**وزارة التعليم العالي والبحث العلمي**

**كلية العلوم السياسية والحقوق**

**جامعة النعامة**

# الامن السيبراني وحقوق الانسان

مذكرة لاستكمال متطلبات نيل شهادة الماستر

تخصص : قانون دستوري

تحت اشراف الاستاذة :

العيفاوي صبرينة

من إعداد الطالبين:

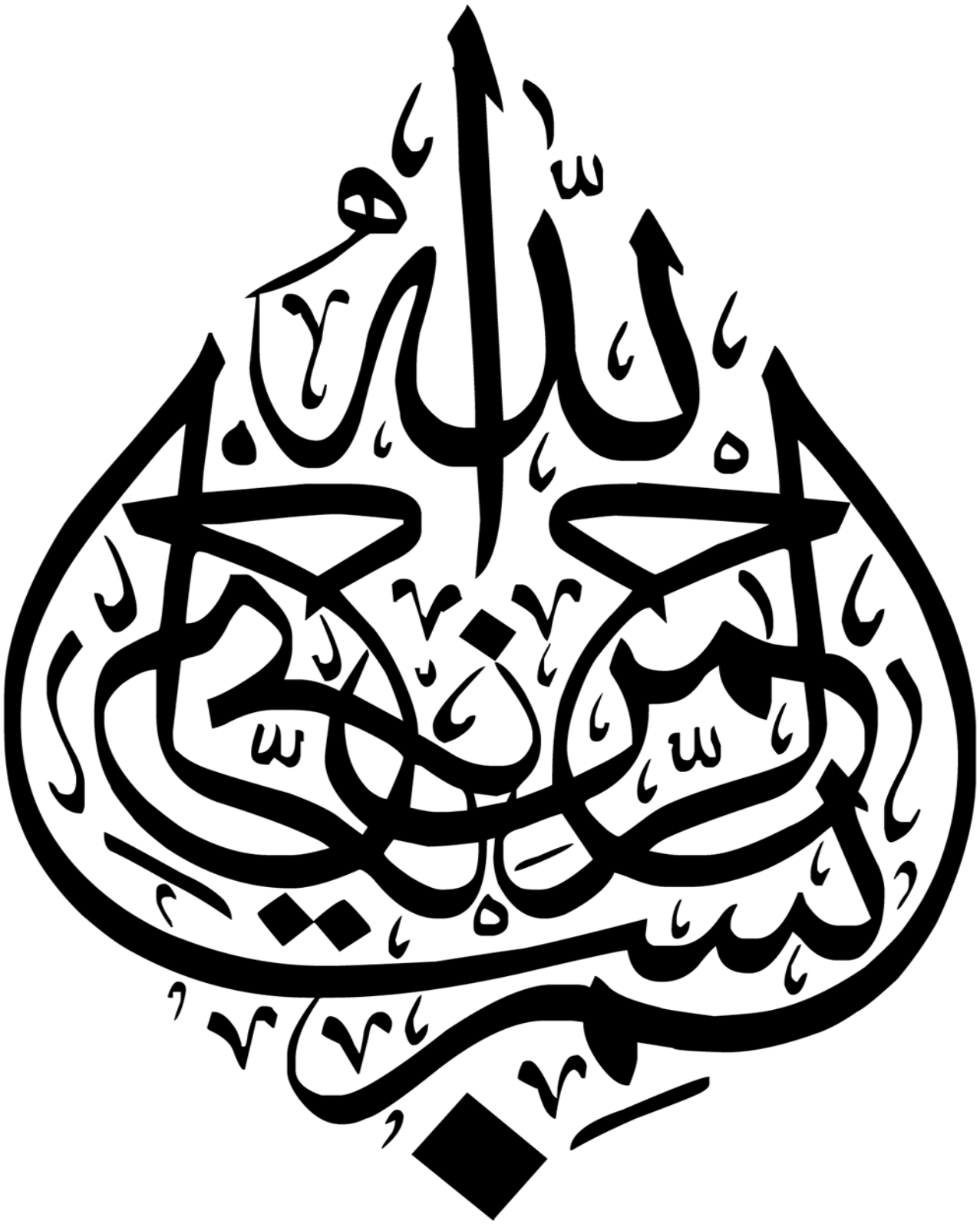
جاب الله سعيد

يعقوبي زكرياء

أعضاء لجنة المناقشة

| اسم ولقب الاستاذ | الرتبة العلمية | الصفة |
|---|---|---|
| عويسات فتيحة | أستاذة التعليم العالي | رئيسا |
| العيفاوي صبرينة | أستاذة محاضرة *أ* | مشرفا ومقررا |
| فيسو اسمهان | أستاذة محاضرة *أ* | مناقشا |

الموسم الجامعي 2026/2025



**قال الله تعالى: «وَلَقَدْ كَرَّمْنَا بَنِي آدَمَ وَحَمَلْنَاهُمْ فِي الْبَرِّ وَالْبَحْرِ وَرَزَقْنَاهُم مِّنَ الطَّيِّبَاتِ وَفَضَّلْنَاهُمْ عَلَىٰ كَثِيرٍ مِّمَّنْ خَلَقْنَا تَفْضِيلًا»**

**[سورة الإسراء: 70]**

الاهداء

إلى من يشتد بهم عضدي، وتكتمل بوجودهم فرحتي، مأمني الأبدي وسندي الداعم إخوتي وعائلتي الغالية.

إلى من قاسمتهم عناء السهر، وتشاركنا معاً شغف العلم ولذة الإنجاز، .أصدقائي وزملائي الأوفياء.

إلى شموع المعرفة التي أنارت لي دروب الفهم، وأصحاب الفضل في تقويم مساري العلمي، أساتذتي الأجلاء وموجّهي الأفاضل.

أهدي هذا العمل المتواضع، قطافاً لرحلة جهد وصبر، راجياً من الله العلي القدير أن يكتب له القبول، ويجعله منارة علمٍ تُنير دروب القادمين.

يعقوبي زكرياء .



# الاهداء

الى من كلّلهما الله بالهيبة والوقار إلى نبع العطاء اللامتناهي، والداي العزيزان حفظهما الله ورعاهما.

إلى من بهم أستند وعنهم لا أميل إخوتي وعائلتي الكريمة، سند الحياة وملاذي في كل حين.

إلى رفقاء المسار الأكاديمي من شاطروني سهر الليالي وشغف البحث وعناء الطلب... أصدقائي وزملائي الأوفياء.

إلى كل من أضاء بعلمه طريقاً كنت أسير فيه ولجميع أساتذتي الأفاضل.

أهدي ثمرة هذا الجهد المتواضع، سائلاً المولى عز وجل أن ينفع به ويجعله خطوة مباركة في مسيرتي المستقبلية

الى من أحاطاني بجميل الرعاية، وغمراني بفيض الدعاء، وكانا لي في هذه الحياة النور والمنارة.

والداي الحبيبان، أطال الله في عمرهما وأدام عليهما الصحة والعافية.

جاب الله سعيد.



# شكر وعرفان

الحمد لله العليّ القدير، الذي بنعمته تتم الصالحات، وبتوفيقه وكرمه تكلل الجهود بالنجاح، فله الحمد والشكر كما ينبغي لجلال وجهه وعظيم سلطانه على ما مَنّ به عليّ من علم وبصيرة وقدرة على إتمام هذا البحث المتواضع.

يطيب لي وأنا أختتم هذا العمل أن أرفع أسمى آيات الشكر والامتنان والتقدير إلى الأستاذة الفاضلة المشرفة عيفاوي صبرينة، التي لم تبخل في رعاية هذا البحث بنصائحها القيمة وتوجيهاتها السديدة، فجزاها الله عني كل خير.

كما أتقدم بتقديري البالغ وخالص ثنائي إلى جميع أساتذتي الأجلاء في كلية الحقوق والعلوم السياسية، الذين أناروا لنا دروب المعرفة بالقانون والسياسة، فكنا ننهل من بحر علمهم الوافر ونقتدي بجميل أخلاقهم طوال مسيرتنا الأكاديمية.

وأتوجه بالشكر الجزيل والامتنان العميق إلى السادة الأفاضل أعضاء لجنة المناقشة الموقرة، لتفضلهم بقبول تقييم هذه المذكرة ومراجعتها، والذين ستشكل ملاحظاتهم وتصويباتهم القيمة إضافة حقيقية لإثراء هذا العمل وتقويمه.

وفي الختام، أعبّر عن خالص شكري وتقديري لكل من ساندني ودعمني، وسعى في عوني، أو أسدى إليّ نصحاً أو دعا لي بظهر الغيب ليرى هذا الجهد النور.



## شكر وعرفان

الحمد لله رب العالمين الذي وفّقني بفضله وكرمه، وأنار لي درب العلم والعلماء، ومنحني القوة والصبر لإتمام هذا العمل المتواضع، فله الحمد والشكر والثناء الحسن أولاً وآخراً.

أتقدم بأسمى عبارات التقدير والامتنان وعظيم الشكر والعرفان إلى الأستاذة الفاضلة المشرفة على هذه المذكرة الأستاذةعيفاوي صبرينة التي غمرتنا بنصحها وتوجيهاتها السديدة، ولم تبخل علّينا بوقتها وعلمها الوافر طيلة فترة إعداد هذا البحث.

كما أتوجه ببالغ الشكر، وخالص الود والتبجيل، إلى كافة أساتذتي الأفاضل في كلية الحقوق والعلوم السياسية، الذين كانوا خير منارة تضيء لنا مسالك القانون والسياسة، فنهلنا من علمهم، واقتدينا بأخلاقهم النبيلة، وتلقينا منهم الدعم المعرفي طيلة مسيرتنا الدراسية، فجزاهم الله عنا خير الجزاء.

ويطيب لي أن أتقدم بجزيل الشكر إلى الأساتذة الأفاضل أعضاء لجنة المناقشة الموقرة، لتفضلهم بقبول تقييم هذه المذكرة وقراءتها وإثرائها بملاحظاتهم القيمة.

وفي الأخير، أزجي شكري وخالص امتناني إلى كل من مد لي يد العون والمساعدة، أو ساهم بكلمة طيبة ودعاء صادق من قريب أو من بعيد لإنجاح هذا العمل.



# مقدمة

شهد العالم المعاصر، مع مطلع الألفية الثالثة، طفرة تكنولوجية غير مسبوقة وثورة رقمية متسارعة أعادت تشكيل البنى الهيكلية للمجتمعات، ونقلت نمط التفاعل الإنساني والمؤسساتي من الفضاء المادي التقليدي إلى الفضاء السيبراني الافتراضي.

فلم يعد هذا الفضاء الرقمي مجرد أداة رفاهية أو وسيلة اتصال ثانوية، بل استحال إلى عصب الحياة اليومية والركيزة الأساسية التي تقوم عليها الإستراتيجيات السياسية، والأنشطة الاقتصادية، والمنظومات القانونية للدول الحديثة. هذا الاعتماد الشامل والحيوي على تكنولوجيات الإعلام والاتصال، بقدر ما فتح آفاقاً رحبة للتنمية المعرفية والتمكين الحقوقي، بقدر ما أنتج بيئة افتراضية معقدة وعابرة للحدود الوطنية، أفرزت بدورها أنماطاً مستحدثة من التهديدات والمخاطر الأمنية الجسيمة (كالجرائم السيبرانية، الهجمات المنظمة، والتجسس الرقمي) التي أصبحت تهدد السيادة الوطنية للدول، واستقرار مرافقها الحيوية، وسلامة بيانات أفرادها.

وفي مواجهة هذه التحديات الأمنية اللامتناظرة، برز الأمن السيبراني كحتمية إستراتيجية ومنظومة قانونية وتقنية متكاملة لا غنى عنها لحماية الفضاء الرقمي، ولم يعد مفهوم الأمن هنا مقتصرًا على البعد العسكري أو المادي الكلاسيكي، بل امتد ليشمل حماية الأصول الرقمية، والشبكات، والأنظمة البرمجية، والبنى التحتية الحيوية (مثل قطاعات الطاقة، الصحة، والمال). ويتجاوز الأمن السيبراني في المفهوم المعاصر مجرد كونه "جدار حماية تقني بحت"، ليصبح منظومة متكاملة من التدابير التشريعية، والسياسات التنظيمية، والآليات الضبطية التي تهدف في جوهرها إلى تحقيق الثالوث الأمني المعياري(السرية، السلامة، وإتاحة واستمرارية الخدمات).

بناءً على ذلك، أضحى الأمن السيبراني بمثابة الحصن القانوني والتقني الذي يذود عن مقومات الدولة والمجتمع في بيئة رقمية شديدة السيولة والخطورة.

تكتسي دراسة هذا الموضوع أهمية قانونية وعملية بالغة، تتجلى في محاولة فك الارتباط المعرفي وتحديد طبيعة العلاقة التفاعلية بين متطلبات الأمن الرقمي والالتزامات الحقوقية الدولية والوطنية، خاصة مع بروز "الحقوق الرقمية" كجيل مستحدث من حقوق الإنسان يتطلب تأصيلاً فقهياً وتشريعياً دقيقاً.

وتتضاعف هذه الأهمية في شقها التطبيقي مع تزايد التهديدات السيبرانية التي تستهدف القطاعات الحيوية والحساسة للدول، مما يجعل من رصد وتحليل كفاءة الأطر التشريعية

والآليات الضبطية ضرورة ملحة، ليس فقط لبيان مدى نجاعة الدولة في مكافحة الإجرام المعلوماتي وبسط السكينة الرقمية، بل لضمان عدم انزلاق التدابير الأمنية الاستثنائية نحو المراقبة التعسفية، والوقوف على مدى توفيق المشرع في صياغة معادلة موزونة تحمي الفضاء الرقمي مع صون النواة الصلبة للحريات الفردية والأشخاص الطبيعيين.

تهدف هذه الدراسة إلى تحقيق الغايات التالية:

تأسيس إطار مفاهيمي وقانوني دقيق للأمن السيبراني وعلاقته بحقوق الإنسان و رصد الآثار المترتبة على تدابير الأمن السيبراني، لاسيما فيما يتعلق بالرقابة الإلكترونية والخصوصية ثم تحليل آليات التوازن التي تبناها المشرع الجزائري من خلال الضمانات الدستورية والقانونية المستحدثة .

يعود اختيار هذا الموضوع إلى اعتبارات موضوعية وأخرى ذاتية :

- الموضوعية : تصاعد وتيرة الهجمات السيبرانية التي استهدفت مؤسسات سيادية (مثل وكالة الأنباء الجزائرية ووزارة العدل) وحاجة المشرع لمواكبة هذه التحولات .
- الذاتية : الرغبة في البحث في الأجيال الجديدة لحقوق الإنسان، وتحديداً الحقوق الرقمية، وكيفية مواءمة القوانين التقليدية مع بيئة رقمية متغيرة لا تعترف بالحدود.

و من بين الدراسات التي تطرقت لهذا الموضوع تعدد المقاربات الأكاديمية التي حاولت معالجة التقاطع بين التكنولوجيا والقانون، ومن أبرز الدراسات التي استند إليها هذا البحث :

1. دراسة الباحثة عروس كوثر والدكتورة عروس فوزية بعنوان "إشكالية الموازنة بين متطلبات الأمن السيبراني وضمان الحقوق الفردية" (2026)
2. دراسة الباحثة رمضاني مسيكة بعنوان "التعويض عن انتهاكات حقوق الإنسان في إطار الاتفاقية الأوروبية لحقوق الإنسان" (2021)

كما تمثلت إشكالية الدراسة فيمايلي: هل وفق الأمن السيبراني في حماية حقوق الإنسان ؟

وجاءت التسؤولات الفرعية كما يلي:

1. ما هو الإطار المفاهيمي للأمن السيبراني وكيف تطور تاريخياً؟ .
2. ما هي أبرز الحقوق المتأثرة بتدابير الأمن السيبراني ؟
3. كيف يمارس القضاء دوره في الرقابة على مشروعية إجراءات المراقبة الإلكترونية؟ .

اعتمدت الدراسة على المنهج الوصفي التحليلي لتفكيك المفاهيم القانونية وتحليل النصوص التشريعية والدستورية ، كما تم توظيف المنهج المقارن لبيان أوجه الاختلاف بين النماذج الدولية في التعامل مع الأمن الرقمي وحقوق الأفراد .

خطة البحث لمعالجة هذه الإشكالية، تم تقسيم الدراسة إلى فصلين أساسيين :

الفصل الأول: الإطار المفاهيمي والقانوني للأمن السيبراني وحقوق الإنسان

- المبحث الأول : ماهية الأمن السيبراني .
- المبحث الثاني : حقوق الإنسان في البيئة الرقمية .

الفصل الثاني: أثر تدابير الأمن السيبراني على حقوق الإنسان

- المبحث الأول : مظاهر المساس بحقوق الإنسان باسم الأمن السيبراني .
- المبحث الثاني : آليات التوازن بين الأمن السيبراني وحقوق الإنسان في الجزائر.

# الفصل الأول : الإطار المفاهيمي والقانوني للأمن السيبراني وحقوق الإنسان

**تمهيد :**

يعيش عالمنا اليوم تحولاً رقمياً هائلاً غيّر وجه الحياة اليومية، وبقدر ما وفر هذا الفضاء الإلكتروني من فرص للتطور والتواصل، بقدر ما فرض تحديات ومخاطر حقيقية تمس أمن الأفراد والدول على حد سواء، من هنا، برزت الحاجة الملحّة إلى ما يُعرف بـ "الأمن السيبراني "كدرع حماية لا غنى عنه.

لكن هذه الحماية الرقمية لا تعمل في معزل عن الواقع الإنساني، بل ترتبط ارتباطاً وثيقاً بـ "حقوق الإنسان"، حيث أصبح الحفاظ على خصوصية الأفراد وحرياتهم الأساسية في الفضاء الرقمي تحدياً قانونياً وأخلاقياً كبيراً.

بناءً على ذلك، يسعى هذا الفصل إلى ضبط المفاهيم الأساسية، من خلال استعراض الإطار المفاهيمي والقانوني لكل من الأمن السيبراني وحقوق الإنسان، وتوضيح طبيعة العلاقة التبادلية بينهما، وذلك عبر المباحث التالية:

- المبحث الأول :ماهية الامن السيبراني
- المبحث الثاني: حقوق الانسان في البيئة الرقمية

## المبحث الأول : ماهية الأمن السيبراني

لم يعدالأمن السيبراني مجرد خيار تقني رفيع، بل أضحى ضرورة استراتيجية وحتمية قانونية وحمائية لا غنى عنها لضمان استقرار الدول وحماية الحقوق والحريات الأساسية للأفراد في البيئة الرقمية.

وللإحاطة الشاملة بأبعاد هذه المنظومة الدفاعية المتكاملة، وتفكيك التشابك بين ضرورتها التقنية وأثرها الحمائي، فإننا سنعمد في هذا المبحث إلى دراسة الموضوع عبر ثلاثة مطالب أساسية متكاملة.

المطلب الأول سنتطرق الى مفهوم الأمن السيبراني ونشأته، ثم المطلب الثاني سنعرج بشكل مختصر على أهمية الأمن السيبراني، وسنتوسع في المطلب الثالث من خلال تحليل الأبعاد المتعددة للأمن السيبراني لننتقل بعدها لرصد التهديدات الفعلية والخطيرة التي تواجه القطاعات الحيوية في عصرنا الحالي.

## المطلب الأول : مفهوم الأمن السيبراني ونشأته

في هذا المطلب سنسلط الضوء على التأصيل اللغوي والاصطلاحي لمفهوم الامن السيبراني، وتتبع مساره التاريخي منذ ظهور أولى الفيروسات الرقمية في السبعينات، وصولاً إلى ثورة الحوسبة الرقمية والإنترنت في التسعينات، مع بيان ارتباط هذه النشأة بظهور أجيال جديدة من حقوق الإنسان كالخصوصية الرقمية، من خلال تقسيمه الى فرعين .

### الفرع الأول: مفهوم الامن السيبراني

الأمن السيبراني لغة : مكون من لفظين الأمن و السيبراني .[1]

الأمن : هو نقيض الخوف، أي بمعنى السلام والأمن مصدر الفعل أمن أمنا وأمانا وأمنة، أي اطمئنان النفس وسكون القلب وزوال الخوف.

ويقال : أمن من الشيء، أي سلم منه، وقد عرفه قاموس بنغوين العلاقات الدولية بأنه مصطلح يشير الى غياب ما يهدد القيم النادرة.[2]

والسيبراني : وهي مصطلح السيبرانية الأن، وهو واحد من أكثر المصطلحات ترددا في معجم الأمن الدولي، مأخوذة من كلمة " Cyber " وهي لفظة يونانية الأصل مشتقة من كلمة " Kubemetes " ، ومعناه الشخص الذي يدير دفة السفينة حيث تستخدم مجازا للمتحكم، مع أنه عدد من المؤرخين يرجعون أصلها الى عالم الرياضيات الأمريكي Norbert Wiemers 1894-1964 وذلك للتعبير عن التحكم الألي .[3]

أما اصطلاحا: نجد العديد من التعريفات لمفهوم الأمن السيبراني، فقد عرفه إدوارد أمورسو Amorose بأنه وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها وتوفير الاتصالات المشفرة.[4]

---

[1] _ فارس محمد العمارات، الامن السيبراني المفهوم وتحديات العصر ،الطبعة الاولى، دار الخليج للنشر والتوزيع،2022، ص 13

[2] _ المرجع نفسه ص13

[3] _ المرجع نفسه ص 14

[4] _ المرجع نفسه ص15

وحسب الاتحاد الدولي للاتصالات فالأمن السيبراني هو "مجموعة من الأدوات والسياسات والمفاهيم الأمنية والتحفظات الأمنية والمبادئ التوجيهية ونهج إدارة المخاطر والإجراءات والتدريب، وغيرها من الممارسات وآليات الضمان والتكنولوجيات التي يمكن استخدامها لحماية البيئة السيبرانية وأصول المؤسسات والمستعملين من المخاطر الأمنية ذات الصلة في البيئة السيبرانية " [1]

وتعرفه الموسوعة البريطانية بأنه "حماية نظم الحوسبة والمعلومات من الأضرار والسرقة والاستخدام غير المصرح به." [2]

كما عرفّ إدوارد أموروسو بأن الأمن السيبراني يضم "مجموع الوسائل التي من شأنها الحد من اخطر الهجومات على البرمجيات أو أجهزة الحاسوب أو الشبكات"، فهو يبدأ بـ "الاحساس الفعلي والتخيلي بعدم وجود أو تأثير التهديدات الفيزيقية والتخيلية لبنى المجتمع المعلوماتي(خاصة الحساسة منها) في جوانبها العسكرية، والاجتماعية، والثقافية، والاقتصادية...إلخ، المختلفة أيّا كان مصدرها داخلي، أو خارجي، وتستدعي التأهب و/أو الفعل الاجتماعي و/أو التأهب والفعل الرسمي لمواجهتها" [3]

نستخلص مما سبق أن الأمن السيبراني لم يعد مجرد إجراء تقني بسيط، بل أضحى منظومة دفاعية متكاملة تتسم بالشمولية والديناميكية، فهو يجمع بين الأدوات التكنولوجية المتطورة، والسياسات التنظيمية الصارمة، وبرامج التدريب البشري، تهدف هذه المنظومة في جوهرها إلى بسط الحماية على كافة مكونات الفضاء الرقمي، بدءاً من البنية التحتية والأجهزة وصولاً إلى البيانات في صورها المادية والمنطقية، مما يجعله بمثابة الحصن القانوني والتقني الذي يضمن سلامة البيئة السيبرانية للمؤسسات والدول على حد سواء.

وتتجسد الغاية الوظيفية للأمن السيبراني في تحقيق الثلاثية الأمنية للمعلومات، والمتمثلة في ضمان سريتها، وسلامة محتواها من التلاعب، واستمرارية توافرها للمصرح لهم فقط. ومن هذا المنطلق، يبرز الأمن السيبراني كضرورة استراتيجية لمواجهة طيف واسع من المخاطر المتجددة، والتي تتراوح بين الهجمات الإجرامية المنظمة، والتجسس،

---

[1] _فارس محمد عمارات نفس المرجع السابق ص 15

[2] _الأمن السيبراني مفهومه وتاريخه،موقع https://www.aljazeera.net/encyclopedia، اطلع عليه يوم 2026/04/27 .

[3] _ذياب البداينة، الأمن وحرب المعلومات ، الإصدار 2،الأردن دار الشروق للنشر والتوزيع، 2006، ص 23.

والتخريب الرقمي، وبذلك، فهو يمثل أداة استباقية لإدارة المخاطر تهدف إلى تحصين الأمن القومي والمصالح الحيوية من تداعيات الاختراقات في عصر التحول الرقمي المتسارع.

**الفرع الثاني : نشأة الأمن السيبراني**

ظهر الأمن السيراني مع نهاية الحرب الباردة، وظهور مصطلح حرب الإنترنت أو الحرب السيبرانية، التي جاءت مع بداية اعتماد الدول على أجهزة الكمبيوتر في مؤسساتها وتطوير وحدة المعالجة المركزية في هذه الأجهزة، التي دخلت في عمل المؤسسات والحكومات وحتى في الحياة اليومية، واقتصر دور الأمن السيبراني في الفترة الأولى على الحماية من الفيروسات والبرمجيات الخبيثة[1].

بعد ظهور الأنترنت في التسعينات وانتشارها الواسع أحدث تحولا وأدى إلى تغيير ملامح الحرب السيبرانية وأصبحت الهجمات الإلكترونية أكثر تنوعاً وتعقيداً لفترة يمكن وصفها بالحرب السيبرانية الباردة أصبحت الدول تتسابق على تطوير تقنيات الأمن السيبراني لحماية بنيتها التحتية الرقمية، كما وصل استخدام تقنيات الأنترنت بشكل موسع لدى الجيوش والمؤسسات الأمنية، مما جعل من الأمن السيبراني جزءاً أساسيا من استراتيجيات الدفاع العسكري.

بعد الحرب الباردة وانتهاء الثنائية القطبية، ظهر مفهومين أساسيين وهما حرب الأنترنت (netwar) والحرب السيبرانية (cyberwar)، من هنا تغيرت مفاهيم القوة استجابةً للثورة الرقمية، فمن القوى العسكرية والاقتصادية للدولة ظهرت القوة السيبرانية (cyber power) التي مكنت المجموعات الإجرامية والهاكرز من التأثير على حقوق وحريات الأفراد وحتى الدول، مما أضعف احتكار الدولة للقوة غيّر من أنماط السيطرة داخل الدولة و النفوذ في النظام الدولي.[2]

ومع انفجار الثورة المعلوماتية ودخول العصر الرقمي، واعتبار عدد من الباحثين الفضاء السيبراني بمثابة المجال الخامس في الحروب بعد البر والبحر والجو والفضاء،

[1] _ الأمن السيبراني مفهومه وتاريخه ، موقع https://www.aljazeera.net/encyclopedia ، اطلع عليه 2026/06/01

[2] _فارس محمد العمرات نفس المرجع السابق ض 20

ظهرت الحاجة لتوفير ضمانات أمنية، خاصة مع بداية ظهور التهديدات والجرائم السيبرانية مع دخول القرن الـ21.

ودخل الأمن السيبراني ضمن حقل الدراسات الأمنية، وظهرت تقنيات متطورة مثل التشفير والأمان السحابي والكشف عن التهديدات بالذكاء الاصطناعي، ومع ذلك فإن الهجمات السيبرانية مجال معقد وسريع التطور، مما يستلزم استجابات أمنية سريعة تضاهي وتيرة نموه السريع. [1]

## المطلب الثاني : أهمية الأمن السيبراني

ونستعرض بشكل مختصر من خلال هذا المطلب الغايات الوظيفية للأمن السيبراني، والتي تتمحور حول تحقيق الثلاثية الأمنية للمعلومات (السرية، السلامة، والتوافر)، وكيف يشكل هذا الأمن خط الدفاع الأول لحماية الأنظمة والمجتمعات.

للأمن السيبراني أهمية كبيرة في كافة المجالات تتمثل فيما يلي:

أولا– زيادة الهجمات الإلكترونية : تواجه 60% من منظمات العالم اختراقات بمعدل هجمة كل 39 ثانية، مما يجعل الأمن السيبراني الحل الأمثل للتصدي لها.

ثانيا– التطور التكنولوجي: جبر الشركات على تبني الأمن السيبراني لمواجهة استغلال المخترقين للذكاء الاصطناعي في تزييف الهويات وصياغة هجمات احترافية.

ثالثا– التحول إلى الخدمات السحابية : زاد من حاجة الشركات لتأمين البنية السحابية لحماية بيانات العملاء، وتسهيل العمليات، ودعم منظومة العمل عن بُعد.

رابعا– خسائر الجرائم الإلكترونية : دفعت الشركات لتطبيق الأمن السيبراني تجنباً لتكاليف باهظة كفقدان البيانات، وتوقف الأعمال، والمسؤولية القانونية، وتضرر السمعة[2].

---

[1] _هبة خطاب،الأمن السيبراني مفهومه وتاريخه، https://lcss.gov.ly/articles/blog/post-510/، اطلع عليه 2026/06/02

[2] فوائد الأمن السيبراني ومناط أهميته وإيجابيات وسلبيات التخصص فيه ، https://bakkah.com/ar/knowledge-cente ، اطلع عليه 2026/06/02 .

## المطلب الثالث : ابعاد الأمن السيبراني والتهديدات التي يشكلها

يتسع نطاق الأمن السيبراني ليتخذ أبعاداً متعددة تتجاوز المفهوم التقني الضيق، وفي المقابل، تفرز هذه البيئة الرقمية طيفاً متنامياً من التهديديات السيبرانية التي أصبحت تستهدف عصب القطاعات الحيوية والحساسة التي تقوم عليها حياة الأفراد والمجتمعات.

وللوقوف على هذه الصورة المتكاملة بشقيها (المجالات المتأثرة وطبيعة المخاطر)، سنقسم دراسة هذا المطلب إلى فرعين رئيسيين،الفرع الأول أبعاد الأمن السيبرانيوونناقش فيه الكيفية التي يعيد بها الفضاء السيبراني تشكيل مفاهيم الأمن والقوة عبر خمسة أبعاد أساسية .

الفرع الثاني الأمن السيبراني والتهديدات التي يشكلها وفيه ننتقل من الإطار النظري للأبعاد إلى الواقع التطبيقي للمخاطر، مستعرضين تنامي الجريمة السيبرانية وأثرها التخريبي على ثلاثة قطاعات استراتيجية لا تتحمل الانقطاع أو الاختراق، وهي القطاع المالي والمصرفي، قطاع الطاقة والقطاع الصحي.

### الفرع الأول : أبعاد الأمن السيبراني

تعمل كل الدول للحفاظ على الأمن القومي لها من كل تهديد سيبراني من خلال أمنها السيبراني لعدة مجالات عسكرية، اقتصادية، اجتماعية، سياسة وحتى انسانية نفصل فيها :

أولا – البعد العسكري: يتجلى البعد العسكري للأمن السيبراني في صرورة تأمين الشبكات الاتصال العسكرية وضمان استمرارية قدرتها على تبادل الاوامر والتعليمات والمعلومات بدقة وسرعة فمع التطور التكنولوجي اصبحت الجيوش تعتمد على الأنظمة الرقمية والشبكات المعلوماتية بشكل متزايد وهو ما أتاح فرصا استراتيجية كبيرة لإصابة الاهداف عن بعد. الا أنها كذلك تمثل نقطة ضعف يمكن استغلالها من قبل الخصوم خاصة أذا لم تكن مؤمنة جيدا من الإختراق الذي قد يؤدي الى تدمير قواعد البيانات العسكرية أو قطع

الاتصال بين مراكز القيادة والوحدات الميدانية بل وقد يصل الأمر الى التحكم في بعض منظومات التسليح الحديثة وخروجها عن السيطرة مثل :الطائرات بدون طيار، الصواريخ الموجهة عبر الاقمار الصناعية وأي خلل أمني في هذا المجال يشكل تهديد مباشر للأمن القومي للدولة .[1]

"وقد شكل الهجوم السيبراني الشهير بواسطة دودة "**ستاكسنت (Stuxnet)** "محطة مفصلية ونقطة تحول استراتيجية في تاريخ الصراعات الرقمية، إذ كشف هذا الهجوم عن انتقال التوظيف السيبراني من مجرد عمليات التجسس التقليدية وجمع المعلومات الاستخباراتية، إلى استخدامه كأداة للتخريب المادي الفعلي، وهو ما تجسد في استهداف المنشآت النووية الإيرانية وتعطيل أجهزة الطرد المركزي بها ميكانيكياً." [2]

ثانيا– البعد الاجتماعي : قد جاء في تقرير الاتحاد الدولي للاتصالات[3] 2010 (ITU) بشأن الأبعاد الاجتماعية للأمن السيبراني أن الثورة الرقمية غيرت كيفية التعامل التجاري، وكيفية عمل الحكومات، وأدت العولمة والتقدم التكنولوجي إلى إضعاف البنية التحتية وبالتالي جعلتها هدفاً محتملاً لهجمات إرهابية، حيث تُواجه البلدان مخاطر حقيقية، للأعداء أن يستغلوا مواطن الضعف التي تعاني منها أنظمة المعلومات الدقيقة. فهم يسعون إلى تعطيل البنية التحتية والموارد الأساسية من أجل تهديد الأمن القومي.[4]

يتجاوز أثر الأمن السيبراني النطاق العسكري التقني الصرف ليتشابك بصورة وثيقة مع البعد الاجتماعي، إذ تحولت الفضاءات الرقمية والمنصات الاجتماعية إلى ساحات تفاعلية مفتوحة تتيح للأفراد ممارسة حرياتهم الأساسية، كالتعبير عن الآراء، وتحديد التوجهات السياسية والمجتمعية، والمشاركة الفاعلة في النقاش العام. ومع ذلك، فإن هذه

---

[1] _ فارس محمد عمارات، نفس المرجع السابق ص 27

[2] _ المرجع نفسه ص 27

[3] _يرمز الاختصار ITUإلى الاتحاد الدولي للاتصالات بالإنجليزية ( International Telecommunication Union)

وهو وكالة الأمم المتحدة المتخصصة في تكنولوجيا المعلومات والاتصالات .يقع مقره الرئيسي في جنيف بسويسرا، ويُعد من أقدم المنظمات الدولية حيث تأسس عام 1865

[4] _إسلام فوز ، الأمن السيبرانى :الأبعاد الاجتماعية والقانونية تحليل سوسيولوجى، المجلة الاجتماعية القومية، جامعة دمنهور، المجلد السادس والخمسون، العدد الثانى، مايو 2019 ، ص108 .

الطبيعة المفتوحة للفضاء الرقمي وصعوبة فرض الرقابة الشاملة على محتواه، أفرزت تحديات خطيرة تمس صلب المنظومة الأخلاقية والقيمية للمجتمعات، وتتجلى هذه المخاطر في احتمالية تعرض الهويات الوطنية والثقافية لاختراقات خارجية تهدف إلى زعزعة السلم الاجتماعي عبر توظيف آليات التجسس الرقمي، واستغلال منابر التواصل في بث خطابات الكراهية، ونشر الأخبار الزائفة، وشن حملات التضليل الممنهجة لتوجيه الرأي العام والتلاعب به.[1]

ثالثا– البعد السياسي: يعد التدخل الروسي السيبراني في الانتخابات الأمريكية أكبر دليل على ضرورة وأهمية[2]

الأمن السيبراني في بعده السياسي، إضافة ألى تسريبات الوثائق الحساسة والاختراقات التي غالبا تؤدي غلى أزمات ديبلوماسية بين الدول خاصة في تلك المراسلات والوثائق ذات الطابع السري لذا أصبح الأمن السيبراني عنصرا أساسيا في حماية الكيان السياسي للدولة ومصالحا الاقتصادية والاستراتيجية ومن جهة أخرى أدى التطور التكنولوجي إلى إعادة تشكيل موازين القوى داخل المجتمع ذاته حيث أسبح المواطن فاعلا رئيسيا في المجال السياسي من خلال قدرته على الوصول إلى المعلومات وتحليلها ونشرها ويعزز ذلك حقة في المشاركة السياسية وتكوين رأي عام مستنير لكنه في الوقت نفسه يفتح المجال أمام حملات التأثير والتضليل الذي قد يمس بنزاهة العملية الديمقراطية كما يوظف الفاعلون السياسيون الوسائط الرقمية للوصول إلى أكبر شريحة ممكنة من المواطنين والترويج لسياستهم وهو ما يثير إشكالية أخلاقيات الاستخدام السياسي للتكنولوجيا وحدود المشروعية في جمع المعلومات والبيانات وتحليلها لأغراض انتخابية.[3]

رابعا– البعد القانوني:

البعد القانوني للأمن السيبراني يشير إلى المجموعة الشاملة من القوانين والتشريعات، التي تنظم وتحمي المعلومات والبيانات الرقمية من التهديدات والاختراقات الإلكترونية.

---

[1] محمد فارس العمارات ، نفس المرجع السابق ص29

[2] المرجع نفسه ص 30

[3] المرجع نفسه، ص11.

يهدف البعد القانوني إلى توفير إطار قانوني يحمي الأفراد والمؤسسات من الاعتداءات السيبرانية، ويعاقب المتسببين في الهجمات الإلكترونية، تختلف التشريعات القانونية المتعلقة بالأمن السيبراني من بلد إلى آخر، وتتضمن قوانين حماية البيانات، وقوانين مكافحة الجرائم السيبرانية، وقوانين تنظيم الاتصالات الإلكترونية، وقوانين حقوق الملكية الفكرية، وقوانين الخصوصية الإلكترونية، وقوانين الاعتراف القانوني للتوقيع الإلكتروني، وغيرها من التشريعات ذات الصلة[1].

خامسا– البعد الاقتصادي: يرتبط الأمن السيبراني ارتباطاً وثيقاً وعضوياً بالمنظومة الاقتصادية الحديثة، إذ يتجلى التلازم الواضح بين حماية الفضاء الرقمي واقتصاد المعرفة القائم على التوسع في استخدام تكنولوجيات المعلومات والاتصالات، وتستمد هذه العلاقة أهميتها من القيمة الاستراتيجية والمالية التي تمثلها البيانات والمعلومات المتداولة والمخزنة عبر مختلف المستويات، ففي الوقت الذي تتيح فيه تقنيات الاتصال الحديثة تعزيز التنمية الاقتصادية للدول، وفتح آلاف الفرص الاستثمارية أمام الشركات الدولية والكبرى لإدارة تكاليف إنتاجها بأفضل الشروط والمواصفات، فإنها تفرض في المقابل تحديات أمنية جسيمة.علاوة على ذلك، دخل الاقتصاد العالمي مع العصر الرقمي مرحلة المال الإلكتروني ضمن بيئة تقنية شديدة الديناميكية والحركة، لاسيما بعد إطلاق الخدمات المالية والمصرفية الرقمية وتزايد استثمارات البنوك والمؤسسات المالية في هذا المجال الحيوى. وفي ظل التنافس المحموم بين الشركات لتطوير تطبيقات وحلول تضمن آليات دفع آمنة للأرصدة الافتراضية، سارعت بعض الدول إلى سن تشريعات خاصة لحماية أموالها ومواجهة الصعوبات القانونية والتقنية الناشئة عن هذا التحول[2].

**الفرع الثاني: الأمن السيبراني والتهديدات التي يشكلها**

الجريمة السيبرانية تزداد وتتنامى وتتسارع بشكل كبير، وتظهر لها أيضاً أشكال جديدة باستمرار، ويصبح مرتكبو الجرائم السيبرانية أكثر مرونة، فيقومون باستغلال أدوات

[1] _سعد بوه الشيخ محفوظ، ابعاد الامن السيبراني، https://armee.mr/node/3066 ، اطلع عليه 2026/05/20

[2] _إدريس عطية ، مكانة الامن السيبراني في منظومة ألمن الوطني الجزائري، كلية الحقوق والعلوم السياسية-جامعة العربي التبسي - تبسة/ الجزائر، مجلة المصداقية ، ص 105

التكنولوجيا الحديثة بشكل فائق السرعة، وتتجلى خطورة هذا الاستغلال بوضوح عند تسليط الضوء على القطاعات الحيوية، من بينها ما يلي :

أولا : القطاع المالي

" أدى زيادة اعتماد الخدمات المالية، والمصرفية بصفة خاصة على التكنولوجيا إلى ارتفاع نسبة المخاطر والهجمات السيبرانية على المؤسسات المالية، ففي مجال البنوك على سبيل المثال لم تعد الإجراءات الرقابية المصرفية التقليدية ذات أهمية، فقد تم الاستعانة ببعض الخبراء والشركات في مجال التكنولوجيا لتفعيل وسائل الحماية الحديثة وأصبح القطاع المصرفي أكثر القطاعات المالية استهدافاً من قبل القراصنة، وقد كثر في الآونة ورود اتصالات من أرقام وأسماء لمصارف وطنية من خارج الدول وتحاول الحصول من العملاء على بيانات عن حساباتهم أو بطاقتهم الائتمانية وإساءة استخدامها بعد ذلك فمكافحة الجريمة الالكترونية تعد أهمية قصوى للقطاع المصرفي في هذه الأيام" [1].

ثانياً : قطاع الطاقة

" يعد قطاع الطاقة من أبرز القطاعات المتضررة من الجرائم السيبرانية المرتكبة ضد الدول، حيث يضم محطات وشبكات التحكم في إنتاج وتوزيع الكهرباء والنفط والغاز ومحطات الطاقة النووية وغيرها، ومن صور اختراق الأمن السيبراني لقطاع الطاقة فقد يتضح لنا أن الطاقة المتجددة تعتمد على أنظمة التحكم الصناعية المتطورة وشبكات التوزيع، ونظراً لعدم توفر مصادر الطاقة المتجددة مثل الرياح والطاقة الشمسية على مدار الساعة، فإنه يتطلب أيضاً حلول لتخزين الطاق" .[2]

مما سبق يتضح ان قطاع الطاقة (بما يشمل الكهرباء، والنفط، والغاز، والطاقة النووية والمتجددة) من أكثر القطاعات حيوية واستهدافاً بالجرائم السيبرانية نظراً لاعتماده على أنظمة تحكم رقمية متطور كما تتضاعف هذه المخاطر مع التوجه نحو الطاقة

[1] _مصطفى كامل قرطاس، لأمن السيبراني وحقوق الإنسان الرقمية، المفوضية العليا لحقوق الانسان، قسم النشر والتثقيف، شعبة البحوث والدراسات، سنة 2023، ص 20

[2] _المرجع نفسه، ص 20

المتجددة (كالرياح والشمس)، لأنها تحتاج إلى شبكات توزيع ذكية وحلول تخزين معقدة لتغطية فترات غياب الطبيعة.

ثالثاً: القطاع الصحي

" شكلت العديد من الهجمات التي تستهدف قطاع الرعاية الصحية مصدر قلق للعالم أجمع، نظراً لأن هذا القطاع يشهد عالمياً ضغطاً تشغيلياً كبيراً في محاولة احتواء حالات الطوارئ الصحية حيث يتظاهر المهاجمون أنهم ينتمون إلى منظمة الصحة العالمية بهدف الحصول على الأموال خصوصاً أثناء أزمة كوفيد (19) إذ أصدرت منظمة الصحة العالمية بياناً تحذر فيه من حملات الهندسة الاجتماعية وقد تكرر الاعتداء على قطاع الرعاية الصحية أيضاً عندما تم الاعتداء على المركز الأمريكي للسيطرة على الأمراض والوقاية منها. وتمثل الهجمات في قطاع الرعاية الصحية عالمياً في الربع الأول من عام 2020 بنسبة 13.37% فضلاً عن تلك التي تستهدف الحصول على معلومات عن اللقاح وغيرها، كذلك فإن هذا الوباء سرع من التحول للخدمات الإلكترونية وقابلها محاولات اختراق عديدة للحصول على خدمات غير مشروعة" . [1]

[1] نفس المرجع السابق ص 21/20

## المبحث الثاني : حقوق الانسان في البيئة الرقمية

يهدف هذا المبحث الى تفكيك العلاقة التلازمية بين المنظومة الحقوقية والأمن الرقمي، فإننا نقسم دراسة هذا المبحث إلى ثلاثة مطالب رئيسية متكاملة.

المطلب الأول سنتطرق الى مفهوم حقوق الإنسان، ثم المطلب الثاني المعنون بحقوق الإنسان في الفضاء الرقمي.

وسنختم بالمطلب الثالث تحت عنوان طبيعة العلاقة بين الأمن السيبراني وحقوق الإنسان حيث نخصص فرعين لهذا المطلب.

## المطلب الأول : مفهوم حقوق الانسان

يستعرض هذا المطلب الدلالات اللغوية والاصطلاحية للحق بين المنظورين الشرعي والقانوني، مع بيان جذوره الفلسفية الطبيعية والمدنية، ومن هذا المنطلق، نقسم دراستنا إلى فرعين، نخصص الفرع الأول للبحث في ماهية الحق لغةً واصطلاحاً، بينما نتناول في الفرع الثاني مفهوم حقوق الإنسان بمرتكزاته وأجياله المختلفة.

### الفرع الأول: المعنى اللغوي والاصطلاحي للحق

الحق في اللغة : "جمع حقوق ، الصواب ، ضد الباطل."[1]

المعنى الاصطلاحي للحق : ستتم معالجة مفهوم الحقوق عبر مستويين متكاملين: المستوى الشرعي الإسلامي، والمستوى القانوني الوضعي، وذلك وفقاً للآتي:

في المفهوم الإسلامي يعرف الحق بأنه: "شامل المعنى متكامل الأوجه لا يحده حد، ويشمل سعادة الإنسان في حياته وآخرته، لأنه منزل من السماء وبتشريع إلهي مؤكد التنفيذ".[2]

برز المفهوم الإسلامي للحق كمنظومة شمولية تتجاوز الأطر المادية الضيقة، فهو ليس مجرد نتاج لتوافق بشري بل تشريع إلهي منزل من السماء، مما يضفي عليه قدسية خاصة وقوة إلزامية نابعة من العقيدة والوازع الديني، وتتجلى عبقرية هذا التصور في كونه لا يحدّ بحدود زمنية أو مكانية، إذ يربط بين استحقاقات الإنسان في حياته الدنيا وسعادته في الآخرة، محققاً توازناً دقيقاً بين المصلحة الفردية والمقاصد الشرعية الكبرى.

في المفهوم القانوني استعمل علماء القانون الحق فيما ثبت للإنسان فائدة أو مصلحة عن طريق القانون، فهو اصطلاح قانوني يعني السلطة أو القدرة التي يقررها القانون لشخص، ويكون له بمقتضاها ميزة القيام بعمل معين .[3]

---

[1] _ معجم المعاني https://www.almaany.com/

[2] _لغرس سوهيلة، حقوق الإنسان (مقاربة نظرية في المفهوم والخصائص)، مجلة الاجتهاد للدراسات القانونية والاقتصادية، كلية العلوم الإنسانية والاجتماعية- جامعة مصطفى اسطمبولي معسكر (الجزائر)، المجلد 12، العدد03، سنة 2023، ص 399

[3] _ المرجع نفسه، ص 399

القانون هنا ينظر إلى الحق بصفته سلطة أو قدرة نظامية تُمنح للشخص بمقتضى نصوص تشريعية، تتيح له بموجبها ممارسة أعمال معينة أو اقتضاء استحقاقات محددة تضمن له التفوق على غيره في مركز قانوني معين. ولا يمكن فهم التحول من المفهوم الروحي الشامل (الإسلامي) إلى المفهوم الوظيفي الإجرائي (القانوني) دون العودة إلى الجذور الفلسفية التي ميزت بين أصل الحق وممارسته.

وفي هذا الصدد، يقدم المفكر توماس بين (Thomas Paine) في كتابه حقوق الإنسان (1791) رؤية تحليلية تربط بين الوجود الإنساني والكيان المجتمعي، حيث يقسم الحقوق إلى نوعين متكاملين :

أولا الحقوق الطبيعية" :وهي تلك الحقوق التي يتمتع بها الإنسان بمقتضى حقه في الوجود كحقه في التفكير، التصرف كإنسان،... بحيث لا يتعدى على حقوق الآخرين" [1].

ثانيا الحقوق المدنية" :هي تلك الحقوق التي يتمتع بها الإنسان بمقتضى حقه في الوجود كعضو في المجتمع كحقه في الأمن والحماية وكل حق مدني له أساس في حق طبيعي موجود سلفاً عند الفرد"[2]

من خلال هذين التعريفين للمفكر "توماس بين"، يمكننا استنتاج قاعدة فلسفية وقانونية متكاملة حول أصل الحقوق ومبرر وجود المجتمع، وهي كالتالي :

أولا : أصالة الحقوق الطبيعية: تُعد هذه الحقوق نتاجاً مباشراً للوجود البشري، فهي تولد مع الفرد وتلازمه (كالحق في التفكير)، ولا تُستمد من القوانين الوضعية بل تسبقها.

ثانيا : تقيد الاحترام المتبادل: إن ممارسة الحق الطبيعي محكومة بضابط جوهري يتمثل في عدم الإضرار بالغير، مما يؤسس لمفهوم الحرية المسؤولة داخل المجتمع.

ثالثا :وظيفة الحقوق المدنية: تظهر الحقوق المدنية كضمانة مجتمعية (مثل الحق في الأمن والحماية)، تهدف أساساً إلى تمكين الفرد من ممارسة حقوقه الفطرية في بيئة آمنة ومنظمة.

[1] _Thomas Paine, Rights of Man, London, 1791, p20

[2] _ توماس بين نفس المرجع السابق ص 21

رابعا :الترابط العضوي: لا تنفصل الحقوق المدنية عن أصلها الطبيعي، بل هي مجرد امتداد وتجسيد مؤسساتي لحقوق كانت موجودة سلفاً لدى الفرد قبل انخراطه في الجماعة.

**الفرع الثاني : مفهوم حقوق الانسان**

" تعد حقوق الإنسان (الحقوق الأساسية) حقوقاً غير قابلة للتصرف ومتأصلة في جميع البشر، بغض النظر عن جنسيتهم، أو مكان إقامتهم، أو جنسهم، أو أصلهم الوطني أو العرقي، أو لونهم، أو دينهم، أو لغتهم، أو أي وضع آخر،إن هذه الحقوق جميعها مترابطة، ومتداخلة، وغير قابلة للتجزئة، وفي هذا الصدد، تُعتبر نوعاً من القانون الطبيعي المكفول بموجب القانون الموضوعي في شكل دساتير وطنية أو قوانين دستورية محلية، أو دولياً في شكل معاهدات، وقانون دولي عرفي، ومبادئ عامة ومصادر أخرى للقانون الدولي.

تفرض هذه الحقوق التزامات على عاتق الحكومات، وعادةً ما تكون بالامتناع عن أفعال معينة (حقوق سلبية) أو العمل بطريقة معينة (حقوق إيجابية) ومع ذلك، فإن قائمة حقوق الإنسان قد تختلف بالنظر إلى التطور التاريخي والمجتمع؛ وفي هذا السياق، يتحدث البعض عن ثلاثة أجيال من حقوق الإنسان: الجيل الأول (الحقوق المدنية والسياسية)، الجيل الثاني (الحقوق الاقتصادية والاجتماعية والثقافية)، والجيل الثالث (حقوق التضامن). كما تُعد الحقوق الأساسية (الإنسانية) جزءاً جوهرياً من المفهوم الحديث لسيادة القانون، ولا ينبغي تقييدها إلا نتيجة لمحاكمة عادلة (الإجراءات القانونية الواجبة) ".[1]

ومن خلال القراءة التحليلية للتعريف السالف الذكر، يمكننا استخلاص عدة مرتكزات أساسية تؤطر ماهية حقوق الإنسان وتفكك أبعادها الفلسفية والقانونية، وذلك على النحو الآتي:

أولا / يتضح أن حقوق الإنسان ليست منحة تُعطى، بل هي حقوق لصيقة بالصفة الإنسانية ومكتسبة بالفطرة، ولا تقبل الإسقاط أو التنازل.

[1] European Judicial Training Network (EJTN), Handbook: English for Human Rights EU Law, Brussels, 2017, p. 24

ثانيا / يكشف التحليل عن استمداد هذه الحقوق لجذورها من القانون الطبيعي، إلا أنها تكتسب قوتها الإلزامية وحمايتها الفعلية من خلال صياغتها في قوالب القانون الوضعي.

ثالثا/ يُرتب هذا المفهوم التزامات قانونية مزدوجة على عاتق السلطات العامة التزامات سلبية تتمثل في وجوب امتناع الدولة عن أي تدخل أو تعسف يمس بحريات الأفراد، والتزامات إيجابية تفرض عليها التدخل الفاعل والعمل على توفير البيئة والخدمات اللازمة لإعمال هذه الحقوق وتجسيدها على أرض الواقع.

رابعا/ لا يقتصر التعريف على مقاربة جامدة، بل يعكس مرونة حقوق الإنسان وتطورها المستمر استجابةً للتحولات المجتمعية والتاريخية الإنساني.

**المطلب الثاني : حقوق الإنسان في الفضاء الرقمي**

تناول هذا المطلب ملامح الجيل الرقمي من الحقوق، والشرعية الدولية التي تؤطرها، مستعرضين طائفة من الحقوق اللصيقة بالمواطنة الرقمية مثل الحق في حرية التعبير الرقمي، الحق في الأمن والسلامة الرقمية، وحق الحصول على المعلومات والتواصل الافتراضي.

لقد أشارت المادة 19 من العهد الدولي للحقوق المدنية والسياسية إلى:
" لكل إنسان حق في حرية التعبير، ويشمل هذا الحق حريته في التماس مختلف ضروب المعلومات والأفكار وتلقيها ونقلها إلى الآخرين دونما اعتبار للحدود، سواء على شكل مكتوب أو مطبوع، أو في قالب فني، أو بأية وسيلة أخرى يختارها "[1] ، فنجد أن هذه المادة تبرز حماية الحق في طلب المعلومات وتلقيها ونقلها، وهو ما يرتبط ارتباطاً وثيقاً بواقع الهجمات السيبرانية التي تهدف إلى منع الأفراد من الوصول إلى الخدمات أو المعلومات عبر شبكة الإنترنت أو عبر وسائل الاتصال المختلف، كما يمكن أن تمس الهجمات السيبرانية عدداً من الحقوق الأساسية الأخرى مثل:الحق في الحياة أو الحق في الصحة أو الحق في الغذاء،وذلك تبعاً لطبيعة الهجوم السيبراني وأهدافه، فعلى سبيل المثال، قد يؤدي هجوم سيبراني يستهدف فرض قيود اقتصادية أو تعطيل أنظمة معينة

[1] _ العهد الدولي الخاص بالحقوق المدنية والسياسية، المؤرخ في 16 ديسمبر 1966، تاريخ بدء النفاذ 23 مارس 1976 اعتمد وعرض للتوقيع والانضمام بموجب قرار الجمعية العامة للأمم المتحدة 2200ألف (د- 21)

إلى عرقلة المعاملات المرتبطة بالحصول على الغذاء أو الدواء، مما يبرز أهمية احترام هذه الحقوق حتى في ظل النزاعات أو الهجمات في الفضاء السيبراني .وقد ذهبت بعض الدول الى اعتبار الوصول الى شبكة الانترنت حقا اساسيا من حقوق الانسان داخل مجتمعاتها، وهو ما يعكس تزايد الاعتراف الدولي بأهمية هذا الحق في العصر الرقمي.[1]

ومن ابرز حقوق الانسان الرقمية التي اوردها التنظيم القانوني الدولي ما يأتي:

اولا : قرار الجمعية العامة للأمم المتحدة:

" اصدرت الجمعية العامة للأمم المتحدة قرار أمني بتاريخ 19 ديسمبر 2016 بعنوان الحق في الخصوصية في العصر الرقمي."

ثانيا :ميثاق حقوق الانترنت لجمعيه الاتصالات المتقدمة APC

" صدر هذا الميثاق في فبراير سنة 2010 بمدينة براغ – تشيك، وقد ركز على التأكيد على حق جميع الافراد في الوصول الى شبكة الانترنت اضافة الى ضمان حريه التعبير والتنظيم عبر الفضاء الرقمي، كما اولى الميثاق اهتماما خاصة بحماية الخصوصية وتعزيز مبادئ حكومة الانترنت الى جانب نشر الوعي الرقمي وتفعيل مختلف الحقوق المرتبطة باستخدام الشبكة، وقد شدد كذلك على ان حرية تبادل المعلومات والتواصل عبر الانترنت تمثل عنصرا اساسيا في دعم وترسيخ حقوق الانسان الرقمية استنادا الى المبادئ التي اقرها الاعلان العالمي لحقوق الانسان".[2]

ثالثا : الحق في حريه التعبير الرقمية

يستند هذا الحق الى المبادئ التي جاء بها الاعلان العالمي لحقوق الانسان اضافة الى العهدين الدوليين الخاصين بحقوق الانسان حيث يندرج ضمن نطاق الحق في حرية الرأي والتعبير، ويعني ذلك تمكين كل فرد من التعبير عن أدائه وأفكاره بحرية دون تدخل قيود غير مشروعة، مع مراعات عدم تعارض ذلك مع حقوق الأخرين او مع مقتضيات النظام العام.

وتعد حرية التعبير في الفضاء الرقمي، من الحقوق الأساسية التي أكدت على التشريعات والقوانين الحديثة، مما يستوجب توفير الحماية القانونية اللازمة لها وضمان

[1] _مصطفى كامل قرطاس، نفس المرجع السابق ص 25

[2] _المرجع نفسه ص 26.

احترامها، غير أن هذا الحق قد يتعرض في بعض الأحيان الى انتهاكات من قبل بعض السلطات والأنظمة الحاكمة بموجب القوانين الجائزة التي يتم سنها تحت بند قوانين مكافحة جرائم الإلكترونية. [1]

1. الحق في الأمن الرقمي : "يقصد بالأمن الالكتروني مجموعة التدابير والتقنيات التي يتم اعتمادها لحماية الشبكات والأنظمة والبرمجيات والبيانات من مخاطر الاختراق أو الهجمات أو الوصول غير المصرح به من الهجمات السيبرانية التي تهدف الى الوصول أو تغير أو تدمير المعلومات الحساسة لأغراض شخصية مالية أو دولية مخابراتية أو غير ذلك". [2]

رابعا : حق الحصول على المعلومات

يُشكل الحق في الوصول إلى المعلومات ركيزة جوهرية لممارسة الحقوق المدنية والسياسية؛ إذ يُقصد به تمكين الأفراد من نيل البيانات والمعلومات من الجهات الحكومية، ومراجعة السجلات والوثائق المعنية. كما تكفل تشريعات بعض الدول لأي فرد إمكانية الحصول على هذه المعلومات بحرية ودون الحاجة لتقديم تبرير أو ذكر الأسباب[3].

خامسا :الحق في السلامة الرقمية

يشير هذا الحق إلى ضرورة البيانات الرقمية سليمة من كل الشوائب، وحقيقة آمنة، ودقيقة ضد أي محاولات تغيير أو تعديل من قبل مستخدمين غير مصرح لهم بذلك، وهذا الحق يعتبر من الحقوق الرقمية الأساسية.

سادسا: الحق في التواصل الرقمي:

يسمح هذا الحق لجميع المستخدمين من التواصل فيما بينهم عبر مواقع التواصل الاجتماعي بمختلف أنواعها، ويجب أن يكون هذا الحق مضمون للجميع للتداول وتبادل

[1] _ نفس المرجع السابق ص26

[2] _المرجع نفسه ص27

[3] _بن حيدة محمد، تكريس الحق في الاطلاع على المعلومات في القانون الجزائري، المركز الجامعي بمحاج بوشعيب عين تموشنت،مجلة القانون والعلوم السياسية، المجلد الخامس، العدد01، 2019، ص 2012

المعلومات والآراء والأفكار بين الأفراد والمجتمعات والشعوب، فلا يمكن انتهاك هذا الحق بما أنه من الحقوق الأساسية الرقمية التي يتمتع بها كل الأفراد على حد سواء. [1]

إن موضوع الأمن السيبراني يعد أحد أبرز المواضيع الحديثة التي أخذت نقاشاً واسعاً في القانون الدولي بسبب سرعة تطورها وارتباطها الوطيد مع مفاهيم السيادة والأمن القومي وحقوق الإنسان، فرغم أهمية هذا المجال في الحياة الاقتصادية والسياسية والعسكرية إلا أنه يعاني من فراغ قانوني واضح داخل المنظومة القانونية الدولية؛ فلا نجد أن هناك معايير دولية ملزمة تحدد القواعد القانونية لاستخدام الفضاء السيبراني، فغياب ضبط سلوك الدول في الفضاء السيبراني جعل من القوى الكبرى تستغل هذا الفراغ لتحقيق أطماعها وتحقيق مصالحها الجيوسياسية.

## المطلب الثالث: طبيعة العلاقة بين الامن السيبراني وحقوق الانسان

تتجلى العلاقة الجدلية بين الامن السيبارني وحقوق الانسان في مسارين متكاملين، الأول يتمثل في سعي المجتمع الدولي لبلورة ميثاق أخلاقي وقانوني ينظم سلوك الدول ويحمي المجتمعات من الهجمات العابرة للحدود .والثاني يظهر في السياسات الدفاعية التي تتبناها الدول في مواجهة التهديدات الميدانية التي تمس سيادتها وأمن أفرادها. وبناءً على ذلك، سنقوم من خلال هذا المطلب بتحليل هذه العلاقة عبر فرعين أساسيين.

نخصص الفرع الأول لاستعراض جهود المجتمع الدولي في تنظيم سلوك الفضاء السيبراني وفق رؤية حقوقية، بينما نتناول في الفرع الثاني واقع التهديدات السيبرانية التي واجهتها الجزائر كنموذج تطبيقي يعكس التحديات والمواجهة المؤسساتية.

### الفرع الأول: جهود المجتمع الدولي لتنظيم السلوك في الفضاء السيبراني

يقوم المجتمع الدولي بمناقشات للوصول إلى معاهدة مستقبلية للأمن السيبراني، فهو لم يصل إلى معاهدة شاملة بعد، فهو يعزز القواعد المتفق عليها مبدئياً مثل: معايير الأمم المتحدة لعامي 2015 و2021، كما أنه دعى الأمين العام للأمم المتحدة إلى معاهدة الجرائم السيبرانية" والتي تعتبر خطوة عملية أولى للوصول إلى الهدف المنشود،

[1] _كامل قرطاس نفس المرجع السابق ص 28

غير أن المجتمع الدولي يرسم معالم الطريق لتنظيم سلوك الدول في الفضاء السيبراني، بحيث يتمحور الحوار الدولي الحالي حول مجموعة من المبادئ والاجراءات التي يحتمل أن تشكل جوهر أي اتفاقية مستقبلية تتمثل في العناصر الثلاث التالية :

1/ حظر استهداف البنية التحتية الحيوية : وهي مبدأ أساسي لحماية المجتمع، يتفق المجتمع الدولي على أن البنية التحتية للدول من شبكات الطاقة والمستشفيات وشبكات المياه والأنظمة المالية يجب أن تكون محمية.[1]

2/ منع الأنشطة الضارة من الأراضي الوطنية: بحيث تلتزم الدول بمنع جهات خبيثة من استخدام أراضيها قاعدة هجمات سيبرانية.[2]

إن حظر استهداف البنية التحتية الحيوية لا ينطلق من اعتبارات تقنية فحسب، بل هو التزام بحماية الحقوق الجوهرية للإنسان، وفي مقدمتها الحق في الحياة والحق في الصحة؛ فتعطيل شبكات الطاقة أو المستشفيات يمثل اعتداءً مباشراً على سلامة الأفراد الجسدية. ومن هذا المنطلق، تصبح مسؤولية الدول في منع الأنشطة السيبرانية الضارة المنطلقة من أراضيها تطبيقاً لمبدأ الأمن الشخصي المكفول دولياً، إذ لا يمكن تصور حماية حقيقية لحقوق الإنسان دون بيئة رقمية آمنة تضمن استمرارية المرافق الحيوية. وبذلك، يتحول الأمن السيبراني من مجرد حماية للأنظمة إلى درع قانوني يصون الكرامة الإنسانية ويحمي الأفراد من الآثار الكارثية للهجمات التي قد تحرمهم من حقوقهم الأساسية في الحصول على المياه، الطاقة، والأمن المالي، مما يجعل السيادة الرقمية وسيلة لخدمة الإنسان وضمان استقراره الاجتماعي.

3/ تعزيز التعاون والمساعدة :خاصة في بناء قدرات الدول النامية، وهذه ضرورة لابد منها للحد ومكافحة التهديدات العابرة للحدود، واحترام القانون الدولي وحقوق الإنسان كالالتزام بتطبيق أي تدابير أمنية مع الحفاظ على الخصوصية وحرية التعبير. تعزيز

[1] _الطيب كامش، القانون الدولي ومعايير الفضاء السيبراني بين الفراغ القانوني والاستغلال الجيوسياسي ، مجلة الدراسات القانونية المقارنة، تاريخ النشر 2025/12/25،ص296.

[2] _ المرجع نفسه ص296.

الشفافية والثقة التي من شأنها أن تتضمن إجراءات كالإبلاغ عن الثغرات الأمنية الكبرى أو تباحث حول الحوادث [1].

يمثل تعزيز التعاون الدولي وبناء قدرات الدول النامية تجسيداً لـ الحق في التنمية والعدالة الرقمية العالمية، حيث يساهم سد الثغرات التقنية في حماية المجتمعات الأكثر هشاشة من الاستغلال السيبراني. ومع ذلك، يجب أن تصاغ التدابير الأمنية والشفافية في الإبلاغ عن الحوادث وفق معادلة دقيقة تضمن عدم المساس بـ الحق في الخصوصية أو حرية التعبير فالأمن السيبراني الحقوقي هو الذي يوفر الحماية دون التحول إلى أداة للرقابة التعسفية.

**الفرع الثاني : التهديدات السيبرانية التي شهدتها الجزائر**

لم يكن سعي الدولة الجزائرية نحو الرقمنة، والذي تبلور بشكل جلي مع إطلاق مشروع الجزائر الإلكترونيةE-Algeria 2013 بمنأى عن التحديات الأمنية المعاصرة. فبقدر ما ساهم هذا التحول في تطوير الأداء الإداري والاقتصادي، فقد أدى في المقابل إلى اتساع مساحة الهجوم السيبراني، مما جعل المؤسسات السيادية والقطاعات الحيوية أهدافاً استراتيجية لهجمات متطورة استدعت استجابة مؤسساتية وقانونية عاجلة[2].

أولاً: رصد المؤشرات والوقائع الميدانية للهجمات السيبرانية شهدت الساحة الوطنية في الآونة الأخيرة تصاعداً ملحوظاً في وتيرة الهجمات السيبرانية، حيث لم تقتصر هذه الهجمات على المحاولات العشوائية، بل امتدت لتطال مؤسسات إعلامية وقانونية سيادية، ففي فبراير 2023، تعرض الموقع الرسمي لـ وكالة الأنباء الجزائرية لهجوم تقني مركز، سبقه في مارس 2022 اختراق للحساب الرسمي لـ وزارة العدل على منصة X (تويتر سابقا).[3]

[1] _كامل قرطاس نفس المرجعالسابق ص 296.

[2] _ بن جدو أمساء، أثر سياسات الامن السيبراني على الامن القومي الأمريكي: قراءة في التجربة وفي إمكانية التطبيق على الحالة الجزائرية، جامعة أحممد بوقرة بومرداس الجزائر، المجلد08، العدد 02، ص 146.

[3] _المرجع نفسه ص146

وتعكس الإحصائيات حجم هذا التحدي، حيث تم تسجيل ما يربو على 30 مليون تهديد سيبراني استهدف الفضاء الرقمي الجزائري في شهر ماي 2023 وحده، مما يشير إلى أن الجزائر أصبحت ضمن دائرة الاستهداف المكثف، وهو ما أكدته تقارير منظمة الشرطة الجنائية الدولية (Interpol) ومنظمة الشرطة الأفريقية (Afripol) الصادرة في مارس 2023، والتي حذرت من تنامي استهداف البنية التحتية الرقمية للقطاعات الاستراتيجية الحيوية في الجزائر والدول الأفريقية عامة[1].

ثانياً: التهديدات السيبرانية في سياق التقارير الدولية والجيوسياسية

بالنظر إلى المؤشرات الدولية، نجد أن تقرير الأمم المتحدة لتطور الحكومة الإلكترونية وضع الجزائر في المرتبة 112عالمياً، وهو مركز يعكس حجم الجهود المبذولة، لكنه يبرز في الوقت ذاته الحاجة لتعزيز المنظومات الدفاعية لمواكبة هذا التطور[2].

ولعل أخطر أشكال هذه التهديدات هو ما يكتسي طابعاً تجسسياً جيوسياسياً، كما حدث في عام 2021مع الكشف عن استخدام برنامج التجسس المتطور بيغاسوس (Pegasus) في عمليات اختراق استهدفت قطاعات حساسة في الدولة الجزائرية ودول أخرى، مما نقل التهديد السيبراني من مجرد جريمة معلوماتية إلى تهديد مباشر للسيادة الوطنية والأمن القومي.

ثالثاً: الاستجابة المؤسساتية والتشريعية لتحقيق الأمن السيبراني

أدت هذه الوقائع المتسارعة إلى إحداث نقلة نوعية في الفكر الدفاعي الجزائري؛ حيث تبنى المشرع سياسات قانونية ومؤسساتية رادعة، تجسدت في إنشاء نظام مؤسساتي ذو طابع أمني استراتيجي تحت إشراف وزارة الدفاع الوطني .ويهدف هذا التوجه ليس فقط إلى حماية المنشآت الحيوية للدولة، بل أيضاً إلى كفالة الأمن السيبراني للأفراد، من

[1] _ نفس المرجع السابق ص146
[2] _ المرجع نفسه ص 147

خلال حماية بياناتهم وحقوقهم وحرياتهم الأساسية المرتبطة بالفضاء الرقمي، ضماناً لتوازن دقيق بين المتطلبات الأمنية والضمانات الحقوقية في ظل دولة القانون.[1]

[1] _نفس المرجع السابق ، ص 147

**ملخص الفصل الأول :**

يخلص هذا الفصل إلى أن الأمن السيبراني قد تجاوز بُعده التقني البحت ليصبح ضرورة استراتيجية وقانونية حتمية في ظل التحول الرقمي المتسارع، وذلك لمواجهة التهديدات غير التقليدية والعابرة للحدود التي تستهدف القطاعات الحيوية والأمن القومي. وتبرز في هذا السياق أهمية إيجاد موازنة دقيقة بين متطلبات الدفاع عن البنية التحتية وحمايتها من الاختراقات من جهة، وضمان احترام حقوق الإنسان في الفضاء الرقمي، كالحق في الخصوصية وحرية التعبير، من جهة أخرى. وأمام هذه التحديات الأمنية والجيوسياسية المتصاعدة، تظهر الحاجة الملحة لتبني مقاربة شاملة تبني منظومة دفاعية ومؤسساتية متكاملة، على غرار الجهود المبذولة لتحصين البيئة الرقمية الوطنية، بما يضمن استمرارية واستقرار المؤسسات، ويحمي الحقوق والحريات الأساسية للأفراد في إطار سيادة القانون.

# الفصل الثاني : أثر تدابير الأمن السيبراني على حقوق الإنسان

## تمهيد :

قد أحدث الانتقال إلى العالم الرقمي تغييراً كبيراً في مجرى الحقوق والحريات؛ فمثلما فتحت التكنولوجيا أبواباً واسعة للتعبير والتواصل، خلقت أيضاً مخاطر أمنية معقدة تهدد استقرار الدول وخصوصية الأفراد. بناءً على ذلك، لم يعد الأمن السيبراني مجرد إجراء تقني عادي، بل أصبح ضرورة قصوى لحماية المعلومات والأنظمة. ومع ذلك، فإن هذه الإجراءات الأمنية قد تؤثر أحياناً على حقوق الإنسان، مما يطرح تحدياً حقيقياً في كيفية الموازنة بين فرض الأمن وضمان الحريات الأساسية.

وفي هذا الفصل، سنقوم بتسليط الضوء على هذه العلاقة من خلال مبحثين:

- **المبحث الأول** :وسنخصصه لرصد مظاهر التعدي على حقوق الإنسان باسم الأمن السيبراني، مع التركيز على قضايا المراقبة الرقمية، وانتهاك الحق في الخصوصية، بالإضافة إلى القيود التي قد تفرض على حرية التعبير والوصول إلى المعلومات.
- **المبحث الثاني** :وسننتقل فيه إلى دراسة الحالة في الجزائر، للبحث في كيفية تحقيق التوازن بين متطلبات الأمن الرقمي وحماية حقوق الإنسان، وذلك من خلال استعراض الضمانات الدستورية والقانونية، ودور القضاء والهيئات المختلفة في حماية هذه الحقوق من أي تجاوزات.

## المبحث الأول : مظاهر المساس بحقوق الإنسان باسم الأمن السيبراني

تم تقسيم هذا المبحث إلى ثلاثة مطالب رئيسية حيث يدرس المطلب الأول الرقابة الإلكترونية والحق في الخصوصية وينقسم الى فرعين، ويليه المطلب الثانيندرس فيه تقييد حرية التعبير والوصول للمعلومات من خلال فرعين وأخيراً، يُحلل المطلب الثالث الانتهاكات التقنية المتقدمة للحياة الخاصة التكييف القانوني لتقنية تنقيب البيانات، وينقسم الى فرعين.

## المطلب الأول : الرقابة الالكترونية وحق في الخصوصية

في هذا المطلب سنتطرق لدراسة ماهية الرقابة وضوابطها التقنية والقانونية في التشريع الجزائري، مع بيان شروط الاعتراض القانونيوالإذن القضائي المسبق لحماية خصوصية الأفراد من التجسس التعسفي( الفرع الأول)، وتبيان واقع الرقابة الالكترونية والخصوصية (الفرع الثاني).

### الفرع الاول : مفهوم الرقابة الالكترونية

لقد أفرز التحول الجذري نحو الاعتماد على البيئات التقنية المتقدمة في تفاصيل الحياة اليومية بروز مفهوم حقوق الإنسان الرقمية كاستمرار حتمي وطبيعي للحقوق التقليدية . هذا المفهوم يستهدف بالأساس حماية الفرد في الفضاء الافتراضي، لاسيما أولئك الذين تخضع بياناتهم للتتبع والتحليل المستمر، أو ما يُعرف بالأشخاص الممسوحين رقمياً، مما يفرض ضرورة ملحة لتأمين معطياتهم ضد الانتهاكات المستحدثة. وفي هذا السياق، لم تعد الابتكارات التكنولوجية مجرد أداة لتعزيز حرية التعبير والوصول إلى المعلومات، بل أضحت سلاحاً ذا حدين يفرض تحديات ومخاطر جمة كالمراقبة الرقمية، التحرش الإلكتروني، والتحيز الخوارزمي.[1]

تعتبر الرقابة مفهومًا واسعًا يتغير معناه حسب المجال الذي يُستخدم فيه سوآءا كان إداري، قانوني، أو تقني. وبشكل عام، يمكن القول انها عملية متابعة الأنشطة للتأكد من أنها تسير وفقًا للخطط الموضوعة والقوانين المحددة، بهدف تصحيح الانحرافات.
لقد حدد المرسوم الرئاسي رقم 15-261 (المتعلق بالهيئة الوطنية للوقاية من الجرائم الإلكترونية) مفهوم الرقابة من خلال المهام التقنية والقانونية الموكلة للهيئة في المادة 5 منه، وذلك بالتكامل مع القانون رقم 09-04 الذي يحدد القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها .

يمكن تعريف الرقابة الإلكترونية من منظور هذا المرسوم على أنها عملية تقنية وقانونية تهدف إلى مراقبة حركة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في الوقت

[1] _مصطفى علي العقبي، حماية حقوق الإنسان الرقمية في عصر الذكاء االصطناعي: دراسة أمنية قانونية مقارنة، محاضر في أكاديمية الشرطة، مجلة الدراسات القانونية واالقتصادية – دورية علمية محكمة – المؤتمر الدولي الثاني بعنوان، القاهرة 2026 ، ص 733.

الحقيقي، بهدف الوقاية من الجرائم الإلكترونية أو التحري عنها، شريطة أن تتم تحت إشراف قضائي. [1]

وتجدر الإشارة إلى أن هذه الرقابة لا تُجرى لمجرد التجسس التعسفي، بل إن المرسوم الرئاسي حدد مهام الهيئة في إطار الوقاية من الجرائم الخطيرة، لاسيما تلك الموصوفة بأفعال إرهابية أو تخريبية، أو الجرائم التي تمس بأمن الدولة . [2]

وتمتد هذه الرقابة لتشمل تجميع وتسجيل المعطيات؛،من خلال إتاحة الوصول إلى محتوى المراسلات الإلكترونية وتخزينها لاستخدامها كدليل جنائي، وهو الإجراء الذي يُعرف بـ الاعتراض القانوني للاتصالات. ولضمان حماية الحريات الفردية، قيد المشرع الجزائري هذا الإجراء بشرط قضائي صارم، حيث لا تتم هذه المراقبة بصفة عشوائية، بل تستلزم استصدار إذن مكتوب ومسبق من السلطة القضائية المختصة (وكيل الجمهورية أو قاضي التحقيق)[3]

يقصد بالمراقبة في مجال المعلوماتية بالمراقبة الإلكترونية مراقبة شبكة الاتصالات، أو ذلك العمل الذي يقوم به المُرَاقِب باستخدام التقنية الالكترونية لجمع البيانات والمعلومات حول المشتبه فيه، سواء كان شخصاً أو مكاناً أو شيئاً حسب طبيعته، وذلك مرتبط بالزمن لتحقيق غرض أمني ولأي غرض آخر.[4]

"وكمثال عن الأساليب الحكومية المنتهجة في مجال اللجوء السري للمراقبة الإلكترونية، ما قامت به الصين سنة 2006 حينما صرح الوزير المكلف بالأمن العام لديها عن إطلاق مشروع تحت اسم الدرع الذهبي من خلال تفعيل نظام شامل للمراقبة الإلكترونية، أو ما حدث سنة 2009 أين حاولت الحكومة الصينية فرض تثبيت برنامج تجسس يعرف بالسد الأخضرعلى كل الحواسيب التي تسوق داخل الصين وهو ما يمكنها من بسط سيطرتها

[1] _ المرسوم الرئاسي رقم 15-261، مؤرخ في 24 ذي الحجة عام 1436 الموافق 8 أكتوبر سنة 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 53، الصادرة بتاريخ 11 أكتوبر 2015، المادة 5، الفقرة 4

[2] _ المادة 05 المرجع نفسه

[3] _ القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، المادتان 04 و 05.

[4] _ ربيعي حسين : المراقبة الإلكترونية وحق الفرد في الخصوصية، المجلة الاكاديمية للبحث القانوني، كلية الحقوق جامعة قسنطينة 1 الجزائر، المجلد 13، العدد1، 2016، ص 417.

على كل أنشطة مستخدمي النظام المعلوماتي في الصين غير أنّ هذا الطلب قوبل بالرفض من قبل منظمة التجارة العالمي" [1]

**الفرع الثاني : واقع الرقابة الإلكترونية والحق في الخصوصية**

تم إقرار مشروعية مراقبة الاتصالات الإلكترونية كإجراء استثنائي لمواجهة الإجرام المستحدث، تجسيدا لمضمون الاتفاقيات الدولية التي نادت بضرورة استخدام مثل هذا الإجراء في ظل التطورات التي يشهدها الإجرام المنظم، وعملا بمبدأ سمو المعاهدات الدولية على القوانين الداخلية بادرت الجزائر على تكريس هذا الإجراء صراحة بموجب القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وذلك وفقا لنص كل من المادتين 03 و04 اللتان عبرتا صراحة عن إجازة اللجوء لإجراء المراقبة الإلكترونية في مواجهة الجرائم المعلوماتية[2].

و انطلاقاً من القاعدة القانونية التي تضفي حماية قوية على سرية الاتصالات والمحادثات باعتبارها جزءاً لا يتجزأ من حرمة الحياة الخاصة، فقد قيد المشرع صلاحية المساس بهذه السرية عبر المراقبة الإلكترونية في أضيق الحدود. وطبقاً للفقرة (ج) من المادة الرابعة من القانون، لا يُجاز تفعيل هذا الإجراء الاستثنائي إلا استجابةً لضرورات التحقيق والتحري القضائي، وذلك حصراً في الحالات التي يثبت فيها تعذر أو صعوبة تحصيل الأدلة والنتائج الضرورية لمسار الدعوى الجارية بالوسائل التقليدية .[3]

وتحدد دواعي استخدام تقنيات المراقبة الإلكترونية في التشريع وفق الأطر والضوابط التالية:

- التصدي للجرائم النوعية والأمن القومي :تفعيل المراقبة كإجراء وقائي واستباقي لمواجهة الأفعال المصنفة كجرائم إرهابية أو تخريبية، وكذا كافة الجرائم التي تمس بأمن الدولة واستقرارها.

[1] _ المرجع نفسه ص 419 .

[2] _ مرزوقي كريمة، م| مراقبة الاتصالات الالكترونية وحق الفرد في الخصوصية المعلوماتية ،جلة الأستاذ الباحث للدراسات القانونية والسياسية – المجلد 05 – العدد 02 – السنة 2020 | 1369 ص 1358 – ص 1382

[3] _المادة 04 الفقرة (ج)، القانون رقم 09-04 المؤرخ في 05 أوت 2009، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، الصادر بتاريخ 16 أوت 2009..

- حماية السلامة المعلوماتية والمصالح الحيوية :التدخل عند توفر معطيات حول تهديدات محتملة تستهدف الأنظمة المعلوماتية، لاسيما تلك التي قد ينجم عنها خطر يمس بالنظام العام، الدفاع الوطني، مؤسسات الدولة، أو المقومات الأساسية للاقتصاد الوطني.
- الضرورة الإجرائية في التحقيقات القضائية :اعتماد المراقبة الإلكترونية كأداة لا غنى عنها في التحريات والتحقيقات القضائية، وذلك في الحالات التي يثبت فيها تعذر الوصول إلى نتائج جوهرية تخدم البحث الجاري عبر الوسائل التقليدية.
- تفعيل آليات التعاون الدولي :استخدام هذا الإجراء في إطار الالتزامات الدولية المتعلقة بتنفيذ طلبات المساعدة القضائية المتبادلة بين الدول لمكافحة الإجرام[1].

**المطلب الثاني : تقييد حرية التعبير والوصول الى المعلومات**

سوف ندرس في هذا المطلب حدود التوازن الدستوري والدولي بين كفالة حريتي التعبير والمعرفة كأصل عام، وبين تقييدهما استثنائياً لضرورات الأمن القومي، حماية النظام العام، واحترام حقوق الآخرين من خلال فرعين .

**الفرع الاول: تقييد حرية التعبير**

لا يوجد تعريف محدّد للحقّ نفسه، بل هناك العديد من الأشكال المعترف بها والمتفق عليها لممارسة هذه الحقوق. على أيّ حال، يمكن الإشارة إلى المادة 19 من الإعلان العالميّ لحقوق الإنسان أنَّ "لكلّ فرد الحقّ في حريّة الرأي والتعبير. ويشمل هذا الحقّ حريّة تبنّي الآراء دون تدخّل، والبحث عن المعلومات والأفكار وتلقّيها ونقلها عبر أيّ وسائط وبغض النظر عن الحدود، كما تُحدِّد هذه المادة خطوطاً عريضة وأساسية لحقّ التعبير دون توضيح أو ذِكر التفاصيل، بل تتركُ ذلك للقوانين الوطنيّة والنظُم القانونيّة المحليّة[2] .

بما أن هذه المادة قد رسمت التوجهات العامة تاركةً التفاصيل الإجرائية للتشريعات الوطنية، فقد سارعت الجزائر إلى مواءمة منظومتها مع هذه المبادئ الكونية حيث تضرب جذور

[1] المادة 04 نفس المرجع السابق .

[2] _عمرو الذيب، حريّة التعبير" في عصرنا الرقمي،/https://www.safespace.qa/topic ، اطلع عليه 2026/04/29

الالتزام الجزائري بحماية حقوق الإنسان في عمق التاريخ التشريعي للدولة، وهو ما يظهر من خلال :

أولا – التكريس الدستوري للمواثيق الدولية : بادرت الدولة الجزائرية فور استقلالها إلى تبني المبادئ الكونية لحقوق الإنسان، حيث تمت المصادقة على الإعلان العالمي لحقوق الإنسان لعام 1948 بموجب المادة 11 من دستور عام 1963[1].

– الحماية الجوهرية لحرية الرأي :تتماشى المنظومة القانونية مع المادة 19 من الإعلان العالمي، التي تقر بحق كل فرد الأصيل في التمتع بحرية الرأي والتعبير[2].

ثلنيا – الأبعاد الشمولية لحرية التعبير :لا يقتصر هذا الحق على الجانب الشفهي فحسب، بل يمتد ليشمل الأبعاد التالية:

- حرية الاعتقاد الفكري :كفالة حق الفرد في اعتناق الآراء التي يراها مناسبة دون تعرضه لأي نوع من أنواع المضايقة.
- الحق في البحث عن الأنباء والأفكار، وتلقيها، وإعادة نشرها ونقلها تدفق المعلومات للآخرين.
- ممارسة هذا الحق عبر أي وسيلة اتصال متاحة، مع تجاوز الاعتبارات المتعلقة بالحدود الجغرافية.

على الرغم من إقرار المواثيق القانونية بالحرية المطلقة للفرد في التعبير عن أفكاره ونقل الأنباء والآراء دون قيود مسبقة، إلا أن ممارسة هذا الحق قد تتقاطع مع مصالح عليا تتعلق بسيادة الدول وأمنها القومي. ولضبط هذا التوازن، تضمن العهد الدولي الخاص بالحقوق المدنية والسياسية لسنة 1966 الذي انضمت إليه الجزائر في عام 1989 أحكاماً تقييدية صريحة.

ووفقاً للمادة 19 (الفقرة 3) من العهد المذكور، يجوز إخضاع حرية التعبير لبعض القيود، شريطة أن تكون محددة بنص القانون وأن تكون ضرورية لتحقيق الغايات التالية:

- صون الحقوق المعنوية :لضمان احترام حقوق الآخرين وحماية سمعتهم من أي تجاوز.

[1] _ دستور الجزائر لسنة 1963، المؤرخ في 10 سبتمبر 1963، الجريدة الرسمية للجمهورية الجزائرية، العدد 64، سنة 1963.

[2] _ حري التعبير، https://www.frontlinedefenders.org/ar/right/freedom-expression، اطلع علسه 2026/04/05

- حماية المصالح العامة الكبرى :وتشمل مقتضيات الأمن القومي، الحفاظ على النظام العام، وحماية الصحة العامة أو الآداب العامة[1].

إنَّ تكريس المعاهدات الدولية للحريات العامة لا يعني إطلاقها دون ضوابط بل غالباً ما تتبعها نصوص تقر استثناءات وقيوداً تهدف إلى حماية حقوق الآخرين والحد من تعسف الأفراد في ممارسة حقوقهم. وتنعكس هذه القيود الواردة في المواثيق الدولية بشكل مباشر في التشريعات الوطنية للدول.إذ يجب أن يكون أي تقييد لحرية التعبير أمراً لا غنى عنه ولا مفر منه لصون حقوق الآخرين وحماية أمن الدولة. فالضرورة تقتضي عدم المساس بهذا الحق لأسباب واهية أو بسيطة قد تهدد جوهر الحماية القانونية للحرية.

وفي هذا الصدد، ربطت الاتفاقية الأوروبية تقدير "الضرورة" بمعايير المجتمع الديمقراطي، حيث يتسع مفهوم الضرورة ليشمل حماية الأفكار والمعلومات حتى تلك التي قد "تزعج" السلطة العامة أو تقلقها، وليس فقط المعلومات التي ترضى عنها السلطة .[2]

**الفرع الثاني: تقييد الوصول الى المعلومات**

يعد الحق في الوصول إلى المعلومات أحد الحقوق الجوهرية التي تضمنتها المواثيق والمعاهدات الدولية، حيث يُنظر إليه كاستحقاق أصيل لا ينفصل عن حرية الرأي والتعبير. إنَّ جوهر هذا الحق يكمن في تمكين الأفراد من البحث عن المعلومات وتلقيها ونقلها دون قيود تعسفية، وهو ما تضمنه الإعلانات والعهود الدولية لحقوق الإنسان.وتتجلى الأهمية الجوهرية لهذا الحق في كونه المحرك الأساسي لكافة القطاعات الحيوية التي تمس حياة الأفراد اليومية، ومن أبرزها:

- القطاعات الخدمية : مثل الصحة، التعليم، والمنح، بالإضافة إلى الخدمات الأساسية كالماء والكهرباء والاتصالات.
- الإدارة المالية والحقوقية :وتشمل الموازنة العامة، النفقات والضرائب، معاملات الأراضي، والمنظومة القضائية.

[1] _مرزوقي كريمة، "مراقبة الاتصالات الالكترونية وحق الفرد في الخصوصية المعلوماتية"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 05، العدد 02، جامعة المسيلة، 2020، ص 1369.

[2] Morsli Abdelhak, "La Restriction de la Liberté d'Expression En Droit International des Droits de l'Homme", Revue des études juridiques et politiques, Université Amar Telidji - Laghouat, Vol. 05, N° 02, juin 2019, p299/298

- الفضاء الإعلامي :حيث يعتمد العمل الصحفي وحرية الإعلام بشكل كلي على سيولة تدفق المعلومات وتوافرها من مصادرها الرسمية[1].

تنص المادة 55 من الدستور الجزائري لعام 2020 (المعدل بموجب المرسوم الرئاسي رقم 20-442) على ما يلي:«يتمتع كل مواطن بالحق في الوصول إلى المعلومات والوثائق والإحصائيات، والحصول عليها وتداولها. لا يمكن أن تمس ممارسة هذا الحق بالحياة الخاصة للغير وبحقوقهم، وبالمصالح المشروعة للمؤسسات، وبمقتضيات الأمن الوطني.يحدد القانون كيفيات ممارسة هذا الحق»[2] .

يمكننا أن نستنتج من نص المادة 55 من الدستور الجزائري لعام 2020 أن المشرع قد أرسى دعائم الحق في الوصول إلى المعلومات كأصل عام مكفول لكل مواطن، بما يشمل الوثائق والإحصائيات وحرية تداولها لتعزيز مبادئ الشفافية والمساءلة. غير أن هذا الاستنتاج يقودنا بالضرورة إلى إدراك فلسفة التوازن التي تبناها المؤسس الدستوري حيث لم يترك هذا الحق مطلقاً، بل أحاطه بسياج من القيود الجوهرية التي تتقاطع بشكل مباشر مع مقتضيات الأمن السيبراني والوطني، وذلك من خلال حظر المساس بالحياة الخاصة للغير أو المصالح المشروعة للمؤسسات. وبناءً عليه، فإن هذه المادة ترسم حدود العلاقة بين الفرد والدولة في الفضاء المعلوماتي؛ فبينما تمنح الفرد سلطة الوصول، تفرض على الدولة واجب الحماية للأمن القومي والخصوصية، مما يجعل من التشريعات المنظمة لهذا الحق الأداة الإجرائية الفعلية لتحقيق هذا التوازن الدقيق بين الانفتاح المعلوماتي والضرورات الأمنية

**المطلب الثالث : تنقيب البيانات كأحد مظاهر المساس بالحياة الخاصة.**

شكل تنقيب البيانات ركيزة أساسية لاستخراج الأنماط والرؤى القيمة، وهو ما دفع المشرع الجزائري لإخضاعه لأحكام القانون رقم 18-07 لحماية المعطيات الشخصية .بناءً على ذلك، يرتكز هذا المطلب على محورين.

يدرس الأول تكييف التنقيب كعملية معالجة قانونية، بينما يستعرض الثاني ضوابطه الأخلاقية وحدوده التشريعية.

[1] _قانون الحق في الحصول على المعلومات وحماية الحق من الانتهاك، https://aman-monitor.org/ ،اطلع عليه يوم 2026/05/01

[2] _ المادة 55، الدستور الجزائري لعام 2020، المعدل بموجب المرسوم الرئاسي رقم 20-442 المؤرخ في 15 جمادى الأولى عام 1442 هـ الموافق لـ 30 ديسمبر سنة 2020، المتضمن إصدار الدستور في الجريدة الرسمية للجمهورية الجزائرية، العدد 82، الصادر بتاريخ 30 ديسمبر 2020.

" يشير معنى تنقيب البيانات إلى عملية استخراج الأنماط أو الأفكار المفيدة من كميات كبيرة من البيانات. ويتضمن استخدام تقنيات وخوارزميات مختلفة لاكتشاف الأنماط والاتجاهات المخفية داخل البيانات. بهدف استخراج معلومات قيمة يمكن استخدامها لاتخاذ القرار، حيث يساعد المؤسسات على الكشف عن رؤى قيمة، وتحسين عمليات صنع القرار، وتحديد أنماط سلوك العملاء، واكتشاف الأنشطة" [1]

ولفهم كيفية ضبط المشرع الجزائري لهذه التقنية، يجب إخضاعها لميزان القانون رقم 18- 07 [2] المتعلق بحماية الأشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي، وذلك من خلال مستويين:

**أولا-** تكييف التنقيب كعملية معالجة قانونية ( المادة 03) :

تنص المادة من القانون سالف الذكر **03** على يأتي:

- كل معلومة بغض النظر عن دعامتها متعلقة بشخص معرف أو قابل للتعرف عليه والمشار إليه أدناه،الشخص المعني بصفة مباشرة أو غير مباشرة لاسيما بالرجوع إلى رقم التعريف أو عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية.
- كل شخص طبيعي تكون المعطيات ذات الطابع الشخصي المتعلقة به موضع معالجة.
- معالجة المعطيات ذات الطابع الشخصي المشار إليها أدناه معالجة :كل عملية أو مجموعة عمليات منجزة بطرق أو بوسائل آلية أو بدونها على معطيات ذات طابع شخصي، مثل الجمع أو التسجيل أو التنظيم أو الحفظ أو الملاءمة أو التغيير أو الاستخراج أو الاطلاع أو الاستعمال أو الإيصال عن طريق الإرسال أو النشر أو أي شكل آخر من أشكال الإتاحة أو التقريب أو الربط البيني وكذا الإغلاق أو التشفير أو المسح أو الإتلاف.

[1] _تنقيب البيانات :Data Mining المراحل والأدوات والخوارزميات والكتب https://bakkah.com/ar/knowledge-cente اطلع عليه 2026/05/03

[2] لقانون رقم 18-07 المؤرخ في 10 جوان 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي

- موافقة الشخص المعني :كل تعبير عن الإرادة المميزة يقبل بموجبه الشخص المعني أو ممثله الشرعي معالجة المعطيات الشخصية المتعلقة به بطريقة يدوية أو إلكترونية[1].

**ثانيا** – الضوابط الأخلاقية والحدود القانونية : (المادة 02)

تنص المادة 02 على ما يلي: « يجب أن تتم معالجة المعطيات ذات الطابع الشخصي، مهما كان مصدرها أو شكلها، في إطار احترام الكرامة الإنسانية والحياة الخاصة والحريات العامة وألا تمس بحقوق الأشخاص وشرفهم وسمعتهم».[2]

ومن خلال استقراء نص المادة 03 من القانون رقم 18–07 المتعلق بحماية الأشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي، نجد أن المشرع الجزائري قد تبنى مفهوماً واسعاً لعملية 'المعالجة' يشمل الجمع والتنظيم والاستخراج. وبالتطبيق على تقنيات الأمن السيبراني الحديثة، فإن عملية التنقيب في البيانات تندرج ضمن هذا المفهوم القانوني، كونها تعتمد على استخراج الأنماط السلوكية من المعطيات الضخمة. وهذا ما يفرض على الجهات القائمة على الأمن السيبراني ضرورة الالتزام بالحدود التي رسمتها المادة 02 من ذات القانون، والتي توجب أن تتم المعالجة في إطار احترام الكرامة الإنسانية والحياة الخاصة، وعدم المساس بشرف الأشخاص وسمعتهم.

لم يغفل المشرع الجزائري عن مخاطر التنقيب الآلي في البيانات الحساسة؛ حيث أخضعت المادة 05 من القانون 18–07 كافة المعالجات الآلية للمعطيات الصحية لرقابة قانونية صارمة، لاسيما تلك التي تهدف إلى التقييم والتحليل. ويأتي هذا التوجه لحماية الأفراد من مخاطر 'التنميط الصحي' الذي قد ينتج عن تقنيات الأمن السيبراني عند فحص قواعد البيانات الضخمة، وضمان عدم خروج هذه المعالجات عن إطار البحث والوقاية[3]

[1] _القانون رقم 18–07 المؤرخ في 10 جوان 2018، المتعلق بحماية الأشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية، العدد 34، الصادر بتاريخ 13 جوان 2018، المادة 03.

[2] _المادة 02 من القانون رقم 18-07، المتعلق بحماية الأشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي، مرجع سابق.

[3] _لقانون رقم 18-07، المتعلق بحماية الأشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي، مرجع سابق، المادة 05

## المبحث الثاني : اليات التوازن بين الامن السيبراني وحقوق الانسان في الجزائر

سنقوم في هذا المبحث بتسليط الضوء على ثلاثة مستويات أساسية؛ حيث نخصص المطلب الأول لدراسة الضمانات الدستورية والقانونية، بدءاً من دستور 2020 وصولاً إلى التطورات التشريعية الأخيرة في حماية البيانات الشخصية لعام 2025، لنتناول بعد ذلك في المطلب الثاني دور القضاء كحارس للحريات، ومنهجية رقابته على إجراءات المراقبة والتحري الرقمي، قبل أن نعرج في المطلب الثالث على المقاربات الدولية والوطنية، من خلال تحليل النماذج العالمية (الأمريكية، الأوروبية، والصينية) وموقع النموذج الجزائري "قيد التشكل" ضمن هذه المقاربات الدولية.

## المطلب الاول : الضمانات الدستورية والقانونية

في هذا المطلب سنتطرق إلى التطور الدستوري والتشريعي للضمانات الحمائية في الجزائر، بدءاً من المرجعيات التأسيسية لدستوري 1989 و2020 كصمام أمان للفضاء الرقمي، وصولاً إلى الأطر القانونية الضابطة للمراقبة الإلكترونية والتحيينات الصارمة لحماية البيانات الشخصية لعام 2025.

شكل الدستور الجزائري (لا سيما التعديل الدستوري لعام 2020) صمام الأمان الأول لحماية الحقوق في الفضاء الرقمي. فقد كرس الدستور صراحة حرمة الحياة الخاصة للمواطنين وسرية المراسلات والاتصالات بكافة أشكالها (بما فيها الإلكترونية). وتأسيساً على ذلك، يُمنع أي تقييد أو مساس بهذه الحريات تحت ذريعة الأمن القومي أو السيبراني إلا بموجب نص قانوني واضح، وبناءً على أمر قضائي مسبق، مما يضمن عدم تعسف السلطات التنفيذية والأمنية في الفضاء الرقمي. [1]

في ظل دستور 1989 نصت المادة 60 منه على: «يمارس كل واحد جميع حريات في إطار احترام الحق في الشرف وستر الحياة الخاصة وحماية الأسرة والشبيبة والطفولة[2].» تعد المادة 60 من دستور 1989 مرجعية دستورية أصيلة في رسم معالم الموازنة بين مقتضيات الأمن الرقمي وصون حقوق الإنسان في التشريع الجزائري، حيث تبنى المؤسس الدستوري من خلالها فلسفة الحرية المسؤولة، بجعل ممارسة الحريات الفردية محكومة بضوابط حماية الحق في الشرف وستر الحياة الخاصة. ومن منظور الأمن السيبراني، يمكن استقراء هذا النص كدعامة شرعية تمنح الدولة سلطة التدخل التقني والقانوني لحماية الفضاء المعلوماتي من الهجمات التي تنتهك حرمة الأفراد، مما يجعل من إجراءات الأمن السيبراني وسيلة لحماية الغايات الدستورية المتمثلة في صون الخصوصية وحماية الفئات الهشة كالشبيبة والطفولة. وبناءً عليه، فإن التوازن المنشود لا يتجسد في تقييد الحرية لصالح الأمن، بل في تفعيل الأمن السيبراني كدرع يحمي الإطار القانوني الذي تُمارس فيه تلك

[1] _ دستور 2020، الجريدة الرسمية، العدد82، الصادرة بتاريخ 30ديسمبر 2020، المادة 46

[2] _ دستور 1989 الصادر بموجب المرسوم رقم 89-18 المؤرخ في 28 فيفري 1989 الجريدة الرسمية العدد 09 ،المؤرخة في 1 مارس 1989

الحريات، مع وجوب تقييد هذا التدخل الأمني بضرورة عدم المساس بجوهر الحقوق التي كفلها الدستور.[1]

تُعدّ الضمانات التشريعية من أهم الآليات التي اعتمدها المشرّع الجزائري لتحقيق التوازن بين متطلبات الأمن السيبراني وحماية حقوق الإنسان، خاصة الحق في الخصوصية وسرية المعطيات. وفي هذا الإطار، تنص المادة 9 على أنه" :تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، لا يجوز استعمال المعلومات المتحصل عليها عن طريق المراقبة للنصوص عليها في هذا القانون، إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية.[2]

ويُفهم من هذا النص أن المشرّع قيّد استعمال المعطيات الناتجة عن آليات المراقبة الإلكترونية بضوابط صارمة، بحيث لا يُسمح باستخدامها إلا في نطاق ضيق ومحدد يخدم أغراض التحري والتحقيق القضائي. وهو ما يعكس حرصه على منع أي تعسف أو انحراف في استعمال هذه الوسائل، وضمان عدم المساس التعسفي بحقوق الأفراد.

وبالتالي، تمثل هذه المادة تجسيدًا واضحًا لمبدأ التناسب، حيث توازن بين ضرورة حماية الأمن السيبراني ومكافحة الجرائم المعلوماتية، وبين صون الحريات الأساسية، مما يعزز الإطار القانوني لحماية حقوق الإنسان في البيئة الرقمية بالجزائر.

وقد شكل القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي (المؤرخ في 10 جوان 2018)، الإطار التشريعي الأساسي لتنظيم حماية البيانات في الجزائر، إذ سعى المشرع من خلاله إلى تكريس الحق في الخصوصية وضبط عمليات جمع ومعالجة المعطيات الشخصية، لاسيما في ظل تنامي استخدام الوسائط الرقمية وتزايد مخاطر الاستغلال غير المشروع للبيانات. غير أن التطورات المتسارعة في مجال الأمن السيبراني، وظهور أنماط جديدة من التهديدات الرقمية، إلى جانب التوسع الكبير في المعالجة الآلية للمعطيات، كشفت عن بعض النقائص العملية في أحكام هذا القانون، سواء من حيث فعالية آليات الرقابة أو من حيث ملاءمته لمتطلبات

[1] المادة 60، دستور 1989 المرجع نفسه.

[2] _ المادة 9، القانون رقم 09-04 المؤرخ في 5 أوت 2009، يحدد القواعد الخاصة للوقاية من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، الصادرة في 23 أوت 2009.

الحماية الرقمية الحديثة، الأمر الذي استدعى تدخل المشرع لإعادة النظر في بعض أحكامه وتحيينها بما ينسجم مع المستجدات التقنية والأمنية[1].

استجابةً للتحديات الرقمية المتسارعة، جاء القانون رقم 25-11 المؤرخ في 24 جويلية 2025 ليُحيّن الإطار القانوني الذي وضعه القانون 18-07 .وقد استهدف المشرع من خلاله توفير حماية أكثر فاعلية للأفراد أمام المخاطر السيبرانية، عبر فرض ضوابط أكثر صرامة على عمليات معالجة البيانات، ومنح السلطة الوطنية لحماية المعطيات آليات قانونية أوسع تتيح لها ممارسة رقابة نافذة وفرض جزاءات رادعة على المخالفين.[2]

**المطلب الثاني : دور القضاء في حماية الحقوق والحريات**

في هذا المطلب سنتطرق إلى الدور المحوري للقضاء الجزائري كحارس للحريات الرقمية من خلال تفعيل رقابته المسبقة واللاحقة على إجراءات المراقبة والتحري الإلكتروني، مستندين إلى أحكام القانون رقم 09-04 لبيان شروط الإذن القضائي وضوابط التناسب والضرورة التي تمنع تعسف سلطات الضبط.

يعدّ القضاء أحد أهم الضمانات الأساسية لحماية الحقوق والحريات في مواجهة توسّع سلطات الضبط والمراقبة في مجال الأمن السيبراني، حيث يضطلع بدور محوري في تكريس مبدأ سيادة القانون وضمان عدم التعسف في استعمال الوسائل التقنية الحديثة.
ويتجلى دور القضاء بشكل أوضح من خلال النصوص القانونية التي تحدد الحالات التي يُسمح فيها باللجوء إلى المراقبة الإلكترونية، حيث نصت المادة 4 قانون رقم 09- 04 مؤرّخ في 14 شعبان عام 143على جملة من الحالات، من بينها الوقاية من جرائم الإرهاب والتخريب، وحماية أمن الدولة، أو عند وجود تهديد لمنظومة معلوماتية تمس بالنظام العام أو الاقتصاد الوطني، إضافة إلى مقتضيات التحريات والتحقيقات القضائية، وكذا في إطار التعاون القضائي الدولي[3].

[1] _عروس كوثر، عروس فوزية، إشكالية املوازنة بني متطلبات الأمن السيرباني وضمان الحقوق الفردية، الاكاديمية للدراسات الاجتماعية والإنسانية، المجلد 18، العدد 1، 2026، ص 246 .

[2] _قانون رقم 25-11 المؤرخ في 24 جويلية 2025،

[3] _لمادة 04 من القانون رقم 09-04، المؤرخ في 14 شعبان عام 1430 الموافق لـ 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، الصادرة بتاريخ 25 شعبان عام 1430 الموافق لـ 16 أوت 2009.

غير أن المشرّع، ورغم إقراره بهذه الحالات، لم يترك السلطة مطلقة في مباشرتها، بل قيّدها بضمانة أساسية تتمثل في ضرورة الحصول على إذن قضائي مكتوب من الجهة المختصة، وهو ما يعكس الدور المحوري للقضاء في مراقبة مشروعية هذه الإجراءات. كما منح بعض الصلاحيات المحددة للنائب العام في حالات معينة، مع تقييدها بمدة زمنية وإخضاعها لرقابة مستمرة[1].

ويُفهم من ذلك أن القضاء لا يقتصر دوره على الترخيص فقط، بل يمتد ليشمل التأكد من احترام الضوابط القانونية، خاصة ما يتعلق بضرورة اللجوء إلى المراقبة الإلكترونية كوسيلة استثنائية لا يُصار إليها إلا عند تعذر الوصول إلى نتائج بوسائل أخرى أقل مساسًا بالحقوق والحريات.

**المطلب الثالث : المقاربات الدولية والوطنية في موازنة الامن والحق**

وفي هذا المطلب، سنتطرق إلى الدور المحوري للقضاء الجزائري كحارس للحريات الرقمية من خلال تفعيل رقابته المسبقة واللاحقة على إجراءات المراقبة والتحري الإلكتروني، مستندين إلى أحكام القانون رقم 09-04 لبيان شروط الإذن القضائي وضوابط التناسب والضرورة التي تمنع تعسف سلطات الضبط، وذلك عبر استعراض النماذج الدولية المقارنة وصولاً إلى آليات المقاربة الوطنية على النحو التالي:

يرى الدكتور ميثاق بيات الضيفي في كتابه أكسجين الحرية أن النظام العالمي المعاصر بات يتسم بتعقيد وتشابك شديدين، خاصة مع تزايد عدد الفاعلين القادرين على توظيف تكنولوجيا المعلومات لخلق تهديدات سيبرانية، أو حتى استخدامها من قبل الدول لبسط سيطرة مطلقة على الموارد التقنية. وفي هذا السياق، يبرز الكاتب إشكالية جوهرية تتمثل في الصراع بين مقتضيات الأمن والحفاظ على الحريات،إذ إن اندفاع الأجهزة الأمنية نحو تأمين الفضاء الرقمي قد يقودها إلى انتهاك الخصوصية الفردية وتجاوز الأطر القانونية والحقوقية، مما يضع الدولة في مأزق أخلاقي وقانوني.ولحل هذا التناقض، يقترح الكاتب ضرورة الانتقال من نموذج التعاون القسري إلى نموذج التعاون المتناغم، وهو المسار الذي لا يتحقق إلا من خلال إخضاع المؤسسات الأمنية لرقابة ديمقراطية ومدنية

[1] _االمادة 04 نفس المرجع السابق.

صارمة، وتفعيل دور المجتمع المدني كصمام أمان لمنع إساءة استخدام السلطة، وبما يضمن موازنة دقيقة تحمي أمن الدولة ودون تقويض حقوق المواطن الأساسية[1].

**أ/ النموذج الأمريكي: أولوية الأمن القومي على حساب حقوق الإنسان**

يتمحور النموذج الأمريكي في تنظيم الفضاء السيبراني حول عقيدة الأمن أولاً، حيث تُمنح الأولوية القصوى لحماية الأمن القومي. وقد تعزز هذا التوجه بشكل جذري عقب أحداث 11 سبتمبر، مما أدى إلى توسيع نطاق صلاحيات الأجهزة الاستخباراتية في الرقابة الرقمية، لا سيما بموجب قانون (USA PATRIOT Act) الذي شرعن التوسع في تتبع الاتصالات وجمع البيانات بدواعي مكافحة الإرهاب. ومع كفاءة هذا النموذج في الاستجابة السريعة للتهديدات بفضل بنيته التقنية المتقدمة، إلا أنه يواجه انتقادات حقوقية حادة بسبب تغليب الهواجس الأمنية على الحق في الخصوصية، فضلاً عن افتقاره لإطار فيدرالي موحد لحماية البيانات، مما يخلق فجوة تشريعية وتفاوتاً في حماية الحقوق الفردية بين الولايات .[2]

**ب/ النموذج الأوروبي: مقاربة قانونية قائمة على التوازن وحماية الحقوق الفردية**

يتفرد النموذج الأوروبي برؤية استباقية تجعل من "الثقة الرقمية" حجر الزاوية في فضاء الإنترنت. وقد تكرس هذا النهج عبر اللائحة العامة لحماية البيانات (GDPR) التي أعادت للمستخدم السيادة على بياناته، وصولاً إلى (قانون الذكاء الاصطناعي EU AI Act الذي أرسى فلسفة "تصنيف المخاطر" كبديل للممارسات الأمنية المطلقة. وتعكس استراتيجية الأمن السيبراني لعام 2020 نضج هذا التوجه، حيث تؤكد أن الأمن الحقيقي لا يتحقق بالتضحية بالخصوصية، بل بترسيخ مبادئ الشفافية والمساءلة، بما يضمن عدم تحول التدابير الأمنية إلى ذريعة لتقويض الحريات. [3]

**ج/ النموذج الصيني: تغليب الرقابة المركزية على الحقوق الفردية**

[1] _ميثاق بيات الضيفي، أكسجين الحرية، كتاب رقمي ، نشر سنة 2024 ص 41/40

[2] _عروس كوثر، نفس المرجع السابق ص 263

[3] _ المرجع نفسه ص264

في الصين، يعتمد النموذج على مقاربة أمنية مشددة، حيث تفرض الدولة رقابة صارمة على الفضاء الرقمي من خلال قانون الأمن السيبراني 2017، الذي يمنح السلطات صلاحيات واسعة في مراقبة المحتوى وتخزين البيانات داخل الحدود الوطنية. ورغم أن هذا النظام يوفر مستوى عالياً من السيطرة الأمنية، إلا أنه يتعرض لانتقادات دولية بسبب تأثيره السلبي على حرية التعبير والحق في الخصوصية . تمثّل التجربة الصينية نموذجاً رائداً في تكريس مفهوم السيادة السيبرانية والإنترنت السيادي إذ تسعى من خلالها إلى بسط نفوذ الدولة الكامل على الفضاء الرقمي.كما تعتمد،على مزيج معقد من الأدوات التقنية والتشريعات القانونية لتحقيق أهدافها، وأبرزها:

- الحجب الممنهج :منع الوصول إلى المواقع والمنصات الأجنبية التي تتعارض مع التوجهات الوطنية.
- الرقابة اللحظية :تتبع حركة البيانات والاتصالات وتدفق المعلومات بدقة عالية لضمان الانضباط المعلوماتي[1].

**د/المقاربة الوطنية ( الجزائر كمنظومة في طور التشكيل) :**

لا يمكن قراءة معادلة التوازن بين الأمن السيبراني والحقوق الفردية في الجزائر بمعزل عن الحراك الدولي؛ إذ تمثل النماذج العالمية – مثل النظام الأوروبي (GDPR) والتشريعات الأمريكية والصينية—مرجعيات هامة للاستلهام بما يتوافق مع الخصوصية الوطنية. ويكمن التحدي الجوهري في ابتكار نموذج وطني أصيل يزاوج بين مقتضيات السيادة الرقمية والضمانات الحقوقية، متجاوزاً فكرة المحاكاة العمياء للقوانين الخارجية. وبالنتيجة، فإن الإطار القانوني الجزائري يعيش مرحلة مخاض واعدة تعكس إرادة سياسية جادة، لكنها لا تزال تتطلب تعزيزاً للتكامل بين الأبعاد القانونية والتقنية والاجتماعية، لضمان وضع المواطن في قلب المنظومة الأمنية كهدف أسمى للحماية[2].

[1] _ السيبرانية والحوكمة: بين ممارسة السيادة وحقوق الإنسان، https://hadaracenter.com، اطلع عليه 2026/05/05

[2] _عروس كوثر، نفس المرجع السابق ص 256

## ملخص الفصل الثاني :

عالج هذا الفصل العلاقة الجدلية بين مقتضيات الأمن السيبراني كضرورة استراتيجية للدولة، وبين حماية حقوق الإنسان كثابت أصيل في المنظومة القانونية. حيث رصد الفصل في شقه الأول مظاهر المساس بالحريات الرقمية، لاسيما عبر آليات الرقابة الإلكترونية التي قد تتحول من أداة لمكافحة الإجرام إلى وسيلة لانتهاك الخصوصية، وكذا التقييدات التي تطال حرية التعبير والوصول للمعلومات بداعي الحفاظ على النظام العام. وفي شقه الثاني، استعرض الفصل النموذج الجزائري في إرساءمعادلة التوازن، مبرزاً كيف كرس المؤسس الدستوري (لاسيما في تعديل 2020) والمشرع (عبر القانونين 09-04 و18-07 وتعديلاته الأخيرة لعام 2025) ضمانات حمائية صارمة، جعلت من القضاءحارس الحريات الأول عبر فرض الرقابة المسبقة على إجراءات التحري، مع الاستئناس بالمقاربات الدولية (الأمريكية، الأوروبية، والصينية) لصياغة نموذج وطني يزاوج بين السيادة الرقمية والكرامة الإنسانية.

# الخاتمة

في الختام استلخصنا من خلال فصول هذه المذكرة إلى أن الأمن السيبراني لم يعد مجرد خيار تقني بسيط، بل أضحى منظومة دفاعية وقانونية متكاملة تهدف إلى بسط الحماية على كافة مكونات الفضاء الافتراضي لضمان سرية المعلومات وسلامتها واستمرارية توافرها، كما تبين أن الانتقال إلى هذا الفضاء قد وفر آفاقاً رحبة للتعبير والتواصل، لكنه أفرز في الوقت ذاته تحديات أمنية استوجبت تدابير قد تتقاطع أحياناً مع منظومة الحقوق التقليدية، مما يجعل من الموازنة بينهما ضرورة حتمية في دولة القانون.

ويمكن إجمال أهم النتائج التي توصلنا إليها في ما يلي:

- يُعد الأمن السيبراني ضرورة استراتيجية تتجاوز البعد التقني لتشمل أبعاداً عسكرية، سياسية، اقتصادية، واجتماعية، تهدف في جوهرها إلى حماية الأمن القومي والمصالح الحيوية من التهديدات العابرة للحدود.

- إن حقوق الإنسان في الفضاء الرقمي، كالحق في الخصوصية وحرية التعبير والوصول إلى المعلومة، هي امتداد للحقوق الطبيعية والمدنية اللصيقة بالصفة الإنسانية، وتستوجب حماية قانونية مزدوجة على الصعيدين الوطني والدولي.

- أكد المشرع الجزائري على أن المراقبة الإلكترونية والاعتراض القانوني للاتصالات هي إجراءات استثنائية لا تُفعل إلا لضرورات التحقيق القضائي في جرائم محددة (كالإرهاب والتخريب)، وبشرط الحصول على إذن قضائي مكتوب.

- تندرج عملية تنقيب البيانات ضمن مفهوم معالجة المعطيات الشخصية، مما يفرض على جهات الأمن السيبراني الالتزام بحدود احترام الكرامة الإنسانية والحياة الخاصة وفقاً لما أقره القانون رقم 18-07.

- شهدت الجزائر طفرة تشريعية تهدف لتحقيق التوازن الرقمي، بدأت من القوانين الزجرية لمكافحة الإجرام المعلوماتي وصولاً إلى القوانين الحمائية للمعطيات الشخصية، وأخرها التعديلات الجوهرية لعام 2025.

- يضطلع القضاء بدور محوري في الرقابة على مشروعية إجراءات التحري الرقمي، من خلال التحقق من توافر شروط الضرورة والتناسب لضمان عدم التعسف في استخدام سلطات المراقبة.

وبناءً على ما سبق، يمكننا الإجابة على إشكالية البحث الرئيسية:

إن التوفيق بين بسط الأمن السيبراني وحماية حقوق الإنسان في الجزائر يقوم على مبدأ التناسب والضرورة، حيث لا يجوز تقييد الحريات الرقمية إلا بموجب نص قانوني واضح ولأهداف مشروعة تتعلق بالأمن القومي والنظام العام، وتحت رقابة قضائية صارمة . أما عن فعالية الضمانات التي قررها المشرع الجزائري، فقد أثبتت الدراسة أن الدستور الجزائري (تعديل 2020) يمثل صمام الأمان الأول بتكريسه لحرمة الحياة الخاصة وسرية المراسلات

وتتجسد هذه الفعالية عملياً في وجود ترسانة قانونية متطورة (مثل القانون 25-11 لعام 2025) وهيئات رقابية متخصصة، تعمل على وضع المواطن في قلب المنظومة الأمنية كهدف أسمى للحماية، مما يجعل التجربة الجزائرية نموذجاً يسعى لمزاوجة السيادة الرقمية بالكرامة الإنسانية.

وعليه يمكن الاجابة على الاسئلة الفرعية لدراستنا كما يلي :

يُعرف الأمن السيبراني بأنه منظومة دفاعية وقانونية متكاملة تهدف لحماية مكونات الفضاء الرقمي وضمان سرية وسلامة واستمرارية توافر البيانات .وتاريخياً، تطور هذا المفهوم من مرحلة النشأة في السبعينات لحماية الأنظمة من الفيروسات المحدودة ، إلى مرحلة التسعينات ببروز "الحرب السيبرانية الباردة" واعتماده كجزء من استراتيجيات الدفاع العسكري

وصولاً للعصر الرقمي الراهن كضرورة لحماية الأمن القومي والمصالح الحيوية للدول ضد التهديدات المتجددة والعابرة للحدود .

كما تؤثر تدابير الأمن السيبراني سلباً على الحق في الخصوصية وحرمة الحياة الخاصة نتيجة اللجوء السري لآليات الرقابة الرقمية، واعتراض الاتصالات ، والوقوع في فخ التنميط عبر تقنيات تنقيب البيانات .كما تمس بـ حرية الرأي والتعبير الرقمي عبر فرض قيود جائرة وتوظيف قوانين مكافحة الجرائم الإلكترونية بشكل تعسفي لتكميم الأفواه وتحديد التوجهات . وأخيراً، تؤثر على حق الوصول للمعلومات بتذرع السلطات بالهواجس الأمنية ومقتضيات النظام العام لفرض السرية وحجب البيانات .

يضطلع القضاء بدور محوري كحارس للحريات الرقمية، حيث قيد المشرع الجزائري إجراءات المراقبة الإلكترونية والاعتراض القانوني للاتصالات بضرورة استصدار إذن مكتوب ومسبق من وكيل الجمهورية أو قاضي التحقيق .ويمارس القضاء رقابته عبر إعمال مبدأ الضرورة القصوى، فلا يمنح الإذن إلا في الحالات التي يتعذر فيها تحصيل الأدلة بالوسائل التقليدية . كما يفرض ضابط التناسب لحصر المراقبة في جرائم نوعية محددة كالإرهاب والتخريب ، مع ترتيب البطلان على أي إجراء يتجاوز الأطر القانونية.

بناءً على النتائج التي توصلنا إليها من خلال هذه الدراسة، وإدراكاً منا بأن الفضاء الرقمي يتسم بالتطور التكنولوجي المتسارع الذي يسبق دائماً التشريع القانوني، فهناك جملة من التوصيات نوجز بعض منها فيما يلي :

**أولاً: على الصعيد التشريعي والقانوني**

1. نوصي بضرورة تجميع وتوحيد النصوص القانونية المتناثرة المتعلقة بالأمن السيبراني والجرائم المعلوماتية وحماية البيانات الشخصية في تقنين واحد متكامل.

2. رغم التعديلات الجوهرية التي جاء بها قانون 2025، إلا أننا نقترح ضرورة إدراج آليات مراجعة دورية (كل 3 أو 5 سنوات) للتشريعات الرقمية، لضمان استجابتها لتقنيات الجيل الخامس

3. نوصي بضبط المصطلحات الفضفاضة المتعلقة بـ مقتضيات الأمن الوطني أو النظام العام الرقمي بضوابط دقيقة وحصرية، لمنع أي تأويلات قد تستخدم كذريعة لتقييد حرية التعبير أو حجب المعلومات بشكل تعسفي.

**ثانياً: على الصعيد المؤسساتي والقضائي**

1. تكوين قضاة متخصصين في الأمن السيبراني :نظراً للتعقيد التقني لقضايا المراقبة الإلكترونية وتتقيب البيانات.

2. التمكين التقني لسلطة حماية المعطيات :تفعيل وتعزيز الاستقلالية المالية والتقنية لـ السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، وتزويدها بخبراء في الأمن السيبراني لتمكينها من ممارسة رقابة ميدانية واستباقية فعالة على الشركات والمؤسسات التي تعالج بيانات المواطنين.

**ثالثاً: على الصعيد المجتمعي والتوعوي**

1. إدراج مادة الحقوق والحريات الرقمية ضمن المناهج التعليمية والجامعية، لتوعية المواطن (المستخدم) بآليات حماية بياناته الشخصية، وتكريس وعي مجتمعي يفرق بين الاستخدام الآمن للتكنولوجيا والاستخدام الذي يهدد استقرار الدولة.

# قائمة المصادر والمراجع

## اولا: المصادر

### 1. الدساتير والقوانين


- دستور الجمهورية الجزائرية الديمقراطية الشعبية لعام 1989، الصادر بموجب المرسوم رقم 89-18 المؤرخ في 28 فيفري 1989، الجريدة الرسمية، العدد 09، المؤرخة في 1 مارس 1989.
- دستور الجمهورية الجزائرية الديمقراطية الشعبية لعام 2020، المعدل بموجب المرسوم الرئاسي رقم 20-442 المؤرخ في 15 جمادى الأولى عام 1442 هـ الموافق لـ 30 ديسمبر سنة 2020، المتضمن إصدار الدستور في الجريدة الرسمية للجمهورية الجزائرية، العدد 82، الصادر بتاريخ 30 ديسمبر 2020.
- القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق لـ 05 أوت 2009، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، الصادر بتاريخ 16 أوت 2009.
- القانون رقم 18-07 المؤرخ في 25 رمضان عام 1439 الموافق لـ 10 جوان 2018، المتعلق بحماية الأشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية، العدد 34، الصادر بتاريخ 13 جوان 2018.
- القانون رقم 25-11 المؤرخ في 24 جويلية 2025، المعدل والمحين للإطار القانوني الخاص بحماية البيانات ذات الطابع الشخصي.


### .2النصوص التنظيمية


- المرسوم الرئاسي رقم 15-261 مؤرخ في 24 ذي الحجة عام 1436 الموافق لـ 8 أكتوبر سنة 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 53، الصادر بتاريخ 11 أكتوبر 2015.

**3.الوثائق والاتفاقيات الدولية**

**أ- باللغة العربية:**

- العهد الدولي الخاص بالحقوق المدنية والسياسية، المؤرخ في 16 ديسمبر 1966، تاريخ بدء النفاذ 23 مارس 1976 اعتمد وعرض للتوقيع والانضمام بموجب قرار الجمعية العامة للأمم المتحدة 2200 ألف.

**ب- باللغة الأجنبية:**

- European Judicial Training Network (EJTN), *Handbook: English for Human Rights EU Law*, Brussels, 2017.

**ثانياً: المراجع**

**1.الكتب**

**أ- باللغة العربية:**

- أمراجع عطية السحاتي، *الأمن السيبراني ودوره في حماية الفضاء السيبراني للمؤسسات التي تعمل في المجال الجوي الوطني*.
- ذياب البداينة، *الأمن وحرب المعلومات*، الإصدار 2، الأردن: دار الشروق للنشر والتوزيع.
- فارس محمد العمارات، *الأمن السيبراني المفهوم وتحديات العصر*، الطبعة الأولى، الأردن: دار الخليج للنشر والتوزيع، سنة 2022.
- ميثاق بيات الضيفي، *أكسجين الحرية*، كتاب رقمي، نشر سنة 2024.

**ب- باللغة الأجنبية:**

- Thomas Paine, *Rights of Man*, London, 1791.

**2.المقالات العلمية**

**أ- باللغة العربية:**

- إسلام فوز، "الأمن السيبراني: الأبعاد الاجتماعية والقانونية تحليل سوسيولوجي"، *المجلة الاجتماعية القومية*، جامعة دمنهور، المجلد 56، العدد 02، مايو 2019.

- ربيعي حسين، "المراقبة الإلكترونية وحق الفرد في الخصوصية"، *المجلة الأكاديمية للبحث القانوني*، كلية الحقوق جامعة قسنطينة 1، الجزائر، المجلد 13، العدد 01، سنة 2016.
- عروس كوثر وعروس فوزية، "إشكالية الموازنة بين متطلبات الأمن السيبراني وضمان الحقوق الفردية"، *المجلة الأكاديمية للدراسات الاجتماعية والإنسانية*، المجلد 18، العدد 01، سنة 2026.
- كامش طيب، "القانون الدولي ومعايير الفضاء السيبراني بين الفراغ القانوني والاستغلال الجيوسياسي"، *مجلة الدراسات القانونية المقارنة*، تاريخ النشر 2025/12/25.
- لغرس سوهيلة، "حقوق الإنسان (مقاربة نظرية في المفهوم والخصائص"(، *مجلة الاجتهاد للدراسات القانونية والاقتصادية*، كلية العلوم الإنسانية والاجتماعية – جامعة مصطفى اسطمبولي معسكر (الجزائر)، المجلد 12، العدد 03، سنة 2023.
- مرزوقي كريم، "مراقبة الاتصالات الإلكترونية وحق الفرد في الخصوصية المعلوماتية"، *مجلة الأستاذ الباحث للدراسات القانونية والسياسية*، جامعة محمد بوضياف بالمسيلة، المجلد 05، العدد 02، سنة 2020.
- مصطفى علي العقبي، "حماية حقوق الإنسان الرقمية في عصر الذكاء الاصطناعي: دراسة أمنية قانونية مقارنة"، *مجلة الدراسات القانونية والاقتصادية*، دورية علمية محكمة (المؤتمر الدولي الثاني)، القاهرة، سنة 2026.

**ب- باللغة الأجنبية:**

- Morsli Abdelhak, "La Restriction de la Liberté d'Expression En rsité Droit International des Droits de l'Homme", *Revue des études juridiques et politiques*, Université Amar Telidji – Laghouat, Vol. 05, N° 02, juin 2019.

**3.المواقع الإلكترونية :**

- الأمن السيبراني مفهومه وتاريخه، موقع الجزيرة نت : [https://www.aljazeera.net/encyclopedia](https://www.aljazeera.net/encyclopedia)
- السيبرانية والحوكمة: بين ممارسة السيادة وحقوق الإنسان، مركز حضارة : [https://hadaracenter.com](https://hadaracenter.com)
- تنقيب البيانات :Data Mining المراحل والأدوات والخوارزميات والكتب، منصة بكة https://bakkah.com/ar/knowledge-cente
- عمرو الذيب، "حريّة التعبير في عصرنا الرقمي"، موقع سيف سبايس : [https://www.safespace.qa/topic/](https://www.safespace.qa/topic/)
- قانون الحق في الحصول على المعلومات وحماية الحق من الانتهاك، موقع أمان مونيتور https://aman-monitor.org/
- معجم المعاني https://www.almaany.com/

# قائمة المحتويات

**قائمة المحتويات**


| العنوان | رقم الصفحة |
|---|---|
| الإهداء | |
| شكر وعرفان | |
| **المقدمة** | أ |
| **الفصل الأول: الإطار المفاهيمي والقانوني للأمن السيبراني وحقوق الإنسان** | |
| تمهيد | **01** |
| **المبحث الأول: ماهية الأمن السيبراني** | 02 |
| المطلب الأول: مفهوم الأمن السيبراني ونشأته | **03** |
| الفرع الأول: مفهوم الأمن السيبراني | 03 |
| الفرع الثاني: نشأة الأمن السيبراني | 05 |
| المطلب الثاني: أهمية الأمن السيبراني | 06 |
| المطلب الثالث: أبعاد الأمن السيبراني والتهديدات التي يشكلها | 07 |
| الفرع الأول: أبعاد الأمن السيبراني | 07 |
| الفرع الثاني: الأمن السيبراني والتهديدات التي يشكلها | 10 |
| **المبحث الثاني: حقوق الإنسان في البيئة الرقمية** | 13 |
| المطلب الأول: مفهوم حقوق الإنسان | **14** |
| الفرع الأول: المعنى اللغوي والاصطلاحي للحق | 14 |
| الفرع الثاني: مفهوم حقوق الإنسان | 16 |
| المطلب الثاني: حقوق الإنسان في الفضاء الرقمي | 17 |
| المطلب الثالث: طبيعة العلاقة بين الأمن السيبراني وحقوق الإنسان | 20 |
| الفرع الأول: جهود المجتمع الدولي لتنظيم السلوك في الفضاء السيبراني | 20 |
| الفرع الثاني: التهديدات السيبرانية التي شهدتها الجزائر | 22 |
| ملخص الفصل الأول | 24 |
| **الفصل الثاني: أثر تدابير الأمن السيبراني على حقوق الإنسان** | |

| | |
|---|---|
| **المبحث الأول: مظاهر المساس بحقوق الإنسان باسم الأمن السيبراني** | **26** |
| المطلب الأول: الرقابة الإلكترونية والحق في الخصوصية | **27** |
| الفرع الأول: مفهوم الرقابة الإلكترونية | 27 |
| الفرع الثاني: واقع الرقابة الإلكترونية والحق في الخصوصية | 30 |
| المطلب الثاني: تقييد حرية التعبير والوصول إلى المعلومات | 31 |
| الفرع الأول: تقييد حرية التعبير | 31 |
| الفرع الثاني: تقييد الوصول إلى المعلومات | 33 |
| المطلب الثالث: التنميط الرقمي عبر تنقيب البيانات كأحد مظاهر المساس بالحياة الخاصة | 34 |
| **المبحث الثاني: آليات التوازن بين الأمن السيبراني وحقوق الإنسان في الجزائر** | 37 |
| المطلب الأول: الضمانات الدستورية والقانونية | 38 |
| المطلب الثاني: دور القضاء في حماية الحقوق والحريات | 40 |
| المطلب الثالث: المقاربات الدولية والوطنية في موازنة الأمن والحق | 41 |
| ملخص الفصل الثاني | 44 |
| **الخاتمة** | 46 |
| **قائمة المصادر والمراجع** | 52 |
| **قائمة المحتويات** | 58 |
| **ملخص الدراسة (باللغة العربية )** | 60 |
| **ملخص الدراسة (باللغة بالانجليزية)** | 61 |

**ملخص الدراسة :**

تشكل حماية الأمن السيبراني للدولة من التهديدات الرقمية المتجددة هاجساً يشغل المنظمات الدولية والمشرعين كافة ، حيث تسعى السياسات التشريعية الحديثة إلى ابتكار آليات تحافظ على أمن الدول وتحصن بنيتها التحتية الحيوية من جهة ، وتضمن احترام مبادئ حقوق الإنسان وحرياته الأساسية في البيئة الرقمية (كالخصوصية وحرية التعبير) من جهة أخرى . والهدف الأساسي من هذه الدراسة هو معالجة هذه العلاقة الجدلية، مع التركيز على موقف المشرع الجزائري وتبنيه لسياسة تشريعية ومؤسساتية تساهم في حماية الأمن الرقمي الوطني ضد التهديدات المتصاعدة .وسوف نعالج الموضوع في فصلين أساسيين ، نتناول في الفصل الأول الإطار المفاهيمي والقانوني للأمن السيبراني وحقوق الإنسان مع رصد الأبعاد المختلفة وجهود المجتمع الدولي لتنظيم الفضاء الرقمي ، ثم نتناول في الفصل الثاني أثر تدابير الأمن السيبراني على الحقوق والحريات (كالمراقبة الإلكترونية وتنقيب البيانات) مبرزين واقع وآليات التوازن التشريعي والقضائي في الجزائر مقارنة ببعض النماذج الدولية.

## ABSTRACT

Protecting a state's cybersecurity from evolving digital threats has become a paramount concern for international organizations and legislators worldwide. Modern legislative policies strive to devise mechanisms that maintain national security and safeguard critical infrastructure on one hand , while ensuring respect for human rights principles and fundamental freedoms in the digital environment (such as privacy and freedom of expression) on the other. The primary objective of this study is to address this dialectical relationship, focusing on the stance of the Algerian legislator and the adoption of a legislative and institutional policy that contributes to protecting national digital security against escalating threats. The subject will be examined across two main chapters. The first chapter addresses the conceptual and legal framework of cybersecurity and human rights, exploring its various dimensions and international efforts to regulate the digital space. The second chapter analyzes the impact of cybersecurity measures on rights and freedoms (such as electronic surveillance and data mining), highlighting the reality and mechanisms of legislative and judicial balance in Algeria compared to certain international models.