جامعة بلحاج بوشعيب –عين تموشنت–

كلية الحقوق

قسم الحقوق

# الأمن السيبراني في الجزائر والتدابير التقنية والتشريعية لحمايته

مذكرة مقدمة لنيل شهادة الماستر في الحقوق

تخصص قانون خاص

من إعداد الطالبة

صحراوي فاطمة زهرة

تحت إشراف: د مجاجي سعاد

لجنة المناقشة

| | | | |
|---|---|---|---|
| الرئيس | بن طاع الله زهيرة | أستاذة محاضرة ب | جامعة بلحاج بوشعيب |
| المشرف | مجاجي سعاد | أستاذة محاضرة أ | جامعة بلحاج بوشعيب |
| الممتحن | زعزوعة نجاة | أستاذة محاضرة ب | جامعة بلحاج بوشعيب |

السنة الجامعية 2026/2025

" المعلومات هي عملة العصر الرقمي،

فاجعل خزنتك مغلقة جيدا"

بروس شناير

# شكر وتقدير

الحمد لله رب العالمين حمدا مباركا تطيب به النفوس، والصلاة والسلام على أشرف المرسلين سيدنا وشفيعنا يوم الدين محمد عليه أفضل الصلاة والسلام وعلى آله وصحبه أجمعين.

اشكر الله عز وجل على إعانتي وتوفيقي في إتمام وانجاز مشروع دراستي وتسخير لي كل الجهود لمرافقتي وتقديم يد العون في مشواري الدراسي.

لي الشرف العظيم أن أتقدم بالشكر الجزيل إلى الأستاذة العزيزة التي رافقتني في انجاز هذا العمل والتي عملت على توجيهنا وإرشادنا لإتمام هذا البحث الأستاذة الدكتورة " **مجاجي سعاد** "، فلكم منا كل الشكر والتقدير، وبارك الله فيكم.

كما اشكر كل الأساتذة الأفاضل الذين ووجهوني ولم يبخلوا على بمعلومة ولا بنصيحة في إنجاز هذه المذكرة وإتمامها على الوجه المطلوب.

# إهـــــداء

إلى نفسي التي تحملت المشقة والتعب، وصبرت على الصعاب والتحديات، وسهرت الليالي الطويلة في سبيل تحقيق هذا الهدف.

أهدي هذا العمل إلى نفسي التي لم تستسلم رغم العقبات، والتي واصلت الطريق بإصرار وعزيمة، مؤمنة بأن لكل جهد ثمرة، ولكل تعب نجاحًا يستحق الانتظار.

إلى كل من أكن له الاحترام من أستاذ أو زميل أو رفيق درب.

فاطمة زهـــرة

## قائمة اهم المختصرات

**1- باللغة العربية :**

**ج ر ج ج: الجريدة الرسمية للجمهورية الجزائرية**

**ج: جزء**

**ص ص: من الصفحة الى الصفحة**

**ص: صفحة**

**ط: طبعة**

**ع: عدد**

**مج: مجلد**

**2- باللغة الأجنبية :**

**WI-FI :** Wireless Fidelity.

# مـقـدمة

## مقدمة

إن الانتشار الضخم والواسع للأنترنت عبر العالم قلبت موازن المعاملات بين الدول في شتى المجالات الاقتصادية والتجارية وكذا السياسية، فتحولت التجارة التقليدية إلى إلكترونية، وأصبحت كل المعاملات والعلاقات السياسية والتجارية تتم عبر الفضاء الرقمي والعالم الافتراضي.

ونتيجة للتطور القياسي للأنترنت أصبح الفضاء الرقمي فضاء مفتوح يهدد الأمن القومي للدول، فتحولت الجريمة التقليدية إلى جريمة إلكترونية تتم بواسطة الحاسب الآلي وتحول المجرم التقليدي إلى مجرم إلكتروني مما أدى إلى تزايد خطر الجرائم السيبرانية التي تهدد الأمن السيبراني والقومي للمجتمع الدولي.

إن المعضلة الحقيقية للدول في عصرنا الحالي تخطت حماية الحدود الجغرافية، بل أضحت تبحث عن سبل مواجهة الإرهاب السيبراني الذي يهدد سيادة الدول ويفرض قوانينه وسياسته الخاصة من خلال إرغام الدول عن الامتناع عن القيام بعمل وتعطيل المصالح السياسية والأمنية وذلك من خلال سن هجمات عبر الفضاء الالكتروني وإحداث خلل في أجهزة الكمبيوتر وتعطيل مصالح الدول والحكومات في مختلف بقاع العالم.

أمام هذه التهديدات السيبرانية، كان لابد على الدول من تضافر جهودها للحد من انتشار الجرائم السيبرانية وانتهاج سياسات واستراتيجيات واعدة عن طريق المصادقة على اتفاقيات وإنشاء منظمات حماية لأمنها السيبراني.

يعتبر الأمن السيبراني الحماية الأصلية للبنى التحتية والبيانات من الاستخدام غير المصرح به في عالم تحولت فيه الحروب التقليدية إلى حروب إلكترونية.

كما يعمل الأمن السيبراني على تعزيز الثقة في المعاملات الإلكترونية عبر الفضاء الرقمي من خلال سن قوانين لحماية هذه الفضاءات من أي اختراق يشكل تهديدا سيبرانيا.

إن الجزائر تسعى جاهدة لمواكبة التطور التكنولوجي من خلال إدخال الرقمنة الإلكترونية في جميع المجالات والقطاعات الوطنية العمومية، إلا أنها تبقى مهددة سيبرانيا عبر مختلف الحدود السياسية والاقتصادية

وحتى الاجتماعية، الأمر الذي دفع بالدولة الجزائرية إلى تبني إستراتيجية وطنية لحماية الأنظمة المعلوماتية من خلال تعديل قانون العقوبات وسن قوانين مكملة له وعلى رأسها القانون 09-04[1] الذي ينظم القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، إضافة إلى الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية 2025-2029، التي أصدرها رئيس الجمهورية السيد عبد المجيد تبون بموجب المرسوم الرئاسي رقم 20-05 [2]المؤرخ في جانفي 2020 والتي تهدف إلى تهيئة بيئة ملائمة لجميع الفاعلين الوطنيين المعنيين بالأمن السيبراني لحماية السيادة الرقمية الوطنية.

كما تبنت الجزائر إستراتيجية وطنية لحماية الأنظمة والشبكات المعلوماتية والبني التحتية في ظل الهجمات السيبرانية، حيث أضحت حماية هذه الأنظمة ضرورة حتمية وركيزة أساسية، إذ بدأت في النهوض بالبحث على تقنيات وتدابير أمنية لتعزيز أمنها السيبراني، خاصة بعد انتهاجها للإدارة الالكترونية في جميع القطاعات الوطنية.

لقد أصبحت الجريمة الالكترونية هاجزا بدق ناقوس الخطر في دول العالم أجمع والجزائر خاصة، الأمر الذي دفع بالسياسة الوطنية استحداث جهاز لحماية المعطيات والبيانات الشخصية والبني التحتية الحساسة وذلك يندرج ضمن الأمن السيبراني والتدابير التقنية لحمايته.

هذا ما دفعنا إلى طرح الإشكالية التالية: ماهي الإستراتيجية المتبناة في الجزائر لحماية أمنها السيبراني؟

[1]- القانون رقم 09-04 المؤرخ في 5أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، ج ر ج ج، ع 47، المؤرخة في 16 أوت 2009.

[2] -المرسوم الرئاسي رقم 20-05 المؤرخ في 20 جانفي 2020، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، ج ر ج ج، ع04، المؤرخة في 26 جانفي 2020.

وتتفرع من هذه الإشكالية عدة أسئلة فرعية نذكر منها:

- كيف تبنت الجزائر حماية البيانات والمعطيات في ظل انتشار الجريمة السيبرانية؟
- ماهي التدابير القانونية والتشريعية لمكافحة الجريمة السيبرانية في التشريع الجزائري؟

تتجلى الأهمية العلمية في دراستنا لموضوع الأمن السيبراني والتدابير التشريعية والتقنية لحماية في الجزائر، في كون أنه من المواضيع الحديثة المرتبطة بالعالم الافتراضي والفضاء الرقمي التي لم تعرف دراسات أكاديمية واسعة وكافية لمعالجة هذا النوع من الجرائم الالكترونية والمرتبطة به، فكان إلزاما علينا البحث والتقصي في هذا الموضوع لزيادة المعرفة بالعالم الرقمي والفضاءات الرقمية.

تتجسد أهداف دراستنا الحالية في تبيان أهمية وخطورة الجرائم السيبرانية التي باتت تهدد الأمن القومي للمجتمع الدولي، والتعريف بموضوع الأمن السيبراني والجرائم السيبرانية التي طغت على الجرائم التقليدية ونشر الوعي حول خطورة هذه الجرائم على الأمن القومي للسيادة الوطنية، إضافة إلى تحفيز الباحثين للبحث في مثل هذه المواضيع الحديثة والمتطورة والمواكبة للتطور الرقمي.

لا يمكن أن ينطلق أي بحث علمي من الصدفة وإنما ذلك بفضل عوامل وأسباب تدفع الباحث إلى اختيار موضوع دراسته، ويعود سبب اختيارنا لموضوع دراستنا الحالية إلى عدة أسباب أولهما أسباب ذاتية تتمثل في ميولنا الشخصي لموضوع الأمن السيبراني والجرائم السيبرانية المتعلقة بالفضاء الرقمي ورغبتنا في البحث فيه، الرغبة في إنجاز بحث علمي يواكب تطورات العصر الرقمي وإثراء المكتبة القانونية بمثل هذه المواضيع الحديثة. وثانيهما أسباب موضوعية تتمثل في كون أن موضوع الأمن السيبراني من المواضيع الحديثة الدراسة في المجال المعلوماتي والرقمي، لذا كان السبب وراء هذه الدراسة التطلع لتوضيح أهمية الأمن السيبراني وعلاقته بالحياة الاجتماعية في ظل المعاملات الالكترونية والتهديدات التي تحيط بها.

إن دراسة الأمن السيبراني أضحت من الموضوعات التي تكتسي أهمية وحفاوة في ظل المجتمع الرقمي وهذا من أجل مسايرة التغيرات العالمية التي فرضتها الحروب الالكترونية، إلا أن دراسة موضوع الأمن السيبراني لم تعرف أبحاث ودراسات أكاديمية كافية بالنظر أو بالمقارنة بأهمية وخطورة هذا الموضوع نظرا لكونه موضوع حديث النشأة بميلاد العالم الافتراضي أو الفضاء الرقمي الالكتروني.

ولقد تم الرجوع إلى العديد من الدراسات السابقة ذات الصلة بموضوع دراستنا نذكر منها:

الدراسة الأولى: للطالبة أومدور رجاء، تحت عنوان خصوصية التحقيق في الجرائم المعلوماتية، أطروحة دكتوراه تخصص القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الابراهيمي، برج بوعريريج، قسم الحقوق، 2021، وكانت الاشكالية حول تكريس المشرع الجزائري للأحكام القانونية الملائمة مع خصوصية التحقيق لضمان فاعليته في مواجهة الجرائم المعلوماتية والحد من آثارها، ويرى الباحث أنه لا بد من تظافر الجهود الوطنية والدولية لمحاربة هذا النوع من الجرائم والحد منها.

أما الدراسة الثانية والموسومة تحت عنوان (تأثير الجريمة الالكترونية على الأمن السيبراني في الجزائر)، للطالبتين: مساط شيماء، وبوطيبة عائشة، مذكرة ماستر، تخصص قانون جنائي، قسم القانون العام، شعبة الحقوق، المركز الجامعي عبد الحفيظ بوضياف–ميلة، معهد الحقوق،2024–2025.

هدفت الدراسة إلى تحليل مفهوم الجريمة الالكترونية والكشف عن أسباب انتشارها وخصائصها وأنواعها مع تسليط الضوء على واقعها في الجزائر والتحديات المرتبطة بمواجهتها من خلال الإجابة على إشكالية الدراسة المتمحورة حول كيف يؤثر انتشار الجريمة الإلكترونية على الأمن السيبراني في الجزائر؟، الأمر الذي دفعنا إلى استكمال هذه الدراسة من خلال البحث عن الاليات والتدابير التي وضعها المشروع الجزائري لحماية الأمن السيبراني في الجزائر.

إضافة إلى العديد من الكتب والمقالات العلمية التي اعتمدنا عليها في انجاز دراستنا.

أما عن الصعوبات التي واجهتنا في دراستنا، هي نذره المراجع المتعلقة بموضوع الأمن السيبراني خاصة ما تعلق منها بالجانب القانوني والتشريعي باعتباره من المواضيع الحديثة والمتطورة المواكبة للتكنولوجيا الالكترونية مما يصعب البحث فيها لعدم استقرار هذا النوع من الجرائم السيبرانية المتسارعة والمتجددة في العالم الافتراضي والرقمي، الأمر الذي يدفع الباحثين نحو العزوف عن إقامة دراسات أكاديمية حوله.

محاولة للإجابة على الإشكالية المطروحة، اعتمدنا في هذه الدراسة على المنهج الوصفي، من خلال مناقشة ظاهرة الأمن السيبراني وتأصيلها معرفيا وفقهيا، وتبيان علاقتها وارتباطها ببعض المفاهيم كالحرب السيبرانية والإرهاب السيبراني، كما اعتمدنا أيضا على المنهج التحليلي الذي يظهر من خلال مناقشة وتحليل الآليات والاستراتيجيات التقنية والتشريعية لمكافحة الخطر السيبراني المتصاعد.

ومن أجل الإلمام بمختلف جزيئات الموضوع، تم تقسيم الدراسة إلى فصلين:

الفصل الأول تحث عنوان ماهية الأمن السيبراني.

أما الفصل الثاني نعالج فيه الآليات التشريعية والتدابير التقنية لحماية الأمن السيبراني في الجزائر.

# الفصل الأول
# ماهية الأمن السيبراني

**تمهيد**

تتزايد خطورة الجرائم السيبرانية بتزايد التطور التكنولوجي والتدفق المعلوماتي في الفضاء الرقمي وهيمنة العولمة الرقمية وضرورة استخدامها في شتى المجالات الاقتصادية والسياسية وحتى في العلاقات الدبلوماسية بين الدول، حيث أصبح من الضرورة التعاون بين الدول للحد من الجرائم المعلوماتية التي تهدد كيانها السياسي ومؤسساتها السياسية وسيادتها الأمنية من خلال التنسيق ببذل جهود للتصدي للتهديدات السيبرانية التي تهدد حدودها الوطنية والدولية.

وفي هذا السياق، يعد التعاون الدولي ضرورة ملحة لدفع التهديدات السيبرانية ويتجلى هذا التعاون في مختلف الاتفاقيات المنعقدة بين الدول الأعضاء ومنظمات المجتمع الدولي لحماية حدودها الجغرافية من هاجز الجرائم السيبرانية من خلال تعزيز أمنها السيبراني والقومي.

وبناء على ما سبق، فيما يتمثل الأمن السيبراني وماهي أهم المبادئ الأساسية التي يقوم عليها؟

وفي ذلك خصصنا المبحث الأول حول أهمية وأبعاد الأمن السيبراني.

ومن ناحية أخرى، وفي إطار التعاون الدولي للتصدي للتهديدات الدولية، خصصنا مبحث ثاني بعنوان التهديدات السيبرانية ودور المجتمع الدولي للتصدي لها.

## المبحث الأول: أساسيات حول الأمن السيبراني والجريمة السيبرانية

إن موضوع الأمن السيبراني من المواضيع الحديثة في المجتمع الرقمي المرتبط بشكل أصيل بالجرائم المعلوماتية والالكترونية التي طغت على الجرائم التقليدية، فالأمن السيبراني ما هو إلا آلية ووسيلة لمحاربة هذا النوع من الجرائم بشكل رقمي متطور، وهذا المبحث هو مدخل لموضوع الأمن السيبراني الموسوم تحت عنوان أساسيات حول الأمن السيبراني، ويتضمن مطلبين أساسين.

## المطلب الأول: مفهوم الأمن السيبراني وأهميته

يتضمن هذا المطلب المفهوم اللغوي والاصطلاحي للأمن السيبراني وكيف عرف المشرع الجزائري هذا الأخير، والقوانين المنظمة له، كما نتطرق من خلال هذا المطلب إلى أهم المفاهيم المرتبطة بالأمن السيبراني وإظهار أهميته في محاربة الجرائم السيبرانية والالكترونية والمعلوماتية، كل هذه العناصر سوف نتطرق لها بالتفصيل من خلال الفرعين التاليين.

### الفرع الأول: تعريف الأمن السيبراني والمفاهيم المرتبطة به:

### أولا: تعريف الأمن السيبراني

يتضمن تعريف الأمن السيبراني عدة تعريفات سواء ما تعلق ن=منها بالتعريف اللغوي والاصطلاحي، من الناحية الشريعية.

**أ/ التعريف اللغوي:**

السيبرانية لغة مأخوذة من كلمة (سيبر) وتعني صفة لأي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي، فالسيبرانية تعني (فضاء الأنترنت) وهي كلمة مشتقة من الكلمة اليونانية (Kybernetes) التي وردت بداية في مؤلفات الخيال العلمي، وكان يقصد بها قيادة ربان السفينة.[1]

**ب/ اصطلاحا:**

يشير مصطلح «الأمن السيبراني» أو ما يطلق عليه بـ «أمن نظم المعلومات» إلى أنه عبارة عن مجموعة من الإجراءات والسياسات والأدوات والمفاهيم الأمنية والمبادئ التوجيهية التي تستخدم لتحديد وتقييم وتقليل

[1]–إدريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، مجلة مصداقية، مج 01، ع 01، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي–تبسة، الجزائر، ديسمبر 2019، ص103.

المخاطر التي تهدد البيئة الإلكترونية، والتي تتضمن معالجة المعلومات وحماية الموارد الرقمية وتنظيم أصول المستخدمين.[1]

وعرفه الباحث «إدوار أمورسو» «Amorso Edward» بأنه: وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل والأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها وتوفير الاتصالات المشفرة.[2]

ويمكن تعريف الأمن السيبراني أيضا، بأنه أمن الشبكات والأنظمة المعلوماتية والبيانات والمعلومات والأجهزة المتصلة بالأنترنت، وعليه فهو المجال الذي يتعلق بإجراءات ومقاييس، ومعايير الحماية المفروض اتخاذها أو الالتزام بها لمواجهة التهديدات ومنع التعديات، أو للحد من آثارها في أقسى أو أسوء الأحوال. ويرتبط هذا الأمن ارتباطا وثيقا بأمن المعلومات، فالوصول إلى هذه الأخيرة أو بثها أو الاطلاع عليها والمتاجرة بها أو تشويهها واستغلالها هو ما يقف غالب الأحيان وراء عمليات الاعتداءات على الشبكات وعلى الانترنت بشكل أكثر.[3]

كما يعرف الأمن السيبراني على أنه: " مجموعة من الإجراءات التي تتخذ في الدفاع ضد الهجمات الالكترونية، قراصنة الكمبيوتر وعواقبها وتنفيذ التدابير المضادة المطلوبة، وهو مجموعة من الأدوات والسياسات

[1]– طاهر محمد السعيد وسليماني خالد، متطلبات تطبيق الأمن السيبراني لأنظمة المعلومات المحاسبية في المؤسسات الاقتصادية الجزائرية [دراسة حالة مؤسسة نفطال فرع غرداية (2018–2023)]، مذكرة ماستر أكاديمي، تخصص محاسبة، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة غرداية، 2023، ص22.

[2]–المرجع نفسه، ص 22.

[3]– فارس محمد العمارات وإبراهيم محمد الحمامصة، الأمن السيبراني (المفهوم وتحديات العصر)، ط1، دار الخليج للنشر والتوزيع، عمان–الأردن، 2022، ص 16.

والمفاهيم والضمانات الأمنية والمبادئ التوجيهية والتقنيات التي يمكن استخدمها لحماية البيئة الالكترونية من المخاطر المحدقة بها".[1]

**ج/ التعريف القانوني والتشريعي:**

أما التعريف التشريعي والقانوني للأمن السيبراني، فالمشرع الجزائري أعطى له تعريفا في الفقرة الثالثة من المادة العاشرة من القانون رقم 18-04[2]، المؤرخ في 10ماي 2018، المتضمن القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، بأنه: «مجموع الأدوات والسياسات والممارسات الجيدة، والضمانات والتكنولوجيات التي يمكن استخدامها في حماية الاتصالات الالكترونية، ضد أي حدث من شأنه المساس بتوفير وسلامة البيانات المخزنة أو المعالجة أو المرسلة».

كما سعى المشرع الجزائري في الفصل الثالث من الباب الثاني من الكتاب الثالث من الأمر 156-66 المؤرخ في 08 يونيو 1966 والمتضمن قانون العقوبات والمعدل بموجب القانون رقم 24-06 المؤرخ في 28 أفريل 2024 المتضمن قانون العقوبات، إلى إضافة قسم سابع مكرر عنوانه: المساس بأنظمة المعالجة الآلية للمعطيات، بالقانون04-15[3] ويشمل المواد من 394 مكرر إلى 394 مكرر 7، حيث جاء في هذا القسم بتسطير حماية فعالة لأنظمة المعالجة الآلية للمعطيات، وهو ما تركه ينص على بعض من الجرائم وما يقابلها من عقوبات للحد من ارتكابها.[4]

---

[1]-الدام محمد، الأمن السيبراني، مذكرة ماستر في الحقوق، تخصص: جريمة وأمن، كلية الحقوق والعلوم السياسة، جامعة الشهيد حمه لخضر الوادي، 2023، ص8.

[2] -القانون رقم 18-04، المؤرخ في 10ماي 2018، المتضمن القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، ج ر ج ج، ع 27، المؤرخة في 13 مايو 2018.

[3]- القانون رقم 04-15 المؤرخ في نوفمبر 2004، المتضمن تعديل وتتميم قانون العقوبات الجزائري، ج ر ج ج، ع 71، المؤرخة في 10 نوفمبر 2004.

[4]-القانون رقم 24-06 المؤرخ في 28 افريل 2024، المتضمن قانون العقوبات، ج ر ج ج، ع 30، المؤرخة في 30 ابريل 2024.

## ثانيا: المفاهيم المرتبطة بالأمن السيبراني

هناك العديد من المفاهيم المرتبطة بالأمن السيبراني يمكن حصر أهمها فيما يلي:

### أ. الفضاء السيبراني:

عرفته الوكالة الفرنسية لأمن أنظمة الإعلام (ANNSSI) بأنه فضاء التواصل المشكل من خلالها الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية، فهو إذن بيئة تفاعلية حديثة، تشمل عناصر مادية وعناصر غير مادية، مكون من مجموعة من الأجهزة الرقمية وأنظمة الشبكات والبرمجيات والمستخدمين سواء مشغلين أو مستعملين.[1]

### ب. الجريمة السيبرانية:

هي كل ما يقع على الشبكات وأنظمة تقنية المعلومات والأنظمة التشغيلية ومكوناتها من اختراق، أو تعطيل، أو تعديل، أو استخدام، أو استغلال غير مشروع.

وهي الجريمة التي يكون فيها النظام المعلوماتي وسيلة لارتكاب جريمة تقليدية إما ضد الأموال كالتحويل الالكتروني غير المشروع للأموال أو ضد الأشخاص كجريمة أو القذف عبر الانترنت.[2]

### ج. الردع السيبراني:

يعرف الردع السيبراني بأنه منع الأعمال الضارة ضد الأموال الوطنية في الفضاء والأصول التي تدعم العمليات الفضائية، ويرتكز الردع السيبراني على ثلاثة ركائز هي عماد الإستراتيجية الدفاع السيبراني وتتمثل في: مصداقية الدفاع، القدرة على الانتقام والرغبة في الانتقام.[3]

---

[1]–فارس محمد العمارات، المرجع السابق، ص21.

[2]– سعيد أوغان، الأمن السيبراني ورهانات التحول الرقمي في المغرب– التأصيل المفاهيمي والإستراتيجية التشريعية، مجلة المعرفة، ع 11، كلية العلوم القانونية والاقتصادية، جامعة محمد الخامس– الرباط– المغرب، دجنبر2023، ص103.

[3]–فارس محمود العمارات، المرجع السابق، ص21.

**د. الهجمات السيبرانية:**

عرفها عبد القادر محمد فهمي بأنها: "هجمات تستخدم فيها المنظومة الشبكية والأجهزة الحاسوبية للدولة أو الفاعلين من غير الدول لتعطيل كفاءة السيطرة والقدرة على التحكم في منظومة أجهزة أو شبكات الحاسوب وما تتضمنه من بيانات ومعلومات للفاعلين الآخرين من الدول وغير الدول، وهي أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيلها.[1]

**هـ. التهديدات السيبرانية:**

تتمثل في أي ظرف او حدث قد يؤثر سلبا على العمليات أو الأصول التنظيمية، أو الافراد من خلال نظام المعلومات عبر الوصول غير المصرح به، أو التخريب والإفصاح عن المعلومات وتغييرها او حجب الخدمة.[2]

**و. الإرهاب السيبراني:**

هو نقطة الالتقاء بين الفضاء الإلكتروني والإرهاب، حيث عبر عنه دورثيدينيغ "DorthyDennig" بقوله: " هو تقارب العالم المادي والعالم الافتراضي"، إذ أشار إلى التهديدات الجديدة التي انتقلت إلى العالم الافتراضي، فالإرهاب السيبراني يعني جميع الهجمات الخطيرة التي تحدث خلل في أنظمة الكومبيوتر الخاصة بأفراد، أو شركات، أو دول، أو حكومات لتحقيق أهداف سياسية أو اجتماعية.[3]

---

[1]–محمد الصغير كاوجة، الهجمات السيبرانية بين الواقع وسبل المواجهة، مجلة الرسالة للدراسات الإعلامية، مج 06، ع 03، جامعة قاصدي مرباح ورقلة – الجزائر، سبتمبر2022، ص111.

[2]– وزارة التعليم العالي، الأمن السيبراني، التعليم الثانوي–نظام المسارات، السنة الثالثة، شركة تطوير للخدمات التعليمية، طبعة 1446هـ–2024م، ص09.

[3]– كواشتي عتيقة، تداعيات الإرهاب السيبراني على الأمن القومي الجزائري، المجلة الجزائرية للأمن والتنمية، مج 12، ع 03، جامعة باتنة 1– الجزائر، جويلية 2023، ص208.

**ز. القوة السيبرانية:**

هي مجموعة الموارد المتعلقة بالتحكم والسيطرة على أجهزة الحاسبات والمعلومات والشبكات الالكترونية والبنية التحتية المعلوماتية والمهارات البشرية المدربة للتعامل مع هذه الوسائل، وهي دفع مهم في تدعيم القوة الناعمة للدول من خلال التأثير في توجيهات الرأي العام.[1]

## الفرع الثاني: أهمية الأمن السيبراني

إن من أهم أسباب الحاجة إلى الأمن السيبراني هو الدعوة إلى إطار تشريعي وقانوني وتنظيمي يتناسب مع التحديات التي يواجهها المجتمع أو المنظمات أو الأفراد وهي الحاجة إلى الاتصال بأنظمة الاتصال والانترنت وعدم القدرة على عزل الأجهزة عن الشبكات المحلية وشبكات المنطقة الواسعة لأفرادها لتوفير المعلومات واعتماد المؤسسات المختلفة على توافر المعلومات مع زيادة التطور التكنولوجي وزيادة الشبكات.[2]

للأمن السيبراني أهمية كبيرة في كافة المجالات تتمثل فيما يلي:

- توفير الحماية الفائقة لخصوصية المعلومات والإبقاء على سريتها وذلك بعدم السماح لغير المخولين بالوصول إليها واستخدامها.
- الحفاظ على المعلومات وسلامتها وتجانسها، وذلك بكف الأيادي من العبث بها.
- تحقيق وفرة البيانات وجاهزيتها عند الحاجة إليها.
- حماية الأجهزة والشبكات ككل من الاختراقات لتكون درع واق للبيانات والمعلومات.
- استكشاف نقاط الضعف والثغرات في الأنظمة ومعالجتها.
- استخدام الأدوات الخاصة بالمصادر المفتوحة وتطويرها لتحقيق مبادئ الأمن السيبراني.

[1]–قطاف سليمان وبوقرين عبد الحليم، المرجع السابق، ص49

[2]–المرجع نفسه، ص43

- توفير بيئة عمل آمنة جدا خلال العمل عبر الشبكة العنكبوتية.[1]

## المطلب الثاني: المبادئ الأساسية للأمن السيبراني وأبعاده:

لا يتضح مفهوم الأمن السيبراني إلا من خلال المفاهيم والمصطلحات المرتبطة به والتي تشكل حلقة وصل متداخلة، بحيث يسهل على الباحث المبتدئ في مجال أمن المعلومات بفهم العلاقة السببية بين الجريمة السيبرانية والفضاء السيبراني الذي تقع فيه والذي يكون عرضة للتهديدات والهجمات السيبرانية والإرهاب السيبراني الذي يتم ردعه إلا بقوة سيبرانية وأبعاد مسطرة.

من أجل زيادة توضيح الأهمية البالغة للأمن السيبراني، لا بد من التطرق إلى أهم المبادئ الأساسية المكونة له، وما هي الأبعاد المرتبطة به، هذا ما سوف تتطرق إليه في الفرعين التاليين:

### الفرع الأول: المبادئ الأساسية للأمن السيبراني:

تعد حماية أنظمة الحاسب والشبكات والبيانات من الوصول غير المصرح به والأنشطة الضارة أمر بالغ الأهمية، فمن الضروري الالتزام بالمبادئ الأساسية للأمن السيبراني لإنشاء إطار أمني قوي وفعال، كما يعد فهم هذه المبادئ وتنفيذها أمرا حيويا لحماية المعلومات الحساسة، وضمان دقة البيانات والحفاظ على الوصول غير المنقطع إلى الموارد الهامة، ومن أهم المبادئ الأساسية للأمن السيبراني هي السرية والسلامة والتوافر.

#### أ. السرية:

هي خاصية ترتبط بعدم تغيير البيانات والمعلومات أو فقدها أو إهدارها وإتاحتها فقط لأشخاص وكيانات معتمدة ومصرح لها فقط باستخدامها وتتضمن العمليات التي تستخدم أساليب التشفير والحجب لمحتويات البيانات والمعلومات أو السماح بها في أوقات وفي طرق معتمدة.[2]وتواجه السرية تهديدات محتملة مثل هجمات

[1]–فارس محمد العمارات، المرجع السابق، ص، ص 35،36.

[2]–مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الانترنت بين القانون الدولي الاتفاقي والقانون الوطني، ط1، مركز الدراسات العربية للنشر والتوزيع، جمهورية مصر العربية، 1447هـ–2016 م، ص 500.

التصيد الالكتروني، حيث ينتحل المهاجمون شخصيات كيانات شرعية لخداع الأفراد والحصول على معلومات حساسة[1]

**ب. بالسلامة:**

يقصد بها توكيد دقة البيانات وعدم التلاعب بها، حيث إن سلامة البيانات ضرورية للحفاظ على الثقة في أنظمة المعلومات، فبدونها لا يمكن للمستخدمين الوثوق بدقة المعلومات التي يتلقونها، ويمكن أن تساعد إجراءات مثل لتشفير والتوقيعات الرقمية إلى ضمان سلامة البيانات. ويعد اعتراض البيانات بين طرفين من الأمثلة الشائعة على تهديدات سلامة البيانات حيث يمكن للمهاجم من خلال اعتراض البيانات التسلل إلى شبكة واي فاي (WI-FI) اللاسلكية غير الآمنة والتلاعب بحزم البيانات التي تم إرسالها وتغيير دون علم المرسل أو المستلم.[2]

**ج. التوافر:**

يقصد به الحفاظ على المعدات وإجراء إصلاحات الأجهزة، والحفاظ على تحديث أنظمة التشغيل والبرامج وإنشاء نسخ احتياطية تضمن توفر شبكة والبيانات للمستخدمين المعتمدين، يجب أن تكون الخطط جاهزة للتعافي بسرعة من الكوارث الطبيعية أو الكوارث التي من صنع الإنسان، المعدات أو البرامج الأمنية مثل: الجدران النارية تحميك من هجمات مثل حجب الخدمة عندما يحاول أحد المهاجمين إرباك الموارد بحيث لا تتوفر الخدمات للمستخدمين.[3]

[1]–وزارة التعليم، الأمن السيبراني، مرجع سابق، ص11.

[2]– وزارة التعليم، المرجع السابق، ص11.

[3]–مفيد عوض حسن علي، الأمن السيبراني وأساسياته، مكتبة الدراسات العربية للنشر والتوزيع، سلطة عمان، 2025، ص22.

## الفرع الثاني: أبعاد الأمن السيبراني:

يرتبط الأمن السيبراني بمجالات عديدة ومختلفة تشمل كل من الأبعاد العسكرية والاقتصادية، والسياسية، والاجتماعية، والقانونية.

### أولا: الأبعاد العسكرية

تتمثل الميزة النسبية للقوة السيبرانية في قدرتها على ربط الوحدات العسكرية عبر الشبكات الالكترونية في الفضاء السيبراني، مما يتيح تبادل المعلومات بسهولة وسرعة بالإضافة إلى إصدار الأوامر العسكرية وتحقيق الأهداف من مسافة بعيدة بدقة فائقة، ومع ذلك يمكن أن تتحول هذه الميزة إلى نقطة ضعف إذا لم تكن الشبكات المستخدمة مؤمنة بشكل جيد ضد الاختراقات الخارجية، والهجمات السيبرانية التي يمكن أن تشل أنظمة الدفاع الجوي أو التوجيه الالكتروني وتؤدي إلى تعطيل عمل شبكات الكمبيوتر.[1]

### ثانيا: الأبعاد الاقتصادية

يرتبط الأمن السيبراني ارتباطا وثيقا بالاقتصاد يظهر في اقتصاد المعرفة وتوسع استخدام تقنيات المعلومات والاتصالات والتي تتيح تعزيز التنمية الاقتصادية لبلدان كثيرة عير إفادتها من فرص الاستخدام التي تقدمها الشركات الدولية والشركات الكبرى التي تبحث عن إدارة كلفة إنتاجها بأفضل الشروط. إلا أن هذا التطور والازدهار يطرح إشكالات عديدة حول مقدم الخدمة والعمل أو ما تعلق بحماية المستهلك عبر الانترنت إضافة إلى دخول العالم عصر المال الالكتروني ضمن بيئة تقنية متحركة بعد إطلاق خدمات المحفظة الالكترونية.[2]

[1]–صمودي كريمة وبرقعي سمر، الأمن السيبراني في الجزائر، مذكرة ماستر في القانون، تخصص قانون أعمال، كلية الحقوق والعلوم السياسة، جامعة 8 ماي 1945 قالمة، قسم الحقوق، 2025، ص14.

[2]– قيطة فاطمة الزهراء وصالحي دليلة، تعزيز الأمن السيبراني في الجزائر– الجهود القانونية العلمية والعملية، مخبر التنمية الاجتماعية وخدمة المجتمع، كلية العلوم الاجتماعية والانسانية، جامعة الشهيد لخضر الواد – الجزائر، 2024، ص6.

### ثالثا: الأبعاد السياسية

تسبب الأمن السيبراني مثل التسريبات المختلفة للوثائق الحساسة في مشاكل في العلاقات بين الدول وجعل من الضروري للدول إعادة النظر في سياساتها الخارجية. ويتجلى الدور البارز للشبكات الاجتماعية في تحقيق الأهداف السياسية مثل تنظيم الأحداث الانتخابية أو المظاهرات الافتراضية وحركات الاحتجاج الالكترونية، بالإضافة إلى نشر رسائل سياسية على شبكات التواصل الاجتماعي وتم الكشف عن العديد من الأنشطة في هذه المواقع.[1]

### رابعا: الأبعاد القانونية

تعد العلاقة بين القانون والتكنولوجيا علاقة تبادلية، فالتطورات التكنولوجية المختلفة تفرض مواكبة التشريعات القانونية لها من خلال وضع أطر تشريعات للأعمال القانونية وغير القانونية منها. ولكن بصورة عامة تفتقد الجريمة السيبرانية في الوقت الحالي للأطر القانونية الصارمة للتعامل معها، ولعل ذلك يعود لعوامل مثل طبيعة الجريمة الالكترونية في حد ذاتها وصعوبة تحديد هوية مرتكبي تلك الجرائم ومرونة التعريفات المرتبطة بتكنولوجيا المعلومات، إلى جانب ذلك فإن الجرائم السيبرانية غير مقيدة الحدود، الأمر الذي يقتضي تفعيل التعاون الدولي المشترك لمكافحتها.[2]

### خامسا: الأبعاد الاجتماعية

يهدف إلى تطوير الأمن بالقدر الذي يعزز الشعور بالانتماء والولاء وتعزيز الهوية الوطنية، إذ ساهم تنامي الصراعات الداخلية لأسباب معيارية وهوياتية في تركيز البحوث الأكاديمية على الأمن المجتمعي كبعد محوري في تفسير الظواهر الأمنية لعالم ما بعد الحرب الباردة.[3]

---

[1]–قطاف سليمان وبوقرين عبد الحليم، المرجع السابق، ص 49.

[2]–إدريس عطية، المرجع السابق، ص106.

[3]–كواشتي عتيقة، المرجع السابق، ص209.

وينبغي التشديد على واجب الأمن والمسؤولية الفردية والتدابير الرادعة، وكذلك التداعيات المحتملة في إطار القانون الجنائي التي تترتب على عدم احترام الالتزامات التي يوجهها الأمن وبصورة أكثر عمومية. فإن من الضروري توفير التثقيف والتدريب على تكنولوجيات المعلومات والاتصال، وليس فقط على الأمن والتدابير الرادعة، إذ يجب للثقافة الأمنية أن تغرس داخل ثقافة تكنولوجيا المعلومات[1].

يمكن القول أن الأمن السيبراني أصبح بعدا جديدا ضمن أبعاد الأمن القومي، حيث أجبر هذا الأخير المجتمع الدولي إلى ضرورة التحول والانتقال من العالم التقليدي إلى العالم الافتراضي والرقمي، إذ يفرض الأمن السيبراني على الدول تبني استراتيجيات وآليات لمواجهة الهجمات والتهديدات السيبرانية التي تهدد الأمن القومي.

لا يتضح مفهوم الأمن السيبراني إلا من خلال المفاهيم والمصطلحات المرتبطة به والتي تشكل حلقة وصل متداخلة، بحيث يسهل على الباحث المبتدئ في مجال أمن المعلومات بفهم العلاقة السببية بين الجريمة السيبرانية والفضاء السيبراني الذي تقع فيه والذي يكون عرضة للتهديدات والهجمات السيبرانية والإرهاب السيبراني الذي لا يتم ردعه إلا بقوة سيبرانية وأبعاد مسطرة.

[1]–بارة سمير، الأمن السيبراني في الجزائر (السياسات والمؤسسات)، المجلة الجزائرية الأمن السيبراني، مج 02، ع 04، جامعة قاصدي مرباح ورقلة، 2017، ص262.

## المبحث الثاني: التهديدات السيبرانية ودور المجتمع الدولي في التصدي لها:

التهديدات السيبرانية باختلاف وتباين تسمياتها من جرائم الانترنت وجرائم الحاسوب، فهي تقوم على ركن مادي واحد، وتهدف إلى ضرب فضاء إلكتروني وقرصنة بيانات شخصية.

في هذا المبحث نعالج أهم التهديدات والمخاطر التي تهدد الفضاء السيبراني ونبرز من خلاله آليات الحماية كالتشفير وغيرها.

### المطلب الأول: مهددات الأمن السيبراني:

إن الهدف الأول والأخير للأمن السيبراني هو حماية الأنظمة المعلوماتية والبني التحتية من أي اختراق خارجي، وذلك من خلال تعزيز برامج الدفاعية لمنع والتصدي لأي تهديدات أو مخاطر مثل القرصنة الإلكترونية وغيرها من المخاطر.

وعليه ينقسم هذا المطلب إلى فرعين أساسيين أولهما يشمل مظاهر التهديدات السيبرانية، والفرع الثاني يتضمن أنواع التهديدات السيبرانية على سبيل المثال لا الحصر.

#### الفرع الأول: مظاهر التهديدات السيبرانية

#### أولا: الهجمات السيبرانية

وهي فعل يقوض من قدرات ووظائف الكومبيوتر الغرض قومي أو سياسي أو اجرامي، من خلال استغلال نقطة ضعف معينة تمكن المهاجم من التلاعب بالنظام والتحقيق هذه الاهداف تتخذ هذه الهجمات عدة أساليب منها تذكر:

**أ. الأسلوب المستخدم**

**1- هجمات التصيد Phishing**

ويتم تنفيذها عن طريق استراتيجية التحفيز بطرق احتيالية كإرسال محتويات مشابهة للمحتويات المعتادة أو في شكل رابط يودي فتحه او الولوج إليه إلى اصابة الجهاز أو تدميره ببرامج فيروسية خبيثة.

**2- برامج الفدية Ransoeware**

نوع من المواقع الضارة يتم السيطرة من خلاله على ملفات الكومبيوتر، وهو مصمم لابتزاز الاموال عن طريق منع الوصول إلى الملفات أو نظام الكومبيوتر حتى تدفع الفدية

**3- البرمجيات الخبيثة Malware :**

هي برامج خبيثة مصممة للحصول على وصول غير مصرح به الإلحاق الضرر بجهاز الكومبيوتر

**4- الهندسة اجتماعية Social engineering :**

تستخدم هذه الاستراتيجية من طرف المعتدي لخداعك للكشف عن معلومات حساسة يمكنهم طلب دفع نقدي أو الكشف عن بياناتك السرية وتعتمد على أسلوب الاغراء أو بناء الثقة.

**ب. القطاع المستهدف**

قد يكونون أفرادا عاديين يتم اختراقهم بهدف الابتزاز، أو شركات خاصة لسرقة حقوق الملكية الفكرية وبراءات الاختراع، أو القطاع المالي والمصرفي بهدف الاضرار باقتصاد الدولة، أو سرقة الأموال، أو خدمات حكومية، أو أجهزة أمنية بهدف سرقة معلومات استخباراتية، أو خطط عسكرية، أو تصميمات أسلحة، أو مؤسسات إعلامية.

**ج. حسب الهدف من الهجمة**

فقد يكون الهدف "مالي" من خلال اختراق الحسابات البنكية، أو هدف عسكري"، مثل اختراق النظم العسكرية، أو هدف سياسي" للتعبير عن الغضب من قرارات أو تصرفات سياسية، أو هدف إنسان للتعبير عن التعاطف مع قضية إنسانية.

**د. حسب الفواعل المشاركة:**

قد يقوم بهذه الهجمات "قوات مسلحة" وجيوش إلكترونية في إطار الصراعات العسكرية والسياسية بين الدول، أو مجموعات إجرامية وعصابات منظمة من أجل السرقة وغسيل الأموال، أو " جماعات إرهابية كأحد أنواع ممارسة الارهاب الالكتروني.[1]

## ثانيا: الحروب السيبرانية

### أ. مفهوم الحرب السيبرانية

لا يوجد إجماع على تعريف محدد ودقيق لمفهوم الحرب السيبرانية، فيعرفها "**ريتشارد كلارك**"، و"**روبرت كناكي**" على أنها: " أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيلها ".

ويعرفها شاكريان بأنها: «امتداد للسياسة من خلال الإجراءات المتخذة في الفضاء السيبراني من قبل دول أو فاعلين، حيث تشكل تهديدا خطيرا للأمن القومي، ويقترح آخرون أن يتم التركيز بدلا من ذلك على أنواع وأشكال النزاع التي تحصل في الفضاء السيبرانين ويحددون مستوياتها كالتالي: القرصنة السيبرانية، وتقع

[1] محمودي سعيد، الأمن السيبراني في الجزائر: بين المعالجة الأمنية والحماية القانونية، مجلة الناقد للدراسات السياسية، مج7، ع2، جامعة بشار، 2023، ص198.

في المستوى الأول، ومن أمثلته القيام بعمليات قرصنة المواقع الالكترونية أو بتعطيل الحواسيب الخادمة من خلال إغراقها بالبيانات».

الحروب السيبرانية: «وهي المستوى الأخطر للنزاع في الفضاء السيبراني، وتهدف إلى التأثير على إدارة الطرف المستهدف السياسية وعلى قدرته في عملية صنع القرار، وكذلك التأثير فيما يتعلق بالقيادة العسكرية ولتوجيهات المدنيين في مسرح العمليات الالكترونية»[1].

**ب. خصائص الحروب السيبرانية**

من المتوقع أن تصبح الحرب السيبرانية نموذجا تسعى إليه العديد من الجهات نظرا للخصائص التي تنطوي عليها ومنها:

**1- الحرب السيبرانية حروب لاتناظرية:**

فالتكلفة المتدنية نسبيا للأدوات اللازمة لشن هكذا حروب، بمعنى ليس هناك حاجة لقدرات ضخمة لتشكل تهديدا خطيرا وحقيقيا على دولة بحجم الولايات المتحدة الأمريكية.

**2- تمتع المهاجم بأفضلية واضحة:**

فالحروب السيبرانية تتمتع بالسرعة والمرونة والمراوغة، وبالمقابل يتمتع المهاجم بأفضلية، مما يصعب نجاح عمليات الدفاع.

[1]–فارس محمد العمارات، المرجع السابق، ص ص 123،124.

**3- المخاطر تتعدى استهداف المواقع العسكرية:**

هناك جهود متزايدة لاستهداف البنى التحتية المدنية الحساسة كاستهداف شبكات الكهرباء والطاقة وشبكات النقل والنظام المالي والمنشآت الحساسة النفطية أو المائية أو الصناعية بواسطة فيروس يمكنه إحداث أي أضرار مادية حقيقية تؤدي إلى دمار هائل.[1]

## الفرع الثاني: أنواع التهديدات السيبرانية

### أولا: التجسس الإلكتروني

يعتبر التجسس الإلكتروني من أهم المستويات التمهيدية للعمليات الحربية السيبرانية، ويعرف بأنه وسيلة للاعتراض غير المصرح به الأنظمة الاتصالات والشبكات والبيانات من أجل الحصول على البيانات والمعلومات والتلاعب بها. فالتجسس الإلكتروني أولى اشكال التهديد التي تمس بالأمن القومي الوطني، وتهدد مصالح الدولة والأفراد.

وقد عرفه المؤلف الخاص بحلف الناتو بعنوان: Peacetime Regime for State Activities in Cyberspace بانه: قيام دولة أو جهاز تابع لها أو وكيل عنها بالاطلاع على أو نسخ البيانات السرية غير المتاحة للجمهور أو المحفوظة على أنظمة تكنولوجيا المعلومات أو شبكات الاتصال الموجودة في إقليم أو منطقة خاضعة لولاية دولة أخرى بواسطة عمليات سرية وبذرائع مزيفة أو كاذبة ودون ترخيص أو موافقة من مالكي أو مستخدمي هذه الأنظمة، وقد اهتز المجتمع الدولي عقب اكتشاف فضيحة التجسس المعروفة باسم قضية "برنامج بيغاسوس" التي تورط فيها النظام الصهيوني والمغربي.

[1]- إسماعيل زروقة، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية، مج 10، ع 01، جامعة محمد بوضياف-المسيلة، الجزائر، 2019، ص ص1027، 1028.

ويهدف التجسس عموما عبر الفضاء السيبراني إلى:

- اختراق النظام المعلوماتي بهدف نقل المعلومات أو البرامج كليا أو جزئيا.
- اختراق النظام المعلوماتي للمؤسسات الهامة بهدف الاطلاع على الأسرار.
- اختراق النظام المعلوماتي بهدف تدمير ثروته المعلوماتية جزئيا أو كليا.[1]

## ثانيا: القرصنة الإلكترونية

لقد تم التطرق إلى مسألة القرصنة الإلكترونية في العديد من الدراسات والكتب حسب كل تخصص غير أنه التعريف الشامل والعام للقرصنة الإلكترونية هو أنها: «سرقة المعلومات من برامج وبيانات مخزنة في ذاكرة الكمبيوتر بصورة غير شرعية أو نسخ برامج معلوماتية بصورة غير شرعية بعد تمكن مرتكب هذه العملية من الحصول على كلمة السر أو بواسطة التقاط الموجات الكهرومغناطيسية الصادرة عن الحاسب الآلي أثناء تشغيله وباستخدام هوائيات موصلة بحاسة خاصة».[2]

ويقول محمد أمين الشوابكة بأنها: «جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوبي، وتشمل تلك النتيجة من الناحية المبدئية، جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية».[3]

وتعتبر القرصنة من الآثار السلبية للتكنولوجيا، وهي عبارة عن دخول إلى نظام التشغيل في أجهزة المستخدمين بطرق غير مشروعة لأغراض غير مشروعة كالسرقة والتخريب استنادا إلى نقل أو مسح الملفات،

---

[1] –ربيعي حسين وسمر محمود، الحروب السيبرانية: المخاطر واستراتيجيات تحقيق الأمن السيبراني الدولي والداخلي، المجلة الجزائرية للأمن السيبراني، مج 07، ع2، جامعة الإخوة منثوري قسنطينة 1، ص 182.

[2]– بعوني ليلى، التهديدات في الفضاء السيبراني وانعكاساتها على السيادة الرقمية: القرصنة الالكترونية نموذجا، استراتيجيا–مجلة دراسات الدفاع والاستشراف، مج 08، ع 16، السداسي الثاني، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة الجزائر 3 ،2021، ص4

[3]– سعيد أوغان، المرجع السابق، ص1041.

إضافة ملفات أخرى وبرامج وهمية، ويستغل القراصنة نقاط الضعف في الحواسب الأمنية لمواقع الشبكة العنكبوتية للحصول على معلومات وبيانات خاصة بالزبائن.[1]

### أ. وسائل القرصنة الالكترونية

تطورت وسائل القرصنة الإلكترونية للمصنفات الرقمية بشكل مخيف وهذا ما يجعل من الصعب علينا تحديد جميع الوسائل، لكن سوف نبرز أهمها من خلال:

#### 1. حصان الطروادة Trojan horse

يعتبر حصان الطروادة، برنامجا بضعه القرصان مخبأ داخل البرامج العادية لمنشأة ما ويعمل الكمبيوتر بصورة عادية ويصبح البرنامج مخبأ للبيانات التي جمعها، ويجري تعديلات سرية في الملفات والبرامج، ويدمر أو يمحو البيانات أو حتى يسبب اغلاقا كاملا ويمكن أن تبرمج أحصنة الطروادة لتدمير كل آثار وجودها بعد التنفيذ.

#### 2. البرامج الخبيثة Malware

تسمى البرامج الخبيثة ببرامج ضارة أو البرمجيات الماكرة وهي اختصار لكلمتين (Software) و (Maluman) برزت البرامج الخبيثة إلى العلن بعد الشروع في استعمال الحاسبات بفترة قصيرة وتستهدف أهداف مختلفة فمنها ما يهدف إلى الاستيلاء والاحتيال عن طريق الحاسبات على المال، ومنها ما يسعى لتمييز ومن أخطرها البرامج الذي يسعى لإدخال أوامر إلى الحاسوب لتحقيق أهداف الإجرامية.

[1]– لرقط سمية ومعاليم سعاد، أثر تكنولوجيا المعلومات على الأمن المعلوماتي، مجلة أبحاث اقتصادية وإدارية، مج 15، ع 03، جامعة محمد خيضر– بسكرة، 2021، ص 436.

### 3. الفيروسات virus

تستعمل كلمة فيروس في مجال المعلوماتية، تسبب إتلافا لأنظمة المعالجة الآلية للمعلومات والمعطيات وهي تتسبب في تعطيل أجهزة الكمبيوتر أو إتلاف المكونات المنظمة للحاسب الآلي، أو تعطيل الشبكات عن تأدية عملها وتعرف من الناحية التقنية بأنها "عبارة عن مجموعة من التعليمات التي تتكاثر بمعدل سريع جداً وتصيب النظام المعلوماتي بالشلل، ويعد الفيروس خلية مغنطيسية قائمة ومبرمجة تنشط في وقت محدد لتخريب البرنامج الأصلي وتنتشر في الأجهزة الأخرى التي تتضمنها الشبكة بحيث تفسر ما تحتويه من معلومات".

### 4. القنبلة المعلوماتية Bomb informatique

هي برامج يتم إعداده وتثبيته داخل النظام المعلوماتي بغرض تدمير أو تعطيل البيانات التي يحتويها ويشمل على قنابل المنطقة وقنابل الزمنية تبقى ساكنة لمدة زمنية طويلة وقد يشمل البرنامج تاريخ معين بحيث يفعل البرنامج عند حلوله، وهذه المدة يحددها عادة مؤشر زمني مهامه التهديم وقد لا يرتبط مؤشر التفجير بالزمن، وإنما بشروط منطقية معينة داخل نظام التشغيل أو داخل برنامج أو ملف وذلك حسبما يحدده مبرمج القنبلة. وعليه يمكن تحديد نوعين من القنبلة المعلوماتية هما:

- **القنبلة المنطقية bomb Logique:** هي برنامج أو جزء منه ينفذ في لحظة محددة، يتم وضعه في شبكة المعلومات بهدف تحديد ظروف أو حالة أو فحوى النظام بغرض تسهيل تنفيذ عمل غير مشروع.
- **القنبلة الزمنية time bomb:** وهي قريبة من القنبلة المنطقية وتسمح بتحريك أحداث مستقبلية في تاريخ محدد أو لوقوع أحداث معينة.[1]

[1]– مرابط حمزة، داودي منصور، المرجع السابق، ص ص 38، 39.

**ثالثا: الإرهاب السيبراني**

يمثل الإرهاب السيبراني خطرا وشيكا لحياة البشرية والدول على حد السواء نتيجة صعوبة التنبؤ بحجمه وقوته، بالإضافة إلى مكان الهجوم وتوقيته، ومع تزايد التطور التكنولوجي، تزايد خطر الإرهاب لاستفادة الجماعات الإرهابية من الثورة التكنولوجية لتوجيه هجماتها على الصعيدين المادي والافتراضي.[1]

ويعرفه مكتب التحقيقات الفدرالي الأمريكي باعتباره هجوما متعمدا ضد أنظمة وبيانات الكمبيوتر بهدف التسبب في الضرر والدمار، ويعبر مفهوم الإرهاب السيبراني على كل أنواع التهديد والعدوان سواء كان ماديا أو معنويا باستخدام الوسائل الالكترونية الصادرة عن الدول أو الجماعات أو الأفراد على الإنسان، والتي غالبا ما تهدده في دينه، أو نفسه، أو عرضه، أو ماله.

وقد اعتبر دورثي دينيغ (DORTHY DENANING) أن الإرهاب السيبراني هو نقطة الالتقاط بين الفضاء الإلكتروني والإرهاب، حيث عبر عنه بقوله: "هو تقارب العالم المادي بالعالم الافتراضي "، إذ أشار إلى التهديدات الجديدة التي انتقلت إلى العالم الافتراضي. فالإرهاب السيبراني يعني جميع الحظيرة التي تحدث خلل في أنظمة الكمبيوتر الخاصة بأفراد، أو شركات، أو الدول، أو الحكومات لتحقيق أهداف سياسية، أو اجتماعية.

وقد أكد «باري كولن» (BARRYCOLLIN) في دراسة له أنه من الصعب الوصول إلى تعريف محدد لظاهرة الإرهاب السيبراني، إذ يشير هذا المفهوم إلى استخدام الفضاء الالكتروني كأداة لإلحاق الضرر بالبنية التحتية حيث تكون أهداف الإرهاب السيبراني غالبا سياسية. ويعتبر الاختلاف في عدد الأشخاص والأماكن التي تنطلق منها الهجمات الإرهابية عبر الفضاء الافتراضي الفرق الأساسي بين الإرهاب بمفهومه التقليدي

[1]–كواشي عتيقة، المرجع السابق، ص207

والإرهاب السيبراني، إذ يعد هذا الأخير ذو طابع دولي عابر للحدود والقارات، كما تتميز الهجمات الإرهابية الالكترونية بالدقة والسرعة في ضرب الأهداف.[1]

والإرهاب في الفضاء السيبراني يعد معضلة حقيقية تواجه الدول وتعدد الأمن والعلاقات الدولية، مما يتطلب حشد الجهود الدولية للحد من انتشاره بانتهاج سياسات أمنية واستراتيجيات شاملة وتنسيق إقليمي ومتعدد الأطراف في ظل الفضاء الالكتروني المفتوح الذي يتغير كل يوم ويتطور في كل لحظة ويهدد مباشرة الأمن القومي للدول، من خلال الهجوم على أنظمة صنع القرار والأنظمة الدفاعية للدولة، والسعي للسيطرة على قواعد المعلومات واستهداف الاتصالات وأنظمة المواصلات والخدمات العامة للمواطنين والدولة.[2]

ويتضمن الإرهاب الالكتروني أو الرقمي بهذا المعنى مايلي:

- أعمال اختراق المواقع وأنظمة المعلومات وكافة أشكال القرصنة.
- نشر الرعب وأشكال التهديد الموجهة نحو الأفراد أو الدول.
- استقطاب الأفراد للانخراط في التنظيمات الإرهابية والجهادية والجريمة عبر الوطنية.
- محاولة السيطرة للكاملة على المؤسسات والهياكل الاستراتيجية للدول عن طريق استعمال أسلحة تكنولوجيا المعلومات والاتصالات، أو مواجهة المعلومات من خلال الوسائط الالكترونية، وهو ما يؤدي في نهاية المطاف إلى شلل هذه الأنظمة.[3]

تبقى الجريمة السيبرانية بمختلف أنواعها وطرق قيامها تشكل خطرا وتهديدا لأمن أنظمة المعلومات المحيط بشبكات التواصل والأجهزة الحاسوبية في ظل غياب الوعي المعلوماتي لحماية البيانات والمعطيات

[1]– كواشي عتيقة، المرجع السابق، ص208.

[2]–سعيد أوغان، المرجع السابق، ص 1044.

[3]– المرجع نفسه، ص 1044.

الرقمية الشخصية من أي قرصنة أو اختراق إلكتروني، السبب الذي دفع بالمجتمع الدولي إلى ضرورة التعاون للتصدي لمثل هكذا حروب، وعليه فيما يتمثل دور المجتمع الدولي في مكافحة التهديدات السيبرانية؟

## المطلب الثاني: دور المجتمع الدولي في التصدي للتهديدات السيبرانية:

نظرا للمخاطر التي تهدد المجتمع العالم الحديث بسبب تزايد المعاملات الإلكترونية في مختلف المجالات التجارية والاقتصادية والعسكرية، كان لابد من تظافر جهود المجتمع الدولي للتصدي ومواجهة التهديدات السيبرانية من خلال التعاون والتضامن لحماية البنى التحتية والبيانات الشخصية، ويتجسد هذا التعاون الدولي في الاتفاقيات والمعاهدات التي تبنتها الدول الأعضاء لمكافحة الجريمة السيبرانية.

نعالج في هذا المطلب دور التعاون الدولي في مكافحة التهديدات السيبرانية من خلال الفرع الأول، أما الفرع الثاني فيتضمن أهم الأجهزة الدولية للتصدي لهذه التهديدات وذلك على سبيل المثال لا الحصر.

### الفرع الأول: التعاون الدولي في مكافحة التهديدات السيبرانية:

#### أولا: الاتفاقية المتعلقة بالجريمة الإلكترونية لعام 2001

تمثلت هذه الاتفاقية في اتفاقية «بودابست» التي أبرمت من طرف المجلس الأوروبي في العاصمة المجرية بودابست في سياق مكافحة الجريمة المعلوماتية، وتعد الأولى في هذا المجال، حيث شملت العديد من الجرائم التي تتم عبر الأنترنت مثل: الاختراق غير القانوني، والاحتيال الإلكتروني، تزوير بطاقات الائتمان، دعارة الأطفال وغيرها، كما تحدد إجراءات لجمع الأدلة الرقمية وحفظها.[1]

كما حددت المعاهدة الطرق الواجب إتباعها في التحقيق في جرائم الأنترنت، وتعهدت الدول الموقعة بالتعاون من أجل محاربتها، كما حاولت المعاهدة إقامة التوازن بين الاقتراحات التي تقدمت بها أجهزة الشرطة وتناولت أيضا أنواع الجرائم الالكترونية وهي الدخول غير القانوني المتعمد والاعتراض غير القانوني المتعمد

[1]–بن أوذينة سندس، الجهود الدولية في مواجهة الجرائم السيبرانية، مذكرة ماستر، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة غرداية، 2025، ص20.

والتدخل المتعمد على البيانات والمعلومات بهدف تدميرها أو حذفها أو فسادها أو تغييرها أو تعديلها أو كبتها أو إخمادها، والتدخل المتعمد في الأنظمة بهدف تعطيلها أو تدميرها، وإساءة استخدام الأجهزة واستخدام الكمبيوتر في التزوير أو الاحتيال، وجرائم دعارة الأطفال والجرائم المرتبطة بحق المؤلف.[1]

لقد كفل دستور الجزائر لسنة 2020 حماية حقوق الأساسية والحريات الفردية، وعلى أن تضمن الدولة عدم انتهاك حرمة الإنسان وقد تم تكريس هذه المبادئ الدستورية في التطبيق بواسطة نصوص تشريعية أوردها قانون العقوبات والإجراءات الجنائية وقوانين خاصة أخرى والتي تحظر كل مساس بهذه الحقوق، ومن أهم المبادئ الدستورية العامة:

**المادة 35:** الحريات الأساسية وحقوق الإنسان والمواطن مضمونة.

**المادة 47:** " –لكل شخص الحق في حماية حياته الخاصة وشرفه.

–لكل شخص الحق في سرية مراسلاته واتصالاته الخاصة في أي شكل كانت.

–لا مساس بالحقوق المذكورة في الفقرتين الأولى والثانية إلا بأمر معلل من السلطة القضائية.

– حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي.

–يعاقب القانون على كل انتهاك لهذه الحقوق".

**المادة 6/54:**" الحق في نشر الأخبار والأفكار والصور والآراء في إطار القانون، واحترام ثوابت الأمة وقيمها الدينية والأخلاقية والثقافية".[2]

[1]–العيداني محمد، المرجع السابق، ص22.

[2]– التعديل الدستوري لسنة 2020 ، الصادر بموجب المرسوم الرئاسي رقم 20–442، المؤرخ في 30 ديسمير 2020، المتعلق بإصدار التعديل الدستوري 2020، ج ر ج ج، ع 82، الصادرة بتاريخ 30 ديسمبر 2020.

## ثانيا: إتفاقية الجامعة العربية لمكافحة الجريمة السيبرانية

صدر عن جامعة الدول العربية قانونا استرشادي لمكافحة تقنية الفضاء السيبراني، حيث سعت الدول العربية لتقنين وتجريم الأعمال الغير مشروعة المرتكبة من خلال استخدام الفضاء السيبراني بالتوقيع على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في 2010/12/21 لتعزيز التعاون بين الدول العربية لمكافحة الجرائم السيبرانية والحفاظ على أمنها وسلامة مجتمعاتها.[1]

كما تحتوي هذه الاتفاقية على 43 مادة، وتتضمن خمسة فصول.

من أهم أهداف هذه الاتفاقية:

- تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات لدرء أخطاء هذه الجرائم.
- الحفاظ على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها.
- التعاون القانوني والقضائي بين دول الأعضاء.
- كما دعى المجلس الدول العربية للمصادقة على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات إلى موافاة الأمانة الفنية للمجلس باتخاذه من إجراءات لمواءمة تشريعاتها مع أحكام الاتفاقية وتجريم الصور المستحدثة من الجرائم الالكترونية لمنع المجرمين من استخدام الأنترنت وتعزيز التعاون مع المنظمات الدولية والإقليمية المعنية لمواجهة كافة أشكال الجرائم السيبرانية.[2]

[1]– الدام محمد، المرجع السابق، ص 43.

[2]–سليمان قطاف وعبد الحليم بوقرين، المرجع السابق، ص81.

### ثالثا: اتفاقية الاتحاد الإفريقي حول الأمن السيبراني وحماية البيانات ذات الطابع الشخصي

تشكل اتفاقية «مالابو» نص قانوني استراتيجي في مجال مكافحة الجرائم السيبرانية في إفريقيا، بحيث تضمنت مكافحة الجريمة السيبرانية وحماية البيانات الشخصية والإشراف على المعاملات الإلكترونية، وهي تهدف على غرار الاتفاقيات ذات الصلة إلى:

- تعزيز ومواءمة التشريعات الحالية للدول الأعضاء والمجموعات الاقتصادية الإقليمية في مجال تكنولوجيا المعلومات والاتصالات مع احترام الحريات الأساسية وحقوق الانسان والشعوب.
- إنشاء وثيقة معيارية مناسبة تتوافق مع البيئة القانونية والثقافية والاقتصادية والاجتماعية الافريقية.
- التأكيد على حماية البيانات الشخصية والخصوصية.
- تعزيز استخدام تكنولوجيا المعلومات والاتصالات وزيادة التدفق وإنقاض أسعار الأنترنت.
- العمل على تعهد كل دولة طرف باعتماد تدابير تشريعية أو تنظيمية لتحديد القطاعات التي تعتبر حساسة لأمنها القومي ورفاهية اقتصادية.[1]

### الفرع الثاني: الأجهزة الدولية في التصدي للتهديدات السيبرانية:

تتظافر الجهود الدولية في مكافحة الجريمة السيبرانية رغم كل العوائق التي تحول دون ذلك حيث نادى بعض الدول إلى ضرورة إنشاء وحدات خاصة بمكافحة جرائم الاعتداء على المعلومات الخاصة في الأنترنت.

ونجد من أهم جهات البحث الجنائي الوطنية والدولية «الأنتربول»

### أولا: المنظمة الدولية للشرطة الجنائية الأنتربول

يعد «الأنتربول» أهم آليات التعاون الدولي لمكافحة الجرائم العالمية العابرة للحدود الوطنية بصفة عامة والجريمة المعلوماتية بصفة خاصة.

[1]–الدام محمد، المرجع السابق، ص 44.

فمهمة الأنتربول الأساسية تفعيل التعاون بين أجهزة الشرطة التابعة للدول الأعضاء في المنظمة بتوحيد البيانات وتبادل المعلومات لتسيير خدمات التحقيق لضبط وملاحقة المجرمين الهاربين وتسليمهم إلى الدولة التي تطلب تسلمهم، وإنشاء وتطوير كل النظم القادرة على المساهمة بفاعلية في الوقاية والعقاب على جرائم القانون العام.[1]

تم إنشاء منظمة الشرطة الجنائية الدولية «الأنتربول» في 7 سبتمبر 1923، وتظم حاليا 190 دولة وهي تعد من أهم المنظمات الناشطة في مكافحة الجريمة العابرة للحدود بمختلف أنواعها وكذا تعمل على مد الأجهزة الأمنية المختصة بمعلومات عن الجرائم المتشبعة المرتكبة في عدة دول الممتدة إلى إقليم دول أخرى، ومن بين هذه الجرائم: جرائم المعلومات.

كما أنشأت المنظمة الدولية للشرطة الجنائية سنة2003 وحدة خاصة لمكافحة جرائم التكنولوجيا، كما قامت بوضع استراتيجية مع الدول الثمانية الكبرى لمجابهة هذا النوع من الجرائم من خلال:

- إنشاء مركز اتصالات أمن عبر الشبكة يعمل على مستوى مصالح الشركة في الدول.
- استخدام قاعدة البيانات المركزية للصور الإباحية من قبل الدول الأطراف للتحليل والمقارنة الأتوماتيكية للصور.
- تزويد الدول الأطراف بكتيبات إرشادية حول الجرائم المعلوماتية وكيفية التدريب على مكافحتها والتحقيق منها.[2]

## ثانيا: شرطة الويب الدولية

أنشئت هذه المنظمة في الولايات المتحدة الامريكية عام 1986م لتلقي شكاوى مستخدمي الشبكة وملاحقة الجناة والقراصنة إلكترونيا والبحث عن الأدلة ضدهم وتقديمهم للمحاكمة، ويضم فريق العمل بهذه المنظمة

[1]–فارس محمد العمارات، المرجع السابق، ص 150.

[2]–بوفليج محمد السعيد، المرجع السابق، ص 10.

متخصصين من هيئات إنفاذ القانون والمؤسسات الحكومية وضباط الشرطة ومتطوعين فنيين من 61 دولة حول العالم يسهل الأمر لفريق العمل بتتبع الأنشطة الإجرامية التي ترتكب من خلال الأنترنت على مستوى العالم، وفي إطار الضوابط القانونية التي تحكم حركة مرور المعلومات عبر شبكة الأنترنت.[1]

[1]–العيداني محمد، المرجع السابق، ص 22.

# الفصل الثـــاني

# التدابيـر التقنية والآليـــات التشريـعية لحمـاية الامن السيـبرانـــي فـــي الجزائر

**تمهيد:**

تعتبر الجزائر من بين الدول المستهدفة داخليا وخارجيا سواء كان التهديد في الفضاء العادي أو الفضاء الافتراضي قصد ضرب أسطولها السيادي الضخم خاصة بتزايد انتشار الجرائم الالكترونية والمعلوماتية التي تمس البيانات الشخصية والبنى التحتية، الأمر الذي يدفع المشرع الجزائري إلى اتخاذ تدابير وقائية وآليات حماية لمكافحة الجرائم السيبرانية والتضييق على الهجوم السيبراني من خلال التعديلات في القوانين التشريعية ورفع العقوبات المتعلقة بالجرائم الإلكترونية، بل ولم يكتفي المشرع بتسليط عقوبات أصلية فقط، فقد أضاف إلى جانبها عقوبات تكميلية مقيدة لحرية المجرم الإلكتروني نظرا لخطورة هذه الجريمة التي تمس أمن الدولة وسيادتها.

تبنى المشرع الجزائري العديد من القوانين المتعلقة بمحاربة ومكافحة الجريمة الإلكترونية، إضافة إلى الرؤية المستقبلية التي تمثلت في الاستراتيجية الوطنية لحماية أمن الأنظمة المعلوماتية 2025-2029، المسطرة من طرف السيد رئيس الجمهورية عبد المجيد تبون.

كل هذه المعطيات سوف نتطرق لها بالتفصيل في هذا الفصل من خلال تقسيمه إلى مبحثين أساسيين، نتناول في المبحث الأول الإجراءات والوسائل المتعلقة بالأمن السيبراني، والمبحث الثاني نتطرق لأهم الآليات المتخذة لمحاربة الجريمة السيبرانية وفق التشريع الجزائري.

## المبحث الأول: إجراءات ووسائل الامن السيبراني في ظل أنظمة المعلومات:

يعتمد الأمن السيبراني على العديد من الإجراءات والوسائل الناجحة لحماية أمن أنظمة المعلومات والتي تناولها المشرع الجزائري في مختلف القوانين المتعلقة بحماية المعطيات الشخصية في مجال تكنولوجيا الإعلام والاتصال.

حيث لا يمكن الحديث عن هذه الإجراءات دون التطرق لمفهوم الجريمة الالكترونية في التشريع الجزائري وما هي مختلف القوانين التي تضبطها؟

## المطلب الأول: دور الأمن السيبراني في محاربة الجريمة السيبرانية:

يشهد العالم الحديث تطور تقنيا متسارعا، أدى إلى ظهور أنواع وأشكال من الجرائم المعلوماتية والالكترونية غير مسبوقة تهدد أمن المجتمع الدولي، الأمر الذي استدعى إلى ضرورة إعادة صياغة الجريمة من مفهومها التقليدي الكلاسيكي إلى المفهوم المرتبط بالعالم الافتراضي والرقمي.

فالجريمة الالكترونية بشكل عام هي كل فعل غير مشروع يستهدف الأنظمة المعلوماتية والبنى التحتية للدول، ونتيجة للتطور الهائل والمتزايد في أشكالها، بات من الضروري وضع تعريف ومفهوم دقيق ووضع آليات لمكافحتها والتصدي لها.

### الفرع الأول: مفهوم الجريمة السيبرانية:

### أولا: تعريف الجريمة السيبرانية

الجريمة السيبرانية هي كل ما يقع على شبكات وأنظمة تقنية المعلومات والأنظمة التشغيلية ومكوناتها (الأجهزة والبرمجيات والخدمات) من اختراق، أو تعطيل، أو تعديل، أو استخدام، أو استغلال غير مشروع.

وهي الجريمة التي يكون النظام المعلوماتي فيها وسيلة لارتكاب جريمة تقليدية إما ضد الأموال كالتحويل الالكتروني غير المشروع للأموال أو ضد الأشخاص كجريمة السب أو القذف عبر الانترنت[1].

هي كل فعل غير مشروع يستهدف تغيير البيانات، أو المعلومات بالحذف، أو الإضافة، أو المعالجة، أو السرقة، أو تحويل المعلومات، أو تعديلها لغايات غير مشروعة بواسطة الكمبيوتر، أو أية وسيلة تكنولوجية أخرى[2].

كما تعرف بأنها الجرائم التي لا تعرف الحدود الجغرافية، والتي يتم ارتكابها بأداة هي الحاسب الآلي عن طريق شبكة الانترنت وبواسطة شخص على دراية فائقة.

وهي مجموعة من الأفعال المرتبطة بالمعلوماتية والتي يمكن أن تكون جديرة بالعقاب.[3]

---

[1]–سعيد أوغان، المرجع السابق، ص1039.

[2]– العيداني محمد، التهديدات السيبرانية وجرائم المعلومات، مجلة الاجتهاد للدراسات القانونية والاقتصادية، مج 13، ع 01، المركز الجامعي الشريف بوشوشة أفلو(الجزائر)، 2024، ص17.

[3]–بومحراث ليندة، إجراءات التحقيق الخاصة بالجرائم السيبرانية، يوم دراسي حول: الجريمة السيبرانية، جامعة الأمير عبد القادر للعلوم الإسلامية قسنطينة، 2022، ص9

وتتميز الجريمة السيبرانية بعدة خصائص تميزها عن غيرها من الجرائم التقليدية وهو الأمر الذي يجعل منها تمثل تهديدا قانونيا وحقيقيا في هذا الفضاء الافتراضي الرقمي ومن بين الخصائص المميزة لهذه الجريمة أنها تعتبر من بين أهم الجرائم الخفية لأنها تقع في بيئة رقمية أو فضاء سيبراني لا حدود له وفي الغالب لا يشعر بها المجني عليه كسرقة البيانات أو إرسال الفيروسات إلى الجهاز المضيف، حيث تتسم بالحدوث في البيئة الافتراضية لأنها تعد من الجرائم الناعمة وذلك كون أن الجاني يتمتع بقدرات فنية تمكنه من تنفيذ جريمته بدقة دون إحداث أي فوضى ذات طابع مادي الأمر الذي يؤدي إلى صعوبة كشف هوية الفاعل.

كما تختص الجرائم المرتكبة عبر شبكة الانترنت بالغموض وصعوبة الاكتشاف على غرار الجرائم التقليدية كالسرقة أو الاختلاس أو التخريب، حيث أن السبب الرئيسي الكامن في صعوبة إثبات الجريمة السيبرانية يتمثل في أن البيانات الموجودة عبر شبكة الانترنت تكون على هيئة نبضات إلكترونية غير مرئية ورموز مخزنة في وسائط تخزين ممغنطة بلغة الصفر والواحد.

ومن بين صعوبة الوصول إلى الدليل في الجرائم السيبرانية المرتكبة أيضا، هو قيام كبرى المواقع العالمية بإحاطة البيانات المخزنة على صفحاتها بسياج من الحماية أو ما يسمى بجدار الحماية الناري لمنع التسلل والوصول غير المشروع إليها لتسريبها أو تبديلها أو الاطلاع عليها ونسخها.[1]

أما التشريع الجزائري، فلم يعطي أي تعريف لها إلا بصدور القانون رقم 09-04[2] المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وعرفها بأنها: " جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية ".[3]

ويعرفها مكتب تقييم التقنية في الولايات المتحدة الأمريكية بأنها الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دوار رئيسيا. أو هي فعل إجرامي يستخدم الحاسب في ارتكابها كأداة رئيسية.

---

[1]–مباركة حنان كركوري، التأصيل القانوني للجرائم السيبرانية المرتكبة عبر الوسائط الرقمية، المجلة الافريقية للدرسات القانونية والسياسية، مج 07، ع 01، مخبر قانون الأسرة، جامعة أحمد دراية، أدرار–الجزائر، 2023، ص ص129،128.

[2]– القانون رقم 09-04 المؤرخ في 5أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، ج ر ج ج، ع 47، المؤرخة في 16 أوت 2009.

[3]–خرشي عثمان وعمارة فتيحة، الترصد الالكتروني كآلية لمكافحة الجرائم المعلوماتية، مجلة الدراسات الحقوقية، مج 7، ع 3، جامعة سعيدة – الجزائر، 2020، ص797.

## ثانيا: أشكـــالـــــها

قد يأخذ هذا التهديد عدة أشكال منها:

- تعطيل الخدمات سواء المدنية أو العسكرية أو الحرمات منها مؤقتا، أو إحداث ارتباك، أو شلل كلي، أو جزئي.
- التجسس السيبراني على الأشخاص، أو الكيانات والمؤسسات الحكومية، أو غير الحكومية، أو العسكرية.
- الإرهاب السيبراني من خلال نشر الفكر الإرهابي للجماعة، أو المنظمة، أو التهديد، أو طلب الفدية.
- سرقة المعلومات والبيانات الحكومية، أو العسكرية.
- تزييف، أو تحريف المعلومات والبيانات، أو إتلافها، أو تدميرها إلكترونيا، أو التلاعب به وإعادة إدراجها بشكل مخالف[1].
- التجسس: وهي عمليات الاختراق الالكتروني التي تتم عن طريق استعمال التقنيات العالية من طرف أجهزة الاستخبارات الجنبية للوصول إلى المعلومات السرية المخزنة في المواقع الحيوية والإستراتيجية للدولة على شاكلة تسريبات ويكي ليكس.
- الابتزاز: كنشر معلومات، أو صور، أو بيانات صحيحة، أو غير صحيحة عن شخص بغرض الحصول على المال، أو علاقة غير شرعية.
- التحايل والتصيد: وهو عندما يخدع الإلكترونيون الأشخاص للكشف عن ذلك التصيد الاحتيالي.

[1]–بوفليج محمد السعيد، أطر التعاون الدولي للتصدي للتهديدات السيبرانية، مجلة الدراسات القانونية التطبيقية، مخبر الدراسات القانونية التطبيقية، مج 01، ع02، جامعة الإخوة منتوري قسنطينة 1، 2020، ص06.

- التأثير السلبي على الرأي العام من خلال التلاعب بحقيقة البيانات، أو التحريض، أو نشر الإشاعات وغيرها.[1]

## ثالثا: خصائص الجريمة السيبرانية

تتميز الجريمة المعلوماتية بصفة عامة عن الجريمة التقليدية في عدة نواحي سواء كان هذا التميز في السمات العامة أو في الباحث على تنفيذها أو في طريقة هذا التنفيذ، ومن أهم خصائصها:

### أ. صعوبة اكتشاف الجريمة الالكترونية:

تتسم الجرائم الناشئة عن استخدام الأنترنت بأنها خفية ومستترة في أغلبها، لأنها الضحية لا يلاحظها رغم أنها قد تقع أثناء وجوده على شبكة الأنترنت، كما أن وسيلة تنفيذها في أغلب الأحيان تتميز بالطابع الثقفي الذي يضفي عليها الكثير من التعقيد.[2]

### ب. صعوبة إثبات الجريمة الإلكترونية:

فالجريمة الالكترونية تتم في بيئة غير تقليدية يصعب إثباتها أثناء التحقيق الالكتروني لعدة أسباب منها:

- غياب الدليل المرئي.
- صعوبة الوصول إلى الدليل بسبب وسائل الحماية التقنية التشفير، كلمة السر.
- ضخامة المعلومات والبيانات الواجب فحصها مع إمكانية خروجها على النطاق الإقليمي للدولة بسبب البعد الجغرافي بين الجاني والمجني عليه.[3]

---

[1]–قيطة فاطمة زهرة وصالحي دليلة، المرجع السابق، ص 05.

[2]–عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماستر المهني الطور الثاني، تخصص: إدارة التحقيقات الاقتصادية والمالية، جامعة قاصدي رابح–ورقلة، ميدان العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، 2019، ص10.

[3]–بومحراث ليندة، المرجع السابق، ص10

## رابعا: تقسيمات الجرائم السيبرانية:

وفقا للمفوضية الأوروبية، فإن الجرائم الالكترونية تشمل ثلاث فئات من النشاط الاجرامي، وهي:

- صور الجرائم التقليدية مثل الاحتيال والتزوير المعلوماتي.
- نشر المحتوى غير المشروع بالوسائل الالكترونية منها المتعلق بالعنف الجنسي ضد الأطفال وانتهاك حقوق الملكية الفكرية.
- الاعتداءات الخاصة بالشبكات الالكترونية كالقرصنة.[1]

وقد تنقسم الجرائم السيبرانية إلى ثلاثة أقسام وهي:

**أ. الجرائم ضد الأفراد:**

وقد سميت بالجرائم الالكترونية الشخصية، وقد تتمثل في سرقة الهوية ومنها الايميل الالكتروني وانتحال شخصية أخرى بطريقة غير شرعية عبر الانترنت بهدف الاستفادة من هذه أو لإخفاء هوية المجرم لتسهيل عملية الاجرام.

**ب. الجرائم ضد الملكية:**

تتمثل في ارسال مواقع أو روابط ضارة المضمنة في بعض البرامج التطبيقية والخدمية أو غيرها، والتي تهدف إلى تدمير الأجهزة أو البرامج المملوكة للشركات الحكومية أو البنوك أوحتى الممتلكات الشخصية.

[1]–مهدي رضا، الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري، مجلة إيليز للبحوث والدراسات، مج 06، ع 02، جامعة محمد بوضياف المسيلة (الجزائر)،2021، ص 216.

**ج. الجرائم ضد الحكومات:**

يقصد بها مهاجمة مواقع الحكومات الرسمية وأنظمة الشبكات الحكومية والتي تستخدم تلك التطبيقات على المستوى المحلي والدولي كالهجمات الإرهابية على شبكة الانترنت، وهي تهدف إلى تدمير البنى التحتية ومهاجمة شبكات الكمبيوتر وغالبا ما يكون هدفها الأساسي وتستخدم غالبا في الحروب[1].

## الفرع الثاني: مفهوم المجرم الالكتروني وخصائصه

### أولا: تعريف المجرم الالكتروني

يقصد بالمجرم الالكتروني هو المجرم الذي له القرة على تحويل لغته الى لغة رقمية وتخزينها واسترجاعها باستخدام الحاسوب الالكتروني في ملحقاته ووسائل الاتصال الرقمية، وذلك بأداء فعل الامتناع عنه مما يحدث اضطرابات في المجتمع الدولي والمحلي نتيجة لمخالفة واعداد الضبط الاجتماعي محليا او دوليا.

أو هو مجرم سلك سبيل التقنية لارتكاب جرائمه والممثل في استخدامه لتقنية المعلومات. وهو كل شخص طبيعي او معنوي يتوافر لديه كشرط أساسي معرفة كافية بالية عمل وتشغيل الحاسب الالي، يقوم بعملية اما بحسن نية أو سوء نية كأعمال الاتلاف او الغش.[2]

يطلق خبراء أمن المعلومات الإلكترونية مصطلح" hackers" وهي جمع الكلمة هاكر وهو الإنسان الذي يقوم بعمليات الاختراق والتخريب عبر شبكة الانترنيت كما يطلقون مصطلح كراكرز " crackers" على المتخصصين بفك شفرات البرامج، وليس تخريب الشبكات فهم نوع من الهاكرز المتخصص.[3]

---

[1]–محمد الصغير كاوجه، المرجع السابق، ص 113.

[2] –بكوش محمد أمين وهروال نبيلة هبة، خصوصية المجرم الالكتروني – مجرم الأنترنت نموذجا، مجلة البحوث في الحقوق والعلوم السياسية، مج 07، ع 01، جامعة تيارت – الجزائر، 2021، ص 76.

[3] –خليلي سهام، خصوصية المجرم الالكتروني، مجلة المفكر، مج 12، ع 15، جامعة محمد لمين دباغين – سطيف 2، 2017، ص405.

## ثانيا: خصائص مرتكبي الجريمة السيبرانية:

تختلف الجريمة الإلكترونية عن الجريمة التقليدية في طريقة ملابساتها والقائم بها، فالمجرم الالكتروني يتمتع بجملة من الخصائص:

أ. **المجرم لا يتواجد على مسرح الجريمة:** بل يرتكب جريمته عن بعد وهو ما يعني عدم التواجد المادي للمجرم السيبراني فقد يوجد الجاني في بلد ما ويستطيع الدخول الى ذاكرة الحاسب الآلي الموجود في بلد آخر، ويظهر أكثر في البرامج الخبيئة (Viruses) حيث يتم نسخها في بلد وترسل الى دول مختلفة من العالم.

ب. **المجرم الإلكتروني ذكي ومتخصص:** في الغالب يتميز المجرم الإلكتروني بالذكاء، حيث يمتلك هذا المجرم من المهارات ما يؤهله للقيام بتعديل وتطوير في الأنظمة الأمنية الإلكترونية، حيث يستطيع المجرم الإلكتروني أن يكون تصور كاملا لجريمته حتى لا يتمكن من ملاحقته وتتبع أفعاله الإجرامية من خلال الشبكات أو داخل أجهزة الكمبيوتر، فالمجرم الإلكتروني عادة يمهد لارتكاب جرائمه بالتعرف على كافة الظروف المحيطة به، لتجنب ما من شأنه ضبط أفعاله والكشف عنه، كما أنه يتمتع بقدرة ومهارة تقنية يستغلها في اختراق الشبكات وكسر كلمات المرور أو الشفرات بغاية الحصول على البيانات والمعلومات الموجودة في أجهزة الكمبيوتر ومن خلال الشبكات.

ج. **المجرم الإلكتروني شخص سوي واجتماعي:** يتميز بأنه إنسان اجتماعي، فهو لا يضع نفسه في حالة عداء مع المجتمع الذي يحيط به، بل على العكس من ذلك نجده إنسان متوافق مع مجتمعه ولكنه يقترف هذا النوع من الجرائم بدافع اللهو أو بغاية إظهار تفوقه على آلة الكمبيوتر أو على البرامج التي يتم تشغيله بها، أو بدافع الحصول على الأموال أو بهدف الانتقام.[1]

[1] العيداني محمد، المرجع السابق، ص 19.

إن الجريمة الالكترونية باختلاف خصائصها التي تميزها عن الجريمة التقليدية خاصة المتعلق بالفضاء الافتراضي عكس الواقعي الملموس، وكذا الهدف من وقوعها الذي يبنى عن إظهار المهارات والمعارف التقنية بتكنولوجيا المعلومات، في حين تكون الجريمة التقليدية مادية، إلا أنها تبقى جريمة متكاملة الأركان في معظم التشريعات الجزائية.

## الفرع الثالث: العقوبات الردعية للجرائم الالكترونية في التشريع الجزائري:

سن المشرع الجزائري جملة من القوانين التي تنظم وتضبط الجرائم الالكترونية والمعلوماتية التي تهدد أمنها القومي والسيبراني، وذلك بتنظيم عقوبات ردعية ضد مرتكبيها، والأكثر من ذلك هو معاقبة المجرم الالكتروني بعقوبات تكميلية مقيدة لحريته بهدف محاربة الجريمة الالكترونية والحد من انتشارها.

### أولا: العقوبات الأصلية للجرائم الالكترونية

ينص المشرع الجزائري في المادة 394 مكرر من قانون العقوبات رقم 25-06 على عقوبة الحبس من ستة أشهر إلى سنتين، وبغرامة من 60.000 دج إلى 200.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك، تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير معطيات المنظومة.

كما جاء القانون 18-07 بعقوبة الحبس من سنتين إلى خمس سنوات، وبغرامة من 200.000.00 دج إلى 500.000.00 دج كل شخص يخالف أحكام المادة الثانية من هذا القانون، أما بالنسبة للشخص المعنوي الذي يرتكب الجرائم المنصوص عليها في هذا القانون، فتطبق عليه أحكام قانون العقوبات.[1]

[1]-نادية لاكلي، الجرائم الالكترونية في الجرائم والعقوبات المقرر لها، مجلة الاجتهاد القضائي، مج 15، ع 01، مخبر أثر الاجتهاد القضائي على حركة التشريع، جامعة محمد خيضر بسكرة، 2023، ص 268.

## ثانيا: العقوبات التكميلية

يقصد بها تلك العقوبات التي يحكم بها إلى جانب العقوبات الأصلية وتكون منظمة بمجموعة من القوانين التي يطلق عليها مصطلح قانون العقوبات التكميلي أو القوانين الملحقة بقانون العقوبات.

وقد شدد المشرع العقوبات على مرتكبي الجرائم الالكترونية من خلال الحكم على المجرم الالكتروني بعقوبات تكميلية تتمثل في مصادرة الأجهزة والبرامج والوسائل المستخدمة، مع إغلاق المواقع محل الجريمة وكذلك إغلاق محل أو مكان الاستغلال في حالة ارتكاب الجريمة بعلم المالك، وهذا ما أقرته صراحة المادة 394 مكرر 6 من قانون العقوبات كغلق مقهى إلكتروني ارتكبت فيه الجريمة الالكترونية بعلم مالكه.[1]

ونشير إلى أن المشرع الجزائري قد جاء ببعض التدابير الوقائية التي تتخذ مسبقا من طرف المصالح المعنية لتفادي أو الكشف عن الجرائم الإلكترونية وذلك بموجب القانون رقم 09-04 السالف الذكر والمتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، إذ تنص المادة الثالثة منه على أنه: "مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائرية، وفي هذا القانون وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية.[2]

يستخلص مما تقدم عرضه أن الجريمة الالكترونية جرائم تتم بواسطة كل وسيلة أو أداة ترتبط بالحاسوب وتهدد المعطيات والبيانات المخزنة في أجهزة الحاسوب أو الهاتف تشكل خطرا على أمن أنظمة المعلومات

[1]–قانون رقم 06-02 المؤرخ في 19 يونيو 2016، المتضمن قانون العقوبات، ج ر ج ج، ع 37، المؤرخة في 22 يونيو2016، ص 142.

[2]–نادية لاكلي، المرجع السابق، ص269.

للمؤسسات الحكومية وكذا المؤسسات الاقتصادية والأمنية، الأمر الذي دفع المشرع في تشديد العقوبات المتعلقة بالجرائم الالكترونية منها الأصلية والتكميلية نظرا لخطورتها على الأمن القومي والسيبراني للدولة.

## المطلب الثاني: الاليات التقنية لأمن الأنظمة المعلوماتية

يتم اللجوء لمجموعة من طرق الحماية من أجل الحفاظ على أمن المعلومات، فهناك العدد من الطرق البسيطة التي يجب اتباعها لضمان سرية البيانات وسلامتها وحمايتها من الاختراق او الضياع وتشمل هذه الاليات مجموعة من الوسائل التقنية متل البرامج الكاشفة، الجدار الناري، وتشفير البيانات.

### الفرع الأول: الجدران النارية

ان الجدار الناري هو عبارة عن جهاز او تطبيق ويتم وضعه عند الخادم وعند مصافي الشبكة، كل حسب احتياجاته، وقد جاءت فكرة الجدار الناري من الطريقة الأمنية المعروفة قديما وهي عبارة عن حفر خندق حول قلعة لمنع أي شخص من الدخول أو الخروج من القلعة، ويمكن تفتيشه من قبل الحراس. لذا يقصد بالجدار الناري مجموعة أنظمة توفر سياسات أمنية بين الأنترنت والشبكة الخاصة لتصبح جميع عمليات العبور الى الشبكة أو الخروج منها تمر من خلال الجدار الناري الذي يصد المستعملين غير المرغوب فيهم، فالجدار الناري يقوم بالتحقق من صلاحية المستعمل المحلى والمستعمل الخارجي، ونظام الدخول والخروج وتشفير المعلومات وإجراءات الحماية من الفيروسات.[1]

- **<u>مزايا الجدار الناري:</u>**

- توفير الحماية اللازمة للشبكة والمعلومات.
- توفير خدمات التشفير في تكنلوجيا الجدار الناري.
- تخزين العمليات والمعلومات التي تمر من طريق الجدار الناري.
- متابعة المستخدمين للشبكة ومن يحاول العبث بها.

[1]– حزام فتيحة، حماية الأنظمة الرقمية بين الاليات التقنية وأجهزة الحماية – قراءة في احكام المرسوم الرئاسي 05–20، مجلة الحقوق والعلوم الإنسانية، مج 13، العدد 03، جامعة بومرداس – الجزائر، 2020، ص174.

## الفرع الثاني: البرامج الكاشفة

إن مسألة تعرض جهاز الحاسب الآلي للهجمات الفيروسية أمر وارد والذي بالنتيجة يؤدي حتما لتلف المحررات الإلكترونية بسبب العدوى التي تحدثها تلك الفيروسات، لذا كان من الضروري التفكير في إيجاد آليات تحول دون حصول ذلك، وعليه، فقد أنشئت برمجيات تحتوي عددا من الموظفين من إداريين ومحللي نظم ومبرمجين لتصميم وإعداد وكتابة برامج الكشف عن الفيروسات، ومن ثم تدميره قبل أن يبدأ عمله في النظام. نجد أغلب برامج الكشف عن الفيروسات ومكافحتها تستطيع التعرف إلى ملفات التجسس وتقوم بإزالتها من الجهاز، لكن هناك ملفات التجسس قد لا تستطيع برامج مكافحة الفيروسات اكتشافها. رغم كل تلك التدابير إلا أن الجهاز لايزال غير آمن، لهذا يجب تجنب وضع قوائم بكلمات السر أو الاستخدام على الجهاز، وخصوصا أرقام الحسابات البنكية، وبطاقات الائتمان مع التقليل من الدخول على الحسابات البنكية عبر الأنترنت، وعدم الاحتفاظ بتقارير سرية تحوي أرقاما مهمة على القرص الصلب، لكون المخترقين يعملون بجد لاختراق كل الأنظمة والبرامج.[1]

## الفرع الثالث: التشفير الالكتروني

يعرف التشفير على أنه مجموعة من التقنيات التي تهدف إلى حماية المعلومات عن طريق استعمال بروتوكولات سرية، تجعل البيانات المشفرة غير مفهومة لدى الغير بواسطة البرامج المخصصة لذلك.

كما يعرف على أنه: تدبير تكنولوجي يهدف لحماية المنصات الرقمية من القرصنة عن طريق استخدام رموز وإشارات وأرقام وحروف تجعل البيانات مشفرة غير مفهومة للغير، تكبح الاستعمال غير المشروع للمصنف إلا لمن يملك فك الشفرة بناء على ترخيص أصحاب الحقوق.

وعرفه المشرع الجزائري من خلال استعمال مصطلح الترميز بدلا من مصطلح التشفير، وذلك في نص المادة 14 من المرسوم التنفيذي رقم 98-257 المتعلق باستغلال خدمات الانترنت المعدل بموجب المرسوم

[1] – حزام فتيحة، المرجع السابق، ص 175.

التنفيذي رقم 2000-307 المؤرخ في 14 أكتوبر 2000 الذي يضبط شروط وكيفيات إقامة خدمات الأنترنت واستغلالها.[1]

وعرف المشرع الجزائري مفتاح التشفير الخاص والعام في القانون المتعلق بالتوقيع والتصديق الالكترونيين في المادة الثانية الفقرة 08 و09 على التوالي[2]، وكان من الأجدر على المشرع معالجة التشفير بشكل أكثر تفصيل من خلال تناول جوانبه وأحكامه لضمان أمن وسلامة المعلومات المشفرة في ظل التطور التكنولوجي الكبير وما صاحبها من تزايد الاعتداءات في الفضاء الرقمي[3].

التشفير هو عملية تحويل المعلومات إلى صيغ بحيث يتعذر على الأطراف غير المصرح لهم قراءتها، ويمتلك الأشخاص الموثوق بهم فقط الذين يمتلكون المفاتيح السرية أو كلمات المرور القدرة على تشفير البيانات والوصول إليها في صيغتها الأصلية، والتشفير في حد ذاته لا يمنع أي شخص من توقع البيانات، بل يمكنه فقط منع الأشخاص غير المرخص لهم من عرض المحتوى أو الوصول إليه.

والذي يعتبر من أكثر أنواع الاختراقات انتشارا وأخطرها، والتي برمجت لاختراق الأجهزة الالكترونية المختلفة والمتصلة بشبكة الانترنت، حيث تقوم بنشر الفيروسات وذلك بعد استغلال الثغرات الأمنية في النظام ثم تقوم بتشفير الملفات داخل الجهاز ومن ثم يقوم الهاكر بطلب مبالغ مالية من الضحية مقابل حصوله على مفتاح فك الشفرة والذي غالبا يكون غير موجود، أي لا توجد ضمانات لإعادة البيانات[4].

---

[1]– مرسوم تنفيذي رقم 2000-307، المؤرخ في 14 أكتوبر 2000، يعدل المرسوم التنفيذي رقم 98-257، المؤرخ في 25 غشت 1998، الذي يضبط شروط وكيفيات إقامة خدمات الأنترنت واستغلالها، ج ر ج ج، ع 60، المؤرخة في 15 أكتوبر 2000.

[2] –القانون رقم 15-04، المؤرخ في 01 فبراير 2015، يحدد القواعد المتعلقة بالتوقيع والمصادقة الالكترونيين، ج ر ج ج ، ع 06، المؤرخة في فبراير 2015.

[3]–مرابط حمزة وداودي منصور، التشفير كآلية لحماية المصنعات الرقمية من القرصنة الالكترونية، مجلة الحقوق والعلوم السياسية، مج 10، ع 01، جامعة خنشلة، 2023، ص ص41،40.

[4] – مفيد عوض حسن علي، المرجع السابق، ص 71

## أولا: أهداف التشفير

للتشفير عدة أهداف أهمها ضمان سرية وسلامة البيانات إضافة إلى عدم إنكار البيانات لمن صدرت منه نتناولها كالتالي:

### أ. سرية البيانات

يكمن الهدف الأول من عملية التشفير في الحفاظ على سرية المعلومات وخصوصيتها. وذلك بالاحتفاظ بالمعلومات في صيغة مخفية عن أي شخص آخر غير الشخص المقصود. وهذا ما يوفر الثقة في التعاملات الإلكترونية عن طريق منع الغير من مستخدمي الشبكة من الدخول للبيانات والحفاظ على سريتها، باستخدام وسائل إلكترونية أو رموز معينة لا يعلمها إلا أطراف التعامل الإلكتروني وذلك باستخدام أدوات ووسائل تحويل المعلومات بهدف إخفاء محتوياتها بما لا يتيح استخدامها غير المشروع، بحيث يتم التأكد من أن المعلومات التي تسلمها المرسل إليه هي ذات البيانات التي قام المرسل بالتوقيع عليها.

### ب. سلامة البيانات

أما سلامة البيانات فهي وظيفة موجهة لأغراض احتواء التغييرات غير المسموح بها للبيانات من قبل الأشخاص غير المرخص لهم، وبذلك فالتشفير يحمي البيانات من وصولها مشوهة إلى الطرف الآخر، دون أي خلل أو اعتداء من الغير عليها.

### ج. عدم الانكار

يعد التشفير بوجه عام وتطبيقاته العديدة وفي مقدمتها التواقيع الالكترونية، الوسيلة الوحيدة لضمان عدم انكار التصرفات عبر الشبكات الالكترونية، وبذلك فان التشفير يمتل الاستراتيجية الشمولية لتحقيق اهداف

الأمن من جهة، وهو مكون رئيس لتقنيات ووسائل الأمن الأخرى خاصة في بيئة الأعمال الالكترونية، التجارة والرسائل الالكترونية وعموما البيانات المتبادلة بالوسائط الالكترونية.[1]

## ثانيا: تقنيات التشفير

### أ. التشفير بالمفتاح المتماثل

ويسمى كذلك بالمفتاح التناظري أو السيمتري ويستعمل هذا النوع من التشفير مفتاح سري واحد يتبادل بين المرسل والمستقبل، كما يعتمد نظام التشفير المتماثل أو المتناظر على استخدام نفس المفتاح من طرف مصدر الرسالة وإعادة فك رموزها بمعنى أن عملية إغلاق وفتح بيانات المحرر تكون بمفتاح واحد، وذلك وفقا للخطوات التالية:

– في هذا النظام يتم استخدام المفتاح الخاص (السري) المستند إلى وضع عملية رياضية معقدة " خوارزميات" في عملية استبدال البيانات برموز وحروف بغرض الحصول على رسالة مشفرة.

–يقوم المستقبل بعد تلقي الرسالة المشفرة بحل الرموز، وذلك باستخدام نفس المفتاح الخاص (كلمة المرور) التي يملكها المرسل حيث أنه تم الاتفاق مسبقا بين الطرفين على كلمة المرور التي تقوم برمجيات التشفير بتحويلها إلى ثنائي " إضافة إلى رموز أخرى" هو المفتاح الخاص.

– بعد استخدام المستقبل لكلمة المرور بتشكيل المفتاح الذي يقوم بتحويل الرسالة المستقبلية من صورتها المشفرة إلى صورتها غير المشفرة وغير المفهومة إلى صورتها الأصلية الواضحة. ومما يعاب على هذه الطريقة إمكانية تسرب المفتاح السري الوارد في أثناء التبادل بين الطرفين، ويمكن اقتحامه واستعماله من قبل لصوص أو قراصنة أو أي شخص آخر غير مرخص باستعماله، وذلك بسب عدم توفر وسيلة مؤمنة وخاصة لنقله.[2]

[1]– عبان عميروش، النظام القانوني للتشفير كألية للتصديق الالكتروني في التشريع الجزائري وتشريعات المقارنة، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، مج 07، ع 01، جامعة عبد الحميد بن باديس–مستغانم، 2022، ص1240.

[2] –المرجع نفسه، ص 1244.

**ب. التشفير اللاتماثلي أو الثنائي:**

إن التشفير غير المتماثل يعتمد على زوج من المفاتيح غير المتماثلة (مفتاح عام ومفتاح خاص) الأول يكون معروفا للجميع ويحتفظ به سرا والثاني فهو خاص بصاحبه وعليه الإحتفاظ به سرا ، ومالك هذا الزوج من المفاتيح عليه الاحتفاظ بالمفتاح الخاص سريا حيث من خلاله يستطيع تشفير رسالته وبالتالي عدم قدرته على رفض ما جاء فيها، وتكمن ميزة هذا النظام في أن معرفة المفتاح العام لا يمكن منه معرفة أو تشكيل المفتاح الخاص، وأن كل مفتاح يقوم بعكس عمل الآخر بمعنى أن ما يشفره الأول يقوم الآخر فقط بحله لبيان كيفية استخدام التوقيع الرقعي من خلال عملية التشفير، كما يجب تزامن عمليتي التشفير وفكه. إن تقنية التشفير كما سبق بيانه.[1]

## المبحث الثاني: آليات مكافحة الجرائم السيبرانية في الجزائر:

حرصا على حماية السيادة الوطنية من أي اختراق أو تهديد إرهابي أو سيبراني للمعطيات وكذا للحدود الوطنية، سطر للمشرع الجزائري مجموعة من الآليات لمكافحة الجرائم السيبرانية المتوقع حدوثها مستقبلا.

تمثلت هذه الآليات في مختلف الجهود الوطنية لمكافحة الجريمة المعلوماتية والسيبرانية من خلال إنشاء هيئات مكلفة بالدفاع على الأمن السيبراني الوطني يترأسها كل من أجهزة الدرك الوطني والمديرية العامة للأمن الوطني بالتنسيق فيما بينها للتصدي للعدوان المترصد سواء داخلي أو خارجي.

وعليه قمنا بتقسيم هذا المبحث إلى مطلبين أساسيين، تناولنا في المطلب الأول الجهود الوطنية للتصدي ومكافحة الجريمة السيبرانية والمطلب الثاني تطرقنا لمواجهة تحديات الأمن السيبراني المستقبلية في الجزائر.

[1] –حزام فتيحة، المرجع السابق، ص177.

## المطلب الأول: الجهود الوطنية للتصدي ومكافحة الجريمة السيبرانية:

إن تحقيق الأمن السيبراني الوطني يتطلب استقرار أمن قومي بالدرجة الأولى، إضافة تضافر الجهود الوطنية للأجهزة الأمنية بمختلف مهامها للتصدي لكل المخاطر والتهديدات السيبرانية التي تولد من الجرائم الإلكترونية في الفضاء الرقمي.

### الفرع الأول: الهيئات الوطنية المكلفة بالأمن السيبراني:

لا يخفى علينا أن الجزائر تعد من أقوى الدول عسكريا في العالم وفي الوطن العربي خاصة، لما تملكه من أسطول دفاع وحماية في المجال الجوي والبحري والبري، الأمر لم يتوقف على هذه الأساطيل وعند هذه الحماية فقط، بل سعت الجزائر إلى استحداث أجهزت أمنية لحماية المعطيات المتعلقة بتكنولوجيا الإعلام والاتصال للتصدي للجرائم السيبرانية التي تهدد أمنها القومي، ومن أهم هذه الأجهزة نجد:

#### أولا: الوكالة الوطنية لتطوير الرقمنة

عالج المشروع الجزائري أحكام الوكالة الوطنية لتطوير الرقمنة بموجب القانون 19-317[1] المتضمن إنشاء الوكالة الوطنية لتطوير الرقمنة، إذ تعد هذه الوكالة الذراع التنفيذي المسؤول عن دعم ومواكبة عملية التحول الرقمي في مختلف قطاعات الدولة، وتهدف إلى تعزيز استخدام التقنيات الحديثة وتطوير البنية التحتية الرقمية لبناء اقتصاد رقمي مبتكر ومستدام.[2]

[1]– المرسـوم الرئاسـي رقم 19-317، المؤرخ في 26 نوفمبر 2019، المتضـمن انشـاء وكالة وطنبة لتطوير الرقمنة وتحديد مهامها وتنظيمها وسيرها، ج ر ج ج، ع 74، مؤرخة في نوفمبر 2019.

[2]–صـمودي كريمة وبرقعي سـمير، الأمن السـيبراني في الجزائر، مذكرة ماسـتر في القانون، تخصـص: قانون أعمال، قسـم الحقوق، كلية الحقوق والعلوم السياسية، جامعة 8 ماي 1945 قالمة، 2025، ص ص51، 52.

## ثانيا: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال

تضمن القانون رقم 09-04 الصادر في 16 غشت 2009، في مادته 13 ضرورة إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها.[1]

تم تأسيس الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال بموجب مرسوم رئاسي رقم 19-172 المؤرخ 05 اوت 2019، حيث حدد هذا المرسوم تشكيلة وتنظيم وكيفيات سير هذه الهيئة.

وقد تم إعادة تشكيل وتنظيم وكيفية تسيير هاته الهيئة بموجب المرسوم الرئاسي رقم 19-172 المؤرخ في 2019/06/09، وأصبحت تحت سلطة وزارة الدفاع الوطني وفقا للمادة الثانية منه.[2]

## ثالثا: القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الاعلام والاتصال

واصل المشرع مسيرة الإصلاحات لتحقيق الامن السيبراني المستدام فأنشأ على مستوى محكمة مقرر المجلس قضاء الجزائر القطب الجزائي الوطني المتخصص في المتابعة والتحقيق في الجرائم المتصلة بتكنولوجيا الاعلام والاتصال والجرائم المرتبطة بها، وذلك وفقا للقانون رقم 25-14، المتضمن قانون الإجراءات الجزائية، المؤرخ في 03 غشت 2025.[3]

لقد نصت المادة 338 من القانون أعلاه مع مراعاة أحكام الفقرة الثانية من المادة 335 أعلاه، يختص وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الاعلام والاتصال وقاضي

---

[1] -قانون رقم 09-04 مؤرخ في 5 غشت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر ج ج، ع 47، مؤرخة في 16 غشت 2009، ص 8.

[2]-مرسوم رئاسي رقم 19-172، مؤرخ في 06 يونيو 2009، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها وتنظيمها وكيفيات تسييرها، ج ر ج ح، ع 37، المؤرخة في 9 يونيو 2009، ص5.

[3]-صورية نواصر، الأمن السيبراني في ظل التشريع الجزائري، تويقر، كلية الحقوق والعلوم السياسية، جامعة باجي مختار-الجزائر، 2024، ص 88.

التحقيق ورئيس ذات القطب حصريا بالمتابعة والتحقيق والحكم في الجرائم المتصلة بتكنولوجيات الاعلام والاتصال أكتر والجرائم المرتبطة بها.[1]

## رابعا: المعهد الوطني للأدلة الجنائية وعلم الإجرام

وهو جهاز تابع للدرك الوطني أنشأ سنة 2004 بموجب المرسوم الرئاسي رقم 04-183، يتكون من إحدى عشرة دائرة متخصصة في عدة مجالات تضمن الخبرة والتكوين والتعليم وتقديم المساعدات التقنية والبحوث والدراسات والتحاليل في علم الجريمة[2].

حيث تكلف دائرة الاعلام الآلي ولإلكترونيك بمعالجة تحليل وتقديم كل دليل إلكتروني وتماثلي للعدالة، كما تقدم مساعدة تقنية للمحققين في التحقيقات المعقدة.

ولإنجاز المهام المنوط بها، تنقسم الدائرة إلى ثلاثة مخابر وكل مخبر مزود بفصيلة مهمتها اقتناء المعطيات من حوامل المعلومات وضمان نزاهة وشرعية دليل:[3]

### أ. مخبر الإعلام الآلي:

يختص بتحليل ومعالجة حوامل المعطيات الرقمية (الهاتف، الشريحة، القرص الصلب، دائرة الفلاش)، كما يقوم بتحديد التزوير الرقمي للبطاقات البنكية.

### ب. مخبر الفيديو:

يختص بإعادة بناء مسرح الجريمة بالتشكيل ثلاثي الأبعاد، كما يعمل على تحسين نوعية الصورة (فيديو، صورة) بمختلف التقنيات، ومقارنة الأوجه، وشرعية الصور، والفيديو.

---

[1]-القانون رقم 25-14، ص 50.

[2]- المرسوم الرئاسي 04-183، المؤرخ في 26 جوان 2004، يتضمن احداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، ج ر ج ج، ع 41، الصادر في 27 جوان 2004، ص18.

[3]-أومدرو رجاء، خصوصية التحقيق في مواجهة الجرائم المعلوماتية، أطروحة دكتوراة الطور الثالث ل. م. د، تخصص: القانون الخاص، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي برج بوعريريج ،2021، ص100.

**ج. مخبر الصوت:**

يختص بمعرفة وتحديد المتكلم، وتحديد شرعية التسجيلات الصوتية ويعمل على تحسين نوعية إشارة الصوت بنزع التشويش وتعديل السرعة.[1]

## خامسا: مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني

أنشئ هذا المركز في سنة 2008 ويعتبر الجهاز الوحيد المختص بهذا الصدد في الجزائر، يهدف إلى تأمين منظومة المعلومات لخدمة الأمن العمومي، واعتبر بمثابة مركز توثيق متواجد ببئر مراد رايس يعكف هذا المركز على تحليل معطيات وبيانات الجرائم المرتكبة وتحديد هوية أصحابها سواء كانوا أشخاص فرادى أو عصابات، وهذا كله من أجل تأمين الأنظمة المعلوماتية والحفاظ عليها، لاسيما تلك المستعملة في المؤسسات الرسمية والبنوك والبيوت. كما يهدف إلى مساعدة باقي الأجهزة الأمنية الأخرى في أداء مهامها، واستطاعت قيادة الدرك من خلال التكوين المستمر لأفرادها والملتقيات الدولية والوطنية وتبادل الخبرات مع دول أخرى أن توفر القوى الهائلة وذات الكفاءة من مهندسي الاعلام الآلي، رجال القانون، وهذا من أجل الفهم الصحيح للجريمة المعلوماتية والتصدي لها.

استطاع المركز من معالجة أزيد من 100 جريمة إلكترونية سنة 2014 وما يفوق 500 قضية رقمية خلال سنة 2015، منها 300 جريمة تتعلق بمواقع التواصل الاجتماعي "فايسبوك" و20 جريمة رقمية تعلقت باختراق مواقع رسمية لمؤسسات خاصة وعامة، استهدف مجرموها أنظمة المعالجة الآلية للمعطيات.[2]

[1]–أومدرو رجاء، المرجع السابق، ص101.

[2]–بارة سمير، المرجع السابق، ص435.

### سادسا: المصلحة المركزية لمحاربة الجريمة الالكترونية للأمن الوطني

استجابة لتحولات الفضاء السيبراني، أنشأت المديرية العامة للأمن الوطني أول فصيلة على مستواها سنة2011، ثم تم توسيع استحداثها إلى 48 ولاية سنة 2013، ومع تطور انتشار مخاطر وشبكات الإجرام الالكتروني، تم إنشاء مصلحة مركزية على مستوى مديرية الشرطة القضائية سنة2015، وقد استجابت هذه الهيئة لعدد كبير من الشكاوى المحلية والدولية، وتمكنت من معالجة قضايا تتعلق بجرائم ماسة بخصوصية الأفراد والمؤسسات، إضافة إلى جرائم الإرهاب الإلكتروني وشبكات الجريمة العابرة للحدود واستغلال الأطفال. وكانت أول قضية دولية تعاملت معها الشرطة الجزائرية تتعلق بقرصنة بيانات بنكية إثر بلاغ من مكتب التحقيقات الأمريكية FBI سنة2009، وتعد الشرطة الجزائرية ذات كفاءة وسمعة دولية نتيجة للمؤهلات البشرية والوسائل التقنية العالية، كما تساهم الجزائر في مجال التكوين الدولي وتبادل الخبرة والانخراط في مجال محاربة الجريمة الالكترونية العابرة للقارات بالتعاون مع مكتبي الإنتربول والأفريبول.[1]

## الفرع الثاني: الجانب التشريعي في مواجهة الجريمة السيبرانية:

### أولا: تعديل قانون العقوبات

على غرار أن الدستور الجزائري أعلى قانون في الدولة والذي جرم مختلف أشكال الجريمة بما فيها الجريمة الالكترونية والمعلوماتية.

قام المشرع الجزائري بتعديل قانون العقوبات بموجب القانون رقم 04-15 من أجل تجريم الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثره بما أفرزته الثورة المعلوماتية من أشكال جديدة من الإجرام، حيث جاء التعديل في المواد 394 مكرر إلى المادة 394 مكرر 7 تحت عنوان المساس بأنظمة المعالجة الآلية.[2]

---

[1]–محمودي سعيد، المرجع السابق، ص205.

[2]– القانون رقم 04-15 المؤرخ في نوفمبر 2004، المتضمن تعديل وتتميم قانون العقوبات الجزائري، ج ر ج ج، ع71، المؤرخة في 10 نوفمبر 2004.

كما أضاف المشرع الجزائري سنة 2006م تعديلات جديدة مست القسم السابع مكرر منه، وجاء هذا التعديل لتشديد العقوبة المقرر لهذه الجرائم دون المساس بنص المواد في هذا القسم إلى جانب زيادة الوعي بخطورة مثل هذه الجرائم المستحدثة.

وتتجسد الجرائم التي نصت عليها التعديلات كما يلي:

- جريمة الدخول والبقاء غير المصرح بهما في المادة 394 مكرر.
- جريمة الاعتداء على المعطيات: المادة 394 مكرر 1.
- جريمة التعامل في المعلومات غير المشروعة: المادة 394 مكرر2.

أما المادة 394 مكرر 3 فنصت على مضاعفة العقوبة المنصوص عليها في هذا القسم، إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الاخلال بتطبيق عقوبات أشد.[1]

وشدد المشرع في المادة 394 مكرر4 على معاقبة الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي. وجاء في المادة 394 مكرر5 أن كل من شارك في مجموعة أو اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليهما وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقرر للجريمة ذاتها. ليختم هذا التعديل بنص المادة 394 مكرر 7 التي تنص على أنه: "يعاقب الشروع في ارتكاب الجنح المنصوص عليها بالعقوبات المقرر للجنحة".[2]

[1]– قانون العقوبات رقم 24–06، المؤرخ في 28 ابريل 2024، المتضمن تعديل وتميم قانون العقوبات، ج ر ج ج، ع 30، المؤرخة في 30 ابريل 2024.

[2]–بارة سمير، المرجع السابق، ص 265.

## ثانيا: تعديل قانون الإجراءات الجزائية

استحدث المشرع الجزائري بموجب قانون الإجراءات الجزائية مجموعة من الإجراءات الخاصة التي تتماشى مع العالم الافتراضي، وتتمثل في اعتراض المراسلات والتقاط الصور وتسجيل الأصوات وإجراء التسرب.

حيث سمح المشرع باللجوء إلى اعتراض المراسلات والتقاط صور وتسجيل الأصوات لمقتضيات التحري والتحقيق في جرائم محددة متمثلة في الإذن وطبيعة الجريمة، وكتمان السر المهني، وتحرير محضر من طرف ضباط الشرطة القضائية المأذون له بالعملية.[1]

وكإجراء آخر فقد أجاز المشرع اللجوء إلى التسرب بموجب نص المادة 121 في فقرتها الثانية من قانون الإجراءات الجزائية الجزائري رقم 25-14[2]، وذلك إذا اقتضت ضرورة التحري والتحقيق ذلك في الجرائم المحددة حصرا، ومن بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، حيث أجاز لكل من العون أو ضابط الشرطة القضائية من إخفاء هويته وصفته الحقيقية أثناء مباشرة المهمة، حيث انه قد جعل من شروط صحت هذه العملية اجراءها في سرية وبهوية مستعارة وان كل ما يخالف ذلك يعرض هذا الاجراء للبطلان.

ويقصد بالتسرب حسب نص المادة 121 من قانون 25-14 قيام ضابط أو عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف.[3]

---

[1]–مهدي رضا، المرجع السابق، ص117.

[2]– القانون رقم 25-14، المؤرخ في 03 غشت 2025، المتضمن قانون الإجراءات الجزائية، ج ر ج ر، ع 54، المؤرخة في 13 غشت 2025.

[3] – المادة 121، من القانون رقم 25-14.

## الفرع الثالث: الأمن السيبراني وفقا للقوانين الخاصة

حرص المشرع في الأمر رقم 03-05 على تجريم الأفعال الماسة بحقوق المؤلف والحقوق المجاورة، حيث قرر من خلال المادة 158 العقوبات المناسبة وذلك بشأن جنح التقليد المذكورة بالمادتين 151 و152 من نفس القانون من بينها التقليد الذي يتم عن طريق منظومة المعالجة المعلوماتية.[1]

وبهدف تحقيق الأمن السيبراني، أصدر المشرع الجزائري القانون رقم 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، حيث نص على جملة من القواعد الموضوعية والاجرائية.[2]

تضمن النوع الأول، التدابير الاحترازية، ونصت عليها المادة 13 منه وتتمثل في ضرورة إنشاء قطب وطني متخصص في الجرائم السيبرانية وحددت المادة 14 منه مهامه، كما تضمنت المادة 10 منه الالتزامات المفروضة على كل من مقدمي الخدمات، ومقدمي خدمات الأنترنت.

وفي سنة 2018 قام المشرع بتعزيز الترسانة القانونية لتحقيق الامن السيبراني عن طريق سنه للقانون رقم 18-04 المؤرخ في ماي 2018 والذي يحدد العلاقات العامة المتعلقة بالبريد والاتصالات الالكترونية.

حيث استحدث سلطة ضبط من بين مهامها للسهر على احترام متعاملي البريد والاتصالات الالكترونية للأحكام القانونية والتنظيمية المتعلقة بالبريد والاتصالات الالكترونية والأمن السيبراني، إضافة إلى تحريم انتهاك سرية المراسلات المرسلة عن طريق البريد، او الاتصالات الالكترونية، أو إفشاء مضمونها، أو نشرها، أو

[1] -أمر رقم 03-05، المؤرخ في 19 يوليو 2003، يتعلق بحقوق المؤلف والحقوق المجاورة، ج ر ج ر، ع 44، المؤرخة في 23 يوليو 2003.

[2] – القانون رقم 09-04 المؤرخ في 5أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، ج ر ج ر، ع 47، المؤرخة في 16 أوت 2009.

استعمالها دون ترخيص من المرسل، أو المرسل إليه، أو الأخبار بوجودها وتجريم محاولة فتح، أو تخريب، أو تحويل البريد، أو المساعدة في ارتكاب هذه الجريمة[1].

وفي أواخر سنة 2018 أصدر المشرع قانون 18-07[2] المؤرخ في جويلية 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، من خلال وضع مجموعة من الآليات التي يمكن إنجازها في عدة نقاط:

- استحداث سلطة وطنية لحماية المعطيات ذات الطابع الشخصي.
- وضع مجموعة التزامات ملقاة على عاتق المسؤول عن المعالجة الآلية للمعطيات ذات الطابع الشخصي.
- اتخاذ السلطة الوطنية لمجموعة إجراءات إدارية في حالة خرق أحكام القانون من طرف المسؤول عن المعالجة.
- يمكن للسلطة الوطنية القيام بالتحريات ومعاينة المحلات والأماكن التي تتم فيها المعالجة باستثناء محلات السكن، كما يمكنها الولوج إلى المعطيات وجميع المعلومات والوثائق أيا كانت دعامتها.
- تأهيل أعوان الرقابة للقيام ببحث ومعاينة الجرائم المتعلقة بالمعطيات ذات طابع شخصي تحت إشراف وكيل الجمهورية.
- يمكن للمدعي بالمساس بحق من حقوقه المنصوص عليها في هذا القانون أن يطلب من الجهة القضائية اتخاذ أي إجراءات تحفظية للحد من التعدي أو للحصول أو على تعويض.
- تختص الجهة الجزائية بمتابعة هذه الجرائم التي ترتكب خارج إقليم الجمهورية من طرف جزائري أو شخص أجنبي مقيم في الجزائر أو شخص معنوي خاضع للقانون الجزائري، كما تختص بمتابعة الجرائم المنصوص

[1]–مهدي رضا، المرجع السابق، ص121

[2]– القانون رقم 18-07، المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي، ج ر ج ر، ع 34، المؤرخة في 10 يونيو 2018.

عليها في هذا القانون وفقا لقواعد الاختصاص المنصوص عليها في المادة 588 من قانون الإجراءات الجزائية.[1]

كما صدر القانون رقم 20-05، المؤرخ في 28 أبريل 2020 المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتها، كما تضمن إنشاء المرصد الوطني للوقاية من التمييز وخطاب الكراهية في المواد من 9 إلى المادة15 من نفس القانون.[2]

كما صدر القانون رقم 25-11، المؤرخ في 24 يوليو 2025، الذي يعدل ويتمم القانون رقم 18-07، والمتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.[3]

## المطلب الثاني: مواجهة تحديات الأمن السيبراني المستقبلية في الجزائر:

حرصت الجزائر على تعزيز أمنها السيبراني عن طريق سن العديد من القوانين والمراسيم المتعلقة بمحاربة ومكافحة الجرائم الالكترونية والمعلوماتية وكذا تعديل القوانين الأساسية المتعلقة بالجرائم التقليدية مثل قانون العقوبات وقانون الاجراءات الجزائية بهدف وضع نصوص خاصة بالجرائم الالكترونية، غير أن هذه التعديلات لم تكن كافية لرد مثل هذه الجرائم في الفضاء الرقمي، الأمر الذي دفع بضرورة مواكبة تطور هذه الجرائم من خلال وضع استراتيجية مستقبلية لمكافحة الجرائم السيبرانية على المدى البعيد، على راسها الاستراتيجية الوطنية لأمن أنظمة المعلوماتية، إضافة إلى التعاون الدولي من خلال الإمضاء على الاتفاقيات مع الدول الأخرى لحماية أمنها من التهديدات والارهاب السيبراني.

---

[1]–القانون رقم 18-07 المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي، ج ر ج ج، ع 34، الصادرة بتاريخ 10 يونيو 2018، ص22.

[2]–المادة 09 من القانون رقم 20-05.

[3] – القانون رقم 25-11، المؤرخ في 24 يوليو 2025، المتضمن حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج ر ج ج، ع 48، مؤرخة في يوليو 2025.

## الفرع الأول: الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية 2025-2029

تبنت هذه الاستراتيجية تكريس الجهود الوطنية لحماية البنى التحتية من خلال وضع آليات ملائمة للتصدي للاعتداءات الخارجية وذلك من خلال وضع منظومة وطنية لأمن الأنظمة المعلوماتية بموجب المرسوم الرئاسي رقم 20-05[1] المؤرخ في 20 جانفي سنة2020 والتي أتاحت إحداث وكالة أمن الأنظمة المعلوماتية.

تضمنت الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية 2025-2029 أربعة محاور رئيسية، تتكون من مجلس وطني وكذا وكالة الأمن الأنظمة المعلوماتية.

تجدر الإشارة أيضا إلى أن الاستراتيجية الوطنية تستند على النصوص التشريعية والتنظيمية السارية المفعول التي تسير مختلف جوانب الأمن السيبراني والمجالات ذات الصلة، حيث يجب التأكيد على ضرورة تحديتها وتعزيزها بشكل مستمر.

كما تندرج هذه الاستراتيجية بصفة شاملة، في إطار الرؤية الوطنية المتعلقة برقمنة مؤسسات الدولة والقطاع الاجتماعي والاقتصادي مع الاخذ بعين الاعتبار التطور المستمر للتكنولوجيات الحديثة للرقمنة، بالإضافة الى تنامي التهديد السيبراني الذي يمكن ان يشكل خطرا على أمن الانظمة المعلوماتية الوطنية.[2]

### اولا: اهداف الاستراتيجية الوطنية لأمن انظمة المعلوماتية

- يتمثل الهدف الرئيسي من هذه الاستراتيجية في موافقة مؤسسات الدولة والهيئات العمومية والخاصة من خلال تنفيذ نهج تدريجي وشامل ومحكم فيما يتعلق بأمن ومرونة الانظمة المعلوماتية الوطنية والبنى التحتية خلال السنوات الاربعة القادمة.

[1] – المرسوم الرئاسي رقم 20-05 المؤرخ في 20 جانفي 2020، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، ج ر ج ج، ع 04، مؤرخة في 26 جانفي 2020.

[2]–الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية، ص9.

- تهيئة بيئة ملائمة لجميع الفاعلين الوطنيين المعنيين بالأمن السيبراني من خلال توفير كل الظروف اللازمة للمساهمة في حماية السيادة الرقمية الوطنية والحفاظ عليها.
- بلوغ أقصى حد من الأداء من حيث الأمن والمرونة السيبرانية للأنظمة المعلوماتية الوطنية والبنى التحتية الحساسة في كافة القطاعات.
- تزويد بلادنا بقدرات الوقاية والكشف والاستجابة للحوادث السيبرانية سواء كانت غير مقصودة أو خبيثة، من خلال توفير الوسائل الفعالة.

إضافة إلى أربعة أهداف رئيسية تتمثل في:

1- بناء المرونة السيبرانية للأنظمة المعلوماتية الوطنية.

2- العمل على وضع نظام بيئي وطني ملائم في مجال الأمن السيبراني.

3- إنشاء إطار وطني من أجل تطوير موارد بشرية مؤهلة في الأمن السيبراني.

4- تعزيز التعاون الدولي في الأمن السيبراني.[1]

## ثانيا: المبادئ التوجيهية للاستراتيجية الوطنية لأمن الأنظمة المعلوماتية

تعتبر هذه المبادئ كعناصر مرجعية للاستراتيجية الوطنية لأمن الأنظمة المعلوماتية وتتمثل فيما يلي:

- تعزيز السيادة الرقمية الوطنية.
- مرافقة التحول الرقمي المباشر من طرف الدولة.
- الحفاظ على المكاسب المحققة.
- تشجيع العمل التنسيقي الشامل.
- تثمين شارك الموارد.
- تحديد أهداف قابلية للتحقيق في آجالها المحددة وقابلة للقياس.[2]

[1]-الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية 2025-2029، المرجع السابق، ص6.

[2]-المرجع نفسه، ص8.

## الفرع الثاني: محاور الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية

في إطار تحقيق الأهداف الاستراتيجية المدرجة ضمن هذه الاستراتيجية الوطنية، تتوزع الجهود الواجب بذاتها على المحاور الأربعة التالية:

**المحور الأول: القدرات التقنية –العملياتية**

يرمي تطوير القدرات التقنية– العملياتية في مجال حماية ومرونة الأنظمة المعلوماتية الوطنية والبنى التحتية الحساسة إلى تزويد بلادنا بوسائل الوقاية والكشف والاستجابة للحوادث السيبرانية، من خلال السعي إلى تحقيق الأهداف التالية

- تدعيم حماية الأنظمة المعلوماتية الوطنية والبنى التحتية الحساسة.
- تعزيز القدرات التقنية–العملياتية الوطنية من الحوادث والكشف عنها والاستجابة لها.[1]

**المحور الثاني: الإطار القانوني والتنظيمي والمعياري**

يتضمن هذا المحور الأهداف المدرجة إلى تزويد بلادنا بإطار قانوني وتنظيمي ومعياري ملائم يمكنه من تحقيق الرؤية الاستراتيجية السالف وصفها، وبذلك ضمان المرونة السيبرانية الوطنية، وذلك من خلال:

- تعزيز الإطار القانوني والتنظيمي.
- إرساء إطار معياري.

**المحور الثالث: التكوين والبحث والتطوير والتحسيس:**

ركز هذا المحور إلى تزويد العنصر البشري بالكفاءات والمعارف الضرورية التي تسمح له بممارسة مهامه في الفضاء السيبراني بطريقة آمنة وفعالة من خلال:

- التوفر على موارد بشرية مؤهلة في مجال الأمن السيبراني.

[1]- الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية 2025–2029، المرجع السابق، ص9.

- ترقية البحث والتطوير والابتكار في مجال الأمن السيبراني.
- ترسيخ ثقافة في الأمن السيبراني.[1]

**المحور الرابع: التعاون الوطني والدولي:**

يهدف التعاون على الصعيد الوطني إلى تحسين وتشارك وسائل العمل وكذا ترقية تبادل المعلومات في جميع الجوانب المتعلقة بالأمن السيبراني بين القطاعين الخاص والعام ووكالة أمن الأنظمة المعلوماتية.

علاوة على ذلك، وعلى الصعيد الدولي، يشكل التعاون في مجال الأمن السيبراني وسيلة لا غنى عنها لبلدنا، من أجل إضفاء التناسق على الأعمال ومجابهة التهديدات السيبرانية بصفة جماعية، من خلال إقامة روابط عملياتية فعالة.

كما يهدف هذا المحور إلى ضرورة:

- تعزيز وتتمين التعاون والشراكة في مجال الأمن السيبراني بين كل الأطراف المعنية على المستوى الوطني.
- تأطير التعاون الدولي على المستويين الاستراتيجي والتقني–عملياتي في مجال الأمن السيبراني.
- المساهمة بفعالية في عملية إعداد الإطار القانوني والمعياري على المستوى الدولي في مجال الأمن السيبراني.[2]

[1]–الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية 2025–2029، المرجع السابق، ص9.

[2]–المرجع نفسه، ص10.

## الفرع الثالث: مستقبل الأمن السيبراني في الجزائر:

لا يمكن مناقشة مستقبل الأمن السيبراني دون النظر في الاتجاهات الناشئة في مجال التكنولوجيا والتهديدات المرتبطة باستخدامها، إذ تقوم المنظمات المختصة بتطوير واعتماد التكنولوجيا المتصلة بالبيانات الكبيرة والحوسبة الإدراكية، مما يجعل الأبعاد السيبرانية تنمو في الحجم والتعقيد بصورة مطردة.[1]

ومع زيادة الوعي بأهمية الأمن السيبراني، يبدو مستقبل هذا التخصص في الجزائر واعدا جدا حيث يتوقع أن تشهد السنوات المقبلة زيادة كبيرة في عدد الوظائف المتاحة في هذا المجال، خاصة مع تزايد التهديدات الالكترونية وتطور تقنيات الذكاء الاصطناعي.

وفي ظل تزايد الهجمات السيبرانية على مستوى العالم، بدأت الجزائر في اتخاذ خطوات حثيثة لتعزيز أمنها السيبراني، تمثل هذه الخطوات جزءا من استراتيجية وطنية تهدف إلى بناء بنية تحتية قوية للأمن السيبراني، ومن بين هذه الخطوات البارزة، افتتاح مدرسة جديدة متخصصة في الأمن السيبراني تهدف إلى تلبية الحاجة المتزايدة للخبراء في هذا المجال وتقديم برامج تعليمية متقدمة تغطي أحدث التقنيات وأساليب الحماية وهذا التطور يعكس التزام الجزائر بتعزيز قدراتها في مواجهة التهديدات السيبرانية.

[1]–إدريس عطية، المرجع السابق، ص116.

# الخـــاتـــمـــة

حاولنا من خلال تناولنا لهذا الموضوع الموسوم بـ"الأمن السيبراني في الجزائر والتدابير التقنية والتشريعية لحمايته" معالجة إشكالية البحث التي تتمحور حول أهم متطلبات الأمن السيبراني لحماية الأنظمة المعلوماتية.

نستخلص في نهاية دراستنا أن الحروب السيبرانية هي ثورة معلوماتية يشهدها عصر الحداثة والتطور التكنولوجي والرقمي تدفع المجتمع الدولي عامة والجزائر خاصة بضرورة توحيد موازين القوى بين الدول المصادقة على الاتفاقيات والمعاهدات المنظمة لمكافحة ومواجهة التهديدات السيبرانية.

ولا يخفى علينا أن الدولة الجزائرية تسعى بطريقة موازية إلى حماية سيادتها الوطنية وأمنها القومي من خلال تعديل القوانين المتعلقة بالجرائم الإلكترونية ووضع استراتيجيات وتدابير تقنية لحماية أنظمة المعلومات خاصة ما تعلق بقانون العقوبات وكذا قانون الإجراءات الجزائية، إضافة إلى مختلف المراسيم الرئاسية الملحقة.

إن السياسة المتبناة من طرف السيد رئيس الجمهورية في وضع استراتيجية لحماية أمن الأنظمة المعلوماتية هي رؤية مستقبلية لمكافحة التهديدات السيبرانية والإرهاب السيبراني، إلا هذه التعديلات والقوانين لم تكن كفيلة بإعطاء مفهوم عام ومبسط للأمن السيبراني.

وقد سمحت لنا هذه الدراسة باستخلاص مجموعة من النتائج والتوصيات المقترحة نوجزها في النقاط التالية:

## أولا: النتائج

بالرغم من حرص المشرع الجزائري على تعزيز الحماية القانونية التي تعمل على تحقيق الأمن السيبراني، إلا أن معدل الجريمة السيبرانية في تزايد مستمر بشكل مهول، مما يستدعي إلى ضرورة القيام بتعديلات مستمرة مواكبة للتطور التكنولوجي في القوانين التشريعية.

إن تعميم الرقمنة والمعاملات الالكترونية في المؤسسات العمومية خاصة المؤسسات الحساسة كقطاع الصحة والتربية معرضة للمخاطر السيبرانية خاصة بوجود نقاط ضعف تتمثل في عدم انتشار الوعي الثقافي بضرورة الحماية للبنى التحتية لهذه المؤسسات في ظل القرصنة الالكترونية والاختراق السيبراني، وخير مثال على ذلك ما حدث من اختراقات في فترة جائحة كورونا 2020.

## ثانيا: التوصيات

- العمل على إعادة التفكير في تعديل قانون العقوبات وقانون الإجراءات الجزائية الجزائري، ووضع مفهوم واضح ودقيق للأمن السيبراني.
- ضرورة تكاثف الجهود الوطنية والجهود الدولية للقضاء على الإرهاب السيبراني.
- تعزيز البنية التحتية للأمن السيبراني الوطني عن طريق زيادة عدد المراكز المتخصصة في مراقبة ومكافحة الجريمة الإلكترونية.
- إدراج مقياس خاص بالأمن السيبراني الوطني في مختلف الأطوار الدراسية لنشر ثقافة الوعي المعرفي بخطورة التهديد السيبراني وعقوبة الجريمة الإلكترونية.
- تدريب وتأهيل موارد بشرية في مجال الأمن السيبراني لفهم واستخدام التقنيات الحديثة بشكل يتلاءم مع التطور الرقمي.

# قـائمة الـمصـادر والمـراجـع

## قائمة المصادر والمراجع:

### أولا: المصادر

#### أ. النصوص القانونية الوطنية

**1- الدستور:**

- التعديل الدستوري لسنة 2020، الصادر بموجب المرسوم الرئاسي رقم 20-442، المؤرخ في 30 ديسمبر 2020، المتعلق بإصدار التعديل الدستوري 2020، جريدة رسمية، العدد 82، الصادرة بتاريخ 30 ديسمبر 2020.

**2- القوانين:**

- القانون رقم 04-15 المؤرخ في نوفمبر 2004، المتضمن تعديل وتتميم قانون العقوبات الجزائري، جريدة رسمية، العدد 71، المؤرخة في 10 نوفمبر 2004.
- القانون رقم 09-04 المؤرخ في 5أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، جريدة رسمية، العدد47، المؤرخة في 16 أوت 2009.
- القانون رقم 15-04، المؤرخ في 01 فبراير 2015، يحدد القواعد المتعلقة بالتوقيع والمصادقة الالكترونيين، جريدة رسمية، العدد 06، المؤرخة في فبراير 2015.
- القانون رقم 16-02 المؤرخ في 19 يونيو 2016، المتضمن قانون العقوبات، جريدة رسمية، العدد 37، المؤرخة في 22 يونيو2016.
- القانون رقم 18-04، المؤرخ في 10ماي 2018، المتضمن القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، جريدة رسمية، العدد:27، المؤرخة في 13 مايو 2018.
- القانون رقم 18-07، المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي، جريدة رسمية، العدد:34، المؤرخة في 10 يونيو 2018.
- القانون رقم 19-11، المؤرخ في 11 ديسمبر 2019، المتضمن قانون الإجراءات الجزائية، المعدل للأمر رقم 66-115، جريدة رسمية، العدد78، مؤرخ في 2019/12/18.
- القانون رقم 24-06 المؤرخ في 28 ابريل 2024، المتضمن قانون العقوبات، جريدة رسمية، العدد 30، المؤرخة في 30 ابريل 2024.
- القانون رقم 25-11، المؤرخ في 24 يوليو 2025، المتضمن حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، جريدة رسمية، العدد: 48، مؤرخة في يوليو 2025.
- القانون رقم 25-14، المؤرخ في 03 غشت 2025، المتضمن قانون الإجراءات الجزائية، جريدة رسمية، العدد 54، المؤرخة في 13 غشت 2025.

**3- الأوامر:**

- أمر رقم 03-05، المؤرخ في 19 يوليو 2003، يتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية، العدد: 44، المؤرخة في 23 يوليو 2003.
- أمر رقم 21-11 المؤرخ في 25غشت 2021، المتمم للأمر رقم 66-155 المؤرخ في 5 يونيو 1966، المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، العدد: 65، المؤرخة في 26 غشت 2021.

**4- المراسيم:**

- مرسوم تنفيذي رقم 2000-307، المؤرخ في 14 أكتوبر 2000، يعدل المرسوم التنفيذي رقم 98-257، المؤرخ في 25 غشت 1998، الذي يضبط شروط وكيفيات إقامة خدمات الأنترنت واستغلالها، جريدة الرسمية، العدد 60، المؤرخة في 15 أكتوبر 2000.
- مرسوم رئاسي رقم 04-183، المؤرخ في 26 جوان 2004، يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، جريدة رسمية، العدد 41، الصادر في 27 جوان 2004.
- مرسوم رئاسي رقم 19-172، مؤرخ في 6 يونيو 2009، يحدد تشكيلية الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها وكيفيات نسيرها، جريدة رسمية، العدد 37، المؤرخة في 9 يونيو 2009.
- المرسوم الرئاسي رقم 19-317، المؤرخ في 26 نوفمبر 2019، المتضمن انشاء وكالة وطنبة لتطوير الرقمنة وتحديد مهامها وتنظيمها وسيرها، جريدة رسمية، العدد 74، مؤرخة في نوفمبر 2019.
- المرسوم الرئاسي رقم 20-05 المؤرخ في 20 جانفي 2020، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، جريدة رسمية، العدد 04، مؤرخة في 26 جانفي 2020.

## ثانيا: المراجع:

**أ. الكتب:**

- خيرت علي محرز، في جرائم الحاسب الآلي، دار الكتاب الحديث،1436هـ-2012م.
- فارس محمد العمارات وإبراهيم محمد الحمامصة، الأمن السيبراني (المفهوم وتحديات العصر)، الطبعة الأولى، دار الخليج للنشر والتوزيع، عمان –الأردن، 2022م.

- مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الأنترنت بين القانون الدولي الاتفاقي والقانون الوطني، الطبعة الأولى، مركز الدراسات العربية للنشر والتوزيع، 1437هـ-2016م.
- مفيد عوض حسن علي، الأمن السيبراني وأساسياته، مكتبة الدراسات العربية للنشر والتوزيع، سلطة عمان، 2025.
- وزارة التعليم العالي، الأمن السيبراني، التعليم الثانوي-نظام المسارات، السنة الثالثة، شركة تطوير للخدمات التعليمية، طبعة 1446هـ-2024م.

**ب. المقالات:**

- إدريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، مجلة مصداقية، المجلد: 01، العدد:01، كلية الحقوق والعلوم السياسة، جامعة العربي التبسي، تبسة، الجزائر، 2019.
- إسماعيل زروقة، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية، المجلد:10، العدد:01، جامعة محمد بوضياف المسيلة، الجزائر، 2019.
- بارة سمير، الأمن السيبراني في الجزائر (السياسات والمؤسسات)، المجلة الجزائرية للأمن السيبراني، المجلد:02، العدد:4، 2017.
- بعوني ليلى، التهديدات في الفضاء السيبراني وانعكاساتها على السيادة الرقمية: القرصنة الالكترونية نموذجا، ستراتيجيا، مجلة دراسات الدفاع والاستشراق، العدد:16، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة الجزائر3، السداسي الثاني،2021.
- بكوش محمد أمين وهروال نبيلة هبة، خصوصية المجرم الالكتروني – مجرم الأنترنت نموذجا، مجلة البحوث في الحقوق والعلوم السياسية، المجلد:7، العدد:01، جامعة تيارت – الجزائر، 2021.
- بوفليج محمد السعيد، أطر التعاون الدولي للتصدي للتهديدات السيبرانية، مجلة الدراسات القانونية والتطبيقية، المجلد: 01، العدد: 02، مخبر الدراسات القانونية التطبيقية، جامعة الإخوة منتوري قسنطينة1، 2020.
- حزام فتيحة، حماية الأنظمة الرقمية بين الاليات التقنية وأجهزة الحماية – قراءة في احكام المرسوم الرئاسي 05-20، مجلة الحقوق والعلوم الإنسانية، المجلد: 13، العدد: 03، جامعة بومرداس – الجزائر،2020.
- خرشي عثمان وعمارة فتيحة، الترصد الالكتروني كآلية لمكافحة الجرائم المعلوماتية، مجلة الدراسات الحقوقية، المجلد:7، العدد:3، جامعة سعيدة – الجزائر، 2020.

- خليلي سهام، خصوصية المجرم الالكتروني، مجلة المفكر، المجلد: 12، العدد: 15، جامعة محمد لمين دباغين – سطيف 2، 2017.
- ربيعي حسين وسمر محمود، الحروب السيبرانية: المخاطر واستراتيجيات تحقيق الأمن السيبراني الدولي والداخلي، المجلة الجزائرية للأمن السيبراني، المجلد:7، العدد:2، جامعة الإخوة منثوري قسنطينة 1.
- سعيد أوغان، الأمن السيبراني ورهانات التحول الرقمي في المغرب–التأصيل المفاهيمي والاستراتيجية التشريعية، جامعة محمد الخامس–الرباط– المغرب، كلية العلوم القانونية والاقتصادية، مجلة المعرفة، العدد:11، 2023.
- صورية نواصر، الأمن السيبراني في ظل التشريع الجزائري، تويقر، جامعة باجي مختار–الجزائر، كلية الحقوق والعلوم السياسية، 2024.
- عبان عميروش، النظام القانوني للتشفير كألية للتصديق الالكتروني في التشريع الجزائري وتشريعات المقارنة، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد:07، العدد: 01، جامعة عبد الحميد بن باديس–مستغانم، 2022.
- العيداني محمد، التهديدات السيبرانية وجرائم المعلومات، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد:13، العدد:01، المركز الجامعي الشريف أفلو(الجزائر)، 2024.
- قطاف سليمان وبوقرين عبد الحليم، الأمن السيبراني والمضامين المفاهيمية المرتبطة به، مجلة طبنة للدراسات العلمية الأكاديمية، المجلد:05، العدد:02، جامعة الأغواط–الجزائر، مخبر البحث للحقوق والعلوم السياسية.
- قيطة فاطمة الزهراء وصالحي دليلة، تعزيز الأمن السيبراني في الجزائر– الجهود القانونية العلمية والعملية، مخبر التنمية الاجتماعية وخدمة المجتمع، كلية العلوم الاجتماعية والانسانية، جامعة الشهيد لخضر الواد – الجزائر، 2024.
- كواتشي عتيقة، تداعيات الإرهاب السيبراني على الأمن القومي الجزائري، المجلة الجزائرية للأمن والتنمية، المجلد:12، العدد:03، جامعة باتنة1 الجزائر، 2023.
- لرقط سمية ومعاليم سعاد، أثر تكنولوجيا المعلومات على الأمن المعلوماتي، مجلة أبحاث اقتصادية وإدارية، المجلد:15، العدد: 03، جامعة محمد خيضر بسكرة، 2021.

- مباركة حنان كركوري، التأصيل القانوني للجرائم السيبرانية المرتكبة عبر الوسائط الرقمية، المجلة الافريقية للدرسات القانونية والسياسية، مجلد: 07، عدد: 01، مخبر قانون الأسرة، جامعة أحمد دراية، أدرار–الجزائر، 2023، ص، ص128،129.
- محمد الصغير كاوجة، الهجمات السيبرانية بين الواقع وسبل المواجهة، مجلة الرسالة للدراسات الإعلامية، المجلد:06، العدد:03، جامعة قاصدي مرباح ورقلة–الجزائر، 2022.
- محمودي سعيد، الأمن السيبراني في الجزائر: بين المعالجة الأمنية والحماية القانونية، مجلة الناقد للدراسات السياسية، مج7، ع2، جامعة بشار، 2023.
- مرابط حمزة وداودي منصور، التشفير كآلية لحماية المصنفات الرقمية من القرصنة الالكترونية، مجلة الحقوق والعلوم السياسية، المجلد:10، العدد:01، جامعة خنشلة، 2023.
- مهدي رضا، الجرائم السيبرانية وآلية مكافحتها في التشريع الجزائري، مجلة إيليزي للبحوث والدراسات، المجلد:06، العدد:02، جامعة بوضياف المسيلة(الجزائر)، 2021.
- نادية لاكلي، الجرائم الالكترونية في الجزائر والعقوبات المقرر لها، مجلة الاجتهاد القضائي، المجلد:15، العدد:01، مخبر أثر الاجتهاد القضائي على حركة التشريع، جامعة محمد خيضر بسكرة، 2023.

**ج. أطروحات الدكتوراه:**

- أمودور رجاء، خصوصية التحقيق في مواجهة الجرائم المعلوماتية، أطروحة دكتوراه، الطور الثالث ل.م.د، تخصص: القانون الخاص، قسم: الحقوق، جامعة محمد البشير الإبراهيمي برج بوعريريج، كلية الحقوق والعلوم السياسية، 2021.

**د. مذكرات الماستر:**

- طاهر محمد السعيد وسليماني خالد، متطلبات تطبيق الأمن السيبراني لأنظمة المعلومات المحاسبية في المؤسسات الاقتصادية –دراسة حالة: مؤسسات نفطال فرع غرداية (2008–2023)، مذكرة الماستر أكاديمي، تخصص محاسبة، كلية العلوم الاقتصادية والتجارية وعلوم التسيير المالية والمحاسبة، جامعة غرداية، 2023.
- الدام محمد، الأمن السيبراني، مذكرة الماستر في الحقوق، تخصص: جريمة وأمن، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر الوادي، 2023.

- صمودي كريمة وبرقعي سمر، الأمن السيبراني في الجزائر، مذكرة الماستر، تخصص: قانون أعمال، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة 8 ماي 1945 – قالمة، 2025.
- عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، مذكرة الماستر المهني الطور الثاني، تخصص: إدارة التحقيقات الاقتصادية والمالية، جامعة قاصدي مرباح–ورقلة، ميدان العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، 2019.
- بن أوذينة سندس، الجهود الدولية في مواجهة الجرائم السيبرانية، مذكرة الماستر أكاديمي حقوق، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة غرداية، 2025.

**هـ. الأيام الدراسية والمحاضرات:**

- بومحراث ليندة، إجراءات التحقيق الخاصة بالجرائم السيبرانية، يوم دراسي حول الجريمة السيبرانية، جامعة الأمير عبد القادر للعلوم الإسلامية–قسنطينة، 2022.

# فهرس المحتويات

## الفهرس

**ملخص:**

ارتبط مفهوم الأمن السيبراني بالجريمة الإلكترونية التي تهدد الأمن القومي في الفضاء الرقمي في عالم تسيطر عليه التكنولوجيا الرقمية، حيث إن الاستعمال السلبي وقلة الوعي باستخدامه قد يجلب مخاطر تهدد أمن وسلامة المجتمع الدولي، الأمر الذي دفع بالدولة الجزائرية إلى تسطير استراتيجية وطنية لأمن الأنظمة المعلوماتية للتصدي لمختلف التهديدات السيبرانية.

تهدف هذه الدراسة إلى توضيح متطلبات تعزيز الأمن السيبراني وتبيان أهميته لحماية السيادة الوطنية، والإشارة إلى واقع ومستقبل الأمن السيبراني في الجزائر.

**الكلمات المفتاحية:** الأمن السيبراني، الجريمة الإلكترونية، الإرهاب السيبراني، التدابير التشريعية.

## Abstract:

The concept of cyber security is closely linked to cybercrime, which threatens national security with in the digital technology. Misuse of this technology, a long with a lack of awareness regarding its proper utilization, can create risks that threaten the security and safety of society. This has prompted the Algerian state to develop a national strategy for securing information systems in order to confront various cyber threats.

This study aims to classify the concept of mechanisms for enhancing cyber security, demonstrate its importance in protecting national sovereignty and highlight the current reality and future of cyber security in Algeria.

**Keywords:** Cyber security**,** electronic crime(cybercrime)**,** cyberterrorism**,** legislative measures.