جامعة أكلي محند أولحاج –البويرة
كلية الحقوق والعلوم السياسية

الأمن السيبيراني كآلية لمواجهة الجريمة الإلكترونية في الجزائر

مذكرة تخرج لنيل شهادة الماستر في القانون
تخصص: جنائي وعلوم جنائية

إعداد الطالبتين :
- بلقاسم هبة
- رزق الله منال

تحت إشراف الأستاذ:
د- محمودي محمد لمين

لجنة المناقشة:

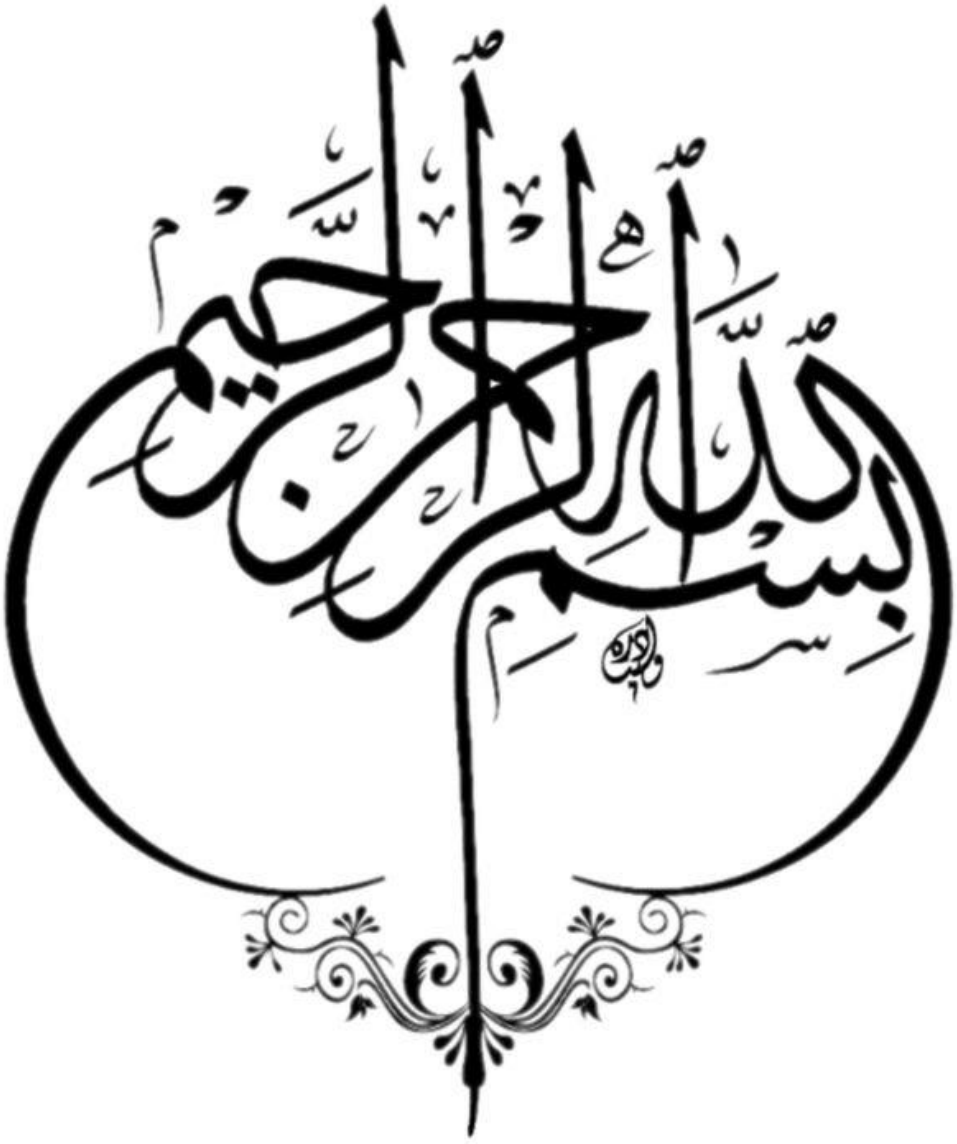
الاستاذ: يحياوي فاتح .....رئيسا

الاستاذ: محمودي محمد لمين.....مشرفا ومقررا

الاستاذ:قريم سكورة .....ممتحنا

تاريخ المناقشة: 2026/06/09

السنة الجامعية: 2026/2025


بسم الله الرحمن الرحيم

الشكر والتقدير

الحمد والشكر لله الحي القيوم أولاً وأخيراً وامتثالاً لقوله صلى الله عليه وسلم:

"من لا يشكر الناس لا يشكر الله"

أتقدم بجزيل الشكر وعظيم الامتنان إلى الأستاذ المشرف على هذه المذكرة، على ما قدّمه لي من توجيهات علمية قيّمة، ونصائح بنّاءة، وملاحظات دقيقة، كان لها بالغ الأثر في توجيه هذا البحث وإخراجه في صورته النهائية، فله مني فائق الاحترام والتقدير.

كما أتوجه بخالص الشكر والتقدير كما لا يفوتنا أن نتقدم بوافر التقدير والاحترام لأعضاء اللجنة المحترمين على عناء قراءة المذكرة وقبولها وتصويبها.

إلى جميع أساتذتي الأفاضل، الذين ساهموا في تكويني العلمي.

إهداء

قال الله تعالى:{و اخر دعواهم ان الحمد لله رب العالمين} . يونس 10 .

الحمد لله طيبا مباركا فيه اهدي ثمرة تخرجي هذا ... إلى نفسي إلى تلك التي صبرت و تعثرت ثم نهضت ... إلى ايماني الذي لم يخفت ، و جهودي التي لم يرها أحد ... أنا فخورة بك ، هذا نجاح ثمرة صبرك و كفاحك

إلى أمي الحبيبة (سميرة)

إلى من كانت دعواتها نورًا يضيء طريقي، وسندًا أستند إليه في كل مراحل حياتي، إلى من سهرت وتعبت وضحت من أجلي دون انتظار مقابل، أهديك ثمرة جهدي المتواضعة هذه...أمي الغالية، مهما كتبت من كلمات فلن أوفيك حقك، فأنتِ مصدر قوتي وعزيمتي، وسبب نجاحي بعد فضل الله تعالى. شكراً لكِ على حبك اللامحدود، وصبرك، وتشجيعك الدائم لي في كل خطوة.

أسأل الله أن يحفظكِ، ويديم عليكِ الصحة والعافية، وأن يجزيكِ عني خير الجزاء، وأن يجعل هذا النجاح فرحةً لكِ كما كان ثمرةً لدعواتكِ.

...إلى أبي الغالي (عبد ناصر)

الذي زين إسمي بأجمل الألقاب، من دعمني بلا حدود وأعطاني بلا مقابل ..... من علمني أن الدنيا كفاحوسلاحه العلم والمعرفة دعمي الأول في مسيرتي وسندي وقوتي وملاذي بعد الله ..... إلى فخري واعتزازي .... طالب بك العمر يا سيد الرجال وطبت لي عمرا يا أبي.

...إلى أخواتي – أية و رحمة و آلاء... –

إلى رفيقات دربي، وشريكات أفراحي وأحزاني، إلى من كنّ مصدر محبة ودعم وسند في مختلف مراحل حياتي، شكراً لكنّ على كلمات التشجيع، وعلى وقوفكنّ إلى جانبي في الأوقات الصعبة قبل السهلة، وعلى كل لحظة دعم ومحبة صادقة منحتنني إياها.وجودكنّ في حياتي نعمة عظيمة، فبكنّ تزداد الأيام جمالاً، وتخفّ الصعاب، وتصبح النجاحات أجمل وأقرب إلى القلب.

...الى صديقاتي...

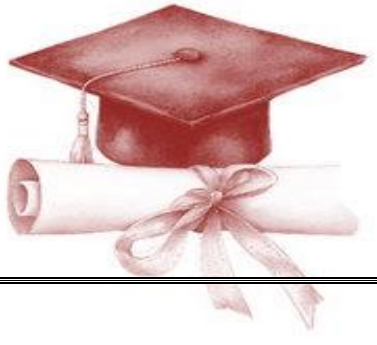
إلى من شاركنني أجمل لحظات حياتي، وكنَّ خير سندٍ وعونٍ لي خلال مسيرتي الدراسية ،شكراً لكنَّ على صداقتكنَّ الصادقة، ودعمكنَّ وتشجيعكنَّ لي طوال مشواري الدراسي. كان لوجودكنَّ أثر جميل في تخفيف الصعاب ومشاركة أجمل اللحظات.

أسأل الله أن يديم بيننا المحبة والوفاء، وأن يوفقكنَّ جميعاً في حياتكنَّ ويحقق لكنَّ كل ما تتمنين.

(منال و هدى و نهى و رانيا)

إلى زوجي وأطفالي، أنتم أجمل دعوة أخبّئها في قلبي أهديكم هذا النجاح قبل أن تجمعنا الأيام "عائلتي المستقبلية."

هبة.



اهداء

قال الله تعالى:{و اخر دعواهم ان الحمد لله رب العالمين} . يونس 10 .

الحمد لله طيبا مباركا فيه اهدي ثمرة تخرجي هذا ... إلى نفسي إلى تلك التي صبرت و تعثرت ثم نهضت ... إلى ايماني الذي لم يخفت ، و جهودي التي لم يرها أحد ... أنا فخورة بك ، هذا نجاح ثمرة صبرك و كفاحك

إلى أبي الغالي (مناد)

الذي زين إسمي بأجمل الألقاب، من دعمني بلا حدود وأعطاني بلا مقابل ..... من علمني أن الدنيا كفاحوسلاحه العلم والمعرفة دعمي الأول في مسيرتي وسندي وقو

...إلى أمي الحبيبة (نعيمة)...

التي من جعل الله الجنة تحت أقدامها واحتضنتني قلبا قبل بدها وسهلت لي الشدائد بدعاتها إلى القلب الحنون .. إلى من ظلت تنفق عمرها لتخيط لنا الطريق مستقيما، لا أعلم أن كنت ما زلتي تذكرين يوم رسوبي لكنني أتذكر جيدا دموعك وانهيارك عند رؤيتك لنتائجي كانت تلك بداية جديدة لي فلولاك لما أكملت الطريق، دمتي لي روحا لا أعيش الا بها.

...إلى أخواتي و إخوتي الأحبة...

إلى من شاركوني تفاصيل حياتي وأيامي، وكانوا مصدر فرح وسند في مختلف مراحل عمري، أهديكم هذا العمل المتواضع.

إلى أخويَّ العزيزين، شكراً لكما على دعمكما وتشجيعكما الدائم، وعلى كل موقف صادق وقفتما فيه إلى جانبي (عبد الغاني و إسحاق).

وإلى أختيَّ الغاليتين، شكراً لكما على محبتكما واهتمامكما ومساندتكما لي، وعلى كل الكلمات الجميلة التي كانت تمنحني القوة والأمل (هدى و فاطمة الزهرة)

أسأل الله أن يحفظكم جميعاً.

...إلى ابنة اختي الصغيرة (رهف)

إلى ملاكي الصغير، وإلى البسمة التي تملأ القلوب فرحاً ، عزيزتي الصغيرة، قد لا تدركين اليوم معنى هذا الإنجاز، لكنني أهديه لكِ بمحبة كبيرة، فأنتِ قطعة من القلب ومصدر للسعادة والبهجة في حياتنا.

...إلى صديقاتي...

إلى من شاركنني أجمل لحظات حياتي، وكنَّ خير سندٍ وعونٍ لي خلال مسيرتي الدراسية ،شكراً لكنَّ على صداقتكنَّ الصادقة، ودعمكنَّ وتشجيعكنَّ لي طوال مشواري الدراسي. كان لوجودكنَّ أثر جميل في تخفيف الصعاب ومشاركة أجمل اللحظات.

أسأل الله أن يديم بيننا المحبة والوفاء، وأن يوفقكنَّ جميعاً في حياتكنَّ ويحقق لكنَّ كل ما تتمنين.

(هبة و هدى و يسرى)

إلى زوجي وأطفالي، أنتم أجمل دعوة أخبّئها في قلبي أهديكم هذا النجاح قبل أن تجمعنا الأيام "عائلتي المستقبلية."

منال

قائمة المختصرات

ج ر: الجريدة الرسمية

ق إ ج ج: قانون الإجراءات الجزائية الجزائري

ق ع ج: قانون العقوبات الجزائري

ص: الصفحة

ص ص: **من** الصفحة الى الصفحة

ط: الطبعة

د ط : بدون طبعة

مقدمة

أصبحت التكنولوجيا الرقمية اليوم جزءًا لا يتجزأ من حياة الأفراد والدول، بعد أن امتد تأثيرها إلى مختلف المجالات الاقتصادية والاجتماعية والإدارية والأمنية، ومع هذا التحول السريع، برزت إلى الواجهة الجريمة الإلكترونية كأحد أخطر التحديات التي تواجه الدول الحديثة، لما تتسم به من قدرات عالية على إحداث أضرار بالغة وبسرعة فائقة، إضافة إلى تجاوزها للحدود التقليدية للسيادة والاختصاص، وهذا ما جعلها من أبرز الجرائم المستحدثة التي تتطلب آليات خاصة لمواجهتها.

نشأة الجريمة الإلكترونية بشكل فعال مع انتشار استخدام الحواسيب وشبكة الإنترنت في القرن العشرين، وإن كانت جذورها تعود إلى جرائم قديمة في استخدام التلغراف في عام 1834 بدأت في الستينيات والسبعينيات عبر التلاعب بالبيانات، ثم تطورت في الثمانينيات لتشمل اختراق الأنظمة ونشر الفيروسات، وتوسعت بشكل كبير في التسعينيات مع انتشار الإنترنت بشكل هائل.

وفي ظل هذا الانتشار المتزايد للجرائم الإلكترونية، ظهر الأمن السيبراني لأول مرة سنة 1972 كفكرة نظرية مرتبطة بحماية الحواسيب وتطور هذا المفهوم مع ظهور أول البرامج لمطاردته، وهو أول برنامج مضاد للفيروسات Reaper ، ثم ابتكار برنامج Creeper وخلال الثمانينات، أدى انتشار الفيروسات إلى دفع الباحثين نحو تطوير مجال حماية الأنظمة، وبدأت المؤسسات الحكومية، خاصة في الولايات المتحدة، بوضع معايير للأمن المعلوماتي كما شهدت هذه الفترة حوادث اختراق خطيرة.

وفي سنة 1987 ظهر أول برنامج تجاري لمكافحة الفيروسات، وتأسست منظمات ومنتديات متخصصة بالأمن المعلوماتي، مما ساهم في ترسيخ ملامح الأمن السيبراني ومع انتشار الجرائم الإلكترونية عبر العالم، بدأت الدول في إصدار قوانين كمجال مستقل الحماية البيانات والنظم المعلوماتية، فقد صدرت تشريعات في السويد (1973)، فرنسا (1978)، والولايات المتحدة (1988)، كما شهدت دول عربية عدة هجمات سيبرانية واسعة، مثل السعودية (2012)، المغرب (2008،2012) والعراق عبر التنظيمات الإجرامية والإرهابية.

وقد أدركت الجزائر مبكرًا خطورة هذا النوع من الجرائم، فسعت إلى وضع إطار قانوني ينظم التعامل مع الجريمة الإلكترونية ويعزز الأمن السيبراني، من خلال إصدار قوانين خاصة وتطوير قدرات الهيئات المختصة بالتحقيق والحماية الرقمية، كما عملت على إنشاء مؤسسات

مكلفة بالأمن المعلوماتي، في محاولة لبناء منظومة وطنية قادرة على مواجهة التهديدات السيبرانية التي تتزايد حدتها وتعقيدها.

أولا: أهمية دراسة الأمن السيبراني كآلية لمواجهة الجريمة الإلكترونية

تكتسي هذه دراسة أهمية خاصة في كون الأمن السيبراني يشكل خط الدفاع الأساسي لحماية الأنظمة المعلوماتية والبيانات من مختلف التهديدات الرقمية المتزايدة، فمع التطور السريع للتكنولوجيا واتساع استخدام الفضاء الرقمي، أصبحت الجريمة الإلكترونية أكثر تعقيداً وانتشاراً، مما يفرض ضرورة تعزيز آليات الوقاية والحماية والاستجابة.

-أهمية حماية الفضاء السيبراني الوطني: تتجلى أهمية هذا الموضوع في كون الأمن السيبراني أصبح يمثل أحد الدعائم الأساسية لحماية الدولة ومؤسساتها ومجتمعها من مختلف الهجمات الإلكترونية المتزايدة، كما أنه يشكل خط الدفاع الأول ضد التهديدات الرقمية التي قد تستهدف الاستقرار الأمني والاقتصادي، مما يجعله عنصراً محورياً في ضمان سيادة الدول في العصر الرقمي.

- أهمية فهم الإطار القانوني الجزائري: إن دراسة هذا الموضوع تتيح الوقوف على مدى فعالية وملاءمة المنظومة القانونية الجزائرية في مواجهة الجريمة الإلكترونية بمختلف صورها، كما تساعد على تحليل مواطن القوة والقصور في النصوص التشريعية الحالية، ومدى قدرتها على مواكبة التطور السريع لأساليب الجريمة الرقمية، بما يضمن تحقيق الردع والحماية القانونية الفعالة.

-تعزيز الأمن الوطني: يساهم فهم التهديدات المرتبطة بالفضاء السيبراني في دعم الأمن الوطني بمفهومه الشامل، من خلال تمكين الدولة من حماية بنيتها التحتية الحيوية والحساسة، مثل قطاعات الطاقة والمياه والصحة والاتصالات، فاستهداف هذه القطاعات رقمياً قد يؤدي إلى آثار خطيرة تمس استقرار الدولة وسير المرافق العامة.

-حماية البيانات والمعلومات: في ظل الاعتماد المتزايد على الأنظمة الرقمية، أصبحت البيانات والمعلومات من أهم الموارد الإستراتيجية، وعليه، فإن حمايتها يعد ضرورة ملحة للحد من مخاطر الاختراقات الإلكترونية، وعمليات التجسس، وسرقة أو التلاعب بالبيانات، مما يضمن الحفاظ على الخصوصية وسلامة المعاملات الإلكترونية.

-تعزيز الوعي الأمني لدى المجتمع: إن نشر الثقافة الأمنية الرقمية يساهم في رفع مستوى إدراك الأفراد والمؤسسات بمخاطر الفضاء السيبراني وأساليب الهجوم الإلكتروني، الأمر الذي يقلل من احتمالية الوقوع ضحية لعمليات التصيد والاختراق والاحتيال الإلكتروني، ويعزز سلوكيات الاستخدام الآمن للتكنولوجيا.

-مواكبة التطور التكنولوجي: إن التطور المتسارع في تقنيات الهجوم والدفاع السيبراني يفرض ضرورة دراسة هذا المجال بشكل مستمر، بهدف مواكبة المستجدات العالمية وتحديث الآليات الوقائية والتشريعية. كما يساهم ذلك في تعزيز جاهزية الدولة لمواجهة التهديدات المستجدة في البيئة الرقمية المتغيرة باستمرار.

ثانياً: أهداف دراسة

تهدف دراسة موضوع الأمن السيبراني كآلية لمواجهة الجريمة الإلكترونية في الجزائر في جملة من المحاور العلمية والقانونية التي تهدف إلى الإحاطة الشاملة بالموضوع من مختلف جوانبه، وذلك على النحو الآتي:

-دراسة الإطار المفاهيمي للأمن السيبراني والجريمة الإلكترونية في التشريع الجزائري من خلال ضبط المفاهيم الأساسية وتحديد طبيعة كل من الأمن السيبراني والجريمة الإلكترونية وخصائصهما، بما يسمح بفهم دقيق لمجال الدراسة.

-بيان العلاقة بين الأمن السيبراني والجريمة الإلكترونية وإبراز كيفية تكامل كل منهما مع الآخر، حيث يشكل الأمن السيبراني خط الدفاع الوقائي، بينما تمثل الجريمة الإلكترونية التهديد الذي يستوجب المواجهة والتصدي.

-تحليل واقع الأمن السيبراني في الجزائر من خلال دراسة البنية المؤسساتية والتقنية والتشريعية المعتمدة في حماية الفضاء السيبراني الوطني.

-تقييم مدى فعالية المنظومة القانونية الجزائرية في مكافحة الجريمة الإلكترونية ومدى قدرتها على مواكبة التطور السريع لأساليب وأنماط الجريمة الرقمية الحديثة.

-تحديد الآليات القانونية والإجرائية التي يعتمدها المشرع الجزائري لمكافحة الجريمة الإلكترونية سواء من خلال القوانين العقابية أو الإجراءات الوقائية ذات الصلة.

-إبراز دور الهيئات الوطنية في تعزيز الأمن السيبراني من خلال استعراض مهام المؤسسات الرسمية ودورها في الوقاية، الرصد، والاستجابة للهجمات الإلكترونية.

-تشخيص أهم التحديات التي تواجه تطبيق الأمن السيبراني في الجزائر سواء كانت تحديات تقنية أو بشرية أو تنظيمية أو تشريعية.

-اقتراح حلول وتوصيات عملية من شأنها تعزيز فعالية الأمن السيبراني وتطوير المنظومة القانونية والمؤسساتية، بما يساهم في الحد من انتشار الجريمة الإلكترونية وحماية الفضاء الرقمي الوطني.

ثالثًا: أسباب اختيار الموضوع

هناك جملة من الأسباب التي كانت وراء اختيارنا موضوع الأمن السيبراني كآلية لمواجهة الجريمة الإلكترونية في الجزائر، و تتمثل في :

-.يقع هذا الموضوع ضمن أهم المحاور في الحقل المعرفي والاهتمامات الشخصية للطالبتين، لاسيما في إطار تخصص القانون الجنائي، باعتباره مجالًا يواكب المستجدات المرتبطة بالجرائم الحديثة، وخاصة الجرائم الواقعة في الفضاء الرقمي وما تفرزه من تحديات قانونية وأمنية متجددة.

-الانتشار المتزايد للجريمة الإلكترونية في الجزائر نتيجة التوسع الكبير في استخدام التكنولوجيا والإنترنت، مما جعل الفضاء الرقمي مجالًا خصبًا لارتكاب مختلف الجرائم.

-الأهمية المتنامية للأمن السيبراني باعتباره أداة أساسية لحماية الأنظمة المعلوماتية والبنية التحتية الرقمية للدولة والمؤسسات والأفراد.

-ارتباط الموضوع بالواقع المعاصر للتحول الرقمي في الجزائر وما يفرضه من تحديات أمنية وقانونية تستوجب دراسة معمقة.

-الحاجة إلى تقييم الإطار القانوني الجزائري ومعرفة مدى قدرته على مواجهة الجرائم الإلكترونية المستجدة ومواكبة تطورها السريع.

-إبراز دور الدولة والمؤسسات الوطنية في تعزيز الأمن السيبراني وحماية الفضاء الرقمي الوطني من التهديدات المتزايدة.

–الاهتمام العلمي والبحثي بالموضوع باعتباره من المواضيع الحديثة التي تجمع بين القانون والتكنولوجيا والأمن.

–الرغبة في فهم العلاقة بين الأمن السيبراني والجريمة الإلكترونية وكيف يمكن للأول أن يشكل آلية فعالة للحد من الثانية.

–الطابع العملي للموضوع من خلال ارتباطه المباشر بحياة الأفراد والمؤسسات، خاصة في ظل الاعتماد المتزايد على الخدمات الرقمية.

–توجيه الاهتمام نحو تخصص مستقبلي مهم يجمع بين القانون والتكنولوجيا ويكتسب أهمية متزايدة في سوق العمل.

رابعاً: المنهج المتبع

–اعتمدنا في هذه الدراسة على المنهج الوصفي التحليلي، وذلك من خلال وصف مختلف المفاهيم المتعلقة بالأمن السيبراني والجريمة الإلكترونية، وتحليل الإطار القانوني والتنظيمي المعتمد في الجزائر لمواجهتها.

– كما تم الاعتماد على هذا المنهج لتفسير العلاقة القائمة بين الأمن السيبراني والجريمة الإلكترونية، وتقييم مدى فعالية الآليات القانونية والمؤسساتية في الحد من هذه الجرائم، مع محاولة استخلاص أهم النتائج والتحديات المرتبطة بالموضوع.

خامسًا: الإشكالية

انطلاقا مما سبق يمكن طرح إشكالية الآتية :

ما مدى نجاعة آلية الأمن السيبراني في مواجهة الجريمة الإلكترونية في الجزائر ؟

ويندرج تحت هذا التساؤل الأسئلة الفرعية الآتية:

_ ما المقصود بالأمن السبراني والجريمة الالكترونية، وما طبيعة العلاقة القائمة بينهما؟

_الى أي مدى اسهمة المنظومة المعلوماتية لمواجهة الجرية الالكترونية وماهي ابرز تحديات التي تواجهها؟

ولمعاجة موضوع و إجابة على الإشكالية تم اعتماد الخطة أدناه :

تم تخصيص الفصل الأول إلى الإطار المفاهيمي للأمن السيبراني و الجريمة الإلكترونية حيث تم تعرض إلى ماهية الأمن السيبراني في المبحث الأول أما المبحث الثاني إلى ماهية الجريمة الإلكترونية ، أما الفصل الثاني نتطرق إلى سبل مواجهة الجريمة الإلكترونية و تحقيق الأمن السيبراني في جزائر ، من خلال الآليات القانونية و الإجرائية لدعم الأمن السيبراني في مواجهة الجريمة إلكترونية في جزائر في مبحث الأول أما في الاخير نتطرق إلى تدابير تعزيز الأمن السيبراني في جزائر .

الفصل الأول:

الإطار المفاهيمي للأمن السيبراني والجريمة الإلكترونية

أفضت البيئة الرقمية في تسهيل تداول المعلومات وتبادلها بشكل سريع، مما عزّز وسائل الاتصال والتواصل بين الأفراد، وفتح آفاقًا واسعة للتطور في مختلف المجالات الاقتصادية والاجتماعية والإدارية، غير أن هذا التقدّم، وعلى الرغم من ايجابياته، أفرز في المقابل مجموعة من السلبيات، نتيجة استغلال بعض الأشخاص لهذه الوسائل الحديثة في ارتكاب أفعال غير مشروعة.

برزت أشكال جديدة من الجرائم، من بينها الجريمة الإلكترونية التي تعتبر نمط إجرامي حديث، غدت مخاطرها تضاهي في جسامتها الجرائم التقليدية، تعد الجريمة الإلكترونية من الظواهر الإجرامية الحديثة نسبيا، وقد أصبحت هذه الظاهرة تشكّل تحدياً حقيقيا يواجه الدولة والمجتمع، نظرا لما تنطوي عليه من مخاطر تمسّ بأمن الأفراد وخصوصيتهم الرقمية، وكذا سلامة الأنظمة المعلوماتية.

ساهمت الطبيعة الافتراضية للفضاء الرقمي في تمكين الجناة من استغلال التقنيات الحديثة لارتكاب أفعال إجرامية تمس الأفراد والمؤسسات على حد سواء، وذلك من خلال اختراق الأنظمة المعلوماتية، أو سرقة البيانات، أو تعطيل الخدمات الرقمية، وفي ظل هذه التهديدات المتزايدة، برزت الحاجة الملحة إلى تعزيز الأمن السيبراني كآلية أساسية لحماية الأنظمة والشبكات الإلكترونية، وضمان سلامة البيانات، والتصدي لمختلف الهجمات الإلكترونية.

يُعدّ الأمن السيبراني من المفاهيم الحديثة التي فرضت نفسها بقوة في ظل التطور المتسارع لتقنيات المعلومات والاتصال، حيث أصبح الفضاء الرقمي جزءًا أساسيًا من الحياة اليومية للأفراد والمؤسسات والدول هذا ما نتطرق إليه في **(المبحث الأول)**، أما الجريمة الإلكترونية تعتبر من الظواهر الإجرامية المستحدثة التي برزت بشكل واضح مع التطور السريع في استخدام تكنولوجيا المعلومات والاتصال، وما رافقه من توسّع في الاعتماد على الفضاء الرقمي في مختلف مجالات الحياة و هذا ما نتطرق إليه في **(المبحث الثاني)**.

المبحث الأول

ماهية الأمن السيبراني

أسفر عن نهاية الحرب الباردة ظهور مصطلحات جديدة مثل الحرب الالكترونية أو ما تسمى كذلك بالحروب السيبرانية، التي جاءت نتيجة التحول الرقمي وتزامنًا مع بداية اعتماد الإنسان على الحاسوب في حياته اليومية، وحتى الدول كذلك بدأت تعتمد هذه التقنية في مؤسساتها وحكومتها، لتصبح جزءا أساسيا لا يتجزأ من عملها.

أدى هذا الأمر إلى بروز الحاجة الملحة للأمن السيبراني لحماية الأنظمة، نتيجة لنشوء جرائم ترتكب عبر الإنترنت تعرف بالجرائم الإلكترونية أو الجرائم السيبرانية، انحصر في البداية نطاق الأمن السيبراني بشكل أساسي في التصدي للفيروسات والبرمجيات الضارة.

توسع الأمن السيبراني تدريجيا ليشمل حماية الشبكات والبيانات الحساسة، ومراقبة التهديدات السيبرانية، حيث أصبح يعتمد على تقنيات ذكية كالتشفير والأمان الحسابي لضمان تصدي الفوري والفعّال للهجمات السيبرانية.

يتعبر الأمن السيبراني كأحد أكثر الميادين التقنية حيوية وطلبًا، إذ لم تعد التهديدات الرقمية والهجمات الالكترونية مجرد توقعات، بل باتت واقعا يوميًا يواجه الأفراد والمؤسسات والشركات على حد سواء، ومع اتساع رقعة الاعتماد على الحلول التقنية، تضاعفت الحاجة إلى توفر أشخاص متخصصين قادرة على تأمين المعلومات وحماية الأنظمة.

من خلال ما سبق، نتطرق في هذا **(المطلب الأول)** إلى مفهوم الأمن السيبراني، و إلى ماهية الجريمة الإلكترونية **(المطلب الثاني)**.

المطلب الأول

مفهوم الأمن السيبراني

لم يعد الأمن السيبراني مجرد خيار تقني، بل أصبح ضرورة إستراتيجية تتجسد في جملة من السياسيات والتدابير المهيأة لتأمين بيئة الاتصالات والمعلومات، من خلال التوفيق بين الحماية الموارد البشرية والمادية وتفعيل آليات الاستجابة الفورية، يعمل الأمن السيبراني كحائط صّد يهدف للحد من تداعيات المخاطر الرقمية وضمان استمرارية العمل في مواجهة الأزمات.

نظرًا للدور الذي يعلبه الأمن السيبراني في استقرار المجتمعات المعاصرة، جعلته العديد من الدول في صدارة أولوياتها الإستراتيجية، خاصة بعد ظهور الحروب الإلكترونية بين بعض الدول الكبرى، مما يشير إلى تراجع الحروب التقليدية القائمة على الأسلحة الثقيلة، وإعلان عصر جديد تتصدره الحروب السيبرانية التي باتت تشكل جوهر النزاعات الدولية الحديثة.

بناءً على ما تطرقنا له، تناول هذا المطلب **(الفرع الأول)** إلى تحليل مفهوم الأمن السيبراني، وفق أبرز التعريفات الدولية والفقهية والقانونية، بينما يتضمن **(الفرع الثاني)** تمييز الأمن السيبراني عن المفاهيم المشابهة له.

الفرع الأول: تعريف الأمن السيبراني

شهدت المجتمعات البشرية مع تطور وتنوع ثقافاتها، واختلاف الخلفيات الفكرية وتباين تخصصات الباحثين ومستوياتهم العلمية، وفي ظل التحول الرقمي المتسارع، تعددت المقاربات المفاهيمية لعدة مصطلحات، ومن بينها مصطلح الأمن السيبراني، الذي برز نتيجة التقدم التكنولوجي واعتماد الإنسان المتزايد على الفضاء الرقمي في مختلف المجالات، وأصبح كآلية ضرورية لحماية المعلومات والأنظمة من التهديدات الإلكترونية، ورغم تعدد مفاهيم الأمن السيبيراني واختلاف صياغتها، فإنها تتفق على نفس المضمون، وسنسعى إلى عرض أهم التعريفات.

أولاً: التعريف اللغوي والاصطلاحي للأمن السيبراني

يمثل مصطلح الأمن السيبراني مزيجاً بين دلالة لغوية متجذرة وأخرى اصطلاحية واكبت الثورة الرقمية والتطور التكنولوجي المتسارع، الأمر الذي أدى إلى اتساع مجالات استخدامه:

1- الأمن السيبراني لغويًا: مكوّن من مصطلحين: "الأمن"، و"السيبراني"

الأمن: هو الاستقرار والسلام وحالة الاطمئنان النفسي وتحقيق الأمان، وزوال الخوف والقلق، والأمن مشتّق من مصدر الفعل "أَمِنَ"و "أَمنًا" و"أَمَانًا" و"أَمَنَةً": أي سكن قلبه وتلاشى عنه الخوف، ويقال: أَمنَ من الشَّر، أي تحصّن من كل مكروه، وضمن سلامة نفسه من التهديدات والمخاطر المحتملة، وقد عرّفه قاموس بنغوين للعلاقات الدولية بأنه:" مصطلح يشير إلى غياب ما يُهدد القيم النادرة.[1]

السيبرانية: مصطلح "السيبرانية" يُنسب أصله عند بعض الباحثين إلى عالم الرياضيات الأمريكي نوربرت وينر (Wiener, Norbert)، الذي استعمله للدلالة على نظرية التحكم والاتصال في الآلة، أما كلمة "cyber" فهي مشتقة من مصطلح"Kybernetes" اليوناني، الذي يعني "ربّان السفينة" أو"المُوجِه"، ومع تطور التكنولوجيا وتزايد الاعتماد على الفضاء الرقمي، أصبح هذا المصطلح من أكثر المفاهيم تداولاً في ميدان الأمن الدولي.[2]

2- الأمن السيبراني اصطلاحًا:

الأمن السيبراني هو مجموعة من التدابير والإجراءات التقنية والتنظيمية التي تهدف إلى حماية الأنظمة المعلوماتية، بما يضمن أمن البيانات والمعلومات، وذلك عبر منظومة من معايير والمقاييس الإلزامية التي تستهدف التصدي للتهديدات الرقمية والحد من آثارها المحتملة.[3]

يعرف كذلك بأنه أمن الفضاء الإلكتروني يهدف لحماية البنية التحتية المعلوماتية وما تتضمنه من شبكات وبيانات وكافة الأجهزة المتصلة بالإنترنت، يُعد المجال الذي يختص بالإجراءات والتدابير والمعايير الوقائية التي يتعين اعتمادها والالتزام بها، بهدف مواجهة التهديدات الإلكترونية، ومنع التعديات الناتجة عن أي اعتداء، وللحد من آثارها.

---

[1] فارس محمد العميرات،"الأمن السيبراني(المفهوم وتحديات العصر)"، دار الخليج للنشر والتوزيع، الطبعة الأولى، الأردن، عمّان، 2022، ص12.

[2] معتوق أم الخير، "كسب رهان الأمن السيبيراني ضمان لتعزيز الأمن ودفاع الوطنيين في الجزائر"، مجلة البحوث في الحقوق والعلوم السياسية، الملحقة الجامعية الشلالة، جامعة تيارت، المجلد09، العدد02، الجزائر، 2024، ص 63، ص ص53-76.

[3] المرجع نفسه، ص 58.

وتبرز أهميته من خلال ارتباطه الجوهري بأمن المعلومات، إذ أن السعي الغير مشروع للوصول إلى المعلومات أو نسخها أو الاطلاع عليها أو الاتجار بها أو تحريفها أو استغلالها، يعتبر الدافع الأساسي وراء الهجمات التي تستهدف الشبكات والأنظمة المعلوماتية والفضاء الرقمي عموما.[1]

تعرفه وكالة الأمن السيبراني وأمن البنية التحتية الأمريكية (سي آي إس إيه) بأنه:الفن المعني بتحصين الشبكات والبيانات والأنظمة ضد أي اختراق أو استغلال غير القانوني، ويهدف بشكل رئيسي إلى حماية المثلث الأمني: السرية، والنزاهة، وتوفر المعلومات.[2]

عرفه التقرير الصادر عن الإتحاد الدولي للاتصالات، حول اتجاهات الإصلاح في الاتصالات للعام 2010-2011م، بأنه: بأنه مجموعة متكاملة من المهام تدمج بين السياسات الأمنية وأدوات إدارة المخاطر، وأفضل الممارسات التقنية، واعتماد المبادئ التوجيهية، إلى جانب برامج التدريب، بهدف بناء إطار دفاعي يحمي الأصول الرقمية للمؤسسات والأفراد ويضمن استمرارية العمل في البيئة السيبرانية آمنة.[3]

أما وزارة الدفاع الأمريكية "البنتاغون" وضعت تعريفًا دقيقًا لمصطلح الأمن السيبراني، فاعتبرته: كافة التدابير التنظيمية المعتمدة لتأمين المعلومات بمختلف وسائطها المادية أو الإلكترونية، بهدف حمايتها من شتى المخاطر والتهديدات السيبرانية، وأعمال التخريب والتجسس، إضافة إلى حوادث عرضية.[4]

وكذلك عرفته شركة "كاسبر سكاي" الدولية الخاصة بالأمن السيبراني بأنه جملة من آليات حماية البنية التحتية الرقمية بما في ذلك الخوادم والبيانات والأجهزة بمختلف أنواعها، من الهجمات الخبيثة، ويطلق عليه أيضا بمصطلح أمن تكنولوجيا المعلومات أو الأمن الإلكتروني للمعلومات.[5]

---

[1] فارس محمد العميرات، مرجع سابق، ص16

[2] الأمن السيبراني: مفهومه وتاريخه، الموقع: https://www.aljazeera.net/amp/encyclopedia/2024/9/19 الجزيرة نت، تم الاطلاع عليه بتاريخ 2026/01/15. على الساعة 13:15.

[3] محمد محمود العمري،"مدخل إلى الأمن السيبراني"، دار زهران للنشر والتوزيع، الطبعة الأولى، عمّان، 2020، ص18.

[4] محمد محمود العمري، مرجع سابق، ص19.

[5] الأمن السيبراني: أهمية حماية البيانات في العصر الرقمي الموقع:https://spskills.com/articles

ثانيا: التعريف الفقهي

الأمن السيبراني هو مجموعة متكاملة من التدابير الفنية والتنظيمية والإدارية، التي تعتمد للحد من الوصول غير المصرح به وحماية نظم الاتصالات من سوء الاستغلال، وضمان استرجاع المعلومات الإلكترونية، مع الأولوية لترسيخ دعائم الخصوصية الرقمية، وضمان سرية البيانات الشخصية للمستخدمين، وحمايتها من أي ولوج غير مشروع، وتوفير بيئة رقمية آمنة كفيلة بحماية الأفراد والمستهلكين في الفضاء السيبراني.[1]

بينما عرّفه إدوارد أمورسو(Amoroso Edward) بأنه: "وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل والأدوات.[2]

ثالثًا: تعريف المشرع الجزائري للأمن السيبراني

تطرق له المشرع الجزائري في القانون رقم: 18-04 في الفقرة الثالثة من المادة 10 بأنه الإطار الجامع للآليات الأمنية، والضمانات التكنولوجية، ومبادئ إدارة المخاطر والممارسات التشغيلية والتأهيلية، التي يلجأ إليها لتأمين البيانات المخزّنة والمعالجة والمرسلة، وضمان صمودها أمام أي اختراق قد يمس بتوفر وسلامة وسرّية البيانات[3].

لقد أعطى المشرع الجزائري اهتمامًا لحماية الفضاء الرقمي من خلال تعديله الأول لقانون العقوبات للفصل الثالث من الباب الثاني من الكتاب الثالث من الأمر رقم 66-156[4]، بإضافته قسم السابع مكرر عنوانه: "المساس بأنظمة المعالجة الآلية للمعطيات"، في القانون

تم الاطلاع عليه بتاريخ 2026/01/10 على الساعة 18:47.

[1] قطاف سليمان، بوقرين عبد الحليم، "الآليات الموضوعية والإجرائية المتبعة لتحقيق الأمن السيبراني (الجزائر نموذجا)"، مجلة الحكومة والقانون الاقتصادي، جامعة عمار ثليجي، المجلد03، العدد02، الأغواط، الجزائر، 2023، ص 83، ص ص 93/80.

[2] محمد محمود العمري، مرجع سابق، ص 20.

[3] قانون رقم 18-04 مؤرخ في 24 شعبان عام 1439 الموافق ل 10مايو سنة 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، الجريدة الرسميّة للجمهورية الجزائريّة، العدد27، الصادرة بتاريخ 13 مايو 2018.

[4] القانون رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق ل8 يونيو سنة 1966، يتضمن قانون العقوبات المعدل والمتمم، الجريدة الرسمية للجمهورية الجزائرية، العدد49، الصادرة في 11 يونيو 1966.

04-15 ويشمل المواد من 394 مكرر إلى 394مكرر7[1]، يهدف هذا التنظيم القانوني الذي وضعه المشرع إلى رصد الأنشطة الإجرامية في هذا المجال وتعيين الجزاءات المناسبة لها للحد من انتشارها.

من خلال ما سبق عرضه من التعاريف الاصطلاحية والفقهية والتشريعية، يتضح لنا أن الأمن السيبراني هو مجموعة من وسائل وإجراءات أمنية واليات تقنية تحمي الفضاء الإلكتروني المتكون من الأنظمة المعلوماتية، الشبكات، البنية الرقمية التحتية، من أي اختراق أو استعمال غير مشروع أو تخريب البيانات أو تعطيلها.

يتطلب تحقيق الأمن السيبراني وجود ثلاثة عناصر أساسية متكاملة تشكل معا جدار الحماية الرقمية والمتمثلة في[2]:

1- العنصر التقني:(Technology)

يمثل البنية التحتية والعمود الفقري لأنظمة المعلومات، وتشمل كافة المكوّنات المادية والبرمجية مثل: شبكات الاتصال والإنترنت، أنظمة الحاسب الآلي والخوادم.

2- عنصر الاجراءات(Processes)

يشمل كافة الآليات التقنية والمادية والقانونية اللازمة لضمان الأمن السيبراني وحماية الأنظمة من التهديدات والهجمات الإلكترونية.

3- العنصر البشري(People)

هو الركيزة الأهم في المعادلة، وتتمثل في القوى العاملة المؤهلة التي تدير هذه الأنظمة، مثل الخبراء المتخصصين في الذكاء الاصطناعي والإعلام الآلي، المهندسين والتقنيين السامين المعنيين بتطوير الأنظمة وحمايتها[3].

---

[1] انظر المواد من 394مكرر إلى 394 مكرر7، من القانون رقم 04-15 المؤرخ في 10 نوفمبر2004، يعدل ويتمم الأمر رقم 66-156 المتضمن قانون العقوبات، الجريدة الرسمية للجمهوية الجزائرية، العدد71، الصادرة قي 2004.

[2] حميدي حياة، طايلب نسيمة،" مدخل مفاهيمي حول الأمن السيبراني"، مجلة مدار للدراسات الاتصالية الرقمية، جامعة الجزائر، المجلد02، العدد02، الجزائر، 2022،ص13، ص ص11-16.

[3] مرجع نفسه، ص 17.

الفرع الثاني: التداخلات المفاهيمية للأمن السيبراني

يلاحظ أنه في مجال الأمن السيبراني يكثر فيه استعمال مصطلحات متعددة، مما قد يحدث خلطاً مفاهمياً لدى القارئ، يصبح من الضروري التمييز بين المصطلحات المرتبطة به، مع توضيح أنها لا تحمل نفس المعنى ولا نفس نطاق التطبيق:

أولاً: الفضاء السيبراني

تعود جذور هذا مصطلح إلى عام 1982،حين صاغه كاتب الخيال العلمي ويليام جيبسون (William Gibdon)ووصفها ب " الهلوسة الجماعية "، تعتمد فكرته على تحويل البيانات الضخمة المخزنة في شبكات الكمبيوتر إلى واجهة مرئية يشارك فيها مليارات المستخدمين يوميًا حول العالم، ويعد مصطلح "الفضاء السيبراني "مصطلحاً حديثًا نتيجة ثورة تكنولوجيا المعلومات، يشمل جميع الحواسيب والبيانات والأجهزة، والبرمجيات والشبكات، موفرًا الإطار الذي يتم من خلاله تنظيم وإدارة الفضاء السيبراني[1].

عرفته الوكالة الفرنسية لأمن أنظمة الإعلام (ANSSI)على أنه: بيئة التواصل الناتجة عن الترابط العالمي لأنظمة المعالجة الآلية للمعطيات، يركز هذا التعريف على الجانب التقني، لكنه لا يغفل الدور الحيوي للعامل البشري، الذي يعد عنصرًا جوهريا لفهم طبيعة هذا الفضاء وآليات عمله[2].

عرفه كذلك الاتحاد الدولي للاتصالات بأنه: المجال المادي والغير مادي الذي يتكون من عناصر جوهرية متمثلة في أنظمة الكمبيوتر والشبكات، والبرمجيات، والمعطيات الرقمية ووسائل النقل والتحكم، بالإضافة إلى المستخدمين الذين يتعاملون مع هذه العناصر[3].

يعرف كذلك بأنه المجال العالمي ضمن البيئة المعلوماتية، يتألف من شبكة مترابطة من البنى التحتية لأنظمة المعلومات، إلا أنه عمليا يتجاوز هذه الشبكات لتشمل كافة العناصر

---

[1]علاء الدين فرحات،" **الفضاء السيبراني: تشكيل ساحة المعركة في القرن 21**"، مجلة العلوم القانونية والسياسية، المدرسة الوطنية العليا للعلوم السياسية، المجلد10، العدد10، الجزائر، 2019، ص93،ص ص 88-107.

[2]إسماعيل زروقة، **الفضاء السيبراني والتحول في مفاهيم القوة والصراع**"، مجلة العلوم القانونية والسياسية، جامعة محمد بوضياف، المسيلة، المجلد 10، العدد1، الجزائر، 2019، ص 1020، ص ص 1016-1031.

[3]أميرة عبد العظيم، محمد عبد الجواد، "**المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام**"، مجلة الشريعة والقانون، العدد35، الجزائر، 2020، ص397، ص ص410،390.

الافتراضية الحديثة، ليمتد إلى كافة الأنماط والأنشطة البشرية، التفاعلية المرتبطة باتصال الرقمي، إذًا يعتبر الأمن السيبراني الدرع الواقي والضمانة الأساسية لاستقرار هذا الفضاء الافتراضي، حيث يهدف إلى تأمين التدفقات المعلوماتية الرقمية وذلك لضمان سلامة المحتويات وحماية أنشطتها[1].

ثانيا : القوة السيبرانية(CyberPwer)

أحدث الفضاء السيبراني تحولاً جوهريًا في بنية قوة الدولة، حيث لم تعد القوة تُقاس فقط بعناصرها التقليدية، بل أصبحت القوة السيبرانيةمأشراً أساسياً في تقييم المكانة الدولية.

يعرف جوزيف ناي(Nye.S Joseph) القوة السيبرانية بأنها: القدرة على تحقيق نتائج عبر استغلال الموارد المعلوماتية المرتبطة بالفضاء السيبراني، أي أنها تمثل قدرة الدولة على استثمار هذا المجال لخلق مزايا إستراتيجية لصالحها، وذلك باستخدام تقنيات سيبرانية تمكّنها من تحقيق أفضلية نسبية على غيرها من الفاعلين[2].

ويضيف ماكس فيبر(Max Weber) أبعادا جوهرية لفهم القوة السيبرانية وخصائصها، إذ يربط ممارستها بوجود علاقة اجتماعية، إذ تتمثل في قدرة فاعل معين على فرض إرادته داخل تلك العلاقة رغم وجود مقاومة محتملة، ومن هنا لا يمكن الحديث عن امتلاك الفاعل للقوة السيبرانية بصورة مطلقة دون تحديد الفاعلين المعنيين بها ونطاق ممارستها، والمجال الذي تُمارس فيه، لأن القوة تقاس بالفعل والتأثير لا بمجرد الادعاء بامتلاكها[3].

أما دانيال تويكل (Daniel T.Kuehl) يرى بأن جوهر القوة السيبرانية يكون في القدرة على توظيف شبكة الإنترنت لخلق مزايا إستراتيجية، فهي قدرة لا تنحصر في العالم الرقمي فقط بل تمتد لتأثر في كافة ميادين العسكرية أو السياسية أو الاقتصادية، مستخدمة الأدوات السيبرانية كأحد عناصر قوة الدولة الشاملة[4].

---

[1]حميدي حياة، طايب نسمة، مرجع سابق، ص 16.

[2]محمد محمود العمري، مرجع سابق، ص21.

[3]محمد محمود زيتون،"القوة السيبرانية أداة للتأثير والسيطرة في الفضاء السيبراني والعلاقات الدولية (بحث مكمل لمناقشة رسالة الدكتوراه)، المجلة العربية للنشر العلمي، الإصدار 8، العدد77، 2025، ص ص202-220.

[4]زمور جمال، بن عيسى ليلى،" **أهمية حوكمة الأمن السيبراني لضمان تحول رقمي آمن للخدمات العمومية في الجزائر**"، مجلة البحوث الاقتصادية المتقدمة، جامعة محمد خيضر بسكرة، المجلد7، العدد2، الجزائر، 2022،ص ص 1572-2676.

أما كولين غراي(ColinS.Gray) يعرف القوة السيبرانية أنها القدرة على تحقيق أفضلية إستراتيجية داخل الفضاء السيبراني، إذ يعتبر هذا تعريف من أبسط وأوضح التعريفات، لأنه يركز على نتيجة نهائية للقوة، أي تحقيق مكسب استراتيجي، وانطلاقا من هذا تعريف،فإن امتلاك القوة السيبرانية لا يعد غاية في حد ذاته، وإنما وسيلة لتمكين الدولة من تعزيز موقعها الاستراتيجي من خلال الأمن السيبراني سواء عبر فرض التأثير، أو تحقيق الردع، أو حماية مصالحها الحيوية[1].

ثالثا: الجريمة السيبرانية

يستخدم مصطلح "الجريمة السيبرانية " في الآونة الأخيرة للدلالة على الجرائم المعلوماتية، والتي ظهرت وتطورت نتيجة طبيعية للتقدم التكنولوجي. تعد الجريمة السيبرانية إحدى الظواهر الإجرامية المرتبطة بالتقدم التكنولوجي والمعلوماتي، إلا أن طبيعتها العابرة للحدود وتطورها المتسارع، جعل من الصعب التوصل إلى تعريف موحد لها،خاصة مع تعدد أشكالها وتنوع تسمياتها مثل: الجرائم الإلكترونية، جرائم الإنترنت، وجرائم الحاسوب،جرائم الجيل الخامس، وجرائم التقنية العالية....إلخ[2].

وقد عرفت الجريمة السيبرانية بأنها نشاط غير قانوني تستعمل فيه تقنيات الحاسوب بصورة مباشرة أو غير مباشرة كأداة أو محل لارتكاب الجريمة، كما تعرف أيضًا بأنها كل سلوك مخالف للقانون أو للأخلاق يتم عبر الشبكات المعلوماتية، حيث تعد من جرائم العصر الرقمي التي تمس الأموال والمعرفة والثقة والسمعة، ويتم تنفيذها باستخدام الوسائل التكنولوجية الحديثة[3].

أما جانب كبير من الفقه القانوني يرى أن الجريمة السيبرانية عبارة عن كل نشاط إجرامي يكون فيه الكمبيوتر أو شبكة الكمبيوتر وسيلة لارتكاب الجريمة أو محلاً لهاغير أن هذا

---

[1]فاتح حارك،"الفضاءالسيبراني والتحول في مفهوم الأمن في الولايات المتحدة الأمريكية"، أطروحة مقدمة لنيل شهادة الدكتوراه، الطور الثالث، كلية العلوم السياسة، قسم العلاقات الدولية، جامعة قسنطينة3 صالح بونيدر، الجزائر، 2024/2023، ص63.

[2]اسيا العمراني،"**التعاون الدولي في مواجهة الجرائم السيبرانية (الجزائر نوذجًا)**"، كلية العلوم السياسية والعلاقات الدولية، جامعة الجزائر 3، المجلد 3، العدد2، الجزائر،2010، ص 54،ص ص63،50.

[3]زينب الياقوت، "دور الإعلام الجزائري في التصدي للجريمة السيبرانية (قناة النهار نوذجاً)، مجلة طينة للدراسات العلمية الأكاديمية، المجلد5، العدد01، الجزائر، 2022، ص1371، ص ص1362-1379.

التعريف لا يخلو من الإشكالات، إذ يتسم بشمولية كبيرة قد تدمج الجرائم التقليدية ضمن النطاق السيبراني.[1]

رابعاً: أمن المعلومات

إفشاء غير مصرح به، ويشمل ذلك وضع مجموعة من سياسات والإجراءات الكفيلة بضمان حماية البيانات.[2]

يعرف أمن المعلومات بأنه منظومة من الضوابط والإجراءات التي تهدف إلى تنظيم وضبط عملية الوصول إلى البيانات، من خلال تحديد الجهات المخوَّلة بالتعامل معها ونطاق الصلاحيات الممنوحة لها، ويعرف كذلك بأنه مجموعة تدابير والاحتياطات التنظيمية والتقنية المتخذة بهدف حماية المعلومات المخزنة في الحواسيب من مختلف المخاطر، وذلك عبر اعتماد تدابير و إستراتيجيات إستباقية تحول دون وقوع الحوادث التقنية أو تعرض للهجمات السيبرانية المعتمدة.[3]

انطلاقا من مفهوم أمن المعلومات يتبين أنه يركز أساسا على حماية المعلومات والحفاظ على سريتها وسلامتها وتوفرها، وهو في ذلك يتشابه مع مفهوم الأمن السيبراني الذي يسعى بدوره إلى تأمين المعلومات، غير أن الاختلاف بينهما يظهر من حيث المفهوم والوظيفة، فأمن المعلومات يركز أساسا على حماية البيانات وضمان سريتها وسلامتها وتوفرها، في حين يتسع نطاق الأمن السيبراني ليشمل حماية الأنظمة المعلوماتية والشبكات والتطبيقات من الاختراقات والهجمات الإلكترونية.[4]

يتضح أن مفهوم الأمن السيبراني لم يعد يقتصر على الجانب التقني فقط، بل أصبح يشكل إطارا شاملا يهدف إلى حماية الأنظمة المعلوماتية والشبكات والبيانات من مختلف التهديدات

---

[1] فاتح حارك، مرجع سابق، ص70.

[2] فهد قطينة، كتاب الأمن السيبراني الموقع: https://www.ktobati.com/book/%D9%8 تم الاطلاع عليه يوم 22 جانفي 2026 على الساعة 22:30

[3] عبد الله بن سعود، محمد السراني، "فعّالية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني"، لرسالة مقدمة لنيل شهادة الدكتوراه، قسم العلوم الشرطية، جامعة نايف للعلوم الأمنية، الرياض، السعودية، 2009، ص23.

[4] ربيعي حسين،"آليات البحث والتحقيق في الجرائم المعلوماتية"، أطروحة مقدمة لنيل شهادة الدكتوراه، كلية الحقوق والعلوم السياسية، جامعة باتنة1، الجزائر، 2016/2015، ص21.

والهجمات الإلكترونية، وقد ساهم التطور التكنولوجي والاعتماد المتزايد على الوسائل الرقمية في إبراز أهمية الأمن السيبراني كضرورة تفرضها متطلبات العصر الرقمي ، كما بينت التداخلات المفاهيمية للأمن السيبراني مدى ارتباطه بعدة مفاهيم متقاربة، على غرار القوة السيبرانية و الجريمة السيبرانية ، وهو ما يعكس اتساع نطاقه وتعدد مجالات تطبيقه، وعليه، فإن تحقيق أمن سيبراني فعال يستوجب اعتماد آليات قانونية وتنظيمية متكاملة، بما يضمن حماية الفضاء السيبراني وتأمين المصالح الحيوية للدول والمؤسسات والأفراد.

المطلب الثاني

أبعاد ومبادئ الأمن السيبراني

يمثل الأمن السيبراني ركيزة جوهرية لتحصين البيئة الرقمية وضمان ديمومة النظم المعلوماتية أمام تصاعد التهديدات المصاحبة للثورة التكنولوجية، وتتجاوز آفاقه تأمين البيانات والشبكات لتشمل حماية الأفراد، والمنشآت، والقطاعات الحيوية من الهجمات الإلكترونية.

ولضمان حماية متكاملة، يستند هذا المجال إلى أبعاد متعددة تدمج الجوانب التقنية، والتنظيمية، والبشرية، والقانونية، مرتكزاً على مبادئ رئيسية : السرية، والسلامة، والإتاحة، بناءً على ذلك، تبرز أهمية دراسة هذه الأبعاد والمبادئ كخطوة أساسية لفهم مقومات الأمن الرقمي ورفع كفاءته في التصدي للتحديات السيبرانية الراهنة.

الأمن السيبراني أصبح يشمل أبعادًا متعددة ومتكاملة تهدف إلى ضمان حماية المعلومات والشبكات والبنى التحتية الرقمية من مختلف التهديدات والهجمات الإلكترونية **(الفرع الأول)**، وتُعد مبادئ الأمن السيبراني الأساس الذي ترتكز عليه سياسات وإستراتيجياته ، إذ تضمن سلامة المعلومات واستمرارية الخدمات الرقمية وتعزيز الثقة في استخدام التكنولوجيا الحديثة **(الفرع الثاني)**.

الفرع الأول: أبعاد الأمن السيبراني

لم يعد الأمن السيبراني مجرد تخصص تقني يحصر في قطاع محدد، لأنه مجال واسع يمسّ كافة القطاعات المعاصرة ويتقاطع معها، لأنه الركيزة التي لا يمكن تجاوزها عند بناء أي إستراتيجية أمنية شاملة، إذ لا يمكن اليوم الحديث عن الأمن الإنساني بمعزل عنه، كما لا يمكن فصل الأمن العالمي عن متطلبات الحماية السيبرانية، وحتى الأمن البيئي بات مرتبطا

بالقدرة على حماية الأنظمة الرقمية التي تدير الموارد الطبيعية وتراقب التغيرات المناخية، ويرجع ذلك إلى الاعتماد المتزايد على الأنظمة الرقمية وشبكات المعلومات في إدارة شؤون الدول والمؤسسات، مما يجعل الأمن السيبراني ركيزة أساسية لضمان استقرار وحماية مختلف المجالات، ويشمل الأمن السيبراني العديد من الأبعاد أبرزها:

أولاً: البعد القانوني

تقوم العلاقة بين القانون والتكنولوجيا على الطابع تفاعلي متبادل، إذ تسعى التشريعات جاهدا لمواكبة القفزات التقنية عبر وضع أطر قانونية تُميز بين السلوكيات المشروعة وغير مشروعة في الفضاء الرقمي، ومع ذلك، لا يزال هناك فجوة تشريعية ونقص في القوانين الرادعة للجرائم السيبرانية، ويرجع ذلك لعدة عوامل، أبرزها: خصوصية هذا النوع من الجرائم وصعوبة تحديد هوية مرتكبيها، والطبيعة العابرة للحدود لهذه الجرائم، والمرونة العالية في مفاهيم تكنولوجيا المعلومات، ونظرا لأن الجريمة السيبرانية لا تعترف بالحدود الوطنية، فقد أضحى التعاون الدولي ضرورة ملحة لمكافحتها وتوحيد الجهود القانونية ضدها[1].

تفرز الأنشطة الفردية والمؤسساتية في البيئة الرقمية، وما يرافقها من دعم وتفاعل، تبعات قانونية والتزامات متعددة تستوجب عناية خاصة لفض النزاعات الناشئة عنها، وهذا يفرض عليها ضرورة مواكبة التحولات المتسارعة في مجتمع المعلومات، وقد استتبع هذا التحول في مجتمع المعلومات إقرار حقوق رقمية مستحدثة، كالحق في النفاذ إلى الشبكة العالمية للمعلومات، مع توسع أنماط الحماية القانونية لتشمل إنشاء المدونات والتجمعات الإلكترونية، وصولاً إلى حماية حقوق الملكية الفكرية للبرمجيات.[2]

ثانيًا: البعد السياسي

يُجسّد التدخل الروسي المفترض في الانتخابات الأمريكية، نموذجاً بارزاً لتوظيف الفضاء السيبراني كأداة للتأثير السياسي وتقويض العمليات الديمقراطية، ولم يقتصر الأمر على الاختراقات التقنية وتسريب الوثائق الحساسة بما قد يؤدي إلى زعزعة الاستقرار الدبلوماسي، بل

---

[1] قطاف سليمان، بوقرين عبد الحليم، مرجع سابق، ص 80.

[2] سمير بارة، الأمن السيبراني في الجزائر السياسات والمؤسسات، المجلة الجزائرية للأمن الإنساني، جامعة قاصدي مرباح، المجلد02، العدد04، الجزائر، 2017، ص 260، ص ص 255-280.

امتد ليشمل ما يُعرف بالحرب النفسية الرقمية، فقد تحوّل الفضاء السيبراني إلى ساحة مفتوحة لشن حملات الدعاية الموجّهة، حيث يتم توظيف الخوارزميات والبيانات الضخمة للتأثير في اتجاهات الرأي العام وتوجيهه، ومن ثمّ أصبح الأمن السيبراني في الوقت الراهن خط الدفاع الأول لحماية السيادة السياسية للدول وصون نزاهة عملياتها الديمقراطية، يمكن تناول هذا العنصر من خلال جملة من نقاط الأساسية[1]:

1-استهداف الفاعلين السياسيين وسلاح " التسريبات " يتمثل التهديد الأول في الاختراقات التي تطال البريد الإلكتروني أوالأجهزة الخاصة لرجال الدولة والسياسيين، هذه التسريبات المعلوماتية لا تكتفي بضرب السمعة الشخصية، بل قد تؤدي إلى أزمات ديبلوماسية حادة أو كشف أسرار الدولة، مما يزعزع الثقة في المؤسسات السياسية ويؤثر على صناعة القرار.

2-هشاشة البنية التحتية وحروب "الجيل الخامس" إن ضعف التحصين السيبراني يجعل الدولة هدفاً سهلاً للهجمات الممنهجة، مما قد يدخلها في أزمات سيادية نتيجة فقدان السيطرة على الأنظمة الحيوية، ويعد الهجوم السيبراني على استونيا (المنسوب لروسيا) نموذجاً كلاسيكياً،حيث شُلت المواقع الحكومية والقطاعات المصرفية وقنوات الاتصال، مما أثبت أن الهجوم الرقمي يمكن أن يعطل دولة كاملة دون إطلاق رصاصة واحدة".

3-الفضاء السيبراني كأداة للتعبئة والتدخل الخارجي تساهم مرونة المعلومات وسرعة انتشارها في تحويل الفضاء الرقمي إلى ساحة لتنظيم الاحتجاجات والمظاهرات، تكمن الخطورة السياسية هنا في إمكانية التوجيه الخارجي، حيث تعمد أطراف دولية إلى تسريب معلومات (حقيقية أو مضللة)تهدف إلى تأجيج الرأي العام الداخلي، وتحريض الجماهير ضد الأنظمة القائمة، مما يجعل " السيادة الرقمية " جزءاً لا يتجزأ منها " السيادة الوطنية.

ثالثاً: البعد الاجتماعي

تؤكد البيانات الإحصائية تجاوز عدد مستخدمي الانترنت عتبة 4 مليارات، في حين يتجاوز عدد مستخدمي مواقع التواصل الاجتماعي 6,2 مليار مستخدم، الأمر الذي يجعل هذه المنصات أكبر فضاء للتفاعل البشري وتبادل الأفكار والخبرات، لكن هذا الازدهار الرقمي

[1] فاتح حارك، مرجع سابق، ص53.

سلاح ذو حدين فبقدر ما يقرب المسافات يهدد المنظومة الأخلاقية لصعوبة ضبط المحتوى ويفتح الباب أمام اختراقات الهوية التي قد تمس بأمن الدولة ونسيجها الاجتماعي.

تمثل المدونات ومنصات التواصل الاجتماعي فضاءً واسعًا يمارس من خلاله المواطنون حقهم في التعبير عن آرائهم وتطلعاتهم السياسية والاجتماعية بعيدًا عن القيود التقليدية، كما يفتح هذا الفضاء المجال أمام مختلف فئات المجتمع ومكوناته للمساهمة في إثراء وتطويره، من خلال الاطلاع على الأفكار والمعلومات المتنوعة والانفتاح على مجتمعات أخرى، والتواصل معها، الأمر الذي يفتح أفاقاً واسعة للتعاون والتكامل، غير أن هذه الحيوية الرقمية تفرض في المقابل ضرورة تحقيق توازن بين حرية الانفتاح من جهة، والحفاظ على استقرار الفضاء السيبراني وحماية النسيج المجتمعي من جهة أخرى[1].

إضافةً إلى ذلك، لا يقتصر دور هذه الوسيلة على توفير قدر من الطمأنينة للمواطن في حياته اليومية والاستفادة من إمكانات تقنيات المعلومات والاتصال في تطوير مختلف الأنشطة، بل يمتد أثرها ليشمل تنمية القدرات والإمكانات في المجالات العلمية والثقافية والخدماتية، كما تتجلى أهميتها بشكل أكبر خلال الأزمات الإنسانية والكوارث الطبيعية، حيث تُعدّ أداة فعّالة في إدارة وتبادل المعلومات، بما يساهم في تنسيق الجهود الإغاثية وضمان إيصال المساعدات إلى مستحقيها في الوقت المناسب[2].

رابعاً: البعد الاقتصادي

يرتبط الأمن السيبراني ارتباطًا وثيقًا بالاقتصاد، إذ يظهر هذا الترابط بوضوح في ظل اقتصاد المعرفة القائم على التوسع في استخدام تقنيات المعلومات والاتصالات، ففي هذا الإطار، لم تعد البيانات مجرد أرقام، بل أصبحت أصولًا إستراتيجية ذات قيمة عالية، وتساهم

---

[1] قطاف سليمان، بوقرين عبد الحليم،"**الأمن السيبراني والمضامين المفاهيمية المرتبطة به**"، مجلة طبنا للدراسات العلمية الأكاديمية، مخبر بحث للحقوق والعلوم السياسية، جامعة الأغواط، المجلد5، العدد2، الجزائر، 2022، ص45،ص ص 37-56.

[2] بوازدية جمال، "الأمن السيبراني"، محاضرات مقدمة لطلبة سنة الثانية ماستر، جامعة الجزائر 3، كلية العلوم السياسية والعلاقات الدولية، الجزائر، 2020-2021، ص16.

هذه التقنيات في تعزيز التنمية الوطنية، من خلال استقطاب استثمارات الشركات العالمية التي تسعى لتعظيم كفاءتها التشغيلية وتقليص تكاليف الإنتاج، ضمن بيئة رقمية آمنة ومحفزة[1].

يُضاف إلى ذلك أن العالم يشهد في الوقت الراهن تحولا متسارعا نحو اقتصاد رقمي قائم على المال الإلكتروني والتكنولوجيا الحديثة، في ظل بيئة تقنية تتسم بالتطور المستمر والاعتماد المتزايد على الوسائل الرقمية في مختلف مجالات الحياة. وقد أصبح الفضاء السيبراني يشكل مجالا حيويا تستقطب إليه مختلف قطاعات المجتمع، سواء الاقتصادية أو الاجتماعية أو الإدارية، الأمر الذي جعل من المعرفة والمعلومة موردا استراتيجيا ومحركا أساسيا للإنتاج والتنمية وتحقيق النمو الاقتصادي، حيث أصبحت عصرنة الاقتصاد مرتبطة ارتباطا وثيقا بمدى التحكم في الاقتصاد الرقمي من قبل مختلف الفاعلين الاقتصاديين والاجتماعيين، حيث أضحى الاستخدام الآمن والفعال للتكنولوجيا عاملا حاسما في تحسين الأداء الاقتصادي وتطوير الخدمات وتعزيز مكانة الدول ضمن الاقتصاد العالمي الرقمي. كما أدى هذا التحول إلى بروز تحديات جديدة تتعلق بحماية المعطيات والأنظمة المعلوماتية، مما جعل الأمن السيبراني ضرورة إستراتيجية لضمان استقرار المعاملات الإلكترونية وحماية المصالح الاقتصادية للدول والمؤسسات.[2]

خامساً: البعد العسكري

تطورت شبكة الإنترنت في بداياتها الأولى ضمن سياق عسكري بحت، لتنتقل لاحقاً إلى الأوساط الأكاديمية والقطاعات المدنية المختلفة، وقد برز البعد العسكري للفضاء السيبراني كأداة إستراتيجية فعالة لربط الوحدات العسكرية وتسهيل التدفق المعلوماتي بينها، مما يعزز من سرعة اتخاذ القرار وتحقيق الغايات الميدانية، وفي هذا الإطار، يمثل الأمن السيبراني الركيزة الأساسية لحماية قنوات الاتصال والأوامر العسكرية عن بُعد، حيث يوفر حصانة ضد الاختراقات السيبرانية التي تستهدف تدمير أو تسريب البيانات الحساسة، وهي اختراقات تتجاوز

---

[1] قطاف سليمان، بوقرين عبد الحليم، مرجع سابق، ص84.

[2] أمال بوجليدة ، **الاقتصاد الرقمي التحول من اقتصاد الصناعي إلى اقتصاد المعلومات** ، مجلة الخبير ، العدد 63 ، جانفي 2016 ، ص 45، ص ص 40-47.

البعد التقني لتمس جوهر الأمن القومي، كما تجسد تاريخياً في هجوم فيروس 'ستوكسنت' (Stuxnet) الذي استهدف البنية التحتية للمنشآت النووية الإيرانية.[1]

يتمثل البعد العسكري للأمن السيبراني في الدور الاستراتيجي الذي يؤديه الفضاء السيبراني في تعزيز كفاءة المنظومات الدفاعية والعسكرية، من خلال ربط الوحدات العسكرية وتيسير تبادل المعلومات والبيانات والأوامر بصورة فورية وآمنة، بما يضمن سرعة التنسيق وتحقيق الأهداف العملياتية المرجوة، كما أتاح الأمن السيبراني للقوات المسلحة إمكانيات متطورة في مجال الاتصال عن بعد، وإدارة العمليات العسكرية بكفاءة عالية، مع توفير الحماية للأنظمة المعلوماتية العسكرية ضد مختلف الهجمات والاختراقات الإلكترونية التي تستهدف تعطيل البنى التحتية الدفاعية أو الاستيلاء على المعلومات الحساسة، وتزداد أهمية هذا البعد في ظل تصاعد التهديدات السيبرانية العابرة للحدود، حيث أصبحت الهجمات الإلكترونية تشكل وسيلة حديثة للحروب غير التقليدية، لما تسببه من أضرار قد تمس الأمن القومي والسيادة الوطنية للدول. وقد تجسد ذلك بوضوح في الهجمات السيبرانية التي استهدفت المنشآت النووية الإيرانية، والتي أبرزت مدى خطورة استخدام الفضاء السيبراني كساحة للصراع العسكري والاستراتيجي بين الدول، الأمر الذي دفع العديد من الحكومات إلى تعزيز قدراتها الدفاعية الرقمية وتطوير استراتيجيات متخصصة في مجال الأمن السيبراني العسكري.[2]

الفرع الثاني: مبادئ الأمن السيبراني

بناءً على الرؤى والتوجيهات المستمدة من الخبراء الإقليميين والأطر الدولية المتعلقة بالأمن السيبراني، وضعت جمعية الإنترنت ركائز أساسية لحماية الفضاء الرقمي وضمان سلامة استخدام شبكة الإنترنت، تهدف إلى تعزيز متانة البنية التحتية للشبكة العالمية وزيادة موثيقتها، وذلك من خلال توجيه جهود مختلف مستعمليها نحو تبني ممارسات أمنية فعّالة،

---

[1] فاتح حارك، مرجع سابق، ص54.

[2] جيلالي شويرب، مراد فائزة، "**مفهوم الحروب السيبرانية والأمن السيبراني**"، مجلة الحقوق والحريات ، المجلد 11 ، العدد 01، افريل 2023، ص161، ص ص 156-170.

والحد من المخاطر السيبرانية المتزايدة، بما يضمن استمرارية عمل الشبكات وحماية البيانات والمعلومات المتداولة عبرها، ومن أبرز هذه المبادئ ما يلي[1]:

-الوعي والإدراك: من الضروري أن تعي كافة الأطراف في القطاعين العام والخاص طبيعة التهديدات والمخاطر التي قد تمس أمن أنظمتها المعلوماتية، وتقدير حجم انعكاس هذه المخاطر ليس فقط على منظوماتهم الخاصة، بل على المنظومة الرقمية ككل النظام البيئي المتكامل للإنترنت.

-المسؤولية المشتركة: يقتضي تعزيز الأمن السيبراني أن تتحمل كل جهة معنية مسؤولية التصدي للمخاطر والتهديدات ضمن نطاق صلاحياتها واختصاصاتها، مع مراعاة الآثار والنتائج التي قد تترتب عن اتخاذ القرارات أو إهمال تنفيذ الإجراءات والتدابير الوقائية اللازمة.

-التعاون العابر للحدود: نظرا للطبيعة العالمية للفضاء الرقمي، فإن تحقيق الأمن السيبراني يتطلب معاونًا مستدامًا وتنسيقًا وثيقًا بين جميع الأطراف المعنية، بما في ذلك الجهات الدولية، وذلك من خلال حوار دائم يهدف إلى ضمان التصدي للتهديدات السيبرانية المتطورة والتقليل من آثارها.

إلى جانب مبادئ جمعية الإنترنت، اتفق الخبراء دوليًا في مجال الأمن السيبراني على نموذج معياري لحماية البيانات يعرف ب"مثلث "، الذي يشكل الإطار المرجعي لأمن المعلومات، وهو يتكون من ثلاثة عناصر جوهرية تضمن سلامة التعامل الرقمي:

1-السرية(Confidentiality): تتمثل في ضمان إتاحة الوصول إلى المعلومات للأطراف المصرح لها فقط، ومنع كشفها أو تسريبها لأي جهة غير مخول لها ذلك، بما يكفل ضمان حماية تامة لخصوصية البيانات المتداولة ومنع تسريبها.

2-السلامة أو أمانة البيانات(Integrity): يقصد بها الحفاظ على دقة المعلومات واتساقها، وحمايتها من أي تعديل أو حذف أو تلاعب غير مشروع، بما يضمن للمستخدمين بقاء البيانات مطابقة لأصلها خلال مراحل النقل أو التخزين أو المعالجة.

---

[1] بن عيلة بن جدو، "**تحديات الأمن السيبراني لمواجهة الجريمة الالكترونية**"، المجلة الجزائرية للأمن الإنساني، جامعة بومرداس، المجلد 07، العدد02، الجزائر، 2022،ص301، ص ص 299-319.

3-التوافر (Availability): ويقصد به ضمان ديمومة وصول الأشخاص أوالجهات المصرح لها إلى المعلومات والخدمات الرقمية في الوقت المحدد وعند الحاجة إليها، دون أي عوائق أو انقطاع[1].

نظرًا للتطور النوعي وابتكار أساليب القرصنة الإلكترونية حديثة ومتطورة، وفي ظل تسارع وتيرة التهديدات السيبرانية، لم تعد حماية البيانات خيارًا ثانويًا، بل أصبح من الضروري تبني استراتيجيات أمنية وآليات قانونية وتقنية متكاملة في مجال الأمن السيبراني، تتضمن إجراءات وقائية وتقنية وتنظيمية، وذلك من أجل ضمان حماية الأصول الرقمية ومواجهة مخاطر العصر الرقمي[2].

تنبثق أهمية تبني سياسات الأمن السيبراني حول الحاجة لتقنين الفضاء السيبراني يواكب التحديات التي تواجه المجتمع والمؤسسات والأفراد، بعد أن أصبح الاعتماد بشكل كبير على أنظمة الاتصال والشبكات الإنترنت من مختلف الجهات، حيث أدى الترابط الشبكي الوثيق وصعوبة عزل الأجهزة التقنية إلى خلق ثغرات أمنية تتجاوز الحدود التقليدية[3].

ومع اعتماد المؤسسات الكلي على تدفق المعلومات واتساع نطاق الشبكات، هذا الفضاء الرقمي المفتوح منح المهاجمين قدرة فائقة على تجاوز الحدود المكانية، مما أدى إلى تفاقم المخاطر وصعبت السيطرة عليها وتتبع مرتكبي الجرائم المعلوماتية ومساءلتهم.

إن تصاعد وتيرة التحول الرقمي في القطاعات الحكومية والاقتصادية يفرض تحديات جسيمة تتعلق بتعقب الجرائم الإلكترونية، مما يستوجب توفير بيئة معلوماتية آمنة شرطا أساسيا لاستمرار الأعمال وحماية الخصوصية، وتتجلى أهمية تطبيق استراتيجيات الأمن السيبراني في مكافحة الجرائم المعلوماتية وتأمين الفضاء الرقمي في مجموعة من النقاط سنتطرق لها فيما يلي[4]:

---

[1] بن علية بن جدو، مرجع سابق،ص 315.

[2] الأمن السيبراني: أهمية حماية البيانات في العصر الرقمي الموقع: https://spskills.com/articles/

تم الاطلاع عليه في تاريخ 2026/01/15. على الساعة 20:46.

[3] قطاف سليمان، بوقرين عبد الحليم،"مرجع سابق"، ص 45.

[4] فوائد الأمن السيبراني ومناط أهميته وايجابيات وسلبيات التخصص فيه، الموقع:

تم الاطلاع عليه يوم 2026/01/15 https://bakkah.com/ar/knowledge

1- تأمين الخصوصية الرقمية: يهدف الأمن السيبراني إلى حماية المعلومات الحساسة المخزنة رقميا (مالية، طبية، حكومية) ويعالج مخاطر تسربها، حيث يبني درع واق يمنع الوصول الغير مشروع لهذه البيانات، بما يضمن خصوصية الأفراد وأمن المؤسسات.

2- تعزيز استدامة الأعمال: تمثل الأنظمة الرقمية الركيزة الأساسية لتسيير مختلف أنشطتها وإدارة عملياتها اليومية، مما يجعل الهجمات السيبرانية تهديدا مباشرا لاستقرارها، لما قد تسببه من تعطيل للخدمات أو فقدان للبيانات أو خسائر مالية فادحة، يعمل الأمن السيبراني كعصام أمان في تحصين هذه الأنظمة ضد المخاطر الرقمية، بما يضمن استمرارية الأداء وانتظام سير العمل بكفاءة واستقرار.

3- حماية البنية التحتية الحسابية: مع التوجه المتسارع للشركات نحو الاعتماد الواسع على البيئات الحسابية (cloud)، سواء لإدارة الأعمال أو لحفظ بيانات العملاء أو دعم منظومة العمل عن بعد وغيرها من الأغراض، استوجب بناء شبكة أمنية فعّالة، لتأمين الأصول الرقمية ونجاح إستراتيجية العمل الحديثة، وصون التطبيقات الحيوية المستضافة في السحابة لضمان مرونة الأعمال وسلامة بياناتها من مختلف التهديدات والمخاطر السيبرانية.

4- انعكاسات الجرائم الإلكترونية وجدوى الحماية: برزت الأهمية الإستراتيجية للأمن السيبراني كاستجابة للخسائر المادية الجسيمة التي عانت منها المؤسسات جراء الهجمات الرقمية، ولم تقتصر هذه الأضرار على الخسائر المباشرة فقط، بل امتدت لتشمل تبعات بعيدة المدى مثل ضياع الملكية الفكرية وتطيل العمليات التشغيلية، مما يضع المؤسسات تحت طائلة المسؤولية القانونية ويعرض مكانتها في السوق للخطر.[1]

إذا أصبح تأمين الفضاء السيبراني ضرورة حتمية لحماية الأنظمة المعلوماتية والبيانات الرقمية من مختلف المخاطر والتهديدات الإلكترونية، كما أن تعدد أبعاد الأمن السيبراني وارتباطه بالجوانب الاقتصادية والأمنية والعسكرية والاجتماعية يعكس اتساع نطاقه وتأثيره المباشر في استقرار الدول والمؤسسات ، و يرتكز الأمن السيبراني على جملة من المبادئ الأساسية التي تهدف إلى حماية المعلومات وضمان سلامتها والحفاظ على استمرارية إتاحتها، بما يسهم في تعزيز الثقة في استخدام الوسائط والتقنيات الرقمية.

[1] بن علية بن جدو، مرجع سابق، ص 305.

المبحث الثاني

ماهية الجريمة الإلكترونية

أدى التطور المتسارع في تقنيات الحاسب والأنظمة المعلوماتية وشبكات الاتصال المعاصرة، على رأسها شبكة الإنترنت، ركيزة أساسية لنهضة شملت كافة القطاعات الحيوية، إلا أنه أفرز إلى تحقيق العديد من الفوائد والمزايا التي انعكست إيجابًا على مختلف مجالات الحياة الاقتصادية والاجتماعية والعلمية.

أصبحت الأنظمة المعلوماتية عرضة لاعتداءات وهجمات إلكترونية مختلفة، مما أفرز إلى ظهور نوع جديد من الأفعال الإجرامية التي ترتكب باستخدام الوسائط الرقمية، والتي تعرف بالجرائم الإلكترونية أو ما تسمى أيضا بالجرائم السيبرانية، وتكمن خطورة هذه الجرائم في طبيعتها التقنية الفريدة، وتتميز بخصائص خاصة تجعل اكتشافها وإثباتها ومكافحتها أكثر صعوبة مقارنة بالجرائم التقليدية.

يُعّد تناول موضوع الجريمة الإلكترونية، كغيره من الموضوعات في مختلف فروع المعرفة، أمرًا يقتضي تحديد مفهومه وإبراز ملامحه الأساسية، وعليه سنقسم هذا المبحث إلى مطلبين: سنتطرق في **(المطلب الأول)** إلى مفهوم الجريمة الالكترونية، أما بالنسبة **(المطلب الثاني)** خصصناه الى أركان الجريمة الإلكترونية وعلاقتها بالأمن السيبراني.

المطلب الأول

مفهوم الجريمة الإلكترونية

تصنف الجرائم الإلكترونية كنمط إجرامي مستحدث يوجه سهامه نحو الأصول الرقمية، من بيانات ومعلومات وبرمجيات متنوعة، سواء من حيث الاحتراق أو التلاعب أو الإتلاف، وغالبًا ما ترتكب هذه الجرائم من قبل أشخاص يمتلكون معارف ومهارات متقدمة في مجال الحاسوب والأنظمة المعلوماتية تمكّنهم من استغلال الثغرات التقنية لتنفيذ أفعالهم غير المشروعة.

تتميز هذه الجرائم بطابعها المعقد وصعوبة اكتشافها أو تعقب مرتكبيها، نظرا لاعتمادها على الوسائط الرقمية والشبكات الإلكترونية، الأمر الذي يفرض ضرورة تطوير وسائل الحماية والتشريعات القانونية لمواجهتها والحد من آثارها السلبية، وبناءً على ذلك سنتطرق في هذا المطلب إلى تعريف الجريمة الإلكترونية في **(الفرع الأول)**، أما بالنسبة إلى**(الفرع الثاني)** سنتناول أنواع الجريمة الإلكترونية والأسباب التي أدت إلى انتشارها.

الفرع الأول: تعريف الجريمة الإلكترونية

تُصنف الجرائم الإلكترونية كأنشطة غير مشروعة تعتمد بشكل أساسي على الحاسب الآلي وشبكة الإنترنت لتنفيذ مخططات إجرامية، وغالبًا ما يكون الهدف من هذه الجرائم تحقيق مكاسب مالية كبيرة، ثم يتم دمج هذه العائدات ضمن الاقتصاد العالمي عبر العملات الرقمية، مثل بطاقات الائتمان وتداول الأسهم الإلكترونية، كمّا يرى خبراء المنظمة الأوروبية للتعاون الاقتصادي الجريمة المعلوماتية بأنها كل سلوك غير مشروع أو غير مصرح به، يتعلق بمعالجة البيانات أو تداولها تقنيًا[1].

أولاً: التعريف الفقهي

يلاحظ غياب اصطلاح موحد يصف هذه الظاهرة الرقمية المستجدة، إذ يطلق عليها البعض تسميات مختلفة مثل الغش المعلوماتي، الاختلاس المعلوماتي، أو الجريمة المعلوماتية، الجريمة السيبرانية، وأمام هذا التباين الاصطلاحي، اتجه الفقه إلى تصنيف تعريف الجريمة الإلكترونية ضمن نطاقين: المفهوم الواسع والمفهوم الضيق[2].

1-التعريف الواسع

سعى بعض الباحثين إلى توسيع نطاق مفهوم الجريمة الإلكترونية، حيث عرفت بأنها كل سلوك إيجابي أو سلبي يرتكب عمدًا عبر الاستغلال غير القانوني للتقنية، مستهدفًا المساس بالحقوق المالية أو المعنوية، كما قدّم الخبير الأمريكي بركار تصورًا واسعًا لهذا النوع من

---

[1]صغير يوسف،" **الجريمة المرتكبة عبر الإنترنت**"، مذكرة لنيل شهادة الماجستير في القانون، تخصص القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2013، ص9.

[2]بولحية شهرزاد، "**تحديات الجريمة الإلكترونية في الجزائر**"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة الجزائر 1، المجلد 04، العدد02، الجزائر، 2019، ص 1985، ص ص1974-2003.

الجرائم أي نشاط إجرامي متعمد يرتبط بالتقنية وينتج عنه إلحاق ضرر بالمجني عليه أو تحقيق ربح غير مشروع للجاني[1].

يعرف الأستاذ فيفون الجريمة الإلكترونية أنها:" مجموعة من الأفعال المرتبطة بالمعلوماتية التي يمكن أن تكون جديرة بالعقاب".

2-التعريف الضيق

تعرف الجريمة الإلكترونية بأنها كل نشاط مخالفًا للقواعد القانونية يتطلب اقترافه، أو كشف ملابساته وتتعبه، توافر قدر عالٍ من الخبرة المتخصصة في تكنولوجيا الحاسبات الآلية

وعرفها الفقيه تايديمان Tiedemann فعرفها بأنها: "كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب باستخدام الحاسب"، أو هي:" كل جريمة تتم في محيط الحسابات الآلية[2].

عرفها كذلك الفقيه دافيد تومصون David thompson الذي عرف هذا النوع من الجرائم بقوله أنها:" أية جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب"[3].

ويرى مازا"Massa" أن المقصود بها:" الاعتداءات غير القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق الربح"، ولا تقتصر الجرائم الإلكترونية في الغالب على السعي وراء المكاسب المادية، بل يتطلب ارتكابه إلمامًا كبيرًا بتكنولوجيا الحاسوب، كما يستلزم هذا قدرًا من المعرفة التقنية أيضًا عند متابعته وكشفه والتحقيق فيه.[4]

وتعرف الجريمة الإلكترونية على أساس الاتفاقية العربية وقانون الجرائم الأمريكية واتفاقية بودابست والاتحاد الدولي للاتصالات بأنها كل سلوك إجرامي سواء كان جنحة أو جناية

---

[1]بولحية شهرزاد، مرجع سابق، ص 1981.

[2]بوحمزة نصيرة،" **التحقيق الجنائي في الجرائم الإلكترونية (دراسة مقارنة)**"، رسالة مقدمة لنيل الدكتوراه في العلوم القانونية' تخصص قانون خاص، كلية والعلوم السياسية، جامعة الجيلالي اليابس، سيدي بلعباس، الجزائر، 2022، ص15.

[3]Thompson(David), **current trends in computer control crime**, computer quarterly, vol 9 N1, 1991, P2.

[4] إيمان فاضل السمرائي، هيثم محمد الزغبي،" **نظم المعلومات الإدارية**"، ط الأولى، دار الصفاء للنشر والتوزيع، عمان، 2005، ص259.

يستهدف الأفراد أو الجماعات بقصد الإضرار بسمعتهم، أو سلامتهم الجسدية، أو كيانهم الفكري والمادي، ويتم هذا الاعتداء عبر وسائط الاتصال الحديثة وشبكة الإنترنت، سواء اتخذ شكلاً مباشرًا أو غير مباشر، ويأتي ذلك في ظل التوسع المتزايد في الانفتاح العالمي، حيث تحولت المجتمعات من أنماطها التقليدية إلى نظم اجتماعية رقمية أكثر تشابكًا وتسارعًا وانصهارًا مع العالم التقليدي[1].

ثانيًا: التعريف القانوني

حدد المشرع الجزائري مفهوم الجريمة الإلكترونية في المادة 2 من القانون 09-04[2]، بأنها:" جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جرائم أخرى ترتكب أو يسهل ارتكابها عبر المنظومة المعلوماتية أو نظام الاتصالات الإلكتروني"، ويبدو أن المشرع قد وفق في هذا التعريف، كونه اعتمد معيارًا شاملاً يدمج بين الحالات التي يكون فيها النظام المعلوماتي محلاً للاعتداء، والحالات التي تستعمل فيها كوسيلة وأداة لارتكاب جرائم تقليدية، مما يمنح هذه الجرائم صبغتها المعلوماتية الفارقة[3].

يعد المشرع الجزائري النظام المعلوماتي ومحتوياته المعنوية محلاً للحماية القانونية، لأنه يعتبر النظام المعلوماتي ومكوناته الغير مادية بحد ذاته محلاً للجريمة، ويُعد وجود "نظام معالجة آلية" شرطًا مفترضًا وأساسيًا سابقًا للتحقيق في الجريمة قبل البحث في مدى توافر أركان جرائم الاعتداء على هذا النظام، فإذا انتفى هذا الوصف، سقطت التهمة لعدم تحقق شرطها الأساسي[4].

استجابةً للتحولات التي فرضتها الثورة المعلوماتية، وتصديًا لأنماط إجرامية مستحدثة لم يعهدها النظام القانوني التقليدي، جرّم المشرع الجزائري الأفعال التي تمسّ بأنظمة الحاسب

---

[1] فريد ناشف،" **آليات التعاون الدولي في مكافحة الجرائم الإلكترونية**"، مجلة البحوث في الحقوق والعلوم السياسية، جامعة البليدة2، المجلد08، العدد 01، 2022، ص ص 430-450.

[2] قانون رقم 09-04 مؤرّخ في 14 شعبان عام 1430 الموافق ل 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر ، العدد 47، الصادرة في 16 غشت 2009.

[3] بوضياف اسمهان،" **الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر**"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف، العدد 11، المسيلة، الجزائر، 2018،ص354، ص ص 348-375.

[4] بولحية شهرزاد، مرجع سابق، ص 1987.

الآلي، وقد تجسد ذلك من خلال تعديل قانون العقوبات بموجب القانون رقم 04-15[1]، حيث خصص القسم السابع مكرر بعنوان "المساس بأنظمة المعالجة الآلية للمعطيات"، وضمّ ثماني مواد من المادة 394 مكرر إلى المادة 394 مكرر 7.

ويلاحظ من خلال تعريف المشرع الجزائري للجريمة الإلكترونية ما يلي:

1-اعتمد المشرع الجزائري منهجًا تكامليًا في تعريف الجريمة الإلكترونية، على الجمع بين ثلاث معايير جوهرية: يتمثل أولها في المعيار الأداتي (وسيلة الجريمة) المتمثل في أنظمة الاتصالات الإلكترونية، أما بالنسبة للمعيار الثاني فهو المعيار الموضوعي (محل الجريمة)الذي يستهدف أنظمة المعالجة الآلية للمعطيات، وصولاً إلى المعيار القانوني (الركن الشرعي) بالاستناد إلى النصوص القانونية الواردة في قانون العقوبات.

2- عمل المشرع الجزائري على توسيع النطاق الإجرائي للجريمة المعلوماتية، إذ لم يكتفي بتجريم الاعتداء المباشر على المنظومات المعلوماتية، بل وسّع نطاقها ليشمل الجرائم التي يسهل ارتكابها عبر الأنظمة المعلوماتية، مما يجعل السياسة الجنائية الجزائرية أكثر شمولية في مواجهة الإجرام التقني[2].

ثالثًا: التعريف الأكاديمي

يقصد بالجريمة الإلكترونية كل فعل إجرامي عمدي يرتبط بالتقنية الرقمية، يترتب عليه مكاسب غير قانونية يجنيها الفاعل أو إلحاق أضرار بالمجني عليه، وبشكل موسع، يمكن تصنيفها وفقًا لدور التكنولوجيا في الجريمة إلى فئتين:

أ-الاعتداء المادي: يستهدف البنية التحتية والمكونات الصلبة للمنظومات التقنية.

ب-الاعتداء الوسائلي: حينما يتم توظيف الأنظمة أو الأجهزة المعلوماتية كقناة لتنفيذ المخطط الإجرامي.[3]

---

[1] قانون رقم 04-15،سالف الذكر.

[2] بوضياف اسمهان، مرجع سابق، ص 350.

[3]بولحية شهرزاد، مرجع سابق، ص 1989.

رابعًا: الطبيعة القانونية للجريمة الإلكترونية

تنفرد الجريمة الإلكترونية بطبيعة خاصة تميّزها عن غيرها من الجرائم التقليدية، حيث تكتسب ذاتيتها من الطبيعة التقنية للوسيلة المستخدمة، والمتمثلة في الشبكة العالمية للإنترنت وما توفره من بيئة رقمية واسعة للتواصل وتبادل المعلومات[1].

تتمحور الإشكالية القانونية للجريمة الإلكترونية حول التكييف الفقهي للبرمجيات والمعطيات الرقمية، فالبحث في طبيعتها القانونية أفرز انقسامًا فقهيًا جليًا، في اتجاهين رئيسيين:

1-الطبيعة الخاصة للمعلومات:

يستند هذا الاتجاه إلى المفاهيم التقليدية للملكية والحيازة، مؤكدًا أن المادية هي مناط الحماية في جريمة السرقة، وبما أن المعلومات والبرمجيات ذات طبيعة معنوية أي غير مادية، فإنها تخرج عن نطاق "الأموال" القابلة للحيازة أو الاستحواذ، إلا في إطار ما تقرره قواعد حماية الملكية الفكرية، وعليه، فإن الاعتداء على المعلومات لا يكيف كسرقة إلا إذا نصبّ الفعل على الوعاء المادي الذي يحويها كالأقراص أو الأشرطة ونحوها.[2]

2- المعلومات مجموعة مستحدثة من القيم:

يتبنى هذا الاتجاه رؤية مستحدثة تعتبر المعلومات قيمًا اقتصادية مستقلة وقابلة للاستحواذ بمعزل عن وسيطها المادي، إذ تمتلك المعلومات قيمة اقتصادية يمكن الحصول عليها بطريقة غير مشروعة، وينطلق أنصار هذا المذهب، وفي مقدمتهم الأستاذان كتالا وفيفون إلى أن العلاقة بين الشخص والمعلومات تعتبر تشبه العلاقة القانونية بين المالك وشيئه، وبناءًا عليه، تصنف المعلومات " كأموال معنوية" تستمد قابليتها للتملك والاستغلال من قيمتها الجوهرية لا من كيانها الفيزيائي، فهي تستحق حماية قانونية ويجب معاملتها بالمثل مع الأموال الأخرى.

تمتد مظاهر الجرائم الإلكترونية أيضا في نطاق معالجة النصوص والبيانات الرقمية، وتكمن صعوبتها في التكييف القانوني نظرًا لطبيعتها الافتراضية، وتكمن المعضلة في عدم قدرة

---

[1] يوسف صغير، مرجع سابق، ص06.

[2] عبد الله دغش العجمي، **"المشكلات العلمية والقانونية للجرائم الإلكترونية (دراسة مقارنة)"**، مذكرة لنيل شهادة الماجستير في القانون العام، جامعة الشرق الأوسط، الأردن، 2014، ص 14.

القواعد الجزائية التقليدية عن استيعاب هذه الظواهر المستحدثة، التي تنعكس سلبًا في صعوبة توثيق الأدلة الرقمية وتحديد الهوية الحقيقية لمرتكبي هذه الجرائم، مما قد يفضي إلى فلاتهم من العقاب.[1]

الفرع الثاني: خصائص ودوافع الجريمة الإلكترونية

تختلف الجريمة الإلكترونية جوهرياً عن الجريمة التقليدية، إذ إنها لا تعترف بالحدود الجغرافية ولا تتطلب مواجهة مادية بين الجاني والضحية، وللإحاطة بهذه الظاهرة المعاصرة والحد من آثارها المدمرة، يصبح من الضروري تفكيك بنيتها من خلال دراسة شقين رئيسيين: خصائصها البنيوية التي تمنحها طابعاً فريداً من حيث السرعة والسرية والامتداد، والدوافع الكامنة وراء ارتكابها.

أولا: خصائص الجريمة الإلكترونية

تتميز الجريمة الإلكترونية بعدة خصائص نذكر منها:

1-جرائم عابرة للحدود:

تتسم البيئة الافتراضية بكونها عابرة للحدود والقيود الجغرافية، حيث يتيح "الفضاء السيبراني" للجاني إرتكاب جريمته من دولة بينما يقع أثرها على ضحايا في دولة أخرى، وقد يمتد الضرر لدول متعددة في آن واحد، وتستفيد هذه الجرائم من خصائص التقنية كاختزال المسافات، وإخفاء الأثر الرقمي، و" اللحظية المعلوماتية " التي تمنح المجرمين سرعة فائقة في التنفيذ عن بُعد دون حاجة للتواجد المادي، ويؤدي هذا الطابع العابر للحدود إلى صعوبة تعقب المجرمين وإثبات العلاقة بين الفعل والنتيجة الإجرامية، الأمر الذي يستلزم تعزيز التعاون الدولي، وتنسيق الجهود التشريعية والأمنية، وتفعيل آليات الملاحقة القضائية وتسليم المجرمين إضافة إلى تجميد العوائد المالية المتحصلة من الجرائم المرتبطة بالأنظمة المعلوماتية[2].

---

[1] عبد الله دغش العجمي، مرجع سابق، ص 15.

[2] مقلاتي مونى، راضيا مشري، "**الجريمة الإلكترونية: دلالة المفهوم وفعالية المعالجة القانونية**"، مجلة الأبحاث القانونية السياسية، جامعة 8ماي 1945، قالمة، المجلد 6، العدد1، 2021،ص497، ص ص491-510.

2-جريمة صعبة الاكتشاف والإثبات:

تتسم الجرائم المعلوماتية بقدر كبير من التعقيد، لاسيما من حيث صعوبة اكتشافها وإثباتها، ويرجع ذلك أساساً إلى طبيعتها غير المادية وعدم ترك مرتكبيها لآثار تقليدية تدل على وقوعها، فغالباً ما تُرتكب هذه الجرائم عبر إدخال أو معالجة رموز وأرقام ضمن أنظمة رقمية دقيقة، الأمر الذي يجعل اكتشافها وإثباتها مسألة معقدة، بحيث لا يتم الكشف عنها في كثير من الأحيان إلا بمحض الصدفة، كما قد يفلت مرتكبوها من المساءلة لغياب أدلة قاطعة تثبت تورطهم، وعلاوة على ذلك، فإن الإجرام المعلوماتي لا يترك وراءه شواهد ملموسة يمكن فحصها أو شهوداً يمكن الاستماع لإفاداتهم.

نظراً لكون الجريمة تدور رحاها في بيئة رقمية تعتمد على تبادل الإشارات والنبضات الإلكترونية، هذا الواقع يفرض تحدياً إضافياً يتمثل في الطبيعة التقنية المعقدة لوسائل التنفيذ، والتي تستوجب توافر خبرات فنية عالية التخصص لفهم أنماط السلوك الإجرامي وتتبع البصمات الرقمية المترتبة عليه، مما يضع المحقق التقليدي غير المتمرس في تكنولوجيا المعلومات أمام عقبات فنية جمة، كما يبرز عائق آخر يتمثل في ندرة العثور على دليل مادي قطعي، إذ يمتلك الجناة أدوات تقنية متقدمة تتيح لهم تنفيذ عملياتهم الإجرامية في أزمنة قياسية لا تتعدى ثوانٍ معدودة، يعقبها مباشرة محو كامل للآثار الرقمية أو تحريفها بمهارة عالية، مما يؤدي إلى طمس معالم الجريمة وإعاقة جهود التحقيق في الوصول إلى الحقيقة[1].

3-ضعف التبليغ وسرعة محو الأدلة في جرائم الإلكترونية:

غالبًا ما تبقى العديد من الجرائم الإلكترونية دون تبليغ، ويرجع ذلك إما إلى عدم اكتشافها من قبل الضحية، أو إلى تخوفه من الآثار السلبية التي قد تنجم عن الإبلاغ عنها، كتشويه السمعة أو التعرض للتشهير، ولهذا السبب لا يتم كشف عدد كبير من هذه الجرائم إلا عرضًا من قبل الجهات الأمنية، وقد يحدث ذلك بعد مرور فترة زمنية طويلة على ارتكابها، ومن ناحية أخرى.

تساهم طبيعة البيانات والمعلومات المتداولة رقمياً في تعقيد مسار التحقيق، إذ يتم تخزينها في هيئة رموز رقمية معقدة على وسائط تخزين مغناطيسية، مما يجعل استخراج الأدلة الرقمية

[1] بولحية شهرزاد، مرجع سابق، ص 1981.

وفهم كنهها تحدياً تقنياً كبيراً، وينتج عن هذا الوضع صعوبة بالغة في تتبع تلك الأدلة للوصول إلى هوية الجاني، لا سيما مع سهولة محو البيانات أو تحريفها على الأنظمة المعلوماتية، وهو ما يُمكّن الجناة من إخفاء الآثار الرقمية التي قد تشكل خيطاً لكشف الجريمة أو دليلاً لإدانة مرتكبها.[1]

4-الجريمة الأقل عنفاً في التنفيذ تُعد الجرائم المعلوماتية من الجرائم التي توصف بـ"الجرائم الهادئة"، نظراً لكونها تُرتكب بعيداً عن مظاهر العنف الجسدي أو الإيذاء المادي التي تميز الجرائم التقليدية كالقتل والسرقة، إذ لا يتطلب ارتكابها في الغالب سوى قيام الجاني ببضع نقرات سريعة على لوحة المفاتيح، تمكنه من التسلل إلى البيانات المخزنة داخل الأنظمة المعلوماتية، بما يتيح له انتهاك سريتها أو حذفها أو تعديلها، بل وقد يصل الأمر إلى تعطيل الأنظمة الحيوية التي تحتضن تلك المعلومات بشكل كلي.

5-نقص الخبرة لدى الأجهزة الأمنية والقضائية وعدم كفاية القوانين: تتسم جرائم الإنترنت بجملة من الخصائص التي تميزها عن سائر الجرائم التقليدية، مما أحدث تغييراً جذرياً في مناهج التحقيق الجنائي ووسائل استخلاص الأدلة، كما فرضت هذه الجرائم أعباء إضافية تتعلق بكيفية كشفها وتتبع أدلتها، مما دفع المشرع والجهات القضائية إلى مراجعة المفاهيم التقليدية للإثبات، وتطوير معايير جديدة تتناسب مع طبيعة الدليل الإلكتروني وقيمته القانونية.[2]

بما أن ارتكاب هذه الجرائم يرتكز على مهارات وتقنيات متقدمة، فإن كشفها يتطلب كفاءة تقنية موازية وأساليب تحقيق استثنائية، غير أن هذا الأمر لم يتحقق بالقدر الكافي لدى الأجهزة الأمنية والقضائية، فإن الضرورة تقتضي تعزيز القدرات التخصصية وتحديث مناهج الاستقصاء لمواكبة هذا تطور الإجرامي.[3]

---

[1] أحلام شناق،" **واقع الجريمة الإلكترونية في مجتمع المدينة الجزائرية (مدينة بسكرة نموذجا)**، أطروحة مكملة لنيل درجة الدكتوراه، الطور الثالث في علم الاجتماع، تخصص علم الاجنماع الحضري، كلية العلوم الإنسانية والاجتماعية، جامعة محمد خيضر، بسكرة، الجزائر، 2025/2024، ص103.

[2] عبد الرحمان جميل، محمود حسين،" **الحماية القانونية لبرامج الحاسب الآلي (دراسة مقارنة)**"، رسالة مقدمة استكمالاً لمتطلبات درجة الماجيستر في القانون الخاص، كلية الدراسات العليا، جامعة النجاح الوطنية، فلسطين، 2008، ص58.

[3] يوسف صغير، مرجع سابق، ص20.

ثانيا: دوافع إرتكاب الجريمة الإلكترونية:

تتسم الجريمة الرقمية بطبيعة مركبة تتداخل فيها الدوافع المتباينة والأهداف المتغيرة للجناة، وتتشكل أنماطها تِباعاً لتطور التقنيات والوسائل السيبرانية المتاحة، فضلاً عن تأثرها بالبيئة النفسية والاجتماعية والثقافية والتقنية التي ينشأ فيها الجاني، ومن أبرز هذه الدوافع:

1-الدوافع الشخصية:

يقصد بها تلك العوامل المرتبطة بشخصية المجرم الالكتروني، والتي تدفعه إلى ارتكاب الجريمة الإلكترونية ويمكن إرجاع هذه الدوافع إلى:

أ- الدافع المادي: يُمثل السعي نحو الثراء السريع المحرك الأساسي للجريمة المعلوماتية، نظرًا للعوائد المادية الضخمة التي تدرّها هذه الأنشطة مقارنة بمخاطرها التقليدية، وتتنوع المحفزات الشخصية لهذا السلوك بين الحاجة لسداد الالتزامات المالية المتراكمة، أو الرغبة في تمويل أنشطة غير قانونية كالمراهنات والمخدرات، وفي مثل هذه الحالات، يلجأ الجاني إلى محاولة تجاوز أزمته المالية من خلال التلاعب بالأنظمة المعلوماتية للبنوك والمؤسسات المالية، وذلك عبر اختراقها واستغلال الثغرات الأمنية الموجودة فيها.[1]

ولا يقتصر الدافع إلى تحقيق المكسب المادي على الأفراد ذوي الكفاءة الفنية العالية والمهارات المتقدمة في مجال التكنولوجيا، بل قد يكون هدفاً أيضاً لدى أشخاص محدودي المعرفة التقنية أو حتى غير المؤهلين في المجال المعلوماتي، وبناءً على ذلك يتباين أسلوب ارتكاب الجريمة تبعاً لمستوى المعرفة، فبينما يعتمد المتخصصون على الاختراق، يلجأ غير المتخصصين إلى أساليب إجرامية ترتبط بالحاسب الآلي دون الولوج المباشر إلى أنظمته المعقدة، مما يجعل نشاطهم الإجرامي محدوداً في نطاقات معينة لا تتطلب مهارات فنية عميقة.[2]

ب- الدافع الذهني: تشكل الدوافع الذهنية والسمات النفسية اللصيقة بالمجرم المعلوماتي أحد المحركات الجوهرية لارتكاب الجريمة، إذ يسعى الجاني من خلالها إلى إثبات الذات وتحقيق

---

[1] غازي عبد الرحمان، هيان رشيد، **" الحماية القانونية من الجرائم المعلوماتية (الحاسب والإنترنت)"**، أطروحة لنيل شهادة الدكتوراه في القانون، كلية الحقوق، الجامعة الإسلامية، لبنان، 2004، ص157-158.

[2] بوحزمة نصيرة، مرجع سابق، ص81.

انتصار معنوي على الأنظمة التقنية المعقدة، كما قد يكون هدفه تحقيق نوع من التفوق على تعقيد الوسائل التقنية أو قهر النظام المعلوماتي، دون أن تكون لديه بالضرورة نية إجرامية مادية مباشرة.

في الوقت الذي يتزايد فيه الاهتمام بأمن الحاسوب وشبكاته من خلال تطوير وسائل متقدمة ومعقدة للحماية، كبرمجيات التشفير التي لا يستطيع فهمها إلا الجهة المستقبِلة لها، تتخذ المؤسسات الكبرى إجراءات أمنية صارمة لحماية بياناتها، وخير مثال ذلك ما تتبعه وزارة الدفاع الأمريكية من بروتوكولات أمنية صارمة تعتمد تغيير أنظمة ترميز البيانات الحساسة بصفة دورية (يومية)، مما يعكس ذروة التطور التقني، ومع ذلك، يظل " تحدي الأنظمة " محركا للهواة والمحترفين، الذين يسعون إلى اختراق هذه الأنظمة المعقدة لإثبات قدرتهم التقنية والتفوق عليها، وقد شهد الواقع حالات تمكن فيها بعضهم من فك شفرات أنظمة معلوماتية حساسة والتلاعب ببياناتها[1].

2-الدوافع الخارجية:

يقصد بذلك أن الإنسان قد يتأثر ويستسلم للمؤثرات والدوافع الخارجية التي تدفعه الارتكاب بعض الجرائم الإلكترونية، نتيجة تواجده في بيئة المعالجة الآلية للمعلومات، وتتحدد بعدة دوافع:

أ- الدافع السياسي: عقب الثورة الكبرى التي شهدها مجال الاتصالات والمعلومات والتطور المتسارع في التكنولوجيا، أصبح الاعتماد على الحاسوب اعتماداً شبه كلي في مختلف مجالات الحياة، لاسيما في المجالين السياسي والعسكري، هذا الاعتماد العميق حوّل الأنظمة المعلوماتية إلى هدف استراتيجي للمجرمين السيبرانيين الساعين لاختراق البيانات الحساسة، وتتنوع غاياتهم بين جني مكاسب مادية باهظة، أو ممارسة ضغوط سياسية تهدف إلى تقويض استقرار الدول وزعزعة أمنها القومي.

يتخذ بعض الجناة من الفضاء السيبراني منصةً لتجسيد مواقفهم السياسية وتنفيذ أجندات أيديولوجية، وهو ما يفرز نمطاً من أخطر الجرائم الرقمية، خاصة عند تقاطعه مع الإرهاب الإلكتروني، الذي شهد انتشاراً ملحوظاً في بعض مناطق العالم، ومنها منطقة الشرق الأوسط،

[1] محمود أحمد عبّانة، "**جرائم الحاسوب وأبعادها الدولية**"، دار الثقافة للنشر والتوزيع، د ط، الأردن، 2005، ص98.

إذ تستغل الجماعات المتطرفة الشبكات الرقمية في تحقيق عدة أهداف، مثل نشر الدعاية، وجمع التبرعات، والتحريض على العنف، أو ممارسة الحرب النفسية، فضلاً عن استهداف المواقع الحكومية أو المؤسسات الأمنية في إطار هذه الهجمات.[1]

ب– دافع الإنتقام: يبرز دافع الانتقام كأحد المحركات الأكثر خطورة في بيئة الجرائم المعلوماتية، وتتضاعف حدته عندما يصدر عمّن يمتلكون صلاحيات الوصول إلى البيانات الحساسة داخل المنظومة، وغالباً ما تتشكل هذه النزعة الانتقامية لدى الموظفين نتيجة قرارات إدارية يراها الجاني مجحفة، مثل الفصل من الخدمة أو الحرمان من الترقيات والمزايا الوظيفية، مما يدفع الموظف (الحالي أو السابق) لتوظيف خبرته التقنية في تقويض مصالح المؤسسة وتخريب أنظمتها رداً على ذلك.[2]

تشير التقديرات إلى أن جزءًا كبيرًا من الجرائم الإلكترونية يرتكبها موظفو الجهة نفسها، ففي الولايات المتحدة، حُكم على موظف في إحدى شركات التأمين بالسجن سبع سنوات وغرامة قدرها 150 ألف دولار، بعد أن أدخل فيروسًا في أنظمة الشركة مما أدى إلى فقدان 160 سجلًا من سجلات العملاء، انتقامًا من الشركة بعد فصله.

يبرز هذا المثال خطورة الجرائم الإلكترونية الداخلية، إذ يمكن للموظف المطلع على أنظمة المؤسسة استغلال معرفته التقنية للوصول إلى بيانات حساسة وإلحاق أضرار جسيمة، مما يستدعي من الشركات تعزيز الأمن الداخلي وفرض ضوابط صارمة لحماية معلوماتها وأنظمتها.

تنفرد الجريمة الإلكترونية بطبيعة ديناميكية غير تقليدية ، حيث تشكل الوسائل الرقمية و البيئات الافتراضية مسرحاً لعملياتها و أداة رئيسية لتنفيذها ، كما أنّ تعدد تعريفاتها يرجع إلى تنوع صورها وأساليب ارتكابها، وتتميز هذه الجريمة بعدة خصائص أهمها السرعة، وصعوبة اكتشاف مرتكبيها، والطابع العابر للحدود، إضافة إلى اعتمادها على المهارات التقنية الحديثة،

---

[1] أحمد محمد الدوسري،" **أنواع الجرائم الإلكترونية وتحديات مكافحتها**"، مجلة منار للدراسات والبحوث القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة يحي فارس، المدية، المجلد 9، العدد01، الجزائر، 2025، ص98.

[2] يوسف صغير، مرجع سابق، ص42.

كما تتعدد دوافع ارتكابها بين دوافع مادية بهدف تحقيق الربح غير المشروع، ودوافع معنوية أو سياسية أو انتقامية، وهو ما ساهم في تزايد خطورتها وتعقيد مكافحتها.

المطلب الثاني

أركان الجريمة الإلكترونية وعلاقتها بالأمن السيبراني

يمثل البنيان القانوني للجريمة الإلكترونية حجر الزاوية في المنظومة الحمائية للفضاء الرقمي؛ فمع تسارع التحول الرقمي، لم تعد الجريمة مجرد اعتداء مادي تقليدي، بل تحولت إلى سلوكيات تقنية معقدة تستهدف تقويض الأمن السيبراني للدول والأفراد، إن الركائز الثلاث للأمن السيبراني (الموثوقية، السلامة، وتوافر البيانات) هي ذاتها المصالح القانونية التي تسعى أركان الجريمة الإلكترونية لتحديد نطاق الاعتداء عليها.

فلا يمكن الحديث عن إستراتيجية وطنية للأمن السيبراني دون ضبط دقيق للركن الشرعي الذي يحدد الأفعال المُجرمة مستحدثة كانت أم تقليدية، والركن المادي الذي يجسد السلوكيات الإجرامية من اختراق وتشفير وتعطيل للنظم، وصولاً إلى الركن المعنوي الذي يستلزم إثبات القصد الجنائي في بيئة تتسم بصعوبة تتبع الأثر وتحديد هوية الجاني.

كما أن فهم هذه الأركان لا ينفصل عن مفهوم الأمن السيبراني، الذي يهدف إلى حماية الأنظمة المعلوماتية والبيانات من مختلف التهديدات والاعتداءات الإلكترونية، لذلك فإن تحليل أركان الجريمة الإلكترونية يساهم في توضيح طبيعة هذه الجرائم وبيان مدى ارتباطها بتعزيز الأمن السيبراني وضمان حماية الفضاء الرقمي من المخاطر والاعتداءات المختلفة.

نتطرق في مطلبنا هذا إلى أركان الجريمة الإلكترونية في الفرع الأول، أما في الفرع الثاني نتناول علاقة الأمن السيبراني بالجريمة الإلكترونية.

الفرع الأول: أركان الجريمة الإلكترونية

لم يعد العالم الرقمي مجرد فضاء للتبادل المعرفي، بل أضحى مسرحاً لنمط مستحدث من الجرائم التي تتجاوز الحدود الجغرافية والقيود التقليدية، وتعرف الجريمة الإلكترونية بأنها كل سلوك غير مشروع يتم استخدامه بواسطة تقنيات المعلومات أو يستهدفها، ولما كانت القاعدة

القانونية تقضي بأنه "لا جريمة ولا عقوبة إلا بنص"، فإن المساءلة الجزائية عن هذه الأفعال تستوجب اكتمال بنيانها القانوني القائم على تظافر ثلاثة أركان أساسية:

أولاً: الركن الشرعي للجريمة الإلكترونية

تجسيدًا لمبدأ الشرعية المنصوص عليه في المادة الأولى من قانون العقوبات الجزائري والتي تنص على:" لا جريمة ولا عقوبة ولا تدابير أمن بغير قانون"، تدخل المشرع بموجب القانون رقم 04-15 لضبط الجرائم الإلكترونية وحدد العقوبات المقررة لمرتكبيها في القسم السابع مكرر بعنوان "المساس بأنظمة المعالجة للمعطيات"، ويندرج هذا القسم ضمن الفصل الثالث المتعلق بالجنايات والجنح ضد الأفراد، وذلك في المواد من 394 مكرر إلى 394 مكرر 08 في قانون العقوبات المعدل والمتمم[1].

لم يقف المشرع الجزائري عند هذا الحد، بل بسط حماية جنائية مشددة على الحياة الخاصة للأفراد، وذلك بموجب القانون رقم 06-23[2]، الذي عدل المادة 303 واستحدث المادة 303 مكرر 1 وما يليها، ويهدف هذا التعديل إلى التصدي الحازم لسوء استخدام الوسائل التقنية الحديثة التي قد تنتهك حرمة المراسلات أو الاتصالات أو الصور الخاصة أو تسجيل الأصوات.[3]

أما القانون رقم 09-04[4]،فقد احتوى قواعد خاصة للوقاية من الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال ومكافحتها، وذلك من خلال اعتماد ترتيبات تقنية للحد من الجرائم الإلكترونية، من خلال مراقبة الاتصالات الإلكترونية وتسجيل وتجميع محتواها في وقت حدوثها، ومنح صلاحيات إجراء التفتيش والتحري داخل المنظومات الإلكترونية.[5]

---

[1] **القانون رقم 04-15**، السالف الذكر.

[2] **القانون رقم 06-23** المؤرخ في29 ذو القعدة عام1427 الموافق ل 20ديسمبر2006 معدل ويتمم الأمر رقم66-156 المؤرخ في 8يوليو1966 المتضمن قانون العقوبات، ج ر، العدد84، الصادرة في24 ديسمبر2006.

[3] إيمان بغدادي، "**أثر تعديل قانون العقوبات الجزائري في التصدي للجريمة الإلكترونية**"، مجلة آفاق للبحوث والدراسات السداسية، كلية الحقوق، جامعة قسنطينة، العدد 04، 2019،ص189، ص ص 184-192.

[4] **القانون رقم 09-04**، السالف الذكر.

[5] حمز حضري، عشاش حمزة،" **خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري**"، مجلة الدراسات القانونية والسياسية، جامعة محمد بوضياف، المجلد06، العدد02، المسيلة، الجزائر، 2020،ص171، ص ص 168-176.

وتجدر الإشارة إلى أن النقاش القانوني أثير حول الطريقة المثلى لإدماج النصوص الجديدة والخاصة المتعلقة بالجرائم الإلكترونية، وما إذا كان الأنسب إدراجها ضمن قانون العقوبات التقليدي أم إفرادها بقانون خاص.

فهناك من أدرجها ضمن الجرائم الواقعة على الأموال، باعتبار إمكانية إضفاء صفة مالية على الكيانات المادية والمعنوية للحاسوب، ويرى آخرون أنها ضمن الأحكام المتعلقة بالملكية، فبينما يمثل الكيان المادي عناصر قابلة للتملك، يندرج الكيان المعنوي ضمن نطاق الملكية الفكرية.[1]

ثانيًا: الركن المادي للجريمة الإلكترونية

يقتضي التجريم وجود سلوك مادي ملموس، سواء القيام بفعل أو امتناعًا عنه يمكن إثباته، إذ لا تعتد بالأفكار التي تدور في ذهن الإنسان ما دامت لم تخرج إلى حيز التنفيذ، لأنها لا تدخل ضمن نطاق التجريم، ويتنوع الركن المادي في الجرائم الإلكترونية بتنوع طبيعة الفعل، مما يحول دون إخضاعها لتكييف قانوني موحد، فبينما تندرج بعض الأفعال كالقذف والتهديد والتحريض ضمن القواعد التقليدية لقانون العقوبات لسريان نصوصه عليه حتى وإن ارتكبت عن طريق الحاسوب أو مواقع التواصل الاجتماعي، غير أن بعض السلوكيات المستحدثة في البيئة الرقمية تختلف عن هذه الأفعال التي تخرج عن نطاق التشريعات التقليدية، مما يفرض ضرورة التدخل التشريعي وتحديد أوصافها.[2]

يقوم الركن المادي للجريمة الإلكترونية على العناصر التقليدية الثلاثة: السلوك الإجرامي، النتيجة، والعلاقة السببية التي تربط بينهما، فير أن الطبيعة التقنية لهذه الجرائم تسمح بتحقيق الركن المادي قانونًا حتى في حال تخلف النتيجة الإجرامية، وذلك متى ما ثبت القصد الجنائي واكتملت عناصر الفعل المادي، مثال ذلك إنشاء موقع إلكتروني بقصد التشهير بشخص معين دون نشره فعليًا على شبكة الإنترنت، إذ يبقى الفعل مستوجبًا للمساءلة والعقاب رغم عدم تحقق النتيجة بشكل كامل.[3]

---

[1] إيمان بغدادي، مرجع سابق، ص186.

[2] بوضياف اسمهان، مرجع سابق، ص351.

[3] –إيمان بغدادي، نفس المرجع ، ص187.

تتعدد مظاهر الركن المادي في الجريمة الإلكترونية تبعًا لطبيعة السلوك الإجرامي، إذ يتجسد في كل نشاط إيجابي يصدر عن اعتداء مباشر على الأنظمة التقنية أو المعطيات الرقمية المخزنة فيها، فطبيعة هذه الجرائم تجعل الأفعال المكونة لها متنوعة ومتجددة تبعًا بتطور وسائل التكنولوجيا الحديثة.

لا تُعدّ الأعمال التحضيرية ركناً لازماً في جميع الجرائم، إذ قد تقع بعض الجرائم دون أن تسبقها أفعال تمهيدية واضحة، غير أنّ التمييز بين العمل التحضيري ومرحلة الشروع يثير إشكالاً كبيراً في نطاق الجرائم الإلكترونية، بالنظر إلى الطبيعة التقنية المعقدة لهذا النوع من الجرائم. فرغم أنّ الأصل في التشريعات الجنائية عدم المعاقبة على الأعمال التحضيرية، إلا أنّ الأمر يختلف في البيئة الرقمية، حيث قد تُشكّل بعض الأفعال السابقة لارتكاب الجريمة خطراً قائماً.[1]

ففي مجال تكنولوجيا الإعلام والاتصال، يُنظر إلى بعض التصرفات مثل اقتناء برامج الاختراق، أو حيازة أدوات فك التشفير وكلمات المرور، أو تخزين واستغلال صور الاستغلال الجنسي للأطفال، على أنّها أفعال مجرّمة مستقلة، لما تنطوي عليه من تهديد مباشر لأمن الأنظمة المعلوماتية والحقوق المحمية قانوناً، كما أن سهولة استعمال الوسائل التقنية وسرعة تنفيذ الهجمات الإلكترونية تجعل من الصعب تحديد اللحظة الفاصلة بين مجرد التحضير والدخول الفعلي في التنفيذ الإجرامي، الأمر الذي دفع العديد من التشريعات إلى توسيع نطاق التجريم ليشمل بعض الأفعال السابقة على وقوع الجريمة الإلكترونية حمايةً للأمن السيبراني والمصلحة العامة.[2]

ثالثًا: الركن المعنوي

يختلف الركن المعنوي في الجريمة الإلكترونية باختلاف صورها وأشكالها، إذ يتطلب في الغالب توافر القصد الجنائي لدى الجاني، وتختلف مظاهره حسب كل جريمة[3]:

---

[1] يوسف صغير، مرجع سابق، ص67

[2]–المرجع نفسه، ص68.

[3]–حمز خضري، عشاش حمزة ، مرجع سابق، ص170

1-جريمة الدخول والبقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات: لتحقق القصد الجنائي في هذه الجريمة يجب أن يحيط الجاني علمًا بكافة العناصر المكونة للجريمة، وأن يدرك أن الفعل الذي يقوم به ينصب على نظام للمعالجة الآلية للمعطيات محمية قانونًا، كما يقتضي الأمر توافر نية الغش لدى الفاعل، والتي تظهر خلال الوسائل الاحتيال المستعملة للدخول إلى النظام، كاختراق آليات الحماية، أما البقاء فيستدل على القصد الجنائي من استمرار تواجد الجاني داخل النظام ومباشرته لعمليات تقنية دون مبرر قانوني أو ضرورة فنية، مع إدراكه التام لانتفاء صفة المشروعة عن هذا التواجد.

2-جريمة الاعتداء على سير نظام المعالجة الآلية للمعطيات: تصنف هذه الجريمة ضمن الجرائم العمدية، لأن الأفعال التي تقوم عليها مثل عرقلة النظام، هي بطبيعتها أفعال مقصودة تتطلب توافر الإرادة والعلم لدي الجاني، وهذا ما يميزها عن حالات الاعتداء غير العمدي على سير النظام، والتي قد تعد ظرفًا مشددًا في جريمة الدخول أو البقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات.

3-الإعتداءات العمدية على المعطيات: تعد من الجرائم العمدية التي يتوافر فيها القصد الجنائي بعنصريه العلم والإرادة، إذ يجب أن يكون الجاني على علم بالفعل الذي يقوم به، وأن تتجه إرادته إلى ارتكاب السلوك المتمثل في إدخال المعطيات أو محوها أو تعديلها داخل نظام المعالجة الآلية للمعطيات، كما يشترط أيضا توافر نية الغش لدى الفاعل.

4-استخدام المعطيات كوسيلة لارتكاب الجرائم الماسة بالأنظمة المعلوماتية: يعد من الجرائم العمدية، إذ يتمثل في قيام بأعمال مثل تصميم أو تجميع معطيات عبر منظومة معلوماتية، وذلك بقصد استغلالها في ارتكاب جرائم تمس بالأنظمة المعلوماتية، ويتم غالبا عن طريق الاحتيال أو الغش، إذ يستلزم توافر القصد الجنائي العام، المتمثل في علم الجاني بطبيعة الفعل الذي يقوم به واتجاه إرادته لارتكابه، كما يتطلب القصد الجنائي الخاص، الذي يتمثل في نية الغض واستعمال هذه المعطيات بطريقة غير مشروعة لتحقيق غرض إجرامي.[1]

أما يرى بعض الفقهاء، استحداث قسم خاص بالجرائم المعلوماتية يكون مستقلا عن التقسيمات التقليدية، نظرا لكون هذه الجرائم تستهدف قيمًا اقتصادية ذات طابع تقني خاص،

[1] حمز خضري، عشاش حمزة، مرجع سابق، ص171.

بينما يقترح فقهاء آخرون، إلى ضرورة إلحاق كل فعل معلوماتي بما يشابهه من الجرائم التقليدية في قانون العقوبات.

الفرع الثاني: علاقة الأمن السيبراني بالجريمة الإلكترونية

تُعد الجريمة الإلكترونية اليوم من أبرز التحديات التي تواجه الأمن السيبراني، نظراً لتنوع أشكالها واتساع نطاق تأثيرها العابر للحدود، فهي لا تقتصر على انتهاك الخصوصية الرقمية وإحداث خسائر اقتصادية كبيرة، بل تمتد لتشكل تهديداً للبنى التحتية الحيوية، كما تغذي أنشطة التجسس والدعاية المتطرفة، وبناءً على هذه المخاطر، يركز هذا الفرع على دراسة آثار الجريمة الإلكترونية على منظومة الأمن السيبراني، من خلال تتبع تأثيراتها على ثلاثة مستويات رئيسية: الفردية، الاقتصادية، والدولية.

1-التأثير على الأفراد:

يمثل التأثير المباشر للجريمة الإلكترونية على الأفراد أحد أخطر جوانب هذا النوع من الجرائم، حيث يستهدف المعتدون الرقميون الحياة الخاصة للضحايا باستخدام وسائل متعددة، مثل سرقة البيانات الشخصية، وانتحال الهوية، والتشهير، والابتزاز، وتتبع هذه الاعتداءات من دوافع متباينة تتراوح بين الجشع المادي والانتقام الشخصي، وصولاً إلى الرغبة في التسلية أو الفضول العبثي، وتلقي هذه الممارسات بظلالها السلبية على المستويات النفسية والاجتماعية والمالية للأفراد، إذ تتسبب في زعزعة الاستقرار الأسري، وتقويض جسور الثقة المجتمعية، فضلاً عن إلحاق خسائر مادية فادحة بالضحايا[1].

تجلى خطر الجريمة الإلكترونية بشكل صارخ مطلع عام 2020 تزامناً مع جائحة كورونا، إذ إستغل مجرمو الفضاء السيبراني حالة الارتباك والقلق العالمي لشن موجة واسعة من هجمات التصيد الاحتيالي، وقد استهدفت هذه الهجمات الأفراد عبر رسائل بريد إلكتروني مضللة، ومثال على ذلك، تم إرسال رسائل إلى مواطنين في إيطاليا تدّعي احتوائها على قائمة بأدوية لعلاج

[1] فتيحة حيمر،" **تأثير الجريمة الإلكترونية على الأمن في إفريقيا**"، مجلة أبحاث قانونية وسياسية، المجلد09، العدد01، 2024، ص542، ص ص540-560.

الفيروس، بينما كانت المرفقات تحتوي في الواقع على برمجيات خبيثة تؤدي إلى اختراق أجهزة الحواسيب وسرقة البيانات[1].

2-التأثير على الاقتصاد:

نظراً لتعدد صور الجريمة الإلكترونية، أضحت هذه الظاهرة تشكل تهديداً استراتيجياً يلقي بظلاله القاتمة على الأمن السيبراني في مختلف القطاعات. ومع تطور المنهجيات الإجرامية، بات المجرمون يستخدمون تقنيات متقدمة لسرقة المعلومات وتزويرها، مثل استنساخ المطبوعات والملفات الصوتية والبرمجيات المستخدمة في أنظمة الحاسوب، ليتم إعادة توزيعها وبيعها بأسعار منخفضة مقارنة بالسعر الأصلي، في انتهاك صارخ لحقوق المؤلف أو للشركة المنتجة[2].

تجسدت خطورة هذه التهديدات في الواقعة التي شهدتها شركة تويوتا اليابانية عام 2019، حيث تعرضت أنظمتها لاختراق سيبراني أدى إلى تسريب البيانات الشخصية لنحو 3,1 مليون عميل، وعلى الرغم من مكانتها في قطاع التكنولوجيا الصناعية، إلا أن هذا الخرق أحدث زلزالاً كبيرا في ثقة المستخدمين، وكبّد المؤسسة خسائر اقتصادية ومعنوية جسيمة، مما يثبت أن الحصانة التقنية للشركات الكبرى تظل عرضة للاختراق أمام تطور أساليب الجريمة الرقمية[3].

3-التأثير على مفاهيم القوة والأمن:

أحدث تطور الفضاء السيبراني تحولاً جذرياً في مفاهيم القوة والأمن القومي، حيث انتقلت طبيعة النزاعات من صورتها التقليدية إلى نمط الحروب السيبرانية التي لم تستثنِ المنظومات العسكرية، ويُستخدم هذا الفضاء في النزاعات للتأثير على سلوك الأطراف الأخرى ودفعها للقيام بأفعال لم تكن لتنفذها بدون هذا الضغط، مثل استهداف البنية التحتية للدولة عبر نشر فيروسات تعطل أجهزتها.

---

[1] ليلى بوعوني، **التهديدات في الفضاء السيبراني وانعكاساتها على السيادة الرقمية: القرصنة الإلكترونية نموذجًا**"، مجلة استراتيجية، العدد 16، 2021، ص16، ص ص10-25.

[2] صباح كزيز،"**أثر الجرائم الإلكترونية على أمن واستقرار الدول: قرصنة الموقع الإلكتروني لوكالة الأنباء القطرية نموذجًا**"، مجلة الناقد للدراسات القانونية، العدد03، 2018، ص،131ص ص130-140.

[3] ليلى بوعوني، مرجع سابق، ص18.

يمنح الفضاء السيبراني الفاعل القدرة على التحكم في أجندات الآخرين وترتيب أولوياتهم، وتؤدي هذه الهجمات إلى إرباك العمليات اليومية، بما يشمل المصارف ونظم الاتصالات ووسائل النقل، وفي ظل هذه التحديات، تواجه الدول مخاطر غير مسبوقة تهدد أمنها واستقرارها نتيجة الهجمات السيبرانية[1]،تعد حادثة اختراق البريد الإلكتروني لحملة المرشحة الرئاسية هيلاري كلينتون عام 2016 إحدى أكثر العمليات السيبرانية إثارة للجدل في التاريخ السياسي المعاصر.

فمن خلال تسريب وثائق حساسة لموقع ويكيليكس، نُسبت العملية إلى فواعل رقمية مرتبطة بروسيا، وقد دفعت هذه الواقعة الإدارة الأمريكية، برئاسة باراك أوباما، إلى طرد 35 دبلوماسياً روسيا، ورغم نفي الرئيس دونالد ترامب لهذه الاتهامات خلال لقائه مع نظيره الروسي فلاديمير بوتين في هلسنكي عام 2018، تظل الحادثة مثالاً واضحاً على قدرة الهجمات السيبرانية على تهديد السيادة السياسية للدول.[2]

4-التأثير على إستراتيجية عمل التنظيمات الإرهابية:

توظف الجماعات الإرهابية الفضاء الإلكتروني كمنصة أيديولوجية لنشر فكرها واستقطاب الكوادر، لا سيما عبر منصات التواصل الاجتماعي[3]، ومن أبرز هذه التنظيمات، تنظيم " داعش"، الذي استغل الإنترنت لنش الدعاية المتطرفة، تجنيد الأتباع، جمع تبرعات، وشن هجومات إلكترونية، وتكشف التقارير إلى أن تنظيم يملك أكثر من 53 ألف موقع إلكتروني وعشرات الآلاف من الصفحات بمختلف اللغات، تُستخدم جميعها في شن حرب نفسية ممنهجة ضد الدول، وتحقيق مآربه في الابتزاز والتمويل والتوسع.[4]

---

[1] سيناء علي محمود،" **التحديات الأمنية للدول في الفضاء السيبراني**"، مجلة القضايا السياسية، كلية العلوم السياسية، جامعة النهرين، العدد80، 2025، ص319، ص ص310-322.

[2] جمال بوزيادية، "**الأمن السيبراني**"، محاضرات مقدمة لطلبة السنة الثانية ماستر، تخصص إستراتيجية ودولية، كلية العلوم السياسية والعلاقات الدولية، جامعة الجزائر3، 2022، ص21.

[3] إيمان عبد القادر،" **أثر الفضاء السيبراني على الأمن القومي العربي خلال فترة من 2011 إلى 2023**"، المجلة الأكاديمية العسكرية للدراسات العليا والإستراتيجية، العدد03، 2024، ص108.

[4] جمال بوزيادية، نفس المرجع، ص21.

يتضح أنه رغم حداثت الجريمة الإلكترونية، لا تخرج عن القواعد العامة للجريمة من حيث قيامها على الركن الشرعي والمادي والمعنوي، غير أنّه تتميز بخصوصية ترتبط بالوسيط الإلكتروني المستعمل في ارتكابها، فالجريمة الإلكترونية تعتمد على الأنظمة المعلوماتية والشبكات الرقمية كوسيلة أو محل للاعتداء، مما يجعل إثباتها ومتابعة مرتكبيها أكثر تعقيداً مقارنة بالجرائم التقليدية ، كما تبرز العلاقة الوثيقة بين الجريمة الإلكترونية والأمن السيبيراني، باعتبار أنّ تنامي التهديدات الرقمية أدى إلى بروز الأمن السيبيراني كآلية أساسية لحماية الأنظمة المعلوماتية والمعطيات الرقمية من مختلف الاعتداءات الإلكترونية، فكلما تطورت أساليب الجريمة الإلكترونية ازدادت الحاجة إلى تعزيز تدابير الأمن السيبيراني من خلال الحماية التقنية.

خلاصة الفصل الأول

يعدّ فهم مفهومي الأمن السيبراني والجريمة الإلكترونية خطوة أساسية لاستيعاب طبيعة التحديات التي يفرضها التطور التكنولوجي، فالأمن السيبراني لم يعد يقتصر على الجانب التقني فقط، بل أصبح يشمل أبعادًا قانونية وتنظيمية وبشرية، تهدف في مجملها إلى حماية الأنظمة المعلوماتية وضمان سرية وسلامة وتوافر البيانات، كما يتداخل هذا المفهوم مع مفاهيم أخرى قريبة، ما يعكس طبيعته المركبة والشاملة.

في المقابل، برزت الجريمة الإلكترونية كأحد أخطر التهديدات الحديثة، نظرًا لخصائصها المتميزة مثل السرعة، وصعوبة الكشف، والامتداد العابر للحدود، وتتنوع دوافعها بين المادية والسياسية وغيرها، مما يزيد من تعقيد مواجهتها، كما تقوم هذه الجريمة على أركان قانونية معروفة، إلا أن تطبيقها في البيئة الرقمية يطرح تحديات خاصة.

وتتجلى العلاقة بين الأمن السيبراني والجريمة الإلكترونية في كون الأول يمثل وسيلة أساسية للوقاية والحماية، بينما تشكل الثانية تهديدًا مباشرًا له، مما يفرض ضرورة تبني مقاربات شاملة تجمع بين الجوانب التقنية والقانونية والتوعوية، ومن ثم، فإن الإلمام بهذه المفاهيم يُعدّ أساسًا ضروريًا لفهم آليات المواجهة وتعزيز الأمن في الفضاء الرقمي.

الفصل الثاني:

سبل مواجهة الجريمة الإلكترونية وتحقيق الأمن السيبراني في الجزائر

أدى التحول الرقمي وربط شبكات الحاسوب ببعضها البعض مع استمرار العولمة، إضافة إلى التطور السريع والكبير في مجال الحواسيب، وإزياد وعي الشعوب بأهمية المعلومة باعتبارها مصدرًا للقوة والثروة، إلى انتشار واسع لاستخدام الحاسوب والانترنت بين مختلف سكان العالم.

أفرز هذا التحول جيلاً جديدًا من التهديدات يعرف "بالجرائم الالكترونية"، والتي تعد من أبرز التحديات الأمنية المعاصرة التي فرضت على المجتمع الدولي ضرورة التكاثف لسّن استراتيجيات وقائية ردعية فعالة، وهي جرائم لا تعترف بالحدود الجغرافية، مما فرض تفعيل قنوات تنسيق أمني مباشر عبر الحدود وتأسيس منصات إستخباراتية رقمية متخصصة لتبادل البيانات وتتبع الأنشطة الإجرامية في الفضاء السيبراني.

في إطار مواجهة هذه التهديدات، تبنت الجزائر نهجًا متكاملاً، من خلال وضع أطر قانونية حديثة وتأسيس هيئات تقنية قوية لملاحقة مرتكبي الجرائم الالكترونية، كما سعت إلى تطوير استراتيجيات وطنية تهدف إلى حماية الفضاء الرقمي وتأمين البنى التحتية المعلوماتية الحساسة من مختلف التهديدات الإلكترونية.

ويقتضي تحقيق الأمن السيبراني في الجزائر وضمان بيئة رقمية آمنة، اعتماد مقاربة كاملة تقوم على الانتقال من مجرد رد الفعل إلى التنبؤ بالهجمات، مع سرعة التدخل عند وقوع اختراق، أي لا تكتفي الأنظمة بالكشف عن الهجمات الالكترونية، بل ترتكز على "الوقاية الذكية" وتحييد المخاطر قبل تفاقمها.

وتوطيد التعاون بين القطاعات الأمنية، والمؤسسات الحكومية والقطاع الخاص لضمان شمولية الحماية، أي خلق حالة من التكامل بين القطاعين العام والخاص والأجهزة الأمنية لحماية مفاصل الدولة، والتركيز على التدريب التخصصي والاحترافي للكوادر البشرية، وتحديد الأدوات التقنية بما يتماشى مع الطفرات التكنولوجية المتسارعة.

في صدد ذلك، نسعى في هذا الفصل إلى دراسة سبل مواجهة الجريمة الإلكترونية وتحقيق الأمن السيبراني في الجزائر من شقين أساسيين:إلى الآليات القانونية والإجرائية لدعم الأمن السيبراني لمواجهة الجريمة الإلكترونية في الجرائر**(المبحث الأول)**، في حين يركز **(المبحث الثاني)** على تدابير تعزيز الأمن السيبراني في الجزائر.

المبحث الأول

الآليات القانونية والإجرائية لدعم الأمن السيبراني لمواجهة الجريمة الإلكترونية في الجزائر

أمام التنامي المتسارع للجرائم الإلكترونية في الجزائر، سعى المشّرع الجزائري إلى التصدي لهذه الظاهرة من خلال إعطائها اهتمامًا خاصًا، من خلال تبني إستراتيجية تشريعية مزدوجة تقوم على "المواجهة العقابية" و"الوقاية السيبرانية"، ترتكز على ملائمة النصوص القانونية مع الطبيعة الرقمية والخوارزمية للجرائم المستحدثة، تم استحداث وتفعيل بعض القوانين الخاصة المرتبطة بالبيئة الرقمية والفضاء السيبراني، باعتباره مجالاً واسعًا ومعقدًا يشكل في الوقت ذاته بيئة خصبة لارتكاب مختلف صور الجرائم الإلكترونية.

كما تجسدت المساعي الوطنية في تفعيل آليات الأمن السيبراني بموجب نصوص قانونية وتنظيمية مستحدثة، استهدفت بالدرجة الأولى حماية الأنظمة المعلوماتية والشبكات الوطنية الحيوية، وتطوير وسائل التحري والمتابعة القضائية، إضافة إلى تكريس التنسيق بين مختلف الهيئات المختصة لمجابهة الجرائم الإلكترونية والتصدي لمختلف المخاطر المرتبطة باستعمال تكنولوجيا الإعلام والاتصال.

بذل المشرع الجزائري جهودًا لمكافحة الجريمة الإلكترونية والحد من مخاطرها، عبر جملة من الإجراءات القانونية لمواجهة الجريمة الإلكترونية وتحقيق الأمن السيبراني بموجب قوانين عامة وقوانين خاصة**(المطلب الأول)**، والإجراءات التنظيمية لمواجهة الجريمة الإلكترونية عن طريق آليات أمنية وآليات إدارية المختصة لمكافحة الجريمة الإلكترونية وضمان الأمن السيبراني **(المطلب الثاني)**.

المطلب الأول

الإجراءات القانونية لمواجهة الجريمة الإلكترونية

تبنّى المشرع الجزائري مجموعة من التشريعات والقوانين التي تهدف إلى التصدي لهذا النوع من الجرائم، وفي مقدمتها أدرج أحكامًا موضوعية رادعة بموجب القانون رقم 04- 15

المعدل والمتمم لقانون العقوبات الجزائري، وبعدها أصدر القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

كما أضاف مجموعة من نصوص قانونية أخرى جاءت لتعزيز الإطار التشريعي والحد من انتشار الجرائم الإلكترونية بما يضمن حماية الفضاء الرقمي وتنظيمه.

المشرّع الجزائري قد سارع إلى إقرار حماية قانونية للوسط السيبراني ولمستخدميه، من خلال إصدار حزمة من النصوص التشريعية التي تنظم هذا المجال، سواء تعلق الأمر بالقوانين العامة أو بالتشريعات الخاصة، بما يعكس توجهًا واضحًا نحو بناء ترسانة قانونية متكاملة تهدف إلى تحصين المحيط الرقمي وبناء نموذج أمني وقانوني قادر على احتواء المخاطر التقنية وتداعياتها.

في سياق ذلك، نوضح الإجراءات القانونية لمواجهة الجريمة الإلكترونية من خلال مكافحتها بموجب قوانين عامة وذلك في **(الفرع الأول)**، وبموجب قوانين خاصة في **(الفرع الثاني)**.

الفرع الأول: مكافحة الجريمة الإلكترونية بموجب قوانين عامة

فرضت الطفرة الرقمية المتسارعة واقعًا جديدًا حتّم على الجزائر تحديث إجراءاتها القانونية والمؤسساتية لمجابهة الأنماط المستحدثة من الإجرام، وهي الجرائم الإلكترونية التي أضحت تشكل تهديدًا جوهريًا لأمن الأفراد واستقرار الدولة، مما دفع المشرّع الجزائري إلى الاستناد على القوانين العامة في مقدمتها الدستور والقانون العقوبات وقانون الإجراءات الجزائية، كأساس لحماية الأفراد وحقوقهم في الفضاء الرقمي.

أولاً: الدستور الجزائري

انتهج الدستور الجزائري مسارًا لحماية حقوق وحريات الأفراد، بدءًا من دستور 1996، وما لحقه من تعديلات لاحقة لا سيما التعديل الدستوري لسنة 2016، وصولاً إلى المراجعات العميقة في التعديل الدستوري لسنة 2020.

فقد أقرّ المؤسس الدستوري صراحة بمسؤولية الدولة عن حماية كرامة الفرد وسلامته الجسدية والمعنوية، وهي مبادئ تُرجمت فعليًا في الترسانة التشريعية الوطنية على رأسها

قانون العقوبات وقانون الإجراءات الجزائية، إلى جانب مجموعة من القوانين الخاصة ذات صلة التي تهدف في مجملها إلى تجريم أي اعتداء يمس بهذه الحقوق أي يهددها، مع إقرار آليات ردعية وإجرائية لضمان فعاليتها، [1] وتتجسد هذه الحماية القانونية من خلال حزمة من المبادئ الدستورية أبرزها:

أرست المادة 37 من التعديل دستوري الجمهورية الجزائرية الديمقراطية الشعبية لسنة 2020 أن كافة المواطنين سواسية أمام القانون، ولهم الحق في التمتع بحمايته على قدم المساواة، ويحظر تمامًا أي تمييز بينهم، سواء كان مرده إلى الأصل أو العرق أو الجنس أو الرأي أو أي اعتبارات أو ظروف أخرى شخصية كانت أم اجتماعية[2].

وتعكس هذه المادة مبدأً أساسيا وهو مبدأ المساواة، ويعني ذلك أن القانون يطبق على الجميع بنفس الكيفية دون تفرقة، فلا يُفضّل شخص على آخر، كما تفرض هذه القاعدة على الدولة واجب توفير حماية قانونية متساوية لكل الأفراد، بما يضمن صون حقوقهم وحرياتهم.

كما تؤكد المادة 47[3] من دستور على أهمية حماية الحياة الخاصة للأفراد في المجتمع، حيث تعتبر الخصوصية من الحقوق الأساسية التي لا يجوز انتهاكها بسهولة، فالدولة ملزمة بضمان سرية الاتصالات، سواء كانت مكتوبة أو إلكترونية أو هاتفية، مما يعزز الثقة والأمان بين الأفراد، كما تشترط تدخل القضاء قبل أي مساس بهذه الحقوق، وهو ما يشكل ضمانة ضد التعسف أو الاستغلال، ومن جهة أخرى، يبرز المادة أهمية حماية البيانات الشخصية في ظل التطور التكنولوجي، إذ تفرض عقوبات على كل من يستغل هذه المعطيات بشكل غير قانوني، بهدف حماية الأفراد من الجرائم الإلكترونية وانتهاكات الخصوصية[4].

---

[1] بوضياف اسمهان، مرجع سابق، ص 361.

[2] المادة 37 من الفصل الأول، **تحت عنوان الحقوق والحريات العامة**، من الدستور 2020، المؤرخ في 15 جمادى الأول عام 1442هـ الموافق ل 30 ديسمبر 2020، ج ر ، العدد82 ، 2020.

[3] المادة47، من دستور 2020، سالف الذكر.

[4] المادة 47 من دستور 2020، السالف الذكر.

يؤكد الدستور على ثنائية المساواة والحرمة الشخصية، حيث يرسخ مبدأ تكافؤ الفرص والحماية القانونية دون تمييز، وبالتوازي يفرض حصانة مطلقة على الحياة الخاصة وصون الشرف والكرامة وإضافة إلى كفالة سرية الاتصالات والمراسلات بمختلف أنواعها، ولا ترفع هذه الحصانة إلا في إطار ما يحدده القانون وبموجب أمر قضائي مسبب، كما يقّر بحماية المعطيات الشخصية كحق أساسي، ويعزز ذلك من خلال تبنّي آليات الأمن السيبراني التي تهدف إلى حماية البيانات والأنظمة المعلوماتية من الاختراق والاستغلال غير المشروع، مع تقرير عقوبات صارمة لكل من ينتهك هذه الضمانات.

ثانًيا: مكافحة الجريمة الإلكترونية في قانون العقوبات الجزائري

تماشيًا مع إفرازات الثورة الرقمية وظهور أنماط إجرامية عابرة للحدود لم تشهدها البشرية من قبل، سارع المشرع الجزائري إلى سّد الفراغ القانوني واهتم بتجريم الأفعال التي تمسّ بأنظمة الحاسب الآلي والحد من آثارها، وقد تجسّد هذا التوجه بوضوح في التعديل الجوهري لقانون العقوبات لتجريم هذه الأفعال بموجب القانون رقم 04- 15[1] بعنوان: "المساس بأنظمة المعالجة الآلية للمعطيات" ويتضمن هذا القسم ثمانية مواد من المادة 394 مكرر إلى 394 مكرر8[2]، واضعًا بذلك الأساس لتجريم الاعتداءات الواقعة على أنظمة المعالجة الآلية للمعطيات.[3]

شهد عام 2006 نقلة تشريعية هامة بموجب القانون رقم 06- 23[4]،حيث تدخل المشرع لتعديل قانون العقوبات وتحديدًا القسم السابع مكرر منه، استهدف هذا التعديل الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، مقررًا تشديدًا ملموسًا في العقوبات.

يرجع هذا التوجه نتيجة تنامي الوعي الاجتماعي والمؤسساتي بخطورة هذا النمط المستحدث من الإجرام، نظرًا لما لها من آثار سلبية على الاقتصاد الوطني، إضافة إلى

---

[1] **قانون رقم 04 15**، المتضمن ق ع، سالف الذكر.

[2] المواد من 394 مكرر إلى 394 مكرر8، من القانون رقم 04-15 المتضمن ق ع، سالف الذكر.

[3] حنان مسكين، " **واقع مكافحة الجريمة المعلوماتية واتجاهاتها التشريعية في الجزائر**"، المجلة الأكاديمية للبحوث القانونية والسياسية، العدد01، المجلد 04، الجزائر، 2020، ص 625، ص ص610- 632.

[4] **قانون رقم 06 -23**، سالف الذكر.

تهديدها لأمن المعلومات والمعاملات الإلكترونية، مما استدعى تحصين قانوني والتصدي لها بصرامة[1].

المشرع الجزائري عاقب حسب نص المادة 394 مكرر كل شخص يقوم بالدخول أو البقاء بطريقة غير مشروعة داخل منظومة للمعالجة الآلية للمعطيات أو يحاول القيام بذلك، حتى ولو لم يحدث أي ضرر فعلي، وذلك أن مجرد الولوج غير المصرح به يعد اعتداءًا على أمن الأنظمة المعلوماتية، وتتشدد العقوبة إذا ترتب عن هذا الدخول حذف أوتعديل في البيانات، وتزداد أكثر إذا أدى الفعل إلى تعطيل أو تخريب نظام عمل المنظومة.[2]

وكذلك يعاقب المشرع الجزائري بموجب المادة 394 مكرر2[3] كل شخص يقوم عمدًا وبطريقة احتيالية بتصميم أو بحث أو جمع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عبر منظومة معلوماتية، متى كانت هذه المعطيات قابلة للاستعمال في ارتكاب الجرائم المنصوص عليها في هذا القسم، باعتبارها تشكل وسيلة وأداة تساعد على تنفيذ الأفعال الإجرامية الإلكترونية أو تسهيلها.

كما تشمل هذه المادة عقاب كل من يقوم بحيازة أو إفشاء أو نشر أو استعمال أو تعديل أو أي تصرف غير مشروع في معطيات تم الحصول عليها نتيجة ارتكاب إحدى الجرائم المعلوماتية وذلك لما يشكله هذا السلوك من خطورة على سلامة الأنظمة المعلوماتية وحماية البيانات الشخصية وحرمة الحياة الخاصة[4].

تمنح المادة 394 مكرر6[5] للقاضي السلطة التقديرية لفرض عقوبات تكميلية إلى جانب العقوبات الأصلية، تشمل مصادرة الوسائل والبرمجيات المستخدمة في الجرائم الإلكترونية،

---

[1] راضية عيمورة، "**الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري**"، المجلة الأكاديمية للبحوث القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الأغواط، العدد1 ، المجلد 6، الجزائر، 2022، ص 94، ص ص87-107.

[2] المادة رقم 394 مكرر من قانون العقوبات رقم 04-15، سالف الذكر.

[3] المادة 394 مكرر2، من **قانون رقم 04-15** المتضمن ق ع، السالف الذكر.

[4] المادة رقم 394مكرر2، من **القانون رقم 04-15** المتضمن ق ع ج، سالف الذكر.

[5] المادة رقم 394 مكرر 6، **القانون رقم 15-04** المتضمن ق ع، سالف الذكر.

وحجب المواقع الإلكترونية ذات الصلة، وصولاً إلى غلق المنشأة أو محل الاستغلال في حال ثبوت علم المالك بالجريمة، مع كفالة حقوق الغير حسن النية.

يتضح أن المشرع الجزائري من خلال تعديل الأخير لقانون العقوبات الجزائري، شدّد العقوبات على الأفعال المرتكبة في منظومة المعالجة الآلية للمعطيات، نظرًا لخطورتها على الأفراد والمؤسسات وما قد تسببه من مساس بالخصوصية وسلامة الأنظمة المعلوماتية، إذًا فالأحكام القانونية لا تهدف فقط للردع، بل تعدّ أيضًا أداة أساسية في تعزيز الأمن السيبراني، من خلال حماية الفضاء الرقمي، والوقاية من الهجمات الإلكترونية، وضمان أمن وسلامة المعطيات والأنظمة المعلوماتية، بما يحقق بيئة رقمية موثوقة.

ثالثًا: مكافحة الجريمة الإلكترونية بموجب قانون الإجراءات الجزائية الجزائرية:

شهد النظام الإجرائي الجزائي قفزة نوعية لمواكبة التطور التقني، حيث استحدث المشرع آليات خاصة للتحري والتحقيق في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال في قانون الإجراءات الجزائية رقم 25- 14[1]، وتتمثل أبرز هذه المستجدات فيما يلي[2]:

1- لضمان فعالية المتابعة القضائية في الجرائم العابرة للحدود، عزز المشرع الجزائري دور الأقطاب الجزائرية المتخصصة، حيث تم تمديد اختصاص المحاكم الجزائية المحلي إلى دائرة اختصاص محاكم أخرى حسب نص المادة 310[3] من قانون الإجراءات الجزائية، ومنح لها صلاحية النظر في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وذلك بموجب المواد 335[4] قانون الإجراءات الجزائية، يهدف هذا التعديل إلى تركيز القضايا المعقدة تقنيا لدى قضاة متخصصين لضمان دقة الأحكام.

---

[1] **القانون رقم 25-14** المؤرخ في 9 صفر 1447، الموافق ل 3 غشت 2025، المتضمن قانون الإجراءات الجزائية الجزائري، الجريدة الرسمية، العدد54، المنشورة في 03 أوت 2025.

[2] حنان مسكين، مرجع سابق، ص219-220

[3] القانون رقم ،310 من القانون رقم 25-14 المتضمن ق ا ج ج، سالف الذكر.

[4] المادة 335، من القانون رقم 25-14 المتضمن ق ا ج ج، سالف الذكر

2- منح المشرع الجزائري بموجب المادة 24[1]ضباط الشرطة القضائية صلاحية تمديد اختصاصهم الإقليمي ليشمل كامل التراب الوطني عند معاينة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، مما يتيح ملاحقة الجناة وجمع الأدلة الرقمية بسرعة وفعالية دون تقيد بحدود الدائرة القضائية.

3- وضع القانون ضوابط صارمة توازن بين مقتضيات التحقيق وحماية الحرمات مع مراعاة خصوصية الدليل الإلكتروني، حيث نصت المادة 78[2] من قانون الإجراءات الجزائية على إجراءات استثنائية لتفتيش النظم المعلوماتية وضبط المعطيات المخزنة فيها، بما يتماشى مع سرعة تلاشي الأدلة الرقمية.

نظرًا لتعقيد التحقيقات التقنية التي تتطلب وقتًا أطول لفك التشفير أو التحليل الجنائي الرقمي، نصت المادة 83 الفقرة[3]6من قانون الإجراءات الجزائية على تمديد فترات التوقيف للنظر بصفة استثنائية في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

4- اعتماد أساليب التحري الخاصة، حيث أقرت التعديلات الأخيرة وسائل تقنية متطورة لجمع الأدلة في الجرائم الإلكترونية الخطيرة، وفقًا ل المواد 114 إلى 120[4] من قانون الإجراءات الجزائية، إجازة اعتراض وتثبيت وتسجيل المراسلات التي تتم عبر وسائل الاتصال السلكية واللاسلكية، والسماح لضباط الشرطة القضائية بالولوج إلى الفضاءات الافتراضية تحت هوية مستعارة لاختراق الشبكات الإجرامية وجمع الأدلة.

يتضح أن المشرع الجزائري من خلال تعديلات قانون الإجراءات الجزائية لعام 2025 عمل على مكافحة الجريمة الإلكترونية من خلال منح صلاحيات أوسع للجهات القضائية وضباط الشرطة القضائية، واعتماد إجراءات خاصة كتمديد الاختصاص والتوقيف للنظر وتفتيش الأنظمة المعلوماتية، إضافة إلى استعمال وسائل تقنية حديثة لاعتراض المراسلات وجمع الأدلة الرقمية، بهدف تسهيل التحري والتحقيق في الجرائم الإلكترونية.

---

[1] المادة 24، من القانون رقم 25-14 المتضمن ق ا ج ج، سالف الذكر.

[2] المادة 78، من القانون رقم 25-14 المتضمن ق ا ج ج، سالف الذكر.

[3] المادة 83، من القانون رقم 25-14 المتضمن ق ا ج ،سالف الذكر.

[4] المواد من 114إلى 120، من القانون رقم 25-14 المتضمن ق ا ج ج، سالف الذكر.

إذًا تأسيسًا على الضمانات الدستورية التي تكرس مبدأ المساواة وحماية الحياة الخاصة وسرية الاتصالات والمعطيات الشخصية، مع إخضاع أي استثناء للضوابط القانونية والقضائية، حرص المشرع الجزائري على بناء إطار قانوني ردعي وإجرائي لمكافحة الجريمة الإلكترونية، حيث واجه في قانون العقوبات التعديات والولوج الغير مشروع للأنظمة المعلوماتية وحذف أو تعديل بياناتها بعقوبات مشددة مع منح القاضي صلاحيات لتوقيع العقوبات المناسبة، وفي الإطار الإجرائي، نصّ قانون الإجراءات الجزائية على آليات خاصة لمكافحة الجريمة الإلكترونية عبر توسيع صلاحيات التحري واعتماد وسائل تقنية لجمع الأدلة الرقمية وتسهيل التحقيق في الجرائم المعلوماتية.

الفرع الثاني: مكافحة الجريمة الإلكترونية بموجب قوانين خاصة

أمام التوسع الكبير للجرائم الإلكترونية وتعدد أشكالها، حرصت الجزائر على تحصين أمنها المعلوماتي عبر استحداث تشريعات جديدة وتعديل القوانين القائمة، شمل ذلك سّن قوانين متخصصة وتطوير التشريعات النافذة لتنظيم الفضاء الرقمي، وتوفير الحماية اللازمة للبيانات الشخصية، مع وضع أطر صارمة لتجريم كافة أشكال الجريمة الإلكترونية.

أولاً: القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها

صدر القانون رقم 09- 04[1] ، والذي يتألف من 19 مادة مقسمة على ستة فصول، وينظم هذا القانون إجراءات المراقبة الإلكترونية بمجموعة من الضوابط، حيث يحظر مباشرتها إلا بموجب إذن قضائي مسبق وفي حالات حصرية.

يعد هذا القانون الإطار التشريعي الأكثر استجابة لخصوصيات الجرائم المرتبطة بوسائل الإعلام والاتصال، ولا سيما تلك الناجمة عن الاستخدام غير المشروع للإنترنت، ومن خلال تحليل مضمونه، نجد أن المشرع قد استحدث آليات غير مسبوقة لمواجهة الجرائم

[1] **القانون رقم 09-04**، المؤرخ في 14 شعبان عام 1430 الموافق ل 5غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر ، العدد 47، الصادرة في 2009.

الإلكترونية، تشمل تدابير وقائية تهدف إلى الكشف الإستباقي عن الاعتداءات وتحديد مرتكبيها بسرعة، بالإضافة إلى إجراءات تقنية التي جاءت لتتمم القواعد الإجرائية المعتادة.[1]

استحدث القانون رقم 09- 04 مجموعة من التدابير الوقائية الإستباقية التي تهدف إلى تحصين الفضاء الرقمي ومنع وقوع الجرائم الإلكترونية أو رصدها وتحديد هوية فاعليها فور حدوثها، وتتمحور هذه التدابير حول ركيزتين أساسيتين:

1- تفعيل الرقابة الإلكترونية: حيث نصت المادة 4[2] من القانون رقم 09- 04 على إرساء آليات لمراقبة الاتصالات الإلكترونية ضمن الأطر القانونية المحددة.

2- إشراك مزودي خدمات الاتصالات الإلكترونية في المنظومة الأمنية للوقاية من الجرائم المعلوماتية: بموجب المواد 12، 11، 10[3] من نفس القانون، فرضت عليهم التزامات جوهرية التي تجعلهم طرفًا فعالاً في الوقاية من الجرائم المعلوماتية ومكافحتها.[4]

إلى جانب الإجراءات الوقائية المشار إليها سابقاً، عزز المشرع عبر القانون رقم 09- 04 المنظومة الإجرائية لمكافحة الجرائم المعلوماتية بآليات إضافية مكملة لقانون الإجراءات الجزائية، والمتمثلة في:

1- منح الجهات القضائية وضباط الشرطة القضائية بالدخول لأغراض التفتيش لاستخراج المعطيات المخزنة واستنساخها، كما أجاز تمديد المعاينة لتشمل أنظمة أخرى مرتبطة تقنياً بالمنظومة الأصلية، بشرط الإخطار المسبق للسلطات المختصة.

2- إقرار إمكانية التنسيق مع السلطات الأجنبية للحصول على البيانات المخزنة خارج الإقليم الوطني، وذلك في إطار الاتفاقيات الدولية ومبدأ المعاملة بالمثل.

يتضح مما سبق أن أحكام القانون رقم 09- 04 قد صيغت بعبارات عامة وشاملة، لتستوعب كافة الجرائم المرتبطة بتقنيات الإعلام والاتصال، حيث يمتد نطاق التجريم ليشمل كافة الأفعال المخالفة المرتكبة عبر الوسائط التقنية، سواء كانت تقليدية، معاصرة كشبكة

---

[1] راضية عيمور، مرجع سابق، ص 104.

[2] المادة04 ، من القانون رقم 09-04 سالف الذكر.

[3] المواد 12،10،11، من القانون رقم 09-04، سالف الذكر.

[4] راضية عيمور، نفس المرجع، ص 105.

الإنترنت أو حتى التقنيات المستقبلية، وهو ما يمنح هذا التشريع مرونة كافية لمواكبة التسارع التكنولوجي المستمر.[1]

ثانيًا: القانون الخاص بالملكية الأدبية والفنية لحماية معطيات الحاسب

يعد صون الإبداع البشري الغاية الأسمى لتشريعات الملكية الفكرية، لكونه المحرك الأساسي للتطور الحضاري، ويهدف إقرار قوانين الملكية الفكرية إلى حماية حق الإنسان في التفكير والإبداع والابتكار، وباعتبار مكونات الحاسب الآلي ثمرة استثمار فكري، وجب وضع حماية قانونية عليها وتجريم الأفعال الماسة بسلامتها وفرض عقوبات جزائية على مرتكبيها.[2]

وقد تماشى التشريع مع النظم القانونية العالمية، من خلال إقرار الحماية لبرامج الحاسب الآلي بموجب الأمر رقم 03- 05[3] المتعلق بحقوق المؤلف والحقوق المجاورة، الذي أضفى صفة المصنف المحمي على مبتكرات الإعلام الآلي مقررًا بذلك جزاءات ردعية لكل اعتداء.

بإدراج المشرع الجزائري لبرامج وبيانات الحاسب الآلي ضمن فئة المصنفات الفكرية الأصلية، أخضعها بصورة مباشرة لمنظومة حماية حقوق المؤلف، وبناءا عليه، فإن أي مساس بالحقوق المعنوية أو المادية للمؤلف يقع تحت طائلة جريمة التقليد بموجب المادة 151 من الأمر 03- 05، ما يستتبع تفعيل العقوبات الردعية الواردة في المواد 153، 156، 157، و158،[4] من ذات الأمر[5].

---

[1] حنان مسكين، مرجع سابق، ص622.

[2] راضية عيمور، مرجع سابق، ص 103-104.

[3] **الأمر رقم 03-05**، المؤرخ في 19 جمادى الأولى عام 1424 الموافق ل 19 يوليو 2003، المتعلق بحقوق المؤلف والحقوق المجاورة، ج ر ، العدد 44، الصادر في 23 يوليو 2003.

[4] المواد من 151 إلى 158، **من الأمر رقم 05-03**، المتعلق بحقوق المؤلف والحقوق المجاورة، سالف الذكر.

[5] بن عبو عفيف، " **الآليات القانونية في الجزائر وتطويرها في مكافحة الجريمة الإلكترونية**"، مجلة حقوق الإنسان والحريات العامة، جامعة عبد الحميد بن باديس، مستغانم، المجلد 09، العدد01، الجزائر، 2024، ص 32،ص ص 21-47.

ومنه المشرع الجزائري أقر حماية قانونية لبرامج الحاسب الآلي باعتبارها من المصنفات الفكرية، وذلك بموجب الأمر رقم 03- 05 المتعلق بحقوق المؤلف، بهدف صون الإبداع البشري في المجال الرقمي، وبناءًا عليه، فإن أي اعتداء على الحقوق المعنوية أو المادية للمؤلف يعد جريمة ترتب عقوبات جزائية.

ثالثا: القانون الخاص المتعلق بالقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية

بموجب القانون رقم 18- 04[1] المتعلق بالقواعد العامة المتعلقة بالبريد والاتصالات الالكترونية تم إرساء آليات قانونية للتصدي للجرائم الافتراضية، من أبرزها تأسيس سلطة ضبط تتولى مراقبة مدى تقييد متعاملي البريد والاتصالات الإلكترونية بالتشريعات السارية، ولا سيما معايير الأمن السيبراني، ويستند هذا الإجراء إلى المادة 13[2] من نفس القانون.

كرّس المشرّع حماية جزائية مشددة لسرية المراسلات البريدية والإلكترونية، حيث جرّم كافة صور الاعتداء عليها بما في ذلك الإفشاء أو النشر أو الاستغلال دون إذن، وصولاً إلى مجرد الإخطار بوجودها، ولم يقتصر التجريم على الفعل التام فقط، بل امتد ليشمل الأفعال التمهيدية والمشاركة، كمحاولة فتح المراسلات أو تخريبها أو تحويل وجهتها، إضافة إلى المساهمة أو المساعدة في ارتكاب هذه الجرائم.[3]

وفي إطار تعزيز الحماية القانونية للمعطيات والاتصالات، أقرّ هذا القانون منظومة عقابية متكاملة تهدف إلى الردع والوقاية، حيث نص على مجموعة من العقوبات تتراوح بين الغرامات المالية والعقوبات السالبة للحرية، وذلك ضمن المواد من 161 إلى 188[4]، بما يعكس حرص المشرع على صون الحياة الخاصة وضمان أمن وسرية الاتصالات في البيئة الرقمية.

---

[1] **القانون رقم 18-04** المؤرخ في 10 ماي 2018، المتضمن القواعد العامة للبريد والاتصالات الإلكترونية، ج ر ، العدد 27، الصادرة بتاريخ 13 ماي 2018.

[2] المادة 13، من **القانون رقم 18-04** المتضمن القواعد العامة للبريد والاتصالات الإلكترونية، سالف الذكر.

[3] مهدي رضا، **"الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري"**، مجلة إليزا للبحوث الدراسات، جامعة محمد بوضياف، المسيلة، المجلد 06، العدد 02، الجزائر، 2021، ص 116، ص 111-125.

[4] المواد من 161 إلى 188، من القانون رقم 18-04، سالف الذكر.

إذًا يهدف قانون رقم 18- 04 إلى تنظيم قطاع البريد والاتصالات الإلكترونية وحماية سرية المراسلات والمعطيات الرقمية، من خلال إنشاء سلطة ضبط تراقب مدى التزام المتعاملين بمعايير الأمن السيبراني، وتجريم مختلف أشكال الاعتداء على الاتصالات مثل الإفشاء أو الاطلاع الغير مشروع، مع توسيع نطاق المسؤولية ليشمل الأفعال التحضيرية والمشاركة، إضافة إلى إقرار عقوبات.

رابعًا: قانون رقم 18- 07[1] المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي

نظم المشرع الجزائري حماية المعطيات الشخصية في الفضاء الرقمي عبر جملة من الآليات القانونية المرتبطة بالفضاء الرقمي، وتتمثل في[2]:

1- تأسيس سلطة وطنية مستقلة تختص بحماية المعطيات ذات الطابع الشخصي، مع إقرار التزامات قانونية صارمة تقع على عاتق المسؤولين عن المعالجة الآلية للمعطيات، بما يضمن احترام قواعد الحياة الخاصة.

2- منح السلطة الوطنية صلاحية اتخاذ تدابير إدارية رادعة في حال ثبوت أي خرق للأحكام القانونية، واتخاذ إجراءات ردعية مناسبة.

3- تمكين السلطة الوطنية من حق التفتيش والتحري ومعاينة أماكن المعالجة، باستثناء المساكن، مع إمكانية الاطلاع على المعطيات المعالجة وكافة الوثائق والمعلومات مهما كانت طبيعتها أو وسيلتها.

4- إعطاء صفة الضبطية القضائية لأعوان رقابة مؤهلين للبحث ومعاينة الجرائم الإلكترونية المرتبطة بهذه المعطيات، تحت إشراف مباشر من وكيل الجمهورية، كما أتاح القانون لكل شخص تضرر من انتهاك أحد حقوقه اللجوء إلى القضاء لطلب اتخاذ تدابير تحفظية لوقف التعدي أو المطالبة بالتعويض عن الأضرار الناجمة عنه.

---

[1] **القانون رقم 18-07**، المؤرخ في 25 رمضان عام 1439 الموافق ل 10يونيو 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج ر، العدد 34، الصادر في 2018.

[2] مهدي رضا، مرجع سابق، ص 121-122.

5- إرساء مبدأ الاختصاص القضائي الموسع، حيث تختص المحاكم الجزائرية بمتابعة الجرائم المرتكبة خارج الإقليم الوطني إذا كان الفاعل جزائريًا، أو أجنبيا مقيمًا في الجزائر أو شخصًا معنوياً خاضعًا للقانون الجزائري وذلك وفقًا لما تقرره قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، تخصيص نظام عقابي رادع بموجب المادة 53 من القانون رقم 18- 07[1] المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

6- كرس القانون مبدأ تجريم الاعتداء على المعطيات ذات الطابع الشخصي، من خلال تقرير عقوبات مالية وأخرى سالبة للحرية، نصّت عليها المواد من 54 إلى 74[2]من القانون رقم 18- 07، يعكس توجّه المشرّع نحو تعزيز الحماية الجزائية لهذه المعطيات في البيئة الرقمية.

يتضح أن المشرع الجزائري كرّس حماية المعطيات الشخصية في الوسط الرقمي من خلال إنشاء سلطة وطنية مستقلة للرقابة، ومنحها صلاحيات التفتيش واتخاذ التدابير، مع تمكين المتضررين من اللجوء للقضاء، كما وسع الاختصاص القضائي ليشمل بعض الجرائم المرتكبة خارج الإقليم، وأقر نظامًا جزائياً يجرّم الاعتداء على المعطيات الشخصية بعقوبات مالية وسالبة للحرية.

---

[1] المادة رقم 53، من **القانون رقم 18-07**، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، سالف الذكر.

[2] المواد من 54إلى 74، من **القانون رقم 18-07**، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، سالف الذكر.

المطلب الثاني

الإجراءات التنظيمية لمواجهة الجريمة الإلكترونية

تعد التدابير التنظيمية والهيكلية الركيزة الجوهرية لضمان فاعلية الإستراتيجيات الوطنية الرامية إلى مجابهة الجرائم الإلكترونية، حيث يرتكز هذا التوجه على استحداث كيانات وهياكل وطنية متخصصة تتمتع بالصلاحيات التقنية والقانونية اللازمة لإدارة هذا النوع من المخاطر المستحدثة.

وفي هذا الإطار، انتهجت الجزائر إستراتيجية وطنية قائمة على جهود مكافحة الجريمة الإلكترونية، تجسدت في إنشاء هيئات ومؤسسات ذات طبيعة نوعية، أنيطت بها مهام حماية السيادة المعلوماتية وتأمين الشبكات الوطنية.

تلعب هذه الهياكل دورًا محورياً في تحصين الأمن السيبراني، مما يساهم في الرفع من كفاءة الدولة وقدراتها الردعية في التصدي لمختلف أنماط الاعتداءات، الرقمية واحتواء تداعي الجزائر من الدول التي تواجه تحديات متزايدة في مجال الأمن السيبراني، حيث شهدت في الفترة الأخيرة عدداً من الهجمات الإلكترونية.

ومن بين الإجراءات التنظيمية التي اعتمدتها الجزائر لمواجهة الجريمة الإلكترونية وتحقيق الأمن السيبراني نجد الآليات الأمنية لمكافحة الجريمة الإلكترونية وتحقيق الأمن السيبراني نتطرق لها في **(الفرع الأول)**، الآليات الإدارية المختصة لمكافحة الجريمة الإلكترونية وتحقيق الأمن السيبراني **(الفرع الثاني)**.

الفرع الأول: الآليات الأمنية لمكافحة الجريمة الإلكترونية وتحقيق الأمن السيبراني في الجزائر

تفرض التحديات السيبرانية المتنامية التي تواجهها الجزائر حتمية صياغة إطار قانوني مرن ومواكبة مؤسساتية متخصصة لردع التهديدات الرقمية، ونظراً لكون الأمن السيبراني جزءاً أساسيا من السيادة الوطنية في العصر الحديث، فقد أصبح لازماً على وزارة الدفاع الوطني، من خلال أجهزتها المختلفة وعلى رأسها الدرك الوطني الجزائري، في مجابهة

الجريمة الإلكترونية والتصدي لها، تبرز آليات أمنية المكلفة بحماية الفضاء السيبراني، ومنها:

أولاً: المصلحة المركزية لمكافحة الإجرام السيبراني للدرك الوطني

في إطار الإستراتيجية الوطنية الرامية إلى مكافحة الجريمة الإلكترونية وتوطيد دعائم الأمن السيبراني، حرصت الدولة الجزائرية على ضمان سلامة أنظمة المعلوماتية من خلال إنشاء مركز متخصص تابع للدرك الوطني[1]، يعود تاريخ هذه الهيئة المتمركزة في "بئر مراد الرايس" إلى سنة 2008، وقد عرفت مساراً تنظيماً بدأ بإنشائها تحت مسمى "مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية"، بموجب قرار وزاري صادر سنة 2018.

تتركز المهمة الجوهرية للمركز في تحليل البيانات الرقمية المرتبطة بالأنشطة الإجرامية وكشف هوية مرتكبيها، كما يمتد نشاطه على المستوى الوطني من خلال محققي الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال، والتابعين للمجموعات الإقليمية المختصة.[2]

يعمل المركز على تطوير آليات التصدي للإجرام المعلوماتي، وقد سجل حظوراً فعالاً في فك رموز ومعالجة قضايا إلكترونية معقدة، لا سيما تلك المتعلقة بالاختراقات وهجمات القرصنة التي استهدفت البنى التحتية الحساسة، بما فيها الأنظمة الأمنية والاتصالية والمواقع الحكومية السيادية.[3]

تتولى المصلحة المركزية مجموعة من المهام المتنوعة لتشمل[4]:

- اليقظة الرقمية عبر الرصد المستمر لشبكة الإنترنت والاتصالات الإلكترونية في حدود الأطر القانونية المعمول بها.

---

[1] معتوق أم الخير، مرجع سابق، ص68.

[2] سيد علي بدرين، "**إستراتيجية الجزائر لمواجهة التهديدات السيبرانية**"، مجلة الشرطة، المديرية العامة للشرطة الجزائرية، العدد 156، الجزائر، 2023،ص61، ص ص 51- 70.

[3] محمودي سعيد، "**الأمن السيبراني في الجزائر: بين المعالجة الأمنية والحماية القانونية**"، مجلة الناقد للدراسات السياسية، جامعة بشار، المجلد 07، العدد 02، الجزائر، 2023، ص199، ص ص 193- 212.

[4] معتوق أم الخير، نفس المرجع ، ص68.

- كما تتمتع المصلحة المركزية بدور إجرائي يتمثل في مباشرة التحريات الإلكترونية لدعم الجهات القضائية ووحدات الدرك الوطني.
- تعمل على تعزيز التعاون والتنسيق بين مختلف المصالح الأمنية والهيئات الوطنية بهدف مكافحة الجريمة الإلكترونية.
- تقدم المصلحة المركزية إسنادًا تقنياً للوحدات الإقليمية من خلال معاينة مسارح الجريمة الرقمية، وجمع الأدلة الإلكترونية وتحليها.

ثانياً: المعهد الوطني للأدلة الجنائية وعلم الإجرام

يُعدّ هذا المعهد هيئة متقدمة، ويمثل صرحاً علمياً متطورًا يرتكز على كفاءات متخصصة في مكافحة الجريمة بشتى صورها، من خلال دمج العلوم الحديثة في صلب منظومة العدالة الجنائية، كما أن إتقانه للتقنيات المتطورة من تعزيز قدراته الإستباقية والعملياتية في مواجهة الأنماط الإجرامية المستحدثة، لا سيما تلك المرتبطة بالفضاء الرقمي والتكنولوجيات المتطورة.[1]

يقع المعهد الوطني للأدلة الجنائية وعلم الإجرام الحلي في منطقة بوشاوي بالجزائر العاصمة، مع جواز تحويله إلى أي موقع آخر عبر الإقليم الوطني بموجب قرار من وزير الدفاع الوطني، ويخضع المعهد لإدارة ضابط سامٍ من صفوف الدرك الوطني، ويتم تعيينه وإنهاء مهامه بموجب مرسوم رئاسي بناءً على اقتراح من وزير الدفاع، أما فيما يخص الاختصاصات الوظيفية، فقد حددت المادة 4 من المرسوم رقم 04- 183[2] مهام المعهد وفق الآتي[3]:

1- إنجاز الخبرات والمعاينات العلمية ضمن مرحلتي التحري الأولي والتحقيق القضائي، بهدف استخلاص الأدلة المادية الكفيلة بتحديد هويات مرتكبي الجنايات والجنح.

---

[1] محمودي سعيد، مرجع سابق، ص204.

[2] **المرسوم الرئاسي رقم 04-183** المؤرخ في 26 يونيو 2004، المتعلق بإحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، ج ر، العدد41، الجزائر، الصادر في 2004.

[3] معتوق أم الخير، مرجع السابق، ص69.

2- تقديم المساندة العلمية في التحريات المعقدة عبر تفعيل آليات وتقنيات الشرطة العلمية المتطورة.

3- إعداد الدراسات والبحوث التحليلية الرامية إلى فهم ظاهرة الإجرام ووضع استراتيجيات للوقاية منها والحد من انتشارها.

4- استحداث وتسيير قواعد بيانات وبنوك معلومات متخصصة لدعم العمل الجنائي.

5- المشاركة الفعالة في صياغة و رسم معالم السياسة الجنائية الوطنية بما يضمن مكافحة فعالة للجريمة.

6- توظيف التقنيات الدقيقة والابتكارات العلمية في كافة البحوث والدراسات المتعلقة بالظاهرة الإجرامية.

في إطار مكافحة الجريمة الإلكترونية، يعمل الدرك الوطني على التحديث المستمر لأداء وحداته المتخصصة، متمثلة في مركز الوقاية من جرائم الإعلام الآلي والمعهد الوطني للأدلة الجنائية وعلم الإجرام، ويرتكز هذا التطوير على محاور أساسية تشمل الجوانب التنظيمية، والبرامج التكوينية، ودعم الوحدات بأحدث التجهيزات التقنية، وذلك لرفع مستوى الجاهزية والفعالية في مجابهة الجرائم الإلكترونية المتطورة والمعقدة.[1]

ثالثاً: المصلحة المركزية لمحاربة الجريمة الالكترونية للأمن الوطني

نظراً للتعقيدات الفنية التي تتسم بها الجرائم المعلوماتية، بادرت الدول المتقدمة إلى تأسيس وحدات شرطية متخصصة تضم نخبة من الخبراء التقنيين، وقد عنيت هذه الوحدات بتأهيل كوادرها عبر برامج تدريبية مكثفة تغطي الجوانب الفنية والقنية، بما يضمن تعزيز قدراتهم على كشف الجرائم واستباق وقوعها، لا سيما من خلال تفعيل الرقابة على الفضاءات العامة مثل نوادي الإنترنت التي تمثل بيئة مواتية لهذه الأنشطة، وتعد فرنسا من النماذج

[1] دليلة العوفي، "**آليات محاربة الجريمة المعلوماتية (دراسة حالة الجزائر 2006- 2009)**"، أطروحة دكتوراه في علوم الإعلام والاتصال، كلية علوم الإعلام والاتصال، جامعة إبراهيم سلطان شيبوط، جامعة الجزائر 3، الجزائر، 2020، ص 323 -324.

السباقة في هذا السياق، حيث أسست عام 2000 الديوان الوطني لمكافحة الإجرام المرتبطة بتكنولوجيات الإعلام والاتصال.[1]

تجسيدًا لمساعي المديرية العامة للأمن الوطني في تكييف منظومتها الأمنية مع التحول الرقمي الشامل، تم استحداث المصلحة المركزية لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، شكلت هذه المصلحة في مرحتها التأسيسية نواة أمنية متخصصة، استهدفت وضع الحجر الأساس لمنظومة مكافحة الجريمة الإلكترونية على مستوى المديرية العامة للأمن الوطني سنة 2011، ليتم بعدها إنشاء المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ضمن الهيكل التنظيمي لمديرية الشرطة القضائية في جانفي 2015، كما سعت المديرية إلى خلق وحدات متخصصة كل وحدة تعالج نوع معين من الجرائم.[2]

وهي المصلحة التي تعنى هذه بأداء مهمتين أساسيتين هما:

1- الوقاية من الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال: ترتكز جهود المصلحة على رصد الأفعال الإجرامية وتحليل خطورتها، خاصة تلك التي تستهدف المستخدمين أثناء تصفحهم للشبكة العنكبوتية، ولا سيما الجرائم الماسة بالأشخاص وحرمة حياتهم الخاصة، ولتحقيق ذلك، تعتمد المصلحة إستراتيجية توعوية شاملة عبر تنظيم حملات تحسيسية في مختلف ولايات الوطن، وذلك من خلال الأبواب المفتوحة، والأيام الدراسة، وإلقاء محاضرات أكاديمية في الجامعات لرفع الوعي بمخاطر الفضاء الرقمي.[3]

2-أما على صعيد المكافحة، فتتمتع المصلحة المركزية بحزمة من المهام العملياتية والتقنية، ومن أبرزها[4]:

---

[1] دلية العوفي، مرجع السابق، ص 315.

[2] إدريس عطية، "**مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري**"، مجلة مصداقية، صادرة عن المدرسة العليا العسكرية للإعلام والاتصال، المجلد01، العدد 01، الجزائر، 2019، ص 115، ص ص 100- 121.

[3] دليلة العوفي، نفس مرجع، ص 317.

[4] نفس المرجع، ص318.

- تقديم الدعم الفني للسلطات القضائية في التحريات الرقمية، وتولي مهام تجميع الأدلة وإعداد الخبرات القضائية المتخصصة.
- تعزيز التعاون المشترك مع مختلف الفاعلين والشركاء في المجال الأمني.
- المشاركة الفعالة في التحقيقات ذات الأبعاد الوطنية والدولية لملاحقة الجرائم الإلكترونية.
- حماية الأنظمة المعلوماتية الوطنية عبر تفعيل آليات "اليقظة التكنولوجية" ورصد المحتويات غير القانونية على الشبكات المفتوحة.
- الإشراف على التكوين النوعي لفرق مكافحة الجريمة الإلكترونية الموزعة عبر ولايات الوطن.

تتبنى المصلحة المركزية لمكافحة الجرائم الإلكترونية إستراتيجية مزدوجة ترتكز على الحماية الإستباقية والردع العملياتي، بهدف تحصين الفضاء الرقمي الوطني، وتتنوع آليات عملها لتشمل الإسناد التقني للقضاء، وتفعيل التعاون الأمني العابر للحدود، وتأمين البنية التحتية المعلوماتية، كما تتولى المصلحة أهمية قصوى لبناء الوعي المجتمعي وتطوير القدرات التخصصية لكوادرها، لضمان استجابة فعالة للتحديات التكنولوجية المتسارعة.

رابعاً: المنظومة الوطنية لأمن الأنظمة المعلوماتية الموضوعة لدى وزارة الدفاع الوطني

عمد المشرع الجزائري إلى تعزيز تدخّله في مجال الأمن السيبراني من خلال استحداث آليات جديدة تحت إشراف وزارة الدفاع الوطني، إدراكاً منه بأن حماية الفضاء السيبراني هي ركيزة أساسية لسيادة الدولة لأمن قضايا الأمن السيبراني ترتبط ارتباطاً وثيقاً بالدولة الجزائرية، وقد جاء ذلك إسناداً إلى أحكام المادة 03 من المرسوم الرئاسي 05/20[1]، التي أرست القواعد المؤسساتية " للمنظومة الوطنية لأمن الأنظمة المعلوماتية"، والتي تتألف هيكلياً من المجلس الوطني والوكالة الوطنية لأمن الأنظمة المعلوماتية.[2]

1 **المرسوم الرئاسي رقم 20-05، المؤرخ** في 10ديسمبر2020، المتضمن وضع المنظومة الوطنية لأمن الأنظمة المعلوماتية، ج ر ، العدد04، الصادر بتاريخ 26 جانفي2020.

2 حزام فتيحة، "**الحماية المؤسساتية للأنظمة الرقمية في الفترة التشريعية الممتدة من 2009- 2020**"، المجلة الأكاديمية للدراسات الاجتماعية والإنسانية، جامعة حسيبة بن بوعلي، الشلف، المجلد13، العدد02، الجزائر 2021،ص280، ص ص -270 289.

الفرع الثاني: الآليات الإدارية المختصة لمكافحة الجريمة الإلكترونية وتحقيق الأمن السيبراني في الجزائر

سعياً من المشرع الجزائري لضمان وحدة الانسجام العملي ومنع أي تقاطع في الصلاحيات بين مختلف الجهات المتداخلة في مجالي الأمن والدفاع الوطني، أرسى إطاراً قانونياً وتنظيمياً دقيقاً لاحترام الإطار الإداري المنظّم لاختصاصات الهيئات المدنية والعسكرية والتقنية، يهدف هذا التأطير إلى حوكمة إدارة الإستراتيجية الوطنية للأمن السيبراني عبر توزيع هيكلي للمؤسسات، ويشمن كفاءة الأداء وسرعة الاستجابة الإستباقية للمخاطر السيبرانية الناشئة.

كما يعكس هذا التوجّه إدراكًا متزايد الأهمية الحوكمة الرشيدة في مجال الأمن السيبراني، من خلال إرساء آليات للتعاون وتبادل المعلومات بين مختلف الفاعلين، وتفادي الازدواجية في اتخاذ القرارات أو تنفيذ المهام، بما يضمن حماية أفضل للأنظمة المعلوماتية والسيادة الرقمية للدولة، ويمكن إبراز ذلك من خلال النقاط الآتية:

أولاً: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

تأسست الهيئة الوطنية للوقاية من الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال ومكافحتها بموجب قانون سنة 2009 تحت وصاية وزارة العدل، ومع ذلك، ظلّ انطلاقها الميداني رهين صدور المرسوم الرئاسي رقم 15- 261[1]، الذي منحها الهيكل التنظيمي والوسائل الإجرائية اللازمة لممارسة مهامها، وبموجب هذا الإطار، أصبحت الهيئة المحرك الأساسي للتنسيق بين الفاعلين، وتطوير آليات الرصد التقني والتحري الرقمي[2].

تعرَّف هذه الهيئة حسب المادة 02 من المرسوم الرئاسي رقم 183/20 على أنها سلطة إدارية مستقلة، مُحصنة بالشخصية المعنوية والاستقلال المالي، وتندرج تنظيمياً تحت الوصاية المباشرة لـ رئاسة الجمهورية، وإذ يتحدد مركزها القانوني في مدينة الجزائر، فقد

---

[1] **مرسوم رئاسي رقم 15-261**، المؤرخ بتاريخ 24 ذي الحجة عام 1436 الموافق 8 أكتوبر سنة 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 37، المؤرخ في 18 يونيو 2015.

[2] محمودي سعيد، مرجع سابق، ص 203 -204.

أجاز المشرع نقل مقرها عبر التراب الوطني بموجب مرسوم رئاسي، وتتكوّن من مجلس توجيه ومديرية عامة، يعملان تحت الإشراف المباشر لرئيس الجمهورية، مع إلزامهما بضمان الشفافية من خلال رفع تقارير دورية توثق حصيلة نشاطاتهما.[1]

تتألف الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهامن نواتين أساسيتين: نواة توجيهية تضم أعضاء من الحكومة ومسؤولي الهيئات الأمنية وقضاة من المحكمة العليا (بناءً على تعيين المجلس الأعلى للقضاء)، ونواة عملياتية تضم قضاة وممارسين من سلك الشرطة القضائية التابعين للأمن الوطني والدرك الوطني ومصالح الاستعلامات العسكرية، ويمارس هذا الطاقم المشترك مهامه تحت مظلة أحكام قانون الإجراءات الجزائية، بما يضمن شرعية وتخصص التحريات التقنية.[2]

أسندت إلى هذه الهيئة مهمة اقتراح مكونات الإستراتيجية الوطنية للوقاية من الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال ومكافحتها، مع تولي الدور القيادي في تنشيط وتنسيق الجهود الوقائية المشتركة، وتمتد ولايتها لتشمل تقديم الإسناد الفني والتقني للجهات القضائية ومصالح الشرطة القضائية، عبر تزويدها بالتدفق المعلوماتي اللازم ونتائج الخبرات القضائية المتخصصة، كما أُوكِل إليها دورٌ سيادي يتمثل في الاعتراض الوقائي للاتصالات الإلكترونية، كآلية إستباقية للكشف عن الجرائم ذات الطابع الإرهابي أو التخريبي التي تستهدف تقويض أمن الدولة.[3]

---

3 المادة 02 من **المرسوم الرئاسي رقم 20-283** المؤرخ في 13 يوليو 2020، المتضمن إعادة تنظيم الهيئة الوطنية الوقاية من جرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 40، الصادرة بتاريخ 18 يوليو 2020.

[2] بارة سمير، مرجع سابق، ص274.

[3] المرجع نفسه، ص275.

تتحدد المهام الأساسية الموكلة للهيئة في سياق الرؤية الوطنية للأمن السيبراني وفق المحاور الآتية[1]:

1- استثمار المعطيات المتاحة لرصد الأنشطة غير المشروعة في الفضاء الرقمي، مما يتيح توجيهاً أمثلاً للموارد البشرية والمالية لسد الثغرات الأمنية، لا سيما في ظل التحولات المتسارعة التي تفرضها تكنولوجيا الإعلام والاتصال.

2- تعزيز التنسيق بين مختلف الفاعلين في هذا المجال، مع التأكيد على ضرورة التعاون بين القطاعين العام والخاص وكذا المجتمع المدني، بهدف ترسيخ ثقافة التصدي لكل الممارسات غير القانونية في الفضاء الرقمي، وضمان حماية الحقوق والحريات الأساسية.

3- السعي لتأسيس إطار معلوماتي مركزي (وحدة بحث) يتولى جمع البيانات والإحصائيات الدقيقة، لتحليل التهديدات بشكل مستمر وتقديم الحلول التقنية الملائمة.

4- التنسيق بين الأجهزة الأمنية والمالية والإدارية ذات الصلة لضبط المسؤوليات وتشديد الرقابة على القطاعات الحيوية المستهدفة من قبل محترفي الإجرام الإلكتروني، ويأتي ذلك دعماً لتوجه الدولة نحو "الحوكمة الإلكترونية" الشاملة، مع الاسترشاد بمعايير البنك الدولي التي تهدف إلى تحويل طبيعة العلاقة بين المؤسسات الحكومية والمواطنين وقطاع الأعمال، بما يعزز الثقة والشفافية[2].

5- الإسهام في إعداد الأرضية اللازمة لتجسيد الإستراتيجية الوطنية للوقاية من الجرائم الإلكترونية ومكافحتها، وهو ما يعكس الأهمية البالغة لإدارة الأمن السيبراني في حماية المصالح العليا للدولة.

6- ترسيخ الجانب التوعوي كركيزة أساسية للحد من الجرائم المعلوماتية، من خلال استهداف كافة الفئات ذات الصلة بالمنظومة الرقمية، ولتحقيق ذلك، تتبنى الدولة برنامجاً متكاملاً يشمل الوسائط السمعية والبصرية، واللقاءات العلمية، والدورات التدريبية، والحملات

---

[1] بوازدية جمال، مرجع سابق، ص 81.

[2] أستاذ شريف بسام، "**واقع الحوكمة الإلكترونية في الدول العربية** "، مجلة العلوم الاجتماعية والإنسانية، جامعة الجزائر3، العدد6،، جوان 2016، ص 161، ص ص 157- 170.

الإعلانية، بمشاركة فعالة من مؤسسات الدولة والمجتمع المدني، لتتكامل التوعية مع الأطر القانونية والتقنية والتعاون الدولي.

إذًا تعد الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها جهازًا مختصًا بتعزيز الأمن السيبراني في الجزائر، ولك من خلال رصد الجرائم الإلكترونية، وتنسيق الجهود الأمنية والقضائية، وتقديم الدعم التقني لحماية الفضاء الرقمي.

ثانياً: مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة

نظرًا للأهمية الإستراتيجية والحساسية البالغة لقطاع الدفاع الوطني، استحدث المشرّع بتاريخ 11 جوان 2015 مصلحة متخصصة تابعة لدائرة الاستعمال والتحضير بأركان الجيش الوطني الشعبي. وقد أُنيطت بها مسؤولية تحصين المنظومات والمنشآت الحيوية في الجزائر ضد كافة التهديدات السيبرانية، بناءً على إستراتيجية دفاعية شاملة ترتكز على سبعة محاور أساسية:[1]

1- المحور الوظيفي والتنظيمي: يهدف إلى هيكلة أعمال الدفاع السيبراني داخل الجيش الوطني الشعبي ضمن تسلسل قيادي وتنظيمي محكم، بما يضمن انسجام الأداء وفعالية العمليات الميدانية.

2- المحور القانوني: يتمثل في العمل المستمر على تحيين وتطوير الإطار القانوني المنظم لاستعمال تكنولوجيات الإعلام والاتصال بصفة عامة، مع التركيز على تأمين وحماية المنظومات المعلوماتية العسكرية بشكل خاص.[2]

3- محور الموارد البشرية: يسعى إلى بناء وتأهيل كادر بشري تقني ذو كفاءة عالية، باعتبار الجاهزية البشرية حجر الزاوية لضمان الدمج الناجح للأمن السيبراني في كافة الأنشطة العملياتية والإدارية للجيش.

---

[1] محمد بوكبشة،"**الأمن والدفاع السيبراني أولوية قصوى**"، مجلة الجيش، العدد 51، أكتوبر 2017،ص 45، ص ص 30 -51.

[2] آسيا العمراني، مرجع سابق، ص74.

4- المحور التقني: يرتكز على التحديث المستمر للقدرات التقنية المتصلة بآليات الحماية، الكشف، والرد على الهجمات، مع تفعيل نظام يقظة دائم لمواكبة الأساليب المتطورة التي ينتهجها المهاجمون.

5- محور الوقاية والتحسيس:يُعنى بحماية وتوعية مستخدمي الجيش الوطني الشعبي من مختلف المخاطر والتهديدات الناجمة عن استعمال تكنولوجيات الإعلام والاتصال، سواء في الإطار المهني أو الشخصي، وذلك بشكل دائم وممنهج.

6- محور البحث والتطوير: يمثل ركيزة جوهرية تعتمد على ابتكار وتطوير أدوات تقنية وطنية وحلول برمجية خاصة بهياكل البحث التابعة للجيش، لضمان استقلالية أنظمة الحماية ضد التهديدات المتقدمة.

7- محور التعاون الدولي: يهدف إلى تعزيز الشراكات في مجال الدفاع السيبراني مع جيوش الدول الصديقة والشريكة، مما يتيح للجيش الوطني الشعبي تبادل الخبرات الميدانية واكتساب أحدث الوسائل التكنولوجية المتطورة.

ومنه تختص مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة بحماية الأنظمة والمنشآة الحيوية للجيش من الهجومات الإلكترونية، من خلال تطوير الوسائل التقنية، وتأهيل الكفاءات وتعزيز التعاون الوطني والدولي في مجال الأمن السيبراني.

ثالثاً: القطب الجزائري الوطني لمكافحة جرائم تكنولوجيات الإعلام والاتصال

استحدث المشرع الجزائري هذا القطب الجزائي بموجب الأمر 21 - 11[1] المتمم لقانون الإجراءات الجزائية ، بتخصيص باب جديد بعنوان القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ضمن المواد من 335 إلى 342[2] من قانون الإجراءات الجزائية، يقع هذا القطب في دائرة اختصاص مجلس قضاء الجزائر، حيث يمارس وكيل الجمهورية لدى القطب الجزائي الوطني صلاحياته على كافة إقليم وطني ،

[1] **الأمر رقم 21-11**، المؤرخ في 15 محرم عام 1443 الموافق ل 24 غشت 2021، يتعلق بمراقبة دستورية للأمر الذي يتمم الأمر رقم 66-155، المؤرخ 8 يونيو سنة 1966، المتضمن ق ا ج ، ج ر ، العدد 65، الصادر في 26 غشت سنة 2021.

[2] المواد من 335 إلى 342، من **القانون رقم 25-14**، المتضمن ق ا ج ، سالف الذكر.

حسب مادة 336 من قانون إجراءات جزائية ، ويمتد إلى جرائم تكنولوجيات الإعلام والاتصال المعقدة حسب المواد 337 إلى 338 [1]من قانون إجراءات جزائية.

منح المشرّع هذا القطب اختصاصًا وطنيًا بهدف تجاوز الصعوبات التي قد تعترض الجهات القضائية، وعليه يمكن التطرق إلى ما يلي:

1- الاختصاص النوعي:

يرتبط الاختصاص النوعي للمحاكم بطبيعة الجريمة المرتكبة، والتي يتم تكييفها بناءً على العقوبة المقررة لها في قانون العقوبات أو النصوص التشريعية المكملة له. وعليه، فإن تحديد الاختصاص النوعي يستوجب ابتداءً حصر الوقائع المادية ومطابقتها مع النموذج القانوني للجريمة، ومن ثمَّ تصنيفها قانوناً (جناية، جنحة، أو مخالفة) وفقاً للحد الأقصى للعقوبة المقررة لها، وبالرجوع إلى أحكام المادة 335 والمادة 337[2] ، فإن القطب المستحدث يخلص بمعالجة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المرتبطة بها.

2- الاختصاص الإقليمي:

منح المشرع الجزائري القطب المستحدث اختصاصا وطنيا بموجب المادة 336[3] ليمارس بذلك كل من وكيل الجمهورية وقاضي التحقيق ورئيس القطب اختصاصهم عبر كافة الإقليم الوطني.[4]

ويتضح أن القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال يعتبر آلية قضائية إدارية متخصصة أنشئها المشرع الجزائري لمواجهة الجرائم الإلكترونية، حيث يتمتع باختصاص وطني يسمح له بمعالجة هذا النوع من الجرائم عبر

---

[1] المواد من 337 إلى 338، من القانون رقم 25-14، المتضمن ق ا ج ، سالف الذكر.

[2] المادة 335 والمادة 337، من القانون رقم 25-14، المتضمن ق ا ج ، سالف الذكر

[3] المادة 336 من القانون رقم 25-14، المتضمن ق ا ج ، سالف الذكر.

[4] بوقرة جمال الدين، "**القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا إعلام والاتصال**"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف مسيلة، المجلد 7، العدد 1، الجزائر، جوان 2020،ص 1680، ص ص 1673- 1693.

كامل التراب الوطني، كم يختص بالتحقيق والمتابعة القضائية للجرائم المرتبطة بتكنولوجيات الإعلام والاتصال، مما يساهم في تعزيز فعالية العدالة ومواكبة التطور التكنولوجي في مجال مكافحة الجريمة الإلكترونية.

المبحث الثاني

تدابير تعزيز الأمن السيبراني في الجزائر

يشهد العالم تحولات رقمية متسارعة أفرزت تغيّرات عميقة في مختلف مجالات الحياة، خاصة مع الانتشار الواسع لتكنولوجيات الإعلام والاتصال واعتمادها بشكل متزايد في تسيير المرافق والخدمات الحيوية، ونظرًا للطبيعة العابرة للحدود التي تتميز بها الجريمة الإلكترونية، لم يعد التصدي لها مقتصرًا على التشريعات الوطنية فحسب، بل أصبح يتطلب تعاونًا دوليًا قائمًا على اتفاقيات ومعاهدات تنظم آليات مكافحة هذه الجرائم وتعزز الأمن السيبراني.

انخرطت الجزائر في الجهود الدولية والإقليمية عبر تبني العديد من الاتفاقيات العربية والدولية المتعلقة بمكافحة الجرائم الإلكترونية وتوطيد التعاون في مجال الأمن السيبراني **(المبحث الأول)**، وذلك في سبيل الاستفادة من الخبرات الدولية وتبادل المعلومات حول التهديدات السيبرانية العابرة للحدود، بما يساهم في توحيد الجهود القانونية.

التحول الرقمي في الجزائر، رغم ايجابياته المتعددة، رافقه تصاعد في الجريمة الإلكترونية التي أصبحت تهديدًا متعدد الأبعاد يمس استقرار الوسط السيبراني، كما أن الأمن السيبراني يواجه جدلية التهديد والاستجابة في ظل تزايد الهجمات ووجود تحديا تقنية وقانونية وتنظيمية **(المبحث الثاني)**، وعليه فإن فهم هذه الانعكاسات والتحديات يعد أساسيًا لتعزيز فعالية الأمن السيبراني في الجزائر.

المطلب الأول

الاتفاقيات الجزائرية لتعزيز الأمن السيبراني

لقد تصدرت الجرائم الإلكترونية قائمة التهديدات المستحدثة الأكثر خطورة وتعقيداً، وباتت تشكل تحدياً جوهرياً يمس مفهوم الأمن القومي والدولي في أبعاده الشاملة، وأمام هذه التحولات الرقمية المتسارعة، أدركت دول العالم، ومن ضمنها الجزائر، حتمية مراجعة وتحديث أطرها القانونية والأمنية لمواكبة الطفرة الإجرامية الجديدة.

إذ أثبتت التجربة أن المقاربات التقليدية لم تعد كافية لاحتواء مخاطر الفضاء الرقمي، وهو ما استوجب تبني إستراتيجية أكثر انفتاحاً وشمولية، تضع "التعاون الدولي والإقليمي" كركيزة أساسية لمجابهة هذه الظاهرة، سواء في شقها الوقائي، أو في جوانب الملاحقة القضائية وتبادل المعلومات والخبرات التقنية.

اكتسبت الاتفاقيات الدولية والإقليمية أهمية متزايدة، باعتبارها إطارًا قانونيًا وتنظيميًا يهدف إلى تنسيق الجهود بين الدول، وتوحيد الرؤى بشأن آليات مكافحة الجريمة السيبرانية، أسهمت هذه الاتفاقيات في دعم التوجه الجزائري نحو تعزيز أمنه السيبراني، وذلك ضمن ثلاثة مستويات رئيسية ومتكاملة، على رأسها الاتفاقية الجزائرية على المستوى العربي في **(الفرع الأول)**، والاتفاقيات الجزائرية على المستوى الأوروبي والدولي **(لفرع الثاني)**.

الفرع الأول: الاتفاقية الجزائرية على المستوى العربي

تُشير الدراسات الأكاديمية وتحليلات المؤسسات المختصة في الأمن السيبراني إلى وجود فجوات جوهرية في حماية الأنظمة المعلوماتية للدول العربية، ورغم توفر بعض الإمكانات البشرية والمادية، إلا أنها لم تنجح بشكل كافٍ في تحييد المخاطر المتنامية، وهو ما تعكسه الثغرات المستمرة والسلبيات التي لا تزال تفرض نفسها على المشهد الرقمي، [1] وأبرزها:

1- تعرف المنظومة التشريعية والتنظيمية في الدول العربية بطئا في التطور، مما يجعلها غير شاملة لكثير من الجوانب الحساسة المرتبطة بالفضاء السيبراني، كما يُلاحظ أن معالجة

[1] بوازدية جمال، مرجع سابق، ص1285.

التهديدات تتم غالبا من خلال تفعيل الجانب العقابي، سواء بإدراج نصوص جديدة أو تعديل القوانين القائمة، وهو ما لا ينسجم مع التوجهات العالمية القائمة على المرونة والتكيف مع التطورات[1].

2- اختلال معادلة الموارد البشرية: وجود فجوة حادة بين الكفاءات المتاحة حالياً وبين المتطلبات الفعلية لمواجهة التهديدات الحديثة، حيث يبرز عجز واضح في تأهيل كوادر قادرة على مواكبة الطفرات التكنولوجية المتلاحقة.

3- ضعف الآليات التنفيذية والمعايير التقنية: تفتقر الإجراءات الأمنية الميدانية للمطابقة مع المواصفات الدولية، وهي حقيقة تؤكدها مؤشرات "الاتحاد الدولي للاتصالات"، ويعود ذلك أساساً إلى العوائق البيروقراطية، فضلاً عن اتساع الفجوة الرقمية بين الدول العربية والدول المتقدمة، مما يعكس ضعفاً في آليات التعاون الدولي.

4- ضعف جدية التعاون على المستوى الداخلي، حيث تشير الأرقام المصرح بها من قبل الأجهزة الأمنية إلى تزايد نسبة الاختراقات، مما يدل على محدودية فعالية هيئات التنسيق في إدارة ملف الأمن السيبراني.

وأمام هذه التحديات، اتجهت الجزائر في مرحلة أولى إلى التعامل مع هذه الجرائم من خلال تفعيل المبادئ العامة المعترف بها دوليا في مجال مكافحتها، لاسيما تبادل المعلومات، وتبادل الخبرات، وتقديم المساعدة الفنية.

أولاً: تفعيل آلية تبادل المعلومات

استجابةً لتصاعد النشاط الإجرامي الرقمي وتعقيدات السيطرة عليه، بادرت الجزائر إلى تفعيل الأحكام المتعلقة بتبادل المعلومات والمساعدة التقنية، استناداً إلى المبادئ المستقرة في الصكوك الدولية وتوصيات مؤتمر الأمم المتحدة السادس لمنع الجريمة.

[1] في قراءة **للاتفاقية العربية لمكافحة جرائم تقنية المعلومات المبرمة في 2010**، يتضح أن التهديدات الخطيرة التي تسببها الجرائم الالكترونية للمساس بالأمن والاستقرار، أصبحت تشكل إحدى أهم الاهتمامات لدى صناع القرار للدول العربية.

وتُعد المعلومة الركيزة الأساسية في المنظومة الدفاعية؛ فمن الناحية الوقائية، تشكل القاعدة الجوهرية لرصد وتتبع الأنشطة الإجرامية قبل وقوعها، أما من الناحية الزجرية (العقابية)، فتمثل دعامة موثوقة تعتمد عليها الأجهزة القضائية والأمنية لإنفاذ القانون وضبط الأدلة الرقمية[1].

ثانياً: تبادل الخبرات والمساعدة التقنية والقضائية

سعت الجزائر إلى تعزيز التكامل بين المؤسسات الأمنية والقضائية العربية من خلال توسيع أطر التعاون لتشمل:[2]

1- الجانب التكويني والاستشاري: تبادل الزيارات الميدانية وتنظيم دورات تدريبية ولقاءات تشاورية للاطلاع على السياسات الجنائية العربية، والاستفادة من النماذج التشريعية والآليات التقنية والقدرات البشرية المسخرة لحماية الفضاء السيبراني.

2- التعاون القضائي الميداني: تفعيل آليات المساعدة التقنية الثنائية والمتعددة الأطراف، لا سيما في مجالي الإنابة القضائية وتسليم المجرمين. ورغم التحديات التي تواجه عملية التسليم —سواء المرتبطة بمبدأ السيادة الوطنية أو التحجج بملفات حقوق الإنسان— فقد نجحت الجزائر في تجاوز هذه العقبات عبر إبرام اتفاقيات تعاون قضائي متخصصة تضمن الحقوق الموضوعية والإجرائية لكافة الأطراف.

ثالثاً: مبادرات البحث العلمي والتطوير التشريعي

واكبت الجزائر الثورة المعلوماتية المتسارعة بتعزيز انخراطها في المنظومة القانونية الدولية والعربية، ويتجلى ذلك في[3]:

---

[1] **اتفاقية الرياض العربية للتعاون القضائي** ، التي وافق عليها مجلس وزراء العدل العرب في المؤتمر العربي الأول بتاريخ أفريل 1983، التي قضت في المادة الأولى على ضرورة تبادل المعلومات بين الدول الأطراف فيما يتعلق بالنصوص التشريعية والتنسيق بين الأنظمة القضائية، كما قضت المادة الخامسة منها بأن ترسل وزارة العدل في الدول الأطراف آخر بيانات الأحكام القضائية النهائية الصادرة ضد المواطنين أو الأشخاص المولودين أو المقيمين في إقليميا.

[2] بوازدية جمال، مرجع سابق، ص 1286.

[3] المرجع نفسه، ص 1287.

1- الاتفاقيات الإطارية: الانضمام الفعال للاتفاقية العربية لمكافحة الإرهاب (1998) والاتفاقية الدولية لمكافحة الجريمة المنظمة عابرة الحدود (2000).

2- المعايير الأمنية: التنسيق بين الدوائر المختصة لتبني مقاييس عالمية في الأمن السيبراني وتجهيز الأرضية القانونية لسن تشريعات وطنية متخصصة.

3- المساهمة الأكاديمية (مركز البحوث والدراسات): برز الدور الجزائري من خلال مشاركة فرق من الخبراء القانونيين في أشغال مركز البحوث التابع لجامعة الدول العربية، حيث ساهموا بفعالية في صياغة ومناقشة مشاريع القوانين والاتفاقيات لمواكبة التحولات التكنولوجية، والتي توجت بمشاريع إستراتيجية أبرزها "الاتفاقية العربية لضمان أمن وسلامة الفضاء السيبراني."

المحاور الأساسية التي عالجتها الاتفاقية:

- إرساء الثقة في الفضاء السيبراني، باعتبارها الغاية الجوهرية التي تسعى الاتفاقية إلى تحقيقها.
- توظيف إمكانيات تكنولوجيات الإعلام والاتصال بما يخدم مسارات التنمية والتقدم البشري.
- تعزيز أمن المجتمعات العربية في البيئة الرقمية، من خلال دعم التعاون بين الحكومات، واعتماد أطر تشريعية وتنظيمية متكاملة ومتناسقة، تقوم على تبادل المعلومات بين الجهات المختصة، وتكثيف التنسيق بين السلطات القضائية لمواجهة الجرائم السيبرانية[1].

ويتضح أنه على الرغم من التحديات القائمة المتمثلة في الفجوات التشريعية ونقص الخبرات المتخصصة وعقبات التنسيق، فقد تبلور توجه جاد نحو تفعيل التعاون الدولي لمجابهة الجرائم السيبرانية، وفي هذا الإطار، بادرت الجزائر بمواكبة هذه التحولات عبر تبني مقاربة شاملة ترتكز على إرساء المبادئ الدولية، لاسيما في مجالات تبادل المعلومات والخبرات وتقديم الدعم التقني، كما عززت الجزائر دورها في الفضاء العربي من خلال

[1] بوازدية جمال، مرجع سابق، ص 1287

الالتزام بالاتفاقيات الثنائية والجماعية والمشاركة الفعالة في المبادرات الإقليمية الرامية لتحصين الأمن الرقمي، بالتوازي مع جهودها المحلية في تحديث الأطر التنظيمية ورفع مستوى التنسيق بين المؤسسات المختصة، سعيًا منها لبناء بيئة رقمية آمنة ومستقرة تدعم مسارات التنمية وتواجه التهديدات المتصاعدة بفعالية.

الفرع الثاني: الاتفاقيات الجزائرية على المستوى الأوروبي والدولي

أفرز التطور المتسارع لتقنيات الإعلام والاتصال تحولات جذرية حوّلت الفضاء السيبراني إلى ساحة حيوية للتبادل الدولي، وفي الوقت ذاته، بيئة خصبة للأنشطة الإجرامية المستحدثة، استجابةً لهذه التحولات العالمية، وضعت الجزائر قضية الأمن السيبراني في صلب اهتماماتها الإستراتيجية، حيث عملت على تحديث ترسانتها القانونية وهيكلها التنظيمي، بالتوازي مع الرفع من كفاءة قدراتها المؤسساتية والتقنية.

ولم يقتصر مجهودها على المستوى الداخلي، بل امتد ليشمل المساهمة الفعالة في المساعي الإقليمية والدولية لمجابهة الجرائم المعلوماتية، مع التركيز على تفعيل قنوات تبادل الخبرات والمساعدة التقنية بما يواكب المعايير الدولية ويعزز حصانتها ضد التهديدات الرقمية المتزايدة.

أولاً: البعد الأوروبي والمتوسطي في الإستراتيجية الجزائرية

في سياق تفعيل "اتفاقية الشراكة الأورو– متوسطية" الموقعة في 22 أفريل 2002، والتزاماً بمخرجات الاتفاق الثنائي مع فرنسا (أكتوبر 2003) بشأن التعاون الأمني ومجابهة الجريمة المنظمة، انتهجت الجزائر مقاربة إقليمية مستحدثة للتصدي للجرائم السيبرانية، مركزةً على تعزيز التنسيق في حوض المتوسط.

وبهدف الاستفادة من التجربة الأوروبية في هذا المجال، تم تنظيم عدة لقاءات داخل الجزائر جمعت خبراء وفاعلين من مختلف الهيئات الوطنية، إضافة إلى مختصين أجانب، وقد أسفرت هذه المشاورات عن مجموعة من التوصيات، من أهمها[1]:

[1] فارس محمد العمارات، مرجع سابق، ص159

- العمل على ملاءمة القوانين الوطنية مع الصكوك الدولية، وفي مقدمتها "اتفاقية بودابست"[1]، لضمان استجابة قانونية فعالة تتوافق مع المعايير العالمية، مع التمسك الصارم بمبادئ السيادة الوطنية وحماية الحقوق والحريات الأساسية.
- الرفع من كفاءة المصالح الأمنية المتخصصة مادياً وبشرياً، وتطوير آليات التنسيق البيني لضمان سرعة الاستجابة للتهديدات الرقمية.
- تكريس الاعتماد على "الدليل الإلكتروني" كركيزة أساسية في الخصومة الجنائية، وضمان استخلاصه ومعالجته وفقاً للأصول القانونية والتقنية السليمة.
- إرساء برامج تكوينية متقدمة للقضاة والفاعلين في الأجهزة الأمنية، تعتمد مناهج علمية دولية لمواكبة القفزات المتسارعة في عالم الإجرام المعلوماتي.
- التعجيل بصياغة وتنفيذ إستراتيجية وطنية متكاملة (تنظيمياً وتقنياً) تهدف إلى تحجيم المخاطر السيبرانية وحماية الفضاء الوطني[2].

ثانيًا: الأبعاد الدولية للتعاون السيبراني في الإستراتيجية الجزائرية

أفرزت مرحلة ما بعد الحرب الباردة واقعاً عالمياً جديداً قائماً على الانفتاح وحرية التبادل، حيث لعب اقتصاد المعرفة وتنامي تكنولوجيات الاتصال دوراً محورياً في إلغاء الحدود الجغرافية وتسهيل المعاملات العابرة للقارات، إلا أن هذا الفضاء الرقمي المفتوح تحول تدريجياً إلى ساحة للأنشطة الإجرامية المستحدثة، مما وضع السلم والأمن الدوليين أمام تحديات غير مسبوقة استوجبت استجابة عالمية موحدة لحماية الحريات الفردية والأمن الجماعي.

وفي إطار "حوكمة الإنترنت"، تضافرت جهود الهيئات الأممية والمنظمات المتخصصة (مثل الاتحاد الدولي للاتصالات) لوضع معايير تقنية وقانونية لضمان سلامة التدفقات المعلوماتية، ويمكن حصر أبرز المحطات والآليات الدولية في هذا المجال فيما يلي:

---

[1] **اتفاقية بيدا بيست الأوروبية**، حول الإجرام المعلوماتي المصادق عليها من طرف المجلس الأوروبي بتاريخ 2001.11.23، دخلت حيز التنفيذ سنة 2004 تعتبر بمثابة الأرضية القانونية التي أعطت دفعا للدول الأوروبية خاصة ودول العالم عامة للإسراع في سن قوانين وفرض إجراءات قانونية وإدارية المحاصرة الإجرام السيبراني، خاصة وان أهم معضلة تواجه التعاون الدولي تسليم المجرمين والإنابة القضائية، قد تم الفصل فيها.

[2] بن علية بن جدو، مرجع سابق، ص 315.

1- إسناد قضايا التنمية وتحسين جودة الخدمات المرتبطة بتكنولوجيا الاتصالات والإنترنت إلى المجلس الاقتصادي والاجتماعي للأمم المتحدة.

2- تكليف لجنة متخصصة في العدالة الجنائية ومنع الجريمة بمتابعة الجهود الدولية لمكافحة الجرائم، بما فيها الجرائم العابرة للحدود والجرائم الإلكترونية.

3- إبرام مذكرة تفاهم بين مكتب الأمم المتحدة المعني بالمخدرات والجريمة والاتحاد الدولي للاتصالات، بهدف تعزيز تبادل الخبرات وتقديم الدعم التقني للدول في مواجهة التهديدات السيبرانية.

4- إعداد مشروع اتفاق دولي سنة 2000 حول مكافحة الإرهاب الإلكتروني، من قبل جامعة ستانفورد بالولايات المتحدة، بما أسهم في تعزيز النقاش الدولي حول هذا النوع من الجرائم.

5- إصدار الأمم المتحدة سنة 2002 مجموعة من القرارات التي تهدف إلى ترسيخ ثقافة الأمن السيبراني، من خلال تشجيع الدول على حماية البنى التحتية للمعلومات وتكثيف التعاون ضد الإرهاب الإلكتروني[1].

6- إنشاء مجموعة الخبراء الحكوميين سنة 2004 لدراسة المخاطر الحالية والمستقبلية المرتبطة بأمن المعلومات، واقتراح أسس دولية لتعزيز حماية أنظمة الاتصالات.

7- دعوة الهيئات الأممية المعنية خلال المؤتمر الحادي عشر للوقاية من الجريمة والعدالة الجنائية المنعقد ببانكوك (2005) إلى تحديد الإطار القانوني للعقوبات وتعزيز التعاون الدولي في مكافحة الجرائم المعلوماتية.

8- تفعيل سياسة دولية قائمة على التحسيس والوقاية، أفضت إلى إصدار اتفاقيات وتشريعات متعددة تهدف إلى مكافحة الجريمة الإلكترونية وتعزيز تبادل المعلومات والدعم الفني بين الدول.

---

[1] نوران شفيق، **اثر التهديدات الإلكترونية على العلاقات الدولية القاهرة** ، المكتب العربي للمعارف، د ط، مصر، 2015 ، ص108.

انعكست هذه الحركية الدولية بشكل مباشر على صياغة الإستراتيجية الجزائرية، التي سارعت إلى التكيف مع مقتضيات التعاون الدولي؛ ويأتي هذا التفاعل في ظل تصاعد وتيرة الهجمات السيبرانية التي لم تعد تستهدف الشبكات العالمية فحسب، بل امتدت لتشمل الأنظمة المعلوماتية الوطنية، واضعةً الأمن القومي والدولي أمام تحديات أمنية حقيقية تستوجب اليقظة الدائمة[1].

من خلال ما سبق يتضح أن الإستراتيجية الجزائرية في مجال مكافحة الجرائم السيبرانية تقوم على مزيج من البعد الإقليمي (الأورو– متوسطي) والبعد الدولي، حيث تسعى من جهة إلى تعزيز التعاون مع دول المتوسط وتطوير التشريعات الوطنية بما يتماشى مع الاتفاقيات الدولية، وتقوية قدرات الأجهزة الأمنية واعتماد الأدلة الإلكترونية والتكوين المتخصص. ومن جهة أخرى، تنخرط الجزائر في الجهود الدولية بقيادة الأمم المتحدة والمنظمات المختصة لمواجهة التهديدات السيبرانية عبر التعاون وتبادل الخبرات ووضع أطر قانونية مشتركة، وبالتالي، تهدف هذه المقاربة المزدوجة إلى تحقيق الأمن السيبراني وطني فعال منسجم مع المعايير العالمية.

المطلب الثاني

انعكاسات الجريمة الإلكترونية على الاستقرار الوطني وتحديات الأمن السيبراني في مواجهتها في الجزائر

في ظل التوجه الإستراتيجي للدولة الجزائرية نحو رقمنة القطاعات الحيوية وتبني نموذج "الاقتصاد الرقمي"، أضحى الفضاء السيبراني ركيزةً أساسية للبناء التنموي والأمني.

ومع ذلك، فإن هذا الانفتاح التكنولوجي لم يكن بمعزل عن التهديدات، إذ برزت الجريمة الإلكترونية كعائق بنيوي يهدد استدامة هذا التحول، نظراً لسرعة تطور أساليبها وتعدد أبعادها التي تتجاوز النطاق التقني من الجوانب الاقتصادية، والسياسية، والاجتماعية. وهو ما جعل الأمن السيبراني في الجزائر يمثل خياراً محورياً لحماية المجال الرقمي الوطني وتدعيم قدرة الدولة على مواجهة هذه التهديدات المتزايدة.

---

[1] بوازدية جمال، مرجع سابق، ص 1288.

أفرزت هذه الجرائم انعكاسات متعددة التي أثرت بشكل مباشر على الأمن السيبراني في الجزائر، حيث أدت إلى تهديد سلامة الأنظمة المعلوماتية، كما يواجه كذلك مجموعة من التحديات المتزايدة نتيجة التطور السريع للهجمات الرقمية وتعقّد أساليبها.

وبناءً عليه، يهدف هذا المطلب إلى تسليط الضوء على شقين أساسيين: يرتكز على انعكاسات الجريمة الإلكترونية على الأمن السيبراني في الجزائر **(الفرع الأول)**، وإلى تحديات التي يواجهها الأمن السيبراني لمواجهة الجريمة الإلكترونية **(الفرع الثاني)**.

الفرع الأول: انعكاسات الجريمة الإلكترونية على الأمن السيبراني في الجزائر

أضحت الجريمة الرقمية متغيراً حرجاً يهدد ركائز الاستقرار الوطني، نظراً لتداعياتها المتشابكة التي تمتد من استنزاف الموارد المالية وزعزعة ثقة المستثمرين، وصولاً إلى استهداف سلامة البنية التحتية المعلوماتية.

ولا تقتصر هذه المخاطر على البُعد الاقتصادي فحسب، بل تمتد لتشكل تهديداً إستراتيجياً يمس السيادة الوطنية والأمن القومي، مما يضع قدرة الدولة على حماية فضاءات السيادية وعلاقاتها الدولية على المحك. ومن هذا المنطلق، تكتسي دراسة الانعكاسات الاقتصادية والسياسية للجرائم الإلكترونية في الجزائر أهمية بالغة، ليس فقط لتوصيف الظاهرة، بل لصياغة استراتيجيات استشرافية للتصدي لها.

أولاً: الانعكاسات الاقتصادية للجرائم الإلكترونية

تعد الجرائم الإلكترونية تهديداً جوهرياً للاقتصاد الوطني في الجزائر، حيث تتجاوز آثارها الخسائر المباشرة لتصل إلى تقويض بيئة الاستثمار ككل، وتتجلى هذه الانعكاسات في النقاط التالية:

1- الخسائر المالية الفادحة تؤكد التقارير الدولية حجم الضرر المالي الناتج عن هذه الظاهرة؛ فوفقاً لبيانات مكتب التحقيقات الفيدرالي، بلغت الخسائر العالمية الناجمة عن الجرائم الإلكترونية أرقاماً قياسية (تجاوزت 12.5 مليار دولار في عام 2023 كمثال حديث)، وفي السياق المحلي، تصنف الجزائر في مراتب متقدمة من حيث التعرض للمخاطر السيبرانية، مما يجعلها هدفاً رئيساً لشبكات الإجرام الرقمي، الأمر الذي يكبّد

الخزينة العمومية والمؤسسات خسائر مالية معتبرة، رغم صعوبة حصرها بدقة بسبب غياب الإحصائيات المحلية الشاملة.[1]

2- ضعف جذب المستثمرين تؤدي الهجمات السيبرانية إلى تراجع ثقة المستثمرين، خاصة عند تسريب أو اختراق بيانات مالية حساسة أو أنظمة مؤسساتية مهمة، وهو ما قد يتسبب في خسائر كبيرة في قيمة الشركات والأسواق[2].

كما أن تزايد المخاطر الرقمية في الجزائر ينعكس سلباً على مناخ الاستثمار، حيث يصبح المستثمر أكثر تحفظاً تجاه التعامل مع بيئة رقمية غير مستقرة أو غير محمية بشكل كافٍ. ويؤثر ذلك بشكل مباشر على النشاط الاقتصادي، خصوصاً في القطاعات التي تعتمد على الخدمات الرقمية والمعاملات الإلكترونية، وقد ساهم هذا الوضع في تراجع ترتيب الجزائر في مؤشرات الجاهزية الرقمية والتنمية الإلكترونية، ما يعكس الحاجة إلى تعزيز الأمن السيبراني لتحسين جاذبية الاقتصاد الوطني.

3- استهداف البنية التحتية الرقمية وعرقلة النمو تواجه الأنظمة المعلوماتية الصناعية في الجزائر تهديدات مستمرة؛ حيث تشير الإحصاءات إلى تعرض نسبة كبيرة من الحواسيب الصناعية لمحاولات اختراق أو برمجيات خبيثة.

- مصادر التهديد: تتنوع المصادر بين الوسائط القابلة للفصل (مثل USB بنسبة 55.22%، والإنترنت بنسبة 20.23%، بالإضافة إلى رسائل البريد الإلكتروني الاحتيالية.
- الأثر الاقتصادي: تؤدي هذه الهجمات إلى تعليق الخدمات الحيوية وزيادة التكاليف التشغيلية للمؤسسات، مما يعرقل مسار النمو الاقتصادي المستدام.

---

[1] FBI, "The FBI Released Its Internet Crime Report 2024", Federal Bureau of Investigation, April 16 2024, available at: https://www.fhi.gov/contact us/field offices/atlanta/news/the fhi released its internet crime report 2024, Accessed in 29 April 2026 at 11:43.

[2] موسى عمرو عادل عبد الفتاح، " **قياس تأثير الإفصاح عن مخاطر الإنترنت على تكاليف رأس المال المفترض والمال المملوك دراسة تطبيقي**"، مجلة الدراسات المالية والإدارية، المجلد 16، العدد 04 ديسمبر 2024، ص 424، ص ص420،435.

4- زعزعة الثقة في التعاملات الرقمية أدت حملات الاحتيال الأخيرة (مثل استهداف مستخدمي تطبيق "بريدي موب") إلى كشف الفجوة في الوعي الرقمي، إن استخدام تقنيات "الهندسة الاجتماعية" لسلب البيانات المالية لا يضر بالأفراد فحسب، بل يمتد أثره ليشمل:

- عزوف المواطنين عن استخدام الخدمات الإلكترونية.
- بطء عملية التحول الرقمي نتيجة الخوف من الوقوع ضحية للاحتيال.

ثانياً: التأثير السياسي والأمني للجريمة الإلكترونية

لا تقتصر مخاطر الجرائم السيبرانية على الجانب المادي، بل تمتد لتنال من سيادة الدولة واستقرارها السياسي.

1- تهديد الأمن الوطني واستقرار الدولة: تمثل الهجمات السيبرانية، خاصة هجمات حجب الخدمة، تهديداً مباشراً للأمن الوطني في الجزائر، حيث يمكن أن تؤدي إلى شلّ أنظمة حيوية مثل الاتصالات والخدمات الإدارية، وقد سُجلت مئات الهجمات ضد قطاعات حساسة، بلغت مستويات عالية من القوة والضغط على الشبكات.

كما أن حصول الجزائر على تنقيط منخفض في مؤشر الأمن السيبراني العالمي (33.95 درجة) يكشف عن ثغرات قد تجعل المؤسسات السيادية هدفاً سهلاً للتجسس الإلكتروني، كما حدث في محاولة اختراق وكالة الأنباء الجزائرية من قبل جهات خارجية.[1]

2- المساس بصورة الدولة وعلاقاتها الدولية: يساهم تكرار عمليات الاختراق التي تستهدف المؤسسات الجزائرية في التأثير سلباً على صورة الدولة داخلياً وخارجياً، حيث يُنظر إلى ذلك كعلامة على ضعف الحماية الرقمية.

كما أن استخدام برمجيات تجسس متطورة ضد مواطنين أو مؤسسات، مثل ما تم تداوله في تقارير دولية حول برامج مراقبة متقدمة، يثير مخاوف تتعلق بحماية البيانات الشخصية ويؤثر على مصداقية الدولة في المجال الرقمي.

---

[1] NETSCOUT Systems,Inc, "Algeria Latest Cyber Threat Intelligence Report," NETSCOUT DDoS Threat Intelligence Report, published for July December 2024 available at **https://www.netscout.com/threatreport/emen/algeria**, accessed in: May 2, 2026 , at 23:20.

هذا الوضع قد يؤدي أيضاً إلى توترات دبلوماسية محتملة، ويزيد من تعقيد العلاقات الدولية في ظل بيئة رقمية تتسم بتزايد التهديدات وغياب الضمانات الأمنية الكافية.[1]

الفرع الثاني: التحديات التي يواجهها الأمن السيبراني في مواجهة الجريمة الإلكترونية

في الجزائر لم يعد الأمن السيبراني مجرد خيار تقني تقتصره الدول على حماية أنظمتها المعلوماتية، بل أضحى قضية وجودية تتقاطع فيها الأبعاد الاجتماعية، الاقتصادية، والسياسية، نظراً لدوره في تأمين المعطيات وحماية الثروة الرقمية والثقافية للأفراد والمؤسسات[2].

وتتسم تحديات الأمن السيبراني بطابعها المعقد والمتداخل، مما يستدعي تبني مقاربة شاملة تقوم على تضافر الجهود السياسية والتقنية والقانونية، بهدف وضع استراتيجيات فعالة وقابلة للتطبيق.

كما أن مواجهة هذه التحديات تتطلب تطوير البنية التحتية الرقمية وتعزيز الوعي والتكوين، إلى جانب إرساء إطار قانوني وتنظيمي متكامل.

ومن ثم، فإن التصدي لمخاطر الفضاء السيبراني لا يمكن أن يتحقق من خلال حلول جزئية، بل يستوجب رؤية متكاملة متعددة الأبعاد تساهم في تعزيز الثقة الرقمية وتحقيق التنمية المستدامة[3].

1- العراقيل الذهنية أو البشرية: يُعدّ العامل البشري من أبرز التحديات التي تعيق فعالية منظومة الأمن السيبراني، إذ غالباً ما يكون الحلقة الأضعف في سلسلة الحماية الرقمية.

ويرجع ذلك إلى ضعف الوعي الأمني لدى المستخدمين، وعدم التزامهم بقواعد الحماية الأساسية عند التعامل مع الأنظمة المعلوماتية، فالكثير من الأفراد يعتمدون كلمات مرور

---

[1] محمد مسلم، "**التحذيرات من الاختراق والتجسس على هواتف الجزائريين**"، الشروق أونلاين 24 جانفي 2022، الرابط: **httpcwwww.echoroukonline.com/%D8%AA%D8%AD%D8%B0%D9%8A%D8%B1%D8%A7%D8**اطلع عليه بتاريخ 03 ماي 2026، على الساعة 17:30.

[2] بن عيلة بن جدو، مرجع سابق، ص305

[3] علاء الدين حميدي، **الأمن السيبراني**: خط الدفاع الأول في العصر الرقمي، الموقع: https://www.aljazeera.net/blogs10/12/2025 تم الاطلاع عليه يوم 08 ماي 2026 على الساعة 14:38.

ضعيفة أو يعمدون إلى مشاركة بياناتهم الشخصية والمهنية دون اتخاذ الاحتياطات اللازمة، مما يُسهّل عمليات الاختراق والاستغلال.

كما أن الاستخدام غير الواعي للتكنولوجيا، مثل فتح الروابط المشبوهة أو تحميل برامج غير موثوقة، يُسهم بشكل مباشر في تعريض الأنظمة لهجمات سيبرانية، ولا يقتصر الأمر على الإهمال فقط، بل قد يتخذ أحياناً طابعاً سلوكياً متعمداً، كمحاولات اختراق الأنظمة أو تجاوز وسائل الحماية، وهو ما قد يُشكّل أفعالاً مجرّمة قانوناً تُرتب مسؤولية جزائية على مرتكبيها، وعليه فإن نقص الثقافة الرقمية وضعف التكوين في مجال الأمن السيبراني يُعدّان من أهم العراقيل التي تحدّ من فعالية جهود الوقاية والمكافحة.

2- العراقيل على مستوى السلطات: واجهت السلطات العمومية عقبات هيكلية وتنظيمية تعيق قدرتها على بسط السيادة الرقمية الكاملة، وأهمها[1]:

- الفجوة بين التشريع والتكنولوجيا: تسارع وتيرة الجريمة الإلكترونية مقابل بطء الإجراءات القانونية والبيروقراطية في مواكبة التقنيات الحديثة.
- تشتت الجهود (ضعف التنسيق): غياب آلية موحدة ومركزية للتنسيق اللحظي بين الهيئات الأمنية والقضائية والتقنية، مما يؤدي إلى تضارب الاختصاصات أو بطء الاستجابة للأزمات السيبرانية.
- محدودية الموارد الإستراتيجية: تواجه الدولة تحديات في تخصيص الميزانيات الكافية لتأمين البنى التحتية الحساسة، بالإضافة إلى صعوبة تقدير التكاليف الاقتصادية الناجمة عن المخاطر المحتملة بشكل دقيق.

3- التحديات التقنية والعملياتية: تفرض الطبيعة الديناميكية للفضاء السيبراني عوائق فنية تتطلب جاهزية عالية، وتتجلى في:

- عدم تماثل الهجمات: يتميز المهاجم السيبراني بقدرته على التخفي واستخدام تقنيات متطورة (مثل الذكاء الاصطناعي والبرمجيات الخبيثة الموجهة)، بينما يضطر المدافع لتأمين كافة الثغرات في آن واحد.

---

[1] حسان زهار، الحروب السيبرانية تتصاعد ضد الجزائر، الموقع : https://elikhbaria.dz/elikhbariaplus/ تم اللإطلاع عليه يوم 10 أفريل 2026، على الساعة 22:30.

- ندرة البيانات والكفاءات: يعاني هذا المجال من نقص حاد في قواعد البيانات الإحصائية الدقيقة حول الهجمات المسجلة محلياً، مما يصعّب بناء نماذج استشرافية للمخاطر، يضاف إلى ذلك "هجرة الأدمغة" ونقص الكوادر المتخصصة القادرة على إدارة الأنظمة الدفاعية المعقدة.[1]
- هشاشة البنية التحتية التكنولوجية: تقادم الأنظمة في بعض القطاعات الحيوية يجعلها غير قادرة على الصمود أمام الهجمات الحديثة، مما يحول عملية إدارة المخاطر إلى مهمة بالغة التعقيد والتكلفة.

4- عراقيل الثقافة الأمنية والرقمية:

تعدّ محدودية الثقافة الأمنية والرقمية من أبرز العراقيل التي تعيق بناء منظومة فعّالة للأمن السيبراني في الجزائر، فبالرغم من تزايد الاعتماد على التكنولوجيات الحديثة، إلا أن مستوى الوعي لدى الأفراد والمؤسسات بمخاطر الفضاء الرقمي لا يزال دون المستوى المطلوب، ويرجع ذلك أساساً إلى ضعف برامج التوعية والتكوين المتخصصة، حيث تبقى المبادرات الإعلامية والتثقيفية محدودة من حيث الانتشار والتأثير، ولا تصل بالشكل الكافي إلى الفئات الأكثر عرضة للتهديدات السيبرانية.

كما يُلاحظ غياب إدماج منهجي ومستدام لمفاهيم الأمن السيبراني ضمن المناهج التعليمية في مختلف الأطوار الدراسية، الأمر الذي يحول دون تكوين جيل متمكن من أساسيات الحماية الرقمية وقادر على التعامل الآمن مع التكنولوجيا.

ويترتب عن هذا الوضع استمرار هشاشة السلوك الرقمي لدى المستخدمين، سواء من حيث حماية المعطيات الشخصية أو التعامل مع التهديدات الإلكترونية، مما يزيد من قابلية التعرض للهجمات، وبالتالي، فإن تعزيز الثقافة الأمنية الرقمية يُعدّ شرطاً أساسياً لنجاح أي سياسة وطنية في مجال الأمن السيبراني.[2]

---

[1] حميدي حياة، مرجع سابق، ص12.

[2] كمال قريني، **"تحديات الأمن السيبراني في مكافحة الجرائم السيبرانية في المجتمع الجزائري"** ، من مؤلف جماعي، بعنوان: الجرائم الاكترونية في المجتمع الجزائري تشخيص الواقع وتحديات الأمن السيبراني، د ط، مارس ، 2022، ص243.

5- عوائق الاستثمار في الأمن السيبراني:

يمثل ضعف الاستثمار في مجال الأمن السيبراني أحد التحديات الجوهرية التي تواجه الجزائر في سياق التحول الرقمي المتسارع، حيث يتطلب بناء بيئة رقمية آمنة تخصيص موارد مالية وتقنية وبشرية معتبرة[1].

غير أن المؤشرات الدولية تُظهر وجود فجوة واضحة بين الجزائر والدول الرائدة في هذا المجال، وهو ما ينعكس على مستوى الجاهزية الرقمية وقدرة الأنظمة على مواجهة التهديدات السيبرانية.

وفي هذا الإطار، تُبرز نتائج مؤشر تطور الحكومة الإلكترونية لسنة 2024 هذا التفاوت، حيث جاءت الجزائر في مرتبة متأخرة مقارنة بعدد من الدول المتقدمة، وهو ما يعكس محدودية الاستثمارات الموجهة لتطوير البنية التحتية الرقمية وتعزيز قدرات الحماية السيبرانية، ولا يقتصر أثر هذا الضعف على الجانب التقني فحسب، بل يمتد ليشمل القدرة على تكوين الكفاءات المتخصصة، وتحديث الأنظمة المعلوماتية، واعتماد الحلول التكنولوجية المتقدمة في مجال الحماية.

كما أن محدودية التمويل تُعيق تطوير استراتيجيات وطنية فعّالة، وتؤخر تبني معايير دولية في الأمن السيبراني، مما يجعل المؤسسات أكثر عرضة للاختراقات والهجمات، وعليه، فإن تعزيز الاستثمار في هذا المجال لم يعد خياراً، بل ضرورة حتمية لضمان الأمن الرقمي، ودعم الثقة في الاقتصاد الرقمي، ومواكبة التحولات العالمية المتسارعة.

6- العراقيل في المنظومة التشريعية: تعدّ المنظومة التشريعية من الركائز الأساسية لضمان فعالية الأمن السيبراني، غير أنها تواجه عدة تحديات في مواكبة التطور السريع والمتلاحق للبيئة الرقمية، إذ يرتبط هذا النوع من العراقيل أساساً بنقص أو عدم اكتمال التأطير القانوني المتخصص في مجال الأمن السيبراني، سواء من حيث تنظيمه أو ضبط ممارساته وآلياته الوقائية والردعية، فالتشريعات غالباً ما تتسم بالجمود النسبي مقارنة

[1] حميدي حياة، طايلب نسيمة، مرجع سابق، ص12

بالديناميكية التي تميز الفضاء الإلكتروني، الذي يشهد تطوراً مستمراً في أنماط الجرائم وأساليب ارتكابها.

كما أن الطبيعة التقنية المعقدة للجرائم السيبرانية تطرح إشكالات قانونية تتعلق بالتكييف القانوني للأفعال، وتحديد المسؤوليات، وإثبات الأدلة الرقمية، وهو ما يستدعي تدخل الفقه والاجتهاد القضائي لسدّ الفراغات التشريعية وتفسير النصوص بما يتلاءم مع خصوصية هذا النوع من الجرائم، ويُضاف إلى ذلك الطابع العابر للحدود لهذه الجرائم، مما يُصعّب من تطبيق القوانين الوطنية ويُبرز الحاجة إلى تعزيز التعاون الدولي وتوحيد الجهود التشريعية.[1]

ومن جهة أخرى، فإن تحقيق الأمن السيبراني فعّال لا يقتصر على سنّ النصوص القانونية فحسب، بل يتطلب تنسيقاً شاملاً بين مختلف مكونات المنظومة المعلوماتية، بما يشمل أمن الشبكات، وأمن الحواسيب، وأمن البيانات، وأمن تطبيقات المعلومات، وأمن الاتصالات، إضافة إلى حماية الأنظمة السحابية وقواعد البيانات، باعتبارها عناصر أساسية في البنية التحتية للمجتمع الرقمي.

غير أن التحدي الأكبر يكمن في الطبيعة المتغيرة للتهديدات السيبرانية، حيث إن نفس التكنولوجيات المستخدمة في الهجوم يمكن توظيفها أيضاً في الحماية، مما يفرض على الدول مواكبة مستمرة للتطورات التقنية في مجال تأمين المعلومات ومعالجتها وتخزينها.

كما يستلزم ذلك اعتماد استراتيجيات استباقية قائمة على التخطيط المسبق، وتطوير آليات للرصد والإنذار المبكر، وتعزيز القدرة على الاستجابة السريعة لمختلف التهديدات، بما يضمن الحدّ من المخاطر وتعزيز فعالية المنظومة الأمنية الرقمية.

7- ضعف التنسيق الدولي: يُعدّ ضعف التنسيق والتعاون الدولي من أبرز العراقيل التي تحدّ من فعالية مكافحة الجريمة الإلكترونية في الجزائر، لاسيما في ظل الطبيعة العابرة للحدود التي تميّز هذا النوع من الجرائم، إذ يستغلّ مرتكبو الجرائم السيبرانية الفوارق القانونية

[1] حميدي حياة، مرجع لسابق، ص13.

والإجرائية بين الدول، إلى جانب اختلاف مستويات التطور التقني، مما يُمكّنهم من الإفلات من المتابعة أو تعقيد عمليات تعقبهم.

وتواجه السلطات الجزائرية صعوبات كبيرة في هذا الإطار، خاصة فيما يتعلق بجمع الأدلة الرقمية أو تتبع مسارات الهجمات عندما تكون البيانات مخزّنة أو مُعالجة خارج الإقليم الوطني، كما أن بطء إجراءات التعاون القضائي الدولي، وتعقيد آليات المساعدة القانونية المتبادلة، يُؤثر سلباً على سرعة وفعالية الاستجابة لهذه الجرائم.

ويُضاف إلى ذلك التفاوت الكبير في مستويات الجاهزية القانونية والتقنية بين الجزائر وباقي الدول، مما يُعيق توحيد الجهود ويحدّ من تبادل المعلومات والخبرات بشكل فعّال، كما أن محدودية الاتفاقيات الثنائية ومتعددة الأطراف في مجال مكافحة الجرائم السيبرانية تُضعف من قدرة الجزائر على الاندماج في منظومة دولية متكاملة لمواجهة هذه التهديدات.

وعليه، فإن تعزيز التعاون الدولي، من خلال إبرام اتفاقيات متخصصة، وتطوير آليات التنسيق بين الأجهزة الأمنية والقضائية، وتكثيف تبادل المعلومات والخبرات، يُعدّ ضرورة حتمية لمواجهة الطابع العابر للحدود للجريمة الإلكترونية، وضمان فعالية الجهود الوطنية في التصدي لها.[1]

[1] بارة سمير، مرجع سابق، ص436.

خلاصة الفصل الثاني:

أبرز هذا الفصل الجهود التي تبذلها الجزائر في مواجهة الجريمة الإلكترونية وتعزيز الأمن السيبراني، من خلال تبني منظومة متكاملة تجمع بين الجوانب القانونية والإجرائية، فقد عمل المشرّع الجزائري على تطوير إطار قانوني يشمل القواعد العامة إلى جانب نصوص خاصة تتلاءم مع طبيعة الجرائم الإلكترونية، بما يضمن تجريم الأفعال المستحدثة وملاحقة مرتكبيها بفعالية، كما تتعزز هذه الجهود بآليات إجرائية تعتمد على تدخل الأجهزة الأمنية المختصة وتطوير قدراتها التقنية والبشرية، إلى جانب إنشاء هيئات إدارية متخصصة تُعنى بحماية الفضاء السيبراني ، وهو ما يساهم في تحسين فعالية الكشف عن الجرائم الإلكترونية والحد من انتشارها.

ومن جهة أخرى، تسعى الجزائر إلى دعم أمنها السيبراني من خلال الانخراط في التعاون الإقليمي والدولي، عبر إبرام الاتفاقيات وتبادل الخبرات، إدراكًا منها للطابع العابر للحدود الذي تتميز به الجريمة الإلكترونية.

ورغم هذه الجهود، فإن الجريمة الإلكترونية تطرح انعكاسات خطيرة على الأمن السيبراني، سواء من حيث تهديد البنى التحتية الرقمية أو المساس بأمن المعلومات، كما تفرض تحديات متزايدة تتعلق بسرعة تطور التقنيات، وصعوبة التتبع، ونقص الكفاءات المتخصصة أحيانًا.

الخاتمة

ختاماً لموضوعنا، يمكن القول أن الأمن السيبراني يشكل آلية مركزية ومحورية في مواجهة الجريمة الإلكترونية في الجزائر، فهو لم يعد مجرد مفهوم تقني مرتبط بحماية الأنظمة والشبكات المعلوماتية فقط بل أصبح نظام متكامل يجمع بين الوقاية والحماية والردع، فهو يقوم على مجموعة من الأبعاد والمبادئ التي تهدف إلى حماية النظم المعلوماتية وضمان استمرارية عملها.

يكتسي الأمن السيبراني أهمية متزايدة باعتباره خط الدفاع الأول ضد الجريمة الإلكترونية، التي تمثل أحد أبرز المخاطر التي تهدد الفضاء السيبراني، حيث تتميز بخصائص تجعلها مختلفة عن الجريمة التقليدية، من حيث عدم المادية، وسهولة التنفيذ، وصعوبة التتبع وسرعة التطور، وهو ما يجعل مكافحتها تتطلب استراتيجيات دقيقة ومتكاملة، لا تعتمد فقط على الردع بعد وقوع الجريمة، بل أيضًا على الوقاية المسبقة وتعزيز منظومة الحماية الرقمية.

مواجهة الجريمة الإلكترونية في الجزائر لا تعتمد على جانب واحد فقط، بل تقوم على تكامل الجهود القانونية والتنظيمية والمؤسساتية، إلى جانب التدابير الوطنية الرامية إلى تعزيز الأمن السيبيراني، حيث تعمل الدولة على تطوير ترسانتها القانونية، وتدعيم أجهزتها الأمنية والإدارية، ومواكبة التحول الرقمي، بما يسمح بالتصدي الفعّال لمختلف التهديدات السيبرانية.

غير أن هذه الجهود، رغم أهميتها لا تزال تصطدم بعدة تحديات، أبرزها التطور السريع والمتواصل لأساليب الجريمة الإلكترونية، ونقص الكفاءات المتخصصة، وضعف الوعي الرقمي لدى بعض المستخدمين، إضافة إلى الحاجة المستمرة لمواكبة التشريعات للتغيرات التكنولوجية العالمية.

نتائج الدراسة:

ومن خلال ما تم التوصل إليه في هذه الدراسة، يمكن استخلاص مجموعة من النتائج تتمثل فيما يلي:

– تُعد الجريمة الإلكترونية من أبرز الآثار السلبية التي أفرزتها الثورة التكنولوجية المتسارعة التي يشهدها العالم في ظل التطور الكبير في تكنولوجيا الإعلام والإتصال.

– اعتماد أنظمة تراسل آمنة تعتمد على التشفير بين مختلف الجهات والمؤسسات، سواء على المستوى الوطني أو في إطار التعاون الدولي، بما يضمن سرية وسلامة المعلومات المتبادلة.

– العمل على تحديث وتطوير الأنظمة الرقمية المعتمدة في الدول الجزائرية بشكل دوري ومنتظم، لا يتجاوز كل ثلاثة إلى ستة أشهر، بما يسمح بمواكبة التطورات السريعة في مجال التكنولوجيا والتهديدات السيبرانية.

– تتميز الجريمة الإلكترونية بصعوبة اكتشافها وإثباتها أمام الجهات القضائية، إضافة إلى كونها جرائم عابرة للحدود، لا تعترف بالحدود الجغرافية أو الزمانية التقليدية، مما يزيد من تعقيد مكافحتها.

– تجنب استعمال وسائل الاتصال والبريد الإلكتروني غير المؤمّن، لما تشكله من خطر على أمن المعلومات وإمكانية تعرضها للاختراق أو التسرب.

– تشجيع البحث والتطوير العلمي من الركائز الأساسية لتعزيز الأمن السيبراني، من خلال دعم الدراسات والأبحاث المتخصصة وتمويلها، مع توظيف نتائجها في صياغة سياسات وطنية تسهم في تطوير حلول تقنية وقانونية فعّالة ومستدامة.

– تطوير البنية التحتية التقنية من أهم التدابير الرامية إلى دعم الأمن السيبراني، من خلال تحديث الوسائل والتقنيات المعتمدة في مجالات الحماية والمراقبة الرقمية، لاسيما على مستوى القطاعات الحيوية والمنشآت الوطنية الحساسة.

–ساهم الاهتمام المتزايد بالأمن السيبراني في نشر الوعي الرقمي لدى الأفراد والمؤسسات بأهمية حماية البيانات واحترام قواعد السلامة المعلوماتية، فضلا عن تشجيع التعاون الوطني والدولي في مجال تبادل الخبرات والمعلومات المتعلقة بمكافحة الجريمة الإلكترونية.

– ساهمت آليات الأمن السيبراني في دعم قدرات الدولة على كشف الهجمات الإلكترونية والتصدي لها، من خلال تطوير وسائل المراقبة الرقمية وتأمين الشبكات وقواعد البيانات، خاصة تلك المرتبطة بالمؤسسات الحيوية والإدارية، وقد أدى ذلك إلى الحد من بعض أشكال الاختراق والاحتيال الإلكتروني وتعزيز حماية المعطيات والمعلومات الحساسة.

– شهدت الجزائر خلال السنوات الأخيرة تصاعدا ملحوظا في وتيرة الجرائم الإلكترونية، حيث انتقلت من أفعال فردية معزولة إلى أنشطة إجرامية منظمة تعتمد على تقنيات وأساليب متطورة، الأمر الذي أدى إلى تنامي التهديدات الموجهة للأمن السيبراني الوطني وفرض تحديات متزايدة أمام جهود الحماية والمكافحة.

– ضرورة تفعيل وتطبيق آليات الأمن السيبراني على مختلف المستويات، سراء داخل المؤسسات العامة أو الخاصة، بما يضمن حماية الأنظمة المعلوماتية من مختلف التهديدات الإلكترونية.

– على الرغم من التوسع الكبير في استخدام الإنترنت والتقنيات الرقمية في الجزائر، إلا أن البنية التحتية الخاصة بالأمن السيبراني ما تزال تعاني من نقائص على المستويين التقني والتنظيمي، وهو ما يحد من قدرة المؤسسات على التصدي للتهديدات والهجمات السيبرانية بكفاءة وفعالية.

– عمل المشرع الجزائري على مواجهة هذا النوع من الجرائم من خلال تخصيص قسم خاص بالجرائم الإلكترونية ضمن التشريع الجزائري، بما يعكس اهتمامه المتزايد بحماية الفضاء المعلوماتي.

– كما منح المشرع الجزائري للسلطات المختصة في إطار مكافحة الجريمة الإلكترونية مجموعة من الصلاحيات الواسعة، مثل المراقبة الإلكترونية والتفتيش الرقمي للأنظمة المعلوماتية وحجزها، غير أن هذه الإجراءات تبقى غير كافية في ظل التطور المستمر للجرائم الإلكترونية وظهور أنماط جديدة أكثر تعقيدًا.

التوصيات:

وتم التوصل أيضا إلى مجموعة من التوصيات، يمكن تلخيصها فيما يلي:

– يُلاحظ عدم الاستقرار على مستوى الفقه وكذا التشريعات المقارنة فيما يتعلق بتوحيد التسمية الخاصة بالجريمة الإلكترونية، حيث يطلق عليها أحيانًا "الجريمة السيبرانية" أو "الجريمة المرتكبة عبر الإنترنت"، ويعود ذلك إلى الطبيعة المتطورة والمستمرة لهذا النوع من الجرائم وإمكانية ظهور صور جديدة منها.

– الاستفادة من التجارب الدولية الناتجة في مجال الأمن السيبراني، من خلال نقل الخبرات وتبني أفضل الممارسات، بهدف تعزيز قدرات الدولة في حماية أمنها القومي ومواجهة الجريمة الإلكترونية بفعالية أكثر.

– تعزيز التكوين والتدريب المستمر للكوادر البشرية المتخصصة في مجال الأمن السيبراني، من أجل رفع الكفاءاتهم في كشف التهديدات والاستجابة لها بسرعة وفعالية.

– نشر الوعي الرقمي بيم مختلف فئات المجتمع، خاصة الشباب حول مخاطر الجريمة الإلكترونية وطرق الوقاية منها، باعتبار أن العنصر البشري يعد الحلقة الأضعف في المنظومة الأمنية الرقمية.

– دعم البحث العلمي والابتكار في مجال الأمن السيبراني داخل الجامعات ومراكز البحث، لتطوير حلول وطنية قادرة على مجابهة التهديدات السيبرانية المتطورة.

– يقتضي إعداد أي إستراتيجية أو سياسة متعلقة بالأمن السيبراني مراعاة مختلف أبعاده، مع الأخذ بعين الاعتبار احتياجات الأفراد والمؤسسات، وكذا حقوقهم والتزاماتهم، بما يضمن وضع خطة متكاملة ومتناسقة تتلاءم مع مستوى الالتزام المتوقع من مختلف الفاعلين في مجتمع المعلومات.

قائمة المراجع

قائمة المراجع

أولا: الكتب

1. إيمان فاضل السمرائي، هيثم محمد الزغبي،" نظم المعلومات الإدارية"، الطبعة الأولى، دار الصفاء للنشر والتوزيع، عمان، 2005.
2. فارس محمد العميرات،"الأمن السيبرانيالمفهوم وتحديات العصر"، دار الخليج للنشر والتوزيع، الطبعة الأولى، الأردن، عمّان، 2022.
3. كمال قريني، "تحديات الأمن السيبراني في مكافحة الجرائم السيبرانية في المجتمع الجزائري" ، من مؤلف جماعي، بعنوان: الجرائم الاكترونية في المجتمع الجزائري تشخيص الواقع وتحديات الأمن السيبراني، د ط، مارس ، 2022.
4. محمد محمود العمري، "مدخل إلى الأمن السيبراني"، دار زهران للنشر والتوزيع، الطبعة الأولى، عمّان، 2020.
5. محمود أحمد عبّانة، "جرائم الحاسوب وأبعادها الدولية"، دار الثقافة للنشر والتوزيع، دون طبعة، الأردن، 2005.
6. نوران شفيق، اثر التهديدات الإلكترونية على العلاقات الدولية القاهرة ، المكتب العربي للمعارف، مصر، 2015 .

ثانيا: الرسائل والمذكرات الجامعية

أ/ رسائل الدكتوراه

1. أحلام شناق،" واقع الجريمة الإلكترونية في مجتمع المدينة الجزائرية مدينة بسكرة نموذجا، أطروحة مكملة لنيل درجة الدكتوراه، الطور الثالث في علم الاجتماع، تخصص علم الاجنماع الحضري، كلية العلوم الإنسانية والاجتماعية، جامعة محمد خيضر، بسكرة، الجزائر، 2025/2024.

2. بوحمزة نصيرة،" التحقيق الجنائي في الجرائم الإلكترونية دراسة مقارنة"، رسالة مقدمة لنيل الدكتوراه في العلوم القانونية، تخصص قانون خاص، كلية والعلوم السياسية، جامعة الجيلالي اليابس، سيدي بلعباس، الجزائر، 2022.
3. دليلة العوفي، "آليات محاربة الجريمة المعلوماتية دراسة حالة الجزائر 2006– 2009"، أطروحة دكتوراه في علوم الإعلام والاتصال، كلية علوم الإعلام والاتصال، جامعة إبراهيم سلطان شيبوط، جامعة الجزائر 3، الجزائر، 2020.
4. ربيعي حسين،"آليات البحث والتحقيق في الجرائم المعلوماتية"، أطروحة مقدمة لنيل شهادة الدكتوراه، كلية الحقوق والعلوم السياسية، جامعة باتنة1، الجزائر، 2016/2015.
5. عبد الله بن سعود، محمد السراني، "فعّالية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني"، لرسالة مقدمة لنيل شهادة الدكتوراه، قسم العلوم الشرطية، جامعة نايف للعلوم الأمنية، الرياض، السعودية، 2009.
6. غازي عبد الرحمان، هيان رشيد،" الحماية القانونية من الجرائم المعلوماتية الحاسب والإنترنت"، أطروحة لنيل شهادة الدكتوراه في القانون، كلية الحقوق، الجامعة الإسلامية، لبنان،2004،.
7. فاتح حارك،"الفضاءالسيبراني والتحول في مفهوم الأمن في الولايات المتحدة الأمريكية"، أطروحة مقدمة لنيل شهادة الدكتوراه، الطور الثالث، كلية العلوم السياسة، قسم العلاقات الدولية، جامعة قسنطينة3 صالح بونيدر، الجزائر، 2024/2023.

ب/ مذكرات الماجستير

1. صغير يوسف،" الجريمة المرتكبة عبر الإنترنت"، مذكرة لنيل شهادة الماجستير في القانون، تخصص القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2013.

2. عبد الرحمان جميل، محمود حسين،" الحماية القانونية لبرامج الحاسب الآلي دراسة مقارنة"، رسالة مقدمة استكمالاً لمتطلبات درجة الماجيستر في القانون الخاص، كلية الدراسات العليا، جامعة النجاح الوطنية، فلسطين، 2008.
3. عبد الله دغش العجمي، "المشكلات العلمية والقانونية للجرائم الإلكترونية دراسة مقارنة"، مذكرة لنيل شهادة الماجستير في القانون العام، جامعة الشرق الأوسط، الأردن، 2014.

ثالثا: المقالات

1. أحمد محمد الدوسري،" أنواع الجرائم الإلكترونية وتحديات مكافحتها"، مجلة منار للدراسات والبحوث القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة يحي فارس، المدية، المجلد 9، العدد01، الجزائر، 2025.
2. إدريس عطية، " مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري"، مجلة مصداقية، صادرة عن المدرسة العليا العسكرية للإعلام والاتصال، المجلد01، العدد 01، الجزائر، 2019، ص ص 100- 121.
3. أستاذ شريف بسام، "واقع الحوكمة الإلكترونية في الدول العربية "، مجلة العلوم الاجتماعية والإنسانية، جامعة الجزائر3، العدد6,، جوان 2016، ص ص 157- 170.
4. إسماعيل زروقة، الفضاء السيبراني والتحول في مفاهيم القوة والصراع"، مجلة العلوم القانونية والسياسية، جامعة محمد بوضياف، المسيلة، المجلد 10، العدد1، الجزائر، 2019، ص ص 1016-1031.
5. اسيا العمراني،"التعاون الدولي في مواجهة الجرائم السيبرانية الجزائر نوذجًا"، كلية العلوم السياسية والعلاقات الدولية، جامعة الجزائر 3، المجلد 3، العدد2، الجزائر،2010، ص54.
6. أمال بوجليدة ، الاقتصاد الرقمي التحول من اقتصاد الصناعي إلى اقتصاد المعلومات ، مجلة الخبير ، العدد 63 ، جانفي 2016 ، ص ص 45-47.

7. أميرة عبد العظيم، محمد عبد الجواد، "المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام"، مجلة الشريعة والقانون، العدد35، الجزائر، 2020.
8. إيمان بغدادي، "أثر تعديل قانون العقوبات الجزائري في التصدي للجريمة الإلكترونية"، مجلة آفاق للبحوث والدراسات السداسية، كلية الحقوق، جامعة قسنطينة، العدد 04، 2019، ص ص 184-192.
9. إيمان عبد القادر،" أثر الفضاء السيبراني على الأمن القومي العربي خلال فترة من 2011 إلى 2023"، المجلة الأكاديمية العسكرية للدراسات العليا والإستراتيجية، العدد03، 2024، ص108.
10. بن عبو عفيف، " الآليات القانونية في الجزائر وتطويرها في مكافحة الجريمة الإلكترونية"، مجلة حقوق الإنسان والحريات العامة، جامعة عبد الحميد بن باديس، مستغانم، المجلد 09، العدد01، الجزائر، 2024، ص ص 21 47.
11. بن عيلة بن جدو، "تحديات الأمن السيبراني لمواجهة الجريمة الالكترونية"، المجلة الجزائرية للأمن الإنساني، جامعة بومرداس، المجلد 07، العدد02، الجزائر، 2022، ص ص 299-319.
12. بوضياف اسمهان،" الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف، العدد 11، المسيلة، الجزائر، 2018، ص ص 348-375.
13. بوقرة جمال الدين، "القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا إعلام والاتصال"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف مسيلة، المجلد 7، العدد 1، الجزائر، جوان 2020، ص ص 1673- 1693.

14. بولحية شهرزاد، "تحديات الجريمة الإلكترونية في الجزائر"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة الجزائر 1، المجلد 04، العدد02، الجزائر، 2019، ص ص1974-2003.

15. جيلالي شويرب، مراد فائزة،" مفهوم الحروب السيبرانية والأمن السيبراني"، مجلة الحقوق والحريات ، المجلد 11 ، العدد 01، افريل 2023، ص ص 156-170.

16. حزام فتيحة، "الحماية المؤسساتية للأنظمة الرقمية في الفترة التشريعية الممتدة من 2009- 2020"، المجلة الأكاديمية للدراسات الاجتماعية والإنسانية، جامعة حسيبة بن بوعلي، الشلف، المجلد13، العدد02، الجزائر 2021، ص ص -270 289.

17. حمز حضري، عشاش حمزة،" خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري"، مجلة الدراسات القانونية والسياسية، جامعة محمد بوضياف، المجلد06، العدد02، المسيلة، الجزائر، 2020، ص ص 168-176.

18. حميدي حياة، طايلب نسيمة،" مدخل مفاهيمي حول الأمن السيبراني"، مجلة مدار للدراسات الاتصالية الرقمية، جامعة الجزائر، المجلد02، العدد02، الجزائر، 2022، ص ص1116.

19. حنان مسكين، " واقع مكافحة الجريمة المعلوماتية واتجاهاتها التشريعية في الجزائر"، المجلة الأكاديمية للبحوث القانونية والسياسية، العدد01، المجلد 04، الجزائر، 2020، ص ص610 -632.

20. راضية عيمورة، "الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري"، المجلة الأكاديمية للبحوث القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الأغواط، العدد1 ، المجلد 6، الجزائر، 2022، ص ص87 107.

21. زمور جمال، بن عيسى ليلى،" أهمية حوكمة الأمن السيبراني لضمان تحول رقمي آمن للخدمات العمومية في الجزائر"، مجلة البحوث الاقتصادية المتقدمة، جامعة محمد خيضر بسكرة، المجلد7، العدد2، الجزائر، 2022،ص ص 1572-2676.

22. زينب الياقوت، "دور الإعلام الجزائري في التصدي للجريمة السيبرانية قناة النهار نوذجاً، مجلة طينة للدراسات العلمية الأكاديمية، المجلد5، العدد01، الجزائر، 2022، ص ص1362-1379.

23. سمير بارة، الأمن السيبراني في الجزائر السياسات والمؤسسات، المجلة الجزائرية للأمن الإنساني، جامعة قاصدي مرباح، المجلد02، العدد04، الجزائر، 2017، ص ص 255-280.

24. سيد علي بدرين، "إستراتيجية الجزائر لمواجهة التهديدات السيبرانية"، مجلة الشرطة، المديرية العامة للشرطة الجزائرية، العدد 156، الجزائر، 2023، ص ص 51- 70.

25. سيناء علي محمود،" التحديات الأمنية للدول في الفضاء السيبراني"، مجلة القضايا السياسية، كلية العلوم السياسية، جامعة النهرين، العدد80، 2025.

26. صباح كزيز،"أثر الجرائم الإلكترونية على أمن واستقرار الدول: قرصنة الموقع الإلكتروني لوكالة الأنباء القطرية نموذجًا"، مجلة الناقد للدراسات القانونية، العدد03، 2018.

27. علاء الدين فرحات،" الفضاء السيبراني: تشكيل ساحة المعركة في القرن 21"، مجلة العلوم القانونية والسياسية، المدرسة الوطنية العليا للعلوم السياسية، المجلد10، العدد10، الجزائر، 2019، ص ص 88-107.

28. فتيحة حيمر،" تأثير الجريمة الإلكترونية على الأمن في إفريقيا"، مجلة أبحاث قانونية وسياسية، المجلد09، العدد01، 2024.

29. فريد ناشف،" آليات التعاون الدولي في مكافحة الجرائم الإلكترونية"، مجلة البحوث في الحقوق والعلوم السياسية، جامعة البليدة2، المجلد08، العدد 01، 2022، ص ص 430-450.

30. قطاف سليمان، بوقرين عبد الحليم، "الآليات الموضوعية والإجرائية المتبعة لتحقيق الأمن السيبراني الجزائر نموذجا"، مجلة الحكومة والقانون الاقتصادي، جامعة عمار ثليجي، المجلد03، العدد02، الأغواط، الجزائر، 2023، ص ص 80/93.

31. قطاف سليمان، بوقرين عبد الحليم،"الأمن السيبراني والمضامين المفاهيمية المرتبطة به"، مجلة طبنا للدراسات العلمية الأكاديمية، مخبر بحث للحقوق والعلوم السياسية، جامعة الأغواط، المجلد5، العدد2، الجزائر، 2022، ص ص 37-56.

32. ليلى بوعوني، التهديدات في الفضاء السيبراني وانعكاساتها على السيادة الرقمية: القرصنة الإلكترونية نموذجًا"، مجلة استراتيجية، العدد 16، 2021.

33. محمد بوكبشة،"الأمن والدفاع السيبراني أولوية قصوى"، مجلة الجيش، العدد 51، أكتوبر 2017.

34. محمد محمود زيتون،"القوة السيبرانية أداة للتأثير والسيطرة في الفضاء السيبراني والعلاقات الدولية بحث مكمل لمناقشة رسالة الدكتوراه، المجلة العربية للنشر العلمي، الإصدار 8، العدد77، 2025، ص ص202-220.

35. محمودي سعيد، "الأمن السيبراني في الجزائر: بين المعالجة الأمنية والحماية القانونية"، مجلة الناقد للدراسات السياسية، جامعة بشار، المجلد 07، العدد 02، الجزائر، 2023، ص ص 193- 212.

36. معتوق أم الخير، "كسب رهان الأمن السيبيراني ضمان لتعزيز الأمن ودفاع الوطنيين في الجزائر"، مجلة البحوث في الحقوق والعلوم السياسية، الملحقة الجامعية الشلالة، جامعة تيارت، المجلد09، العدد02، الجزائر، 2024، ص ص53-76.

37. مقلاتي مونى، راضيا مشري، "الجريمة الإلكترونية: دلالة المفهوم وفعالية المعالجة القانونية"، مجلة الأبحاث القانونية السياسية، جامعة 8ماي 1945، قالمة، المجلد 6، العدد1، 2021، ص ص491-510.

38. مهدي رضا، "الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري"، مجلة إليزا للبحوث الدراسات، جامعة محمد بوضياف، المسيلة، المجلد 06، العدد 02، الجزائر، 2021، ص 111-125.

39. موسى عمرو عادل عبد الفتاح، " قياس تأثير الإفصاح عن مخاطر الإنترنت على تكاليف رأس المال المفترض والمال المملوك دراسة تطبيقي"، مجلة الدراسات المالية والإدارية، المجلد 16، العدد 04 ديسمبر 2024.

رابعا: المحاضرات

بوازدية جمال، "الأمن السيبراني"، محاضرات مقدمة لطلبة سنة الثانية ماستر، جامعة الجزائر 3، كلية العلوم السياسية والعلاقات الدولية، الجزائر، 2020-2021.

خامسا: النصوص القانونية

أ/ الدساتير

الدستور 2020، المؤرخ في 15 جمادى الأول عام 1442هـ الموافق ل 30 ديسمبر2020، ج ر ، العدد82 ، 2020.

ب/ النصوص التشريعية

1. القانون رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق ل8يونيو سنة 1966، يتضمن قانون العقوبات المعدل والمتمم، الجريدة الرسمية للجمهورية الجزائرية، العدد49، الصادرة في 11 يونيو 1966.

2. الأمر رقم 03-05، المؤرخ في 19 جمادى الأولى عام 1424 الموافق ل 19 يوليو 2003، المتعلق بحقوق المؤلف والحقوق المجاورة، ج ر ، العدد 44، الصادر في 23 يوليو 2003.
3. القانون رقم 04-15 المؤرخ في 10 نوفمبر2004، يعدل ويتمم الأمر رقم 66-156 المتضمن قانون العقوبات، الجريدة الرسمية للجمهوية الجزائرية، العدد71، الصادرة قي 2004.
4. قانون رقم 06- 22 مؤرخ في 20 ديسمبر 2006 يعدل ويتمم الأمر رقم 66- 155 يتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد84، الصادر في 24 ديسمبر 2006.
5. قانون رقم 09-04 مؤرّخ في 14 شعبان عام 1430 الموافق ل 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر ، العدد 47، الصادرة في 16 غشت 2009.
6. قانون رقم 18-04 مؤرخ في 24 شعبان عام 1439 الموافق ل 10مايو سنة 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، الجريدة الرسميّة للجمهورية الجزائريّة، العدد27، الصادرة بتاريخ 13 مايو 2018.
7. الأمر رقم 21-11، المؤرخ في 15 محرم عام 1443 الموافق ل 24 غشت 2021، يتعلق بمراقبة دستورية للأمر الذي يتمم الأمر رقم 66-155، المؤرخ 8 يونيو سنة 1966، المتضمن قانون الإجراءات الجزائية، ج ر ، العدد 65، الصادر في 26 غشت سنة 2021.

ج/ النصوص التنظيمية

1. المرسوم الرئاسي رقم 04-183 المؤرخ في 26 يونيو 2004، المتعلق بإحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، الجريدة الرسمية للجمهورية الجزائرية، العدد41، الجزائر، الصادر في 2004.
2. المرسوم الرئاسي رقم 20-05، المؤرخ في 10ديسمبر2020، المتضمن وضع المنظومة الوطنية لأمن الأنظمة المعلوماتية، الجريدة الرسمية للجمهورية الجزائرية ، العدد04، الصادر بتاريخ 26 جانفي2020.
3. مرسوم رئاسي رقم 15-261، المؤرخ بتاريخ 24 ذي الحجة عام 1436 الموافق 8 أكتوبر سنة 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 37، المؤرخ في 18 يونيو 2015.
4. المرسوم الرئاسي رقم 20-283 المؤرخ في 13 يوليو 2020، المتضمن إعادة تنظيم الهيئة الوطنية الوقاية من جرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 40، الصادرة بتاريخ 18 يوليو 2020.

سادسا: المواقع الإلكترونية:

1 الأمن السيبراني: مفهومه وتاريخه، الموقع:
https://www.aljazeera.net/amp/encyclopedia/2024/9/19
الجزيرة نت، تم الاطلاع عليه بتاريخ 2026/01/15. على الساعة 13:15.
2. الأمن السيبراني: أهمية حماية البيانات في العصر الرقمي الموقع:
https://spskills.com/articles تم الاطلاع عليه بتاريخ 2026/01/10 على الساعة 18:47.

3. فهد قطينة، كتاب الأمن السيبراني الموقع:
https://www.ktobati.com/book/%D9%8 تم الاطلاع عليه يوم 22 جانفي 2026 على الساعة 22:30.

4. الأمن السيبراني: أهمية حماية البيانات في العصر الرقمي الموقع:
https://spskills.com/articles/ تم الاطلاع عليه في تاريخ 2026/01/15. على الساعة 20:46.

5. فوائد الأمن السيبراني ومناط أهميته وايجابيات وسلبيات التخصص فيه، الموقع:
تم الاطلاع عليه يوم 2026/01/15 https://bakkah.com/ar/knowledge

6. FBI, "The FBI Released Its Internet Crime Report 2024", Federal Bureau of Investigation, April 16 2024, available at: https://www.fhi.gov/contact us/field offices/atlanta/news/the fhi released its internet crime report 2024, Accessed in 29 April 2026 at 11:43

7. محمد مسلم، "التحذيرات من الاختراق والتجسس على هواتف الجزائريين"، الشروق أونلاين 24 جانفي 2022، الرابط:
httpcwwww.echoroukonline.com/%D8%AA%D8%AD%D8%B0%D9%8A%D8%B1%D8%A7%D8 :اطلع عليه بتاريخ 03 ماي 2026، على الساعة 17:30.

8. علاء الدين حميدي، الأمن السيبراني: خط الدفاع الأول في العصر الرقمي، الموقع:
https://www.aljazeera.net/blogs10/12/2025. تم الاطلاع عليه يوم 08 ماي 2026 على الساعة 14:38.

9. حسان زهار، الحروب السيبرانية تتصاعد ضد الجزائر،
الموقع : https://elikhbaria.dz/elikhbariaplus/ تم اللإطلاع عليه يوم 10 أفريل 2026، على الساعة 22:30.

فهرس المحتويات

فهرس المحتويات