحجم ومدة الاتصال، ونوع الخدمة.

زيادة على ذلك، أفرد المشرع الجزائري مجموعة من الالتزامات الخاصة بمقدّمي خدمات الإنترنت. [2]وتشمل هذه الالتزامات التدخل الفوري لسحب المحتويات المخالفة للقوانين، وتخزينها أو حجب الدخول إليها، إضافةً إلى ضرورة وضع ترتيبات تقنية تحصر إمكانية الدخول إلى الموزّعات التي تحتوي على معلومات مخالفة للنظام العام أو الآداب العامة.

[1] المادة 11 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، ص 07.

[2] المادة 12 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، ص 08.

2. التدابير الإجرائية

أ. تفتيش وحجز المنظومة المعلوماتية

لمقتضيات حماية النظام العام، أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، تم وضع مجموعة من الترتيبات التقنية لمراقبة الاتصالات الإلكترونية، وتجميع وتسجيل محتواها في حينه، والقيام بإجراءات التفتيش والحجز داخل المنظومة المعلوماتية.[1]

غير أن إجراء الحجز قد تعترضه عدة إشكالات، يعود أغلبها لأسباب تقنية، مما يقتضي على السلطات التي تقوم بالتفتيش استعمال تقنيات مناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية أو نسخها، خاصة تلك الموضوعة تحت تصرف الأشخاص المرخّص لهم باستعمال هذه المنظومة.[2]

وجدير بالذكر أن هذا القانون أجاز اللجوء إلى التفتيش، حتى ولو كان عن بعد، على منظومة معلوماتية أو جزء منها، وكذا المعطيات المعلوماتية المخزنة فيها. كما يمكن القيام بالتفتيش عن بعد في منظومة تخزين معلوماتية[3].

ويمكن للسلطات المكلفة بالتفتيش تسخير أي شخص لديه دراية بعمل المنظومة المعلوماتية محل البحث، أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تحتويها، وذلك قصد مساعدتها وتزويدها بكل المعلومات الضرورية.

---

[1] المادة 03 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، ص 06.

[2] المادة 07 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، ص 07.

[3] المادة 07 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، ص 07.

ب. تمديد الاختصاص في النظر بهذه الجرائم

يؤول الاختصاص للمحاكم الجزائرية في النظر في الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني، في حال كانت الجريمة قد ارتكبها أجنبي، وكانت تستهدف مؤسسات الدولة الجزائرية، أو الدفاع الوطني، أو المصالح الاستراتيجية للاقتصاد الوطني.

ج. تبادل المساعدة القضائية الدولية

سمح المشرع الجزائري بإمكانية تبادل المساعدة القضائية الدولية، من أجل جمع الأدلة المتعلقة بالجريمة في شكلها الإلكتروني. كما يمكن الاستجابة لطلبات المساعدة التي تهدف إلى تبادل المعلومات أو اتخاذ أي إجراءات تحفظية، وذلك وفقًا للاتفاقيات الدولية أو بموجب مبدأ المعاملة بالمثل.

د. الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها:

تم استحداث هذه الهيئة بموجب القانون 09-04، وبقيت تشكيلتها وتنظيمها وكيفيات سيرها محددة عن طريق التنظيم، والذي عرف عدة تغييرات، بدءًا من المرسوم الرئاسي لسنة 2015، ثم في سنة 2019، ليأتي المرسوم الرئاسي لسنة 2020 ويعيد تنظيم الهيئة.

وقد عرّفها القانون بأنها سلطة إدارية مستقلة، تتمتع بالشخصية المعنوية والاستقلالية المالية، وتوضع تحت سلطة رئيس الجمهورية، ويُحدّد مقرها في الجزائر.

ويقع مقر الهيئة بالعاصمة، غير أنه يمكن نقله إلى أي مكان آخر من التراب الوطني بموجب مرسوم رئاسي. وتتكوّن الهيئة من مجلس توجيه ومديرية عامة، يُوضعان تحت السلطة المباشرة لرئيس الجمهورية، ويقدّمان عرضًا دوريًا عن نشاطاتهما. وقد نص على ذلك **المرسوم الرئاسي رقم 20-13 المؤرخ في 13 يوليو 2020**، الذي يتضمن

إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.[1]

ومما سبق نلاحظ أن المشرع الجزائري قد خطا خطوة إيجابية من خلال سن هذا القانون وتنظيمه، غير أن ذلك غير كافٍ لمواجهة خطورة الجرائم السيبرانية، مما يستدعي ضرورة مواكبة التطورات التكنولوجية بشكل مستمر.

المطلب الثاني: الآليات الإجرائية لمكافحة الجرائم السيبرانية على المستوى الدولي (اتفاقية بودابست 2001)

في سياق تحليل الآليات الإجرائية لمكافحة الجرائم السيبرانية في الاتفاقيات الدولية، سأتناول الجهود الدولية المبذولة لمكافحة هذا النوع من الجرائم، بالإضافة إلى التدابير الجديدة المعتمدة لاحتوائها على مستوى هذه الاتفاقيات. وسأستعرض هذا الموضوع في عدة اتفاقيات دولية، منها اتفاقية مجلس أوروبا – بودابست لسنة 2001، واتفاقية مجلس أوروبا لسنة 2004، مع تسليط الضوء على التطورات والتحديات التي تأخذها هذه الاتفاقيات بعين الاعتبار لتعزيز الآليات القانونية والإجرائية في مجال مكافحة الجرائم السيبرانية.

في إطار اتفاقية مجلس أوروبا – بودابست لعام 2001، يتم التركيز على الاعتراف بأن النشاط التقني يشكل جزءًا لا يتجزأ من النشاط المادي، وهو خطوة أولى هامة في مسار مكافحة الجرائم السيبرانية.

[1] مرسوم رئاسي رقم 183–20 المؤرخ في 20 يوليو 2020، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 40 الصادر بتاريخ 18 يوليو 2020.

أ. في اتفاقية مجلس أوروبا – بودابست لسنة 2001[1]

أشرنا سابقًا إلى عقد اتفاقية مجلس أوروبا – بودابست في 23 نوفمبر 2001، والتي أُطلق عليها اسم "اتفاقية الجريمة عبر العالم السيبراني (الإنترنت)"، بهدف تقديم إطار قانوني يساعد الدول في مواجهة الجريمة السيبرانية. وقد وقعت عليها 43 دولة أوروبية عضوة في المجلس الأوروبي.

هذه الاتفاقية ألقت الضوء على أهمية النشاط التقني كجزء لا يتجزأ من النشاط المادي في الجرائم السيبرانية، وذلك في مادتها الثالثة التي تشير إلى "استخدام التقنية"، حيث يُفهم بذلك استخدام الحواسب الآلية بكل تقنياتها وتكنولوجيا الاتصالات[2].

تُعد هذه الاتفاقية خطوة رئيسية في مجال مكافحة الجريمة السيبرانية، حيث لا تقتصر على وضع قواعد موضوعية للمكافحة، بل تعالج أيضًا المشكلات الإجرائية التي تواجه جهود مكافحة هذه الجريمة، من خلال فهم الدول الموقعة على الاتفاقية أن مواجهة هذا النوع من الجرائم يتطلب تعاونًا دوليًا. وتنص الاتفاقية على مبادئ وإجراءات جديدة لتوجيه جهود مكافحة الجرائم السيبرانية بشكل فعال، وسأوضح ذلك فيما يلي:

1- المبادئ الإجرائية العامة:

تشير الاتفاقية في مجال المكافحة الإجرائية إلى بعض المبادئ الإجرائية العامة، والتي تتلخص فيما يلي:

---

[1]زيدان زيبحة، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى للطباعة والنشر والتوزيع، عين مليلة الجزائر، 2011 ص159.

[2]نفس المرجع، ص159.

- توفير تنسيق بين عناصر الجرائم السيبرانية والقانون الجنائي الوطني، مع تأمين سلطات التحقيق والملاحقة اللازمة لمكافحة جرائم الحواسب.
- إنشاء نظام فعّال للتعاون الدولي يشمل الإجراءات المحلية والتحقيقات الجنائية لمكافحة الجرائم التي تتعلق بتقنية المعلومات وتوثيق الأدلة الإلكترونية.
- إلزام الدول الموقعة على الاتفاقية بتضمين المعلومات الرقمية أو الإلكترونية في قوانينها الداخلية واستخدامها كأدلة قانونية أمام القضاء، مع التركيز على جرائم الحواسب.
- فرض التفعيل الداخلي للإجراءات المشتقة من القوانين الوطنية، مع ترك مسألة تنفيذ وسريان هذه الصلاحيات في إطار النظام القضائي لكل دولة.
- التأكيد على وجوب قبول الدول للأدلة الرقمية والإلكترونية كجزء من الإجراءات الجنائية والقضائية في مواجهة مختلف أشكال الجرائم السيبرانية[1].

ب. **الإجراءات الجنائية الجديدة في اتفاقية بودابست:**

نصّت هذه الاتفاقية على بعض الإجراءات الجنائية الجديدة لمكافحة الجريمة السيبرانية، وهي كما يلي[2]:

✓ **الحفظ السريع للمعطيات المخزنة:**

تنص الاتفاقية في المادتين 16 و17 على إجراء الحفظ السريع للمعلومات المخزنة، بهدف الاحتفاظ بها بسرعة وتأمينها من التلف. يهدف هذا الإجراء إلى تفادي فقدان الأدلة في جرائم الحواسب نتيجة للتغير السريع في البيانات.

[1] ممدوح عبد الحميد عبد المطلب، جرائم استخدام الكمبيوتر وشبكة المعلومات العالمية، دار الفتح للطباعة والنشر، الامارات الشارقة، 2000، ص 126.

[2] رابحي عزيزة، الاسرار المعلوماتية وحمايتها الجزائية، رسالة لنيل درجة الدكتوراه في علوم القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر تلمسان، 2018 ص 143.

✓ **تجميع المعلومات الخاصة بالمشتركين:**

تُبرز الاتفاقية أهمية جمع المعلومات حول المشتركين في جرائم الحواسب لتحديد هوية الجاني. تشمل هذه المعلومات بيانات الاستخدام وفترة الاشتراك، مما يسهم في تحقيق العدالة في جرائم الحواسب.

✓ **التفتيش المعلوماتي:**

تؤكد الاتفاقية على ضرورة الحصول على إذن رسمي لتفتيش البيانات الإلكترونية، بعد توافر قناعة بوجود بيانات تُسهم في إثبات جريمة سيبرانية. يجب أن تتوفر شروط واضحة للحصول على هذا الإذن، مع ضمان فعالية التفتيش وحجز الأدلة[1].

✓ **الدخول على المعطيات المعلوماتية:**

تلزم الاتفاقية الدول بتخويل سلطاتها المختصة بالتحقيق والدخول إلى المعلومات المخزنة في نظم المعلومات. ويتضمن ذلك التفاعل في الوقت الفعلي لجمع الأدلة الإلكترونية.

✓ **إجراء التنصت:**

تفرض الاتفاقية إجراء التنصت كخطوة جديدة في مكافحة الجريمة السيبرانية، مع التأكيد على أن يتم ذلك بموافقة قضائية. ويُستخدم هذا الإجراء لاعتراض المراسلات عبر وسائل الاتصال السلكية واللاسلكية للحصول على أدلة تثبت وقوع الجريمة.

[1] الرابط: http://conventions.coe.int/Treaty/fr/Reports/Html/185.htm

✓ **التعاون الدولي:**

تشدد الاتفاقية على ضرورة التعاون الدولي لتبادل المعلومات والأدلة بشكل سريع، وتنص على ضرورة وجود إجراءات قانونية إضافية لتأمين البيانات التي تُستخدم كأدلة في الجرائم السيبرانية.

✓ **الالتزام والتنفيذ:**

تلتزم الدول الأطراف بإصدار التشريعات واتخاذ الإجراءات الضرورية لتنظيم مكافحة الجريمة السيبرانية وتحديد المسؤوليات الجنائية. كما يُلزم التعاون الدولي بمواجهة التحديات المتعلقة بتحقيق العدالة في جرائم الحواسب وتقديم المجرمين للمحاكمة.

هذا، وقد طرحت اتفاقية بودابست مسألة مدى إمكانية فرض الالتزام على مقدمي الخدمات بتجميع والاحتفاظ ببيانات المرور خلال فترة زمنية محددة؟ كما ناقشت مشكلة تحديد المصطلحات القانونية المستخدمة في مجال المكافحة الإجرائية للجريمة السيبرانية، وهل يجب الإبقاء على المصطلحات التقليدية المستخدمة في الجرائم التقليدية كمصطلح "التفتيش" و"الضبط".[1]

أم أنه من الأنسب استخدام مصطلحات جديدة أقرب إلى مجال التكنولوجيا، مع مناقشة مسألة تطور المفاهيم في المجال السيبراني؟ وهل ينبغي الإبقاء على المفاهيم التقليدية، مثل التفتيش والضبط، في سياق التحري والوصول إلى أدلة تثبت ارتكاب جريمة سيبرانية، أم اعتماد مفاهيم جديدة أكثر ملاءمة لطبيعة هذا المجال، مثل الولوج، النسخ، أو البقاء غير المشروع.

[1] الرابط: http://conventions.coe.int/Treaty/fr/Reports/Html/185.htm

المبحث الثالث: التدابير التشريعية الوطنية لدعم الأمن السيبراني

تعتبر التدابير التشريعية جزءًا أساسيًا في بناء نظام أمني سيبراني فعال، حيث تسهم التشريعات في توفير إطار قانوني يحمي المعلومات ويعزز التعاون بين المؤسسات المختلفة لمكافحة الجرائم السيبرانية. وقد سعت الجزائر من خلال عدة قوانين وتشريعات إلى تعزيز الأمن السيبراني، بما في ذلك القوانين الخاصة بحماية المعطيات الشخصية، وقانون مكافحة الجرائم السيبرانية، وأطر التعاون بين الجهات المختلفة. في هذا المبحث، سيتم تناول التدابير التشريعية الوطنية من خلال مطلبين رئيسيين:

المطلب الأول: التدابير التشريعية الوطنية لفعالية الأمن السيبراني

المطلب الثاني: القوانين اللاحقة المدعمة للقانون 04-09 للحد من الإجرام السيبراني

المطلب الأول: التدابير التشريعية الوطنية لفعالية الأمن السيبراني[1]

أكد المشرع الجزائري، من خلال المادة (16) من القانون 09-04 السالف الذكر، على مبدأ التعاون الدولي في إطار التحقيقات والتحريات المتعلقة بالجرائم الإلكترونية. حيث يجوز للسلطات القضائية المختصة تبادل المساعدة القضائية على المستوى الدولي من أجل جمع الأدلة المتعلقة بهذه الجرائم المستحدثة، وذلك بالنظر لما تطرحه من صعوبات تقنية كبيرة في الكشف عنها، إثباتها، وملاحقة مرتكبيها، الأمر الذي يتعذر على دولة واحدة القيام به بمفردها.

ونظرًا للطابع الاستعجالي الذي تفرضه إجراءات التحقيق في هذا النوع من الجرائم، فقد أقر المشرع إمكانية قبول طلبات المساعدة القضائية حتى وإن وردت عبر وسائل الاتصال السريعة، مثل البريد الإلكتروني أو الفاكس، شريطة التأكد من صحتها.

---

[1] يزيد بوحليط، *الجرائم الإلكترونية والوقاية منها في القانون الجزائري في ضوء الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، قانون العقوبات، قانون الإجراءات الجزائية، قوانين خاصة*، دار الجامعة الجديدة، الإسكندرية، مصر، 2019، ص362.

كما تخضع هذه الطلبات لمبدأ المعاملة بالمثل، وذلك احترامًا لمبدأ سيادة الدولة، كما ورد في المادة (17) من نفس القانون[1].

ومن المعروف أن الدولة لا تستطيع بمفردها مواجهة الإجرام السيبراني، مهما بلغت من تطور في مجال الأمن السيبراني، لذلك لا بد من التعاون الدولي، لا سيما في الجوانب القضائية والمساعدة القضائية. وقد أكدت على هذا التوجه **اتفاقية بودابست لمكافحة الإجرام السيبراني لسنة 2001**، وكذلك **الاتفاقية العربية لمكافحة الجرائم المعلوماتية لسنة 2010**، حيث شددتا على أهمية التعاون الدولي وآلياته في مواجهة هذا النوع من الإجرام. وتُعد اتفاقية بودابست، رغم كونها إقليمية، ذات طابع دولي، وتشكل مصدرًا مرجعيًا للعديد من الدول في رسم سياساتها لمكافحة الجرائم السيبرانية التي أصبحت تشكل تهديدًا حقيقيًا للدول والأفراد[2].

1. التدابير الهيكلية لفعالية الأمن السيبراني

عمل المشرع الجزائري في إطار محاربة الجريمة الإلكترونية على إنشاء عدة هياكل متخصصة، تُعنى بمكافحة الجريمة السيبرانية، نذكر من بينها:

أ- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

نصت المادة 13 من القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، على ما يلي:

تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. تُحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم[3].

---

[1] يزيد بوحليط، مرجع *نفسه*، ص362.

[2] المرجع نفسه، ص 362.

[3] أسمهان بوضياف، مرجع *سابق*، ص 365.

أما المهام المنوطة بهذه الهيئة، فقد وردت في المادة 14 من نفس القانون، وأُعيد تنظيمها لاحقًا بموجب المرسوم الرئاسي رقم 21-439، الذي نقل الإشراف على الهيئة إلى أمانة رئاسة الجمهورية.

ومن أهم اختصاصات الهيئة كما نصت عليها المادة 4 من المرسوم المذكور[1]:

1. الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.
2. مكافحة جميع أشكال الجرائم الإلكترونية.
3. تبادل المعلومات مع الدول لتعزيز التعاون الدولي والمساعدة القضائية.

ب- الهيئات القضائية الجزائية المتخصصة

يقصد بها الأقطاب الجزائية المتخصصة، المنشأة بموجب القانون رقم 14-04 المؤرخ في 10 نوفمبر 2014، وتختص هذه الهيئات، وفقًا للمواد 37 و40 و329 من قانون الإجراءات الجزائية، بالنظر في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات. وتُضاف إلى صلاحياتها العامة في مجال مكافحة الجريمة، صلاحيات خاصة في التعامل مع الجرائم السيبرانية، من خلال آليات تحقيق ومتابعة فعالة.

ج- جهازي الأمن الوطني والدرك الوطني

بادرت كل من المديرية العامة للأمن الوطني وجهاز الدرك الوطني إلى إنشاء فرق متخصصة لمكافحة الجرائم المعلوماتية.

[1] المرسوم الرئاسي رقم 21-439، المؤرخ في 2 ربيع الثاني 1443هـ، الموافق 7 نوفمبر 2021، المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، *الجريدة الرسمية* للجمهورية الجزائرية، العدد 86، الصادرة بتاريخ 11 نوفمبر 2021، ص 5.

كما تم تكوين عناصر بشرية مؤهلة في هذا المجال، سواء داخليًا أو خارجيًا، مع دعم هذين الجهازين بمخابر علمية وتقنية مزودة بأحدث الوسائل التكنولوجية، بما يُمكّن من كشف وتتبع مرتكبي الجرائم السيبرانية[1].

د- المعهد الوطني للأدلة الجنائية وعلم الإجرام

يتكون هذا المعهد من إحدى عشرة دائرة متخصصة في مجالات متعددة، تتكفل بإنجاز الخبرات الفنية، التكوين والتعليم، وتقديم الدعم التقني[2].

وتُعنى دائرة الإعلام الآلي والإلكتروني على وجه الخصوص بمعالجة وتحليل الأدلة الرقمية، وتقديم الدعم الفني اللازم للمحققين خلال المعاينات.

المطلب الثاني: القوانين اللاحقة المدعمة للقانون 04-09 للحد من الإجرام السيبراني

1. القانون 18-04 المتعلق بالقواعد العامة الخاصة بالبريد والاتصالات الإلكترونية

جاء هذا القانون بمجموعة من الآليات لمواجهة الجرائم المرتبطة بالعالم الافتراضي، من بينها استحداث سلطة ضبط تُعنى بمراقبة احترام متعاملي البريد والاتصالات الإلكترونية للأحكام القانونية والتنظيمية ذات الصلة بالبريد والاتصالات والأمن السيبراني[3].

---

[1] محمد السعيد زناتي، *الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية*، مجلة إيليزا للبحوث والدراسات، المركز الجامعي إيليزي، الجزائر، المجلد 02، العدد 01، ديسمبر 2017، ص 34.

[2] أسمهان بوضياف، *مرجع سابق*، ص 370.

[3] المادة 13 من القانون 18-04 المؤرخ في 10 مايو 2018، الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، الجريدة الرسمية، العدد 27، الصادرة بتاريخ 13 مايو 2018، ص10.

كما نصّ القانون على تحريم انتهاك سرية المراسلات المُرسلة عن طريق البريد أو الوسائل الإلكترونية، أو إفشاء مضمونها أو نشرها أو استعمالها دون إذن من المرسل أو المرسل إليه، أو مجرد الإخبار بوجودها. كما حرّم محاولة فتح أو تخريب أو تحويل البريد، أو المساعدة في ارتكاب هذه الجرائم. وقد خُصصت المواد من 164 إلى 188 من هذا القانون لتحديد العقوبات المرتبطة بهذه الأفعال.

2. القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي

وضع المشرع الجزائري في هذا القانون مجموعة من الآليات المرتبطة بالعالم الافتراضي، يمكن تلخيصها في النقاط التالية:

أ. استحداث سلطة وطنية لحماية المعطيات ذات الطابع الشخصي.

ب .فرض مجموعة من الالتزامات على عاتق المسؤول عن المعالجة الآلية للمعطيات ذات الطابع الشخصي.

ج .منح السلطة الوطنية صلاحية اتخاذ إجراءات إدارية في حال مخالفة أحكام القانون من قبل المسؤول عن المعالجة.

د .يحق للسلطة الوطنية إجراء تحريات ومعاينة المحلات والأماكن التي تتم فيها عمليات المعالجة، باستثناء المساكن الخاصة. كما يمكنها الولوج إلى المعطيات المعالجة، والاطلاع على كافة المعلومات والوثائق، أياً كانت وسيلتها أو طبيعة الدعامة التي تحفظها.

هـ .تم تأهيل أعوان رقابة مختصين للقيام بمهام البحث ومعاينة الجرائم المتعلقة بالمعطيات ذات الطابع الشخصي، وذلك تحت إشراف وكيل الجمهورية.

و .يحق لكل من يدّعي المساس بأحد حقوقه المنصوص عليها في هذا القانون أن يتقدم بطلب للجهة القضائية المختصة لاتخاذ أي تدابير تحفظية تهدف إلى الحد من التعدي، أو لطلب تعويض عن الضرر.

ز .تختص الجهات القضائية الجزائرية بالنظر في الجرائم المرتكبة خارج التراب الوطني إذا كان مرتكبها جزائرياً، أو أجنبياً مقيماً في الجزائر، أو شخصاً معنوياً خاضعاً للقانون الجزائري. كما تمتد اختصاصاتها إلى الجرائم المنصوص عليها في هذا القانون، وفقاً لأحكام المادة 588 من قانون الإجراءات الجزائية.[1]

ح .تم تجريم الاعتداء على المعطيات ذات الطابع الشخصي، مع النص على عقوبات مالية وأخرى سالبة للحرية، وذلك بموجب المواد من 54 إلى 74 من هذا القانون.

[1] المادة 53 من القانون 18-07 المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية عدد 34، الصادرة بتاريخ 22 يونيو 2018، ص22.

خاتمة

خاتمة:

شهد الفضاء الرقمي في العقود الأخيرة تطورًا متسارعًا، رافقه تنامٍ مقلق لظاهرة الجريمة السيبرانية، التي باتت تشكل تحديًا متعدد الأبعاد للدول، لا سيما في ظل تعقيدها وامتدادها العابر للحدود. وانطلاقًا من هذا المعطى، سعت هذه الدراسة إلى تحليل فعالية الأطر القانونية والمؤسساتية في مكافحة الجريمة السيبرانية في الجزائر، من خلال مقاربة متدرجة من العام إلى الخاص، تناولت في فصلها الأول المفاهيم الأساسية للجريمة السيبرانية (تعريفها، خصائصها، أنواعها، وأركانها)، وفي فصلها الثاني الآليات الوطنية والدولية لمكافحتها، مع التركيز على القانون 04-09، والتدابير الأمنية والتقنية، والتشريعات المرافقة.

وقد أفضى هذا المسار التحليلي إلى جملة من النتائج الرئيسية:

1. فعالية محدودة للإطار القانوني الحالي

رغم أن القانون 04-09 يشكل خطوة تشريعية أولى مهمة، إلا أنه يعاني من قصور في مواكبة التطورات التكنولوجية، خاصة في ما يتعلق بجرائم الذكاء الاصطناعي، التزييف العميق، وإنترنت الأشياء. كما أن غياب آليات تنفيذ مرنة، وبطء التعديلات القانونية، يحدّان من نجاعته.

2. قصور مؤسساتي وتقني واضح

لا تزال الجزائر تفتقر إلى هيئة وطنية موحدة للأمن السيبراني تتولى التنسيق بين مختلف الفاعلين. كما تعاني البنية التحتية الرقمية من الهشاشة، وتواجه المؤسسات الأمنية والقضائية نقصًا في الكفاءات التقنية المؤهلة لملاحقة هذا النوع المعقد من الجرائم.

3. ضعف التعاون الدولي

تتسم الجريمة السيبرانية بكونها عابرة للحدود، مما يفرض تعزيز الانخراط في الاتفاقيات الدولية مثل اتفاقية بودابست، وتطوير شراكات ثنائية ومتعددة الأطراف. غير أن التنسيق الدولي لا يزال محدودًا ويشكل نقطة ضعف في المنظومة الجزائرية.

4. تدني مستوى الوعي المجتمعي

لا يحظى الأمن السيبراني بالاهتمام الكافي من طرف الأفراد والمؤسسات، مما يترك ثغرات كبيرة تستغلها الهجمات الرقمية، ويؤثر سلبًا على فعالية جهود الوقاية والمواجهة.

التوصيات المقترحة:

1. تحديث الإطار التشريعي

- مراجعة القانون 04-09 ليشمل الجرائم السيبرانية الحديثة.
- سنّ تشريعات مرنة قابلة للتحديث السريع، تستند إلى رؤية استباقية.

2. تعزيز البنية المؤسساتية والتقنية

- إنشاء هيئة وطنية عليا للأمن السيبراني تتولى رسم السياسات وتنسيق الجهود.
- دعم الأجهزة الأمنية والقضائية بفرق متخصصة في التحقيق الجنائي الرقمي.
- تطوير البنية التحتية الرقمية الوطنية بما يعزز من قدرتها على الاستجابة للهجمات السيبرانية.

3. تنمية الكفاءات وبناء القدرات

- الاستثمار في التكوين المستمر في مجالات الأمن السيبراني.
- دعم البحث العلمي وتشجيع الابتكار في تقنيات الحماية الرقمية.

4. نشر ثقافة الوعي السيبراني

- دمج مفاهيم الأمن الرقمي في المناهج التعليمية منذ المراحل الأولى.
- تنظيم حملات وطنية توعوية موجهة لكافة فئات المجتمع.

5. تعزيز التعاون الدولي

- تفعيل الانخراط في الاتفاقيات الدولية ذات الصلة، لا سيما اتفاقية بودابست.
- إقامة شراكات تقنية وقضائية لتبادل الخبرات والمعلومات.

و عليه و بناء على ما سبق يمكن القول:

إن التصدي للجريمة السيبرانية لم يعد شأنًا تقنيًا فحسب، بل أصبح رهانا استراتيجيًا يمسّ السيادة الرقمية والأمن الوطني. ولتحقيق حماية فعالة في هذا المجال، لا بد من مقاربة شاملة تنسجم فيها التشريعات الذكية، والمؤسسات المتخصصة، والكفاءات الوطنية، مع دعم دولي وتفاعل مجتمعي واسع. وحدها منظومة سيبرانية استباقية ومتكاملة قادرة على مواجهة التهديدات المعقدة لعالم رقمي سريع التحول، وصون مصالح الجزائر ومواطنيها في هذا العصر الرقمي المتقلب.

قائمة المراجع

قائمة المراجع:

اولا: القوانين والمراسيم والوثائق الرسمية

1. القانون رقم 04-09 المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، الصادر بتاريخ 16 أوت 2009.
2. القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006، يعدل ويتمم الأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية عدد 84، 2006.
3. القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006، الذي يعدل ويتمم قانون العقوبات، الجريدة الرسمية رقم 84، 2006.
4. القانون رقم 16-02، المتضمن تعديل قانون العقوبات.
5. القانون 18-04 المؤرخ في 10 مايو 2018، الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، الجريدة الرسمية، العدد 27، 2018.
6. القانون 04-09، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
7. القانون 18-07 المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية عدد 34، 2018.
8. مرسوم رئاسي رقم 183-20 المؤرخ في 20 يوليو 2020، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 40، 2020.

9. المرسوم الرئاسي رقم 21-439 المؤرخ في 7 نوفمبر 2021، المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 86، 2021.

ثانيا: الكتب والمؤلفات

1. الحجازي، عبد الفتاح بيومي. الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت. بهجان للطباعة والتجليد.
2. حسني، محمود نجيب. الفقه الجنائي الإسلامي. دار النهضة العربية.
3. القرعان، محمود أحمد. الجرائم الإلكترونية، دار وائل للنشر والتوزيع، عمان، الطبعة الأولى، 2017.
4. لطفي، خالد حسن أحمد. الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية. الإسكندرية: دار الفكر الجامعي، الطبعة الأولى، 2222.
5. المري، بهاء. شرح جرائم تقنية المعلومات. منشأة المعارف.
6. الصغير، جميل عبد الباقي. القانون الجنائي والتكنولوجيا الحديثة. دار النهضة العربية، 1992.
7. عبد المجيد، محمود سعد. الجرائم السيبرانية وانعكاسات ثورة تكنولوجيا المعلومات والاتصال على النظرية العامة للجريمة من حيث أسباب التكوين والأركان والعناصر وأساسيات المكافحة الجنائية. دار المطبوعات الجامعية، الإسكندرية، 2023.
8. عبد المطلب، ممدوح عبد الحميد. جرائم استخدام الكمبيوتر وشبكة المعلومات العالمية. دار الفتح للطباعة والنشر، الإمارات (الشارقة)، 2000.
9. عبيد، رؤوف. السببية في القانون الجنائي. مطبعة الاستقلال.

10. عطا الله، شيماء عبد الغني محمد. الحماية الجنائية للمعاملات الإلكترونية. دار الجامعة الجديدة، 2007.
11. عياد، سامي علي حامد. الجريمة المعلوماتية وإجرام الإنترنت. الإسكندرية: دار الفكر الجامعي، بدون طبعة، 2007.
12. زين الدين، بلال أمين. جرائم نظم المعالجة الآلية للبيانات. دار الفكر الجامعي، 2008.
13. زيبحة، زيدان. الجريمة المعلوماتية في التشريع الجزائري والدولي. دار الهدى للطباعة والنشر والتوزيع، عين مليلة الجزائر، 2011.

ثالثا: المقالات الدورية والأبحاث المنشورة

1. أحمد بن خليفة، حفوظة الأمير عبد القادر. الجريمة الالكترونية وآليات التصدي لها، العدد 01، 2017.
2. بهاء، عدنان. "انتقال التهديدات من الواقع إلى العالم الافتراضي." مجلة بابل للعلوم الإنسانية، المجلد 27، العدد 4، العراق، 2019.
3. بارة، سميرة. الأمن السيبراني في الجزائر: السياسات والمؤسسات. المجلة الجزائرية للأمن الإنساني، المجلد 02، العدد 04، 2017.
4. بوضياف، أسمهان. الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 03، العدد 03، 2018.
5. العطيان، تركي بن محمد. "البطالة وعلاقتها بالسلوك الإجرامي: دراسة نظرية على المجتمع السعودي". المجلة العربية للدراسات الأمنية، المجلد 21، العدد 41، 2006.

6. زناتي، محمد السعيد. الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية. مجلة إليزا للبحوث والدراسات، المركز الجامعي بإليزي – الجزائر، العدد 02، 2017.

7. الصغير، عبد المؤمن. الطبيعة الخاصة للجريمة الإلكترونية المرتكبة عبر الإنترنت في التشريع الجزائري والتشريع المقارن. مجلة الحقوق والحريات، جامعة محمد خيضر، بسكرة، المجلد 02.

8. طعبة، سعاد. "الجريمة الإلكترونية: تفعيل لآليات القانون من أجل تحقيق العدالة". مجلة الحقوق والعلوم الإنسانية، العدد 15، 2022.

9. عطية، إدريس. مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري. مجلة مصداقية، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي – تبسة، الجزائر، المجلد 01، العدد 01، 2019.

10. وفاء، محمد علي. "الأبعاد الاجتماعية للجرائم الإلكترونية: دراسة تحليلية لمضمون عينة من القضايا في محكمة سوهاج". مجلة كلية التربية في العلوم الإنسانية والأدبية، المجلد 27، العدد 3، 2021.

11. مشوش، مراد. الجريمة المعلوماتية في ظل قانون العقوبات وقانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال. مجلة القانون، المجلد 09، العدد 01، 2020.

12. Chareonwongsak, K. "Globalization and Technology: How Will They Change Society?" Technology in Society, vol. 24, no. 3, 2002.

رابعا: الرسائل الجامعية (ماجستير/دكتوراه)

1. الصغير، يوسف. الجريمة المرتكبة عبر الإنترنت. رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013/2012.
2. مرابط، حياة. الجريمة الإلكترونية في التشريع الجزائري. رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم – الجزائر، 2018.
3. عزيزة، رابحي. الأسرار المعلوماتية وحمايتها الجزائية. رسالة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد/تلمسان.

خامسا: أوراق المؤتمرات والمحاضرات

1. السالك، كامل فريد. الجريمة الإلكترونية. محاضرة ألقيت في ندوة التنمية ومجتمع المعلوماتية، 21–23 أكتوبر 2000، الجمعية السورية للمعلوماتية، حلب، سورية.

سادساً: الاتفاقيات والمعاهدات الدولية (المتاحة عبر الإنترنت)

1. اتفاقية بودابست بشأن الجريمة الإلكترونية. متاح على: http://conventions.coe.int/Treaty/fr/Reports/Html/185.htm

سابعاً: المقالات والمنشورات عبر الإنترنت

1. الروضان، وليد أحمد. "ما الفرق بين أمن المعلومات والأمن السيبراني". صحيفة الجزيرة الإلكترونية، مؤسسة الجزيرة للصحافة والنشر، العدد 16631، 1431هـ. متاح على: https://www.al-jazirah.com/2018/20180411/rj3.htm.