



## مذكرة بعنوان

# الأمن السيبراني تحدي جديد للقانون

مذكرة مقدمة لاستكمال متطلبات الحصول على شهادة ماستر أكاديمي في  
الحقوق تخصص: قانون أعمال

إشراف الأستاذة:

إعداد الطلبة

• د. صياد الصادق

• آية الرحمان حمداوي

• جيهان زادي

لجنة المناقشة

| الاسم و اللقب | الرتبة        | الهيئة المستخدمة      | الصفة         |
|---------------|---------------|-----------------------|---------------|
| قريمس سارة    | أستاذ محاضر ب | جامعة الشاذلي بن جديد | رئيسا         |
| صياد الصادق   | أستاذ مساعد أ | جامعة الشاذلي بن جديد | مشرفا و مقررا |
| بوعشة كمال    | أستاذ محاضر أ | جامعة الشاذلي بن جديد | ممتحنا        |

|                                                                                                                  |                                                                                                                                                                                                                                                        |
|------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| الجمهورية الجزائرية الديمقراطية الشعبية<br>République Algérienne Démocratique et Populaire                       |                                                                                                                                                                                                                                                        |
| وزارة التعليم العالي والبحث العلمي<br>جامعة الشاذلي بن جديد القارف<br>كلية الحقوق والعلوم السياسية<br>قسم الحقوق |  Ministère de L'Enseignement Supérieur<br>Et de La Recherche Scientifique<br>Université et loi<br>Faculté de Droit et des Sciences Politiques<br>Département de Droit |

القرار الوزاري رقم 1082 المؤرخ في 27 ديسمبر 2020 المحدد المنطقة بالقومية من السرة العلمية ومكافئها

## تصريح شرفي خاص بالالتزام بقواعد النزاهة العلمية

أنا الممضي أدناه،

السيد (ة): زادي جيهان  
 الحامل لبطاقة التعريف الوطنية رقم: 110031230003480004  
 الصادرة بتاريخ: 2023/09/13  
 عن دائرة: الترشيحة ولاية الطارف  
 المسجل بقسم: الحقوق والعلوم السياسية والمكلف بإجازة منكرة تخرج ماستر  
 عنوانها: الأمن السيبراني تحدي جديد للقانون

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

التاريخ: 2026/06/10

إمضاء المعنى



الجمهورية الجزائرية الديمقراطية الشعبية  
République Algérienne Démocratique et Populaire

وزارة التعليم العالي والبحث العلمي

جامعة الشاذلي بن جديد الطارف

كلية الحقوق والعلوم السياسية

قسم الحقوق



Ministère de L'enseignement Supérieur

Et de La Recherche Scientifique

Université et loi

Faculté de Droit et des Sciences Politiques

Département de Droit

قرار الوزاري رقم 1082 المؤرخ في 27 ديسمبر 2020 المعدد المتعلقة بملف قضية من السرقة العلمية ومكافئتها

## نصريح شرفي خاص بالالتزام بقواعد النزاهة العلمية

أنا المعني أدناه:

المسيد (ة): حاجوي آية الحصاني

الحامل لبطاقة التعريف الوطنية رقم: 11.00.2070.0000.870000

الصادرة بتاريخ: 2021.02.09

عن دائرة: الزيتونة - الطارف

المسجل بقسم: الحقوق والعلوم السياسية والمكلف بتجارب منكرة تخرج منستر

عنوانها: الأمن السيبراني تحدي جديد للقانون

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

التاريخ: 2026/06/10

إمضاء المعني

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

# شكر و عرفان

بسم الله الرحمن الرحيم

الحمد لله رب العالمين، حمداً كثيراً طيباً مباركاً فيه، الذي بنعمته تتم الصالحات، وبتوفيقه تتحقق الغايات، والصلاة والسلام على سيدنا محمد صلى الله عليه وسلم، خير الخلق أجمعين.

قال الله تعالى: ﴿وَمَا تَوْفِيقِي إِلَّا بِاللَّهِ عَلَيْهِ تَوَكَّلْتُ وَإِلَيْهِ أُنِيبُ﴾.

أتقدم بأسمى آيات الشكر والتقدير والعرفان إلى الأستاذ الفاضل صياد الصادق، على ما بذله من جهد علمي وتوجيهات قيّمة ونصائح سديدة، وعلى دعمه المستمر ومرافقته لنا خلال إنجاز هذا العمل. فكان خير مرشد وموجه، ولم يبخل علينا بعلمه وخبرته، فجزاه الله عنا خير الجزاء.

كما أسأل الله تعالى أن يجعل ما قدمه من علم وعطاء في ميزان حسناته، وأن يبارك له في عمره وعلمه وعمله، وأن يوفقه إلى كل خير، وأن يرزقه الصحة والعافية والسداد.

ووفاءً لأهل الفضل، أتوجه بالشكر إلى كل من ساهم من قريب أو بعيد في إنجاز هذا العمل، سائلاً المولى عز وجل أن يجزيهم خير الجزاء، وأن يوفقهم لما يحبه ويرضاه.

﴿رَبِّ زِدْنِي عِلْماً﴾، و\*\*﴿وَقُلْ اْعْمَلُوا فَسَيَرَى اللَّهُ عَمَلَكُمْ وَرَسُولُهُ وَالْمُؤْمِنُونَ﴾.\*\*

والحمد لله أولاً وآخراً، وظاهراً وباطناً، على نعمة العلم والتوفيق.

## الإهداء

بسم الله الرحمن الرحيم  
قال تعالى: "يَرْفَعُ اللَّهُ الَّذِينَ آمَنُوا مِنْكُمْ وَالَّذِينَ أُوتُوا الْعِلْمَ دَرَجَاتٍ وَاللَّهُ بِمَا  
تَعْمَلُونَ خَبِيرٌ"

### سورة المجادلة 11

الحمد لله الذي ما تم جهد الا بعونه، وما ختم سعي الا بفضله.  
اهدي تخرجي وحصاد ما زرعت الى نفسي التي صبرت وثابرت حتى  
وصلت الى عتبات هذا الانجاز ، والى تحقيق الحلم الذي طال ما  
انتظرته.

وبكل حب وفخر أهدي ثمرة نجاحي الى من قال الله عز وجل فيهم:  
وَقَضَىٰ رَبُّكَ أَلَّا تَعْبُدُوا إِلَّا إِيَّاهُ وَبِالْوَالِدَيْنِ إِحْسَانًا "

### سورة الاسراء 23

الى الحبيب الاولي والضلع الثابت، الى سندي في الحياة الذي لم ييخل  
بشيء من اجلي . الى المعلم الأول الذي علمني الاخلاق وغرس في  
روحي قيم الجد والاجتهاد . الى " ابي الغالي " اطل الله في عمره .  
الى من جعل الجنة تحت اقدامها وسهلت لي الشدائد بدعائها ، الى من  
كانت ملجأى وسر وجودي وفرحتي ، الى التي تمننت ان تراني في يوم  
كهذا " امي العزيزة " حفظها الله وأطل في عمرها .  
الى من يشتد بهم عضدي وتقوى بهم خطاي في هذه الحياة ، الى  
دعمي وسندي " اخي الغالي " و " اختي الغالية "  
الى صديقتي آية الرحمان ، والى كل العائلة الكريمة .  
و أخيرا من قال أنا لها وإن أبت رغما اتيت بها ، ما كنت لأفعل هذا  
لولا توفيق من الله عز وجل .

جيهان

## الاهداء

بسم الله الرحمن الرحيم

"وقل اعملوا فسيرى الله عملكم ورسوله والمؤمنون" التوبة 105.

الحمد لله الذي بنعمته تتم الصالحات، والذي وفقني لأبلغ هذه اللحظة التي طالما حلمت بها، وجعل كل تعب نجاحًا، وبعد كل صبر فرحًا.

أهدي هذا العمل المتواضع أولاً إلى الله عز وجل، ثم نفسي، تلك التي آمنت بحلمها، وصبرت في وجه الصعوبات، وتمسكت بالأمل حتى وصلت إلى هذه المحطة التي تمثل بداية جديدة نحو مستقبل أفضل.

إلى كل من مد لي يد العون، وآمن بقدراتي على الوصول، أو رافقني بدعائه، أهدىكم هذا الإنجاز.

إلى من قال الله تعالى فيهما:

"وقل رب ارحمهما كما ربياني صغيراً". الاسراء 24

إلى من جعل الله الجنة تحت أقدامها، إلى من كان دعاؤها سر نجاحي، والدتي.

إلى من دعمني بلا حدود، وأعطاني بلا مقابل، إلى من علمني أن الدنيا كفاح وسلاحها العلم والمعرفة، الذي غرس في روحي مكارم الأخلاق، داعمي الأول في مسيرتي، وقوتي بعد الله، والدي أحمد.

إلى من شد الله بهم عضدي، فكانوا خير معين، أخوتي:

بلال، محمد الأمين، سيف الدين، رحمة، حنان.

إلى أجمل إضافة إلى عائلتنا، ابنة أخي أفنان براءة.

إلى صديقتي مروي، التي لم تكن مجرد رفيقة درب، بل كانت السند الحقيقي في كل لحظات حياتي، كنت جزءًا مني لا يكتمل بدونه شيء، وجودك نعمة لا يقاس بثمن.

صديقتي العزيزات:

نهلة، عبير، جيهان

آية الرحمان

## قائمة المختصرات:

| المختصر | المعنى                      |
|---------|-----------------------------|
| ص       | صفحة                        |
| ط       | طبعة                        |
| ج.ر.ج.ج | جريدة رسمية جمهورية جزائرية |
| ص ص     | صفحة من الى                 |

## مقدمة

## مقدمة:

يشهد العالم المعاصر ثورة رقمية غير مسبوقة، أدت إلى توسع استخدام تكنولوجيات الإعلام والاتصال في مختلف مجالات الحياة الاقتصادية والاجتماعية والإدارية، وأصبحت الأنظمة المعلوماتية والشبكات الرقمية تشكل العمود الفقري للأنشطة الحديثة، وقد ساهم هذا التطور الهائل في تسهيل المعاملات وتبادل المعلومات وتحقيق مستويات عالية من الكفاءة والسرعة، إلا أنه أفرز في المقابل مخاطر جديدة تمثلت في تزايد التهديدات والهجمات السيبرانية التي تستهدف الأفراد والمؤسسات والدول على حد سواء.

وأمام تنامي الجرائم المعلوماتية وتطور أساليب الاختراق والتجسس الإلكتروني وسرقة البيانات وتعطيل الأنظمة الرقمية، برز مفهوم الأمن السيبراني باعتباره أحد أهم الوسائل الرامية إلى حماية الفضاء الإلكتروني وضمان سرية المعلومات وسلامتها واستمرارية الخدمات الرقمية، ولم يعد الأمن السيبراني مسألة تقنية بحتة، بل أصبح قضية قانونية واستراتيجية تفرض على المشرعين مواكبة التحولات التكنولوجية المتسارعة ووضع أطر قانونية قادرة على مواجهة المخاطر المستجدة.

ويثير موضوع الأمن السيبراني العديد من الإشكالات القانونية المرتبطة بحماية البيانات الشخصية، وتحديد المسؤولية القانونية عن الأفعال المرتكبة في البيئة الرقمية، وإثبات الجرائم الإلكترونية، والتوفيق بين متطلبات الأمن واحترام الحقوق والحريات الأساسية للأفراد، كما تزداد هذه الإشكالات تعقيدا بسبب الطابع العابر للحدود الذي تتسم به الهجمات السيبرانية، الأمر الذي يجعل من التعاون الدولي ضرورة حتمية لضمان فعالية الحماية القانونية.

ومن هذا المنطلق، يكتسي موضوع الأمن السيبراني أهمية بالغة باعتباره تحديا جديدا للقانون، يستوجب إعادة النظر في العديد من المفاهيم والقواعد القانونية التقليدية، والعمل على تطوير منظومة تشريعية متكاملة تستجيب لمتطلبات البيئة الرقمية الحديثة. لذلك تهدف هذه الدراسة إلى تسليط الضوء على مفهوم الأمن السيبراني ومختلف التهديدات التي تواجهه، مع بيان مدى كفاية القواعد القانونية

القائمة في مواجهة المخاطر السيبرانية، واستعراض الآليات القانونية المعتمدة لتعزيز الأمن السيبراني وضمان حماية الفضاء الرقمي

## 1. أهمية الدراسة:

إن أهمية هذا الموضوع " الأمن السيبراني التحدي الجديد للقانون " كون أنه من مواضيع الساعة التي فرضت نفسها على الساحة القانونية ، وهو الأمر الذي جعل دراسته تكتسي أهمية علمية وعملية ، وهو ما سنتناوله على النحو الآتي:

### أ. الأهمية العلمية:

- يعد الأمن السيبراني من المواضيع الحديثة في المجال القانوني ، كون أنه لا يزال يشهد تطور مستمر نتيجة التقدم المتسارع في التكنولوجيا الإلكترونية ، و قد دفع هذا الطابع المستجد الباحثين إلى القيام بدراسات ودورات علمية متخصصة حول هذا الموضوع.

- يساهم هذا الموضوع في إضافة مرجع علمي مهم يمكن الإستفادة منه في إثراء المكتبات الجامعية والبحثية، بإعتباره أحد القضايا المعاصرة ذات الصلة بالتحول الرقمي.
- يساهم في تطوير المعرفة العلمية من خلال تحليل الظواهر بشكل منهجي ودقيق، مما يساعد على إنتاج حلول جديدة لمشكلات القائمة .

### ب. الأهمية العملية:

- تعزيز الوعي بأهمية الأمن السيبراني ودوره في حماية المعطيات والأنظمة والمعلوماتية، كما يساعد على ترسيخ سلوك أكثر حذرا ومسؤولية، وذلك في مواجهة مختلف التهديدات المرتبطة بإستخدام التكنولوجيا الحديثة .
- يساعد في توضيح التطبيق الفعلي للنصوص التشريعية المتعلقة بالفضاء الرقمي على مختلف الوقائع العملية التي تفرزها الجرائم السيبرانية ، كما يدعم تفعيل هذه النصوص بصورة فعالة .

## 2. أسباب إختيار الموضوع:

إن موضوع الأمن السيبراني التحدي الجديد للقانون يعالج مخاطر مرتبطة بحماية المعطيات داخل الفضاء الرقمي وعليها جاء إختيار هذا الموضوع بدافع شخصي وموضوعي والذي يتمثل على النحو الآتي:

### أ. الأسباب الذاتية:

- الإهتمام الشخصي بفهم طبيعة الفضاء السيبراني وإستيعاب عناصره المختلفة بإعتباره عنصرا رقميا متشعبا تتداخل فيه جوانب التقنية، كما أن إتساع نطاق إستخدامه في مختلف المجالات آثار رغبة في فهم آليات عمله.
- الفضول العلمي لدراسة الجريمة السيبرانية كونها من الظواهر الإجرامية الحديثة التي أفرزها التطور التكنولوجي كونها، تختلف عن الجريمة التقليدية من حيث وسائل إرتكابها وطبيعتها، وهو الأمر الذي خلق الإهتمام بفهم خصائصها وصورها المختلفة .

### ب. الأسباب الموضوعية:

- التطور المستمر لأساليب الإخفاء، والتشفير الذي يعتمدها مرتكبو الجرائم الرقمية، لما تثيره هذه التقنيات من صعوبات في كشف الجناة وتتبع أنشطتهم.
- حادثة موضوع الأمن السيبراني التحدي الجديد للقانون، إذ يعتبر من المجالات المستجدة التي فرضت نفسها مع التطور الرقمي السريع، كما أن هذا الطابع الحديث يجعله مجالا مفتوحا للبحث والدراسة لفهم أبعاده وكيفية التعامل مع إشكالاتهم المستحدثة .

## 3. أهداف الدراسة:

-إن لكل بحث علمي يسعى إلى تحقيق غايات وهو ما سنوضحه في دراستنا هذه يهدف هذا البحث في التعرف على الإطار المفاهيمي لكل من الأمن السيبراني والجريمة السيبرانية، وذلك لإزالة اللبس والغموض المحيط بهذين المفهومين.

- كشف أبرز الصعوبات التي تعيق تحقيق القانون الفعال للأمن السيبراني .

- إكمال الدراسات السابقة كونها في شكل مقالات .
- جمع متفرقات من الآليات التشريعية ،المتعلقة بالجريمة الرقمية.

#### 4.الإشكالية:

إن الإشكال الرئيسي ينطلق من تزايد الإعتماد على الفضاء السيبراني في مختلف القطاعات وما صاحبه من تنامي التهديدات ،والجرائم الرقمية مما تمس الأفراد والمؤسسات ودول وهو الأمر الذي فرض ضرورة وضع إطار قانوني ينظم هذا المجال ،ويكفل حمايته من مختلف الإعتداءات وعليه يتمحور الإشكال الرئيسي لهذا الموضوع فيمايلي:

الى أي مدى استطاع التشريع الجزائري مواكبة التحديات التي يفرضها الامن السيبراني في ظل التطور المتسارع للتكنولوجيا الرقمية و الجرائم الالكترونية؟

#### 5. منهج الدراسة:

نظرا لطبيعة هذا الموضوع الذي يدرس مفاهيم للأمن السيبراني والجريمة الرقمية إلى جانب النصوص القانونية ذات الصلة بالمجال الرقمي ،كان من الضروري الإعتماد على مناهج علمية، حيث تساعد على الإحاطة بجوانب البحث المختلفة وتفسيرها بدقة ووضوح ،وهو ما سيتم التطرق إليه على النحو الآتي:

#### أ.المنهج الوصفي:

- تم الإعتماد على هذا المنهج نظرا لضرورة عرض المفاهيم الأساسية المرتبطة بالأمن السيبراني والجريمة السيبرانية ،لما يترتب على ذلك أهمية في توضيح دلالاتهما مع تحديد مضامينها بدقة ،وهو ما يساعد على إستيعاب الموضوع بصورة سليمة ومترابطة.

## ب. المنهج التحليلي:

- لقد تم الإعتماد على المنهج التحليلي نظرا لدوره البارز في تحليل النصوص القانونية ذات الصلة بحماية الفضاء الرقمي، بالإضافة إلى الآليات الوقاية ومختلف الجهود المبذولة على الصعيدين الوطني والدولي، وهذا لفهمه بصورة أشمل وأدق.

- التقسيم العام بخطة البحث:

لقد تم الإعتماد في تقسيم موضوع الدراسة وفق خطة ثنائية قصد الإجابة عن الإشكالية وذلك على النحو الآتي:

### الفصل الأول: الأمن السيبراني والجريمة السيبرانية

#### • المبحث الأول: ماهية الأمن السيبراني

#### • المبحث الثاني: الجرائم السيبرانية ودوافع ارتكابها

### الفصل الثاني: المواجهة التشريعية لحماية الأمن السيبراني.

#### • المبحث الأول: أليات حماية الامن السيبراني والهيئات المختصة لمكافحته

#### • المبحث الثاني: جزاء الاخلال بالأمن السيبراني والتحديات التي تواجهه

## الفصل الأول: الأمن السيبراني والجريمة السيبرانية

## تمهيد

في ظل التقدم العلمي المتسارع في مجال تكنولوجيا الاعلام والاتصال، وما صاحبه من توسع كبير في استخدام الأنظمة المعلوماتية والشبكات الرقمية في مختلف مجالات الحياة الاقتصادية والاجتماعية والإدارية وقد أسهم هذا التطور في تحقيق العديد من المزايا التي قامت بتسهيل تبادل المعلومات بسرعة وفعالية، فأصبح الفضاء السيبراني جزءا أساسيا ومهما في الحياة اليومية للأفراد والمؤسسات والدول، إلا أنه افرز في المقابل ذلك مخاطر وتهديدات جديدة استهدفت أمن المعلومات والأنظمة الالكترونية، وهذا ما جعل مسألة الأمن السيبراني من أبرز القضايا المطروحة على الساحتين الوطنية والدولية.

وأمام تزايد هذه التهديدات، برز الأمن السيبراني كأحد أهم الوسائل الكفيلة بفرض الحماية اللازمة للفضاء الرقمي وضمان سلامة المعلومات من مختلف أشكال الاعتداءات الالكترونية، حيث أصبح معلوما أن أصحاب القرار في الدول الكبرى يصنفون الأمن السيبراني كأولوية في سياساتهم الدفاعية الوطنية تداركا لأي خطر أو هجوم يمكن أن يعترض لهاته المعلومات والبيانات في البيئة الرقمية، وهذا ما استدعى ضرورة وجود ضمانات أمنية داخل هاته البيئة.

إضافة الى ذلك برزت الجريمة السيبرانية كأحد أهم التحديات التي تواجه الأفراد والمؤسسات والدول، نظرا لما تتميز به من خصوصية مرتبطة باستخدام الوسائل التقنية الحديثة، فضلا عن صعوبة اكتشافها واثباتها وملاحقة مرتكبيها، الأمر الذي جعلها تشكل تحديا حقيقيا أمام المنظومة القانونية، وسوف نحاول من خلال هذا الفصل الإحاطة بالمفاهيم المتعلقة بالأمن السيبراني وتبيان أهمية، وكذلك التطرق الى دراسة ماهية الجريمة السيبرانية.

وعليه تم تقسيم هذا الفصل الى مبحثين كما يلي

### ● المبحث الأول: ماهية الأمن السيبراني

### ● المبحث الثاني: الجرائم السيبرانية ودوافع ارتكابها

### المبحث الأول: ماهية الأمن السيبراني

في ظل التطورات التي عرفها العالم في مجال تكنولوجيا المعلومات، أصبح الأمن السيبراني أحد أهم قضايا عصر المعلومات، خاصة مع اعتماد المؤسسات والقطاعات على الأنظمة الرقمية مما زاد من نسبة التهديدات والمخاطر الماسة بالبيانات، مما استلزم ضرورة إحاطة هذا المجال بمفاهيم دقيقة وآليات واضحة لضمان الحماية اللازمة، وعلى هذا النحو قسمنا المبحث إلى مطلبين، حيث يتناول المطلب الأول مفهوم الأمن السيبراني، والمطلب الثاني بعنوان مجالات الأمن السيبراني.

### المطلب الأول: مفهوم الأمن السيبراني

يعتبر الأمن السيبراني ركيزة أساسية لمجتمع المعلومات، كما يعد دعامة هامة لأنشطة الحكومات والأفراد، وعليه سنتطرق في الفرع الأول لنشأة الأمن السيبراني، والفرع الثاني بعنوان الأمن السيبراني، أما الفرع الثالث تم عنونته بالمفاهيم المرتبطة بالأمن السيبراني.

### الفرع الأول: نشأة الأمن السيبراني

يمكن القول أن نشأة الأمن السيبراني لم تكن وليدة لحظة واحدة، بل جاءت نتيجة تطور تدريجي عرفه مجال تكنولوجيا المعلومات والاتصال.

ففي أعقاب انتهاء الحرب الباردة، برز مفهوم الأمن السيبراني تزامنا مع ظهور مصطلح "حرب الأنترنت" أو "الحرب السيبرانية". وجاء هذا مع بداية اعتماد الدول بشكل متزايد على أجهزة الكمبيوتر في مختلف مؤسساتها، وتطور وحدة المعالجة المركزية لهاته الأجهزة، مما أدى إلى دمجها في العمليات المؤسسية والحكومية وصولا إلى الحياة اليومية. واقتصر دور الأمن السيبراني على توفير الحماية من الفيروسات والبرمجيات الخبيثة.<sup>1</sup>

<sup>1</sup> - محمد شايب، تأثير التهديدات السيبرانية على الأمن المجتمعي الجزائري، مذكرة ماستر تخصص علاقات دولية، المدرسة الوطنية العليا للعلوم السياسية، قسم العلاقات الدولية، الجزائر، 2024-2025، ص19.

وفي سبعينيات القرن العشرين، ظهر أول فيروس رقمي على شبكة "أربانت" وهي شبكة رائدة في نقل البيانات بتقنية تبديل الرزم، وعلى الرغم من عدم تسببه في أضرار كبيرة إلا أنه حفز على تطوير أساليب الحماية والأمان للشبكات، يتضح أنه في هذه الفترة بدأ استخدام التشفير في شبكات الاتصال حيث طور معهد ماساتشوستش للتكنولوجيا تقنية (kerberos) عام 1983 والتي أصبحت أساساً لتقنيات الأمن السيبراني الحديثة.<sup>1</sup>

أما في عام 1988 قام الباحث روبرت تابان موريس بتصميم أول فيروس إلكتروني، والذي يعتبر أول دودة حاسوب على الأنترنت. حيث تسبب انتشاره في تعطيل الأنظمة. فحكم على موريس بالسجن مدة ثلاثة سنوات وغرامة قدرها 10000 دولار أمريكي، وأصبح أول شخص يدان بموجب قانون الاحتيال وإساءة استخدام الحاسوب، مما ساهم على الحكم في تطوير القوانين المتعلقة بالأمن السيبراني.<sup>2</sup>

ليقوم بعدها مخترع البريد الإلكتروني "راي توملينسون" من ابتكار برنامج يمكنه من إزالة البرامج الضارة، وأصبح أول نظام لمكافحة الفيروسات الإلكترونية، أما خلال فترة التسعينيات، فقد أدى انتشار خدمة الأنترنت واندماجها في مختلف المجالات إلى تزايد عدد مستخدمي المواقع الإلكترونية، الأمر الذي ساهم في تطور الاجرام السيبراني واتساع نطاقه، وظهور صور مستحدثة من الجرائم الإلكترونية التي استهدفت العديد من المواقع الحساسة أهمها اختراق موقع البيت الأبيض.<sup>3</sup>

<sup>1</sup> - وائل خليل الرحمان بوطمين، البعد السيبراني للأمن القومي الجزائري: دراسة مقارنة لنماذج دولية رائدة، مذكرة ماستر، تخصص علاقات دولية، المدرسة الوطنية العليا للعلوم السياسية، الشهيد دور محمد ابراهيم القاسم، الجزائر، 2024-2025، ص 18.

<sup>2</sup> - محمد الدام، الأمن السيبراني، مذكرة ماستر في جريمة وأمن، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمزة لخضر، جامعة الواد، 2022-2023، ص 07.

<sup>3</sup> - فارس محمد العمارات، "جرائم العصر من الرقمية إلى السيبرانية"، ط 1، دار الخليج للنشر والتوزيع، الأردن، عمان، 2023، ص 07.

أما في فترة القرن الواحد والعشرين ومع التزايد الملحوظ في انتشار الأنترنت وارتفاع معدلات الجرائم الإلكترونية، وما يترتب عنها من خسائر مالية فادحة، أولت الدول اهتماما بالغاً للمخاطر التي تهدد البنية التحتية للمعلومات، وشبكات الاتصالات، ونتيجة لذلك بدأت الحكومات في صياغة استراتيجيات الأمن السيبراني الشاملة بهدف التصدي للجرائم الإلكترونية.<sup>1</sup>

### الفرع الثاني: تعريف الأمن السيبراني

تعتبر مهمة ضبط المفاهيم والمصطلحات تحدياً يواجه مختلف الباحثين والدارسين في مختلف التخصصات، نظراً لصعوبة الاتفاق على تعريفات واضحة ومحددة، ويعد الأمن السيبراني أحد أهم هذه المصطلحات التي عرفت تعدداً وتنوعاً، إذ ارتأينا أن نتناول هذا المفهوم من الناحية اللغوية والاصطلاحية.

### أولاً: تعريف الأمن السيبراني لغة:

هذا المصطلح مكون من كلمتين الأمن، والسيبراني، يشير المعنى اللغوي للأمن إلى نقيض الخوف، أمنا وأماناً وأمانة وإمنا وأمانة اطمأن ولم يخف، فهو آمن وأمن وأمين يقال لك الأمان أي قد آمنتك، والبلد اطمأن فيه أهله والشر ومنه سلم، وفلاناً على كذا وثق به واطمأن إليه أو جعله آميناً عليه.<sup>2</sup>

أما مصطلح السيبراني (cyber) تعني فضاء الأنترنت، وهي كلمة مشتقة من الكلمة اليونانية kybernets بمعنى الشخص الذي يدير السفينة، وتستخدم مجازاً للتعبير عن المتحكم.<sup>3</sup>

<sup>1</sup> - محمد الدام، المرجع السابق، ص 07.

<sup>2</sup> - مجمع اللغة العربية، "المعجم الوسيط"، ط4، مكتبة الشروق الدولية، القاهرة، مصر، 2004، ص 28

<sup>3</sup> - عبد العزيز بن فهد بن محمد بن داود، "الجرائم السيبرانية : دراسة تأصيلية مقارنة"، مجلة الإجتهد للدراسات القانونية والإقتصادية، المجلد 09، العدد 03، جامعة تلمسان، 2020، ص 148.

وجذور الكلمة الإنجليزية (cyber) متأصل في كثير من الكلمات التي يشيع استخدامها في مجال تكنولوجيا المعلومات والاتصالات مثل: الفضاء السيبراني cyber space والخيال العلمي السيبراني cyber punk، ويشير قاموس "المورد" إلى السيبرانية بأنها علم الضبط ومصدرها (cybernetics)، أي ضبط الأشياء عن بعد والسيطرة عليها.<sup>1</sup>

#### ثانيا: تعريف الأمن السيبراني اصطلاحا:

هناك العديد من التعاريف التي قدمت لمفهوم الأمن السيبراني أهمها:

- إذ عرفه إدوارد أمورسو "Amoroso": بأنه وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل والأدوات المستخدمة في مواجهة القرصنة والكشف الفيروسات ووقفها، وتوفير الاتصالات المشفرة.<sup>2</sup>

- وقام بتعريفه كل من Lehto Martit و Makipkka Neittaan بإعتباره مجموعة من الإجراءات التي تتخذ في الدفاع ضد هجمات قرصنة الكمبيوتر وعواقبها، ويتضمن تنفيذ التدابير المضادة المطلوبة.<sup>3</sup>

ومن هنا يتضح أن الأمن السيبراني يعد آلية حديثة وإجراء هدفه التصدي ضد أي هجوم موجه للأجهزة الإلكترونية، وذلك لضمان وتوفير الحماية اللازمة، حيث قدمت وزارة الدفاع الأمريكية "البينتاغون" أيضا تعريفا دقيقا لمصطلح الأمن السيبراني فاعتبرته جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية والإلكترونية من مختلف الجرائم: الهجمات، التخريب، التجسس والحوادث.<sup>4</sup>

<sup>1</sup> - لبنى خميس مهدي، صفاء تغريد، أثر السيبرانية في تطور القوة، مجلة حمورابي، المجلد 8، العدد 33-34، العراق، 2020، ص 148.

<sup>2</sup> - فارس محمد العمارات، ابراهيم الحمامصة، الأمن السيبراني: المفهوم وتحديات العصر، ط1، دار الخليج للنشر والتوزيع، الأردن، عمان، 2022، ص 15.

<sup>3</sup> - المرجع نفسه، ص 15.

<sup>4</sup> - سعيد محمودي، "الأمن السيبراني في الجزائر: بين المعالجة الأمنية والحماية القانونية"، مجلة الناقد للدراسات السياسية، المجلد 7، العدد 2، جامعة بشار، الجزائر، 31 أكتوبر 2023، ص 197.

أما وفق الاتحاد الدولي للاتصالات فإن الأمن السيبراني هو مجموعة من المهمات المتمثلة في جميع الوسائل والسياسات والإجراءات الأمنية، والمبادئ التوجيهية، والمقاربات الخاصة بإدارة المخاطر ومختلف التدريبات والممارسات الفضلى، والتقنيات الممكن استخدامها لحماية البيئة السيبرانية (الرقمية)، وموجودات المؤسسات والمستخدمين.<sup>1</sup>

إضافة إلى ذلك قدم المشرع الجزائري تعريفا للأمن السيبراني في القانون 18-04 الصادر سنة 2018، على أنه: مجموع الأدوات والسياسات، ومفاهيم الأمن والآليات الأمنية والمبادئ التوجيهية، وطرق تسيير المخاطر والأعمال والتكوين والممارسات الجيدة والضمانات والتكنولوجيات التي يمكن استخدامها في حماية الاتصالات الإلكترونية ضد أي حدث من شأنه المساس بتوفر وسلامة وسرية البيانات المخزنة أو المعالجة أو المرسل.<sup>2</sup>

### الفرع الثالث: المفاهيم المرتبطة بالأمن السيبراني

**1- الفضاء السيبراني cyber space:** هو عبارة عن مجال رقمي يضم مكونات رقمية وغير مادية، نظرا لكونه يشمل مجموع الأجهزة وأنظمة الشبكات، والبرامج والمستخدمين المشغلين والمستعملين. ويمكن اعتباره امتدادا للذراع الرابعة للجيش الحديثة.<sup>3</sup> إذ عرفته الوكالة الفرنسية لأمن نظم المعلومات على أنه: "فضاء التواصل المشكل من خلال الربط البيئي العالمي لمعدات المعالجة الآلية للمعطيات الرقمية".<sup>4</sup>

<sup>1</sup> - منى الأشقر جبور، "السيبرانية هاجس العصر"، المركز العربي للبحوث القانونية والقضائية، بيروت، لبنان، 2017، ص 26.

<sup>2</sup> - القانون 18-04 المؤرخ في 10 ماي 2018، المتعلق بالقواعد المتعلقة بالبريد والاتصالات الإلكترونية، ج. ر. ج. ج. العدد 27، الصادر في 31 ماي 2018.

<sup>3</sup> - اسلام مصطفى، جمعة مصطفى، "جريمة اختراق الأمن السيبراني وحماية استخدام البيانات والمعلومات في القانون المصري"، المجلة القانونية، 12، العدد 03 جامعة القاهرة، 2022، ص 724.

<sup>4</sup> - علاء الدين فرحات، الفضاء السيبراني: "تشكيل ساحة المعركة في القرن الحادي والعشرين"، مجلة العلوم القانونية والسياسية، المجلد 10، العدد 03، ديسمبر 2019، ص 90.

**2- التهديد السيبراني:** هو نشاط إلكتروني ضار ينشأ عبر الفضاء الرقمي، ويهدف إلى الإخلال بأمن أنظمة الحاسوب والهواتف الذكية والأجهزة المتصلة بالشبكات المعلوماتية.

وقد يصدر هذا التهديد عن أفراد، أو دول، أو جماعات وتنظيمات تسعى إلى تحقيق أهداف سياسية أو استراتيجية.<sup>1</sup>

**3- الردع السيبراني:** يعرف على أنه منع الأعمال الضارة ضد الأصول الوطنية في الفضاء الرقمي، والأصول التي تدعم العمليات الفضائية.<sup>2</sup>

ويقصد من خلال هذا المفهوم أن الردع السيبراني هو اتخاذ تدابير وإجراءات تهدف إلى منع أو تقليل الهجمات الإلكترونية التي تستهدف الأصول الوطنية أو البنى التحتية الرقمية وذلك من أجل التصدي إلى أي تهديد في الفضاء السيبراني.

**4- القوة السيبرانية:** يعد جوزيف ناي من أبرز المهتمين بالقوة السيبرانية حيث يعرفها بأنها: "القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء السيبراني، أي أنها القدرة على استخدام الفضاء السيبراني لإيجاد مزايا للدولة والتأثير على الأحداث المتعلقة بالبيئات التشغيلية الأخرى، وذلك عبر أدوات سيبرانية."<sup>3</sup>

**5- الهجمات السيبرانية:** هي أي فعل يفوض من قدرات ووظائف شبكة الكمبيوتر لهدف شخصي أو سياسي، وذلك استغلالاً لنقطة ضعف معينة يتمكن من خلالها المهاجم من التلاعب بالنظام.<sup>4</sup>

<sup>1</sup> - ساعد بوقرص، الأمن السيبراني "مخاطر وتحديات وتحديات تتطلب ممارسات وتوصيات واستراتيجيات خاصة"، مجلة الأبحاث

في الحماية الاجتماعية، المجلد 03، العدد 01، الجزائر 2022، ص 65.

<sup>2</sup> - اسلام مصطفى، جمعه مصطفى، المرجع سابق، ص 725.

<sup>3</sup> - فارس محمد العمارات، إبراهيم الحمامصة، المرجع السابق، ص 22.

<sup>4</sup> - المرجع نفسه، ص 21

**6- خدمات الأمن السيبراني:** تعرف بأنها مجموع الأنشطة ذات الطابع الفني والإداري والاستشاري التي تمارس في مجال الأمن السيبراني، وتشمل على وجه الخصوص خدمات التقييم الأمني، المراقبة، التدقيق والخدمات الاستشارية.<sup>1</sup>

**7- الإرهاب السيبراني:** يقصد به كل فعل أو هجوم يرتكب عبر الوسائط الإلكترونية أو ضمن الفضاء السيبراني، يكون من شأنه تهديد الدول أو الحكومات أو الاعتداء عليها بقصد تحقيق أهداف ذات طابع سياسي أو ديني أو أيديولوجي، وأن الهجمة يجب أن تكون ذات أثر جسيم ذو طبيعة تدميرية أو تخريبية يعادل للأفعال المادية المكونة لجريمة الإرهاب.<sup>2</sup>

**8- عمليات الأمن السيبراني:** هي مجموعة من الإجراءات المرتبطة بإدارة ومراقبة واكتشاف حوادث الأمن السيبراني والتهديدات التي تقع ضمن حيز الفضاء السيبراني ووضع خطط لها وتنفيذها.<sup>3</sup>

**9- الحرب السيبرانية:** تعرف بأنها هجوم متعمد وسلوك عدائي غير مشروع يرتكب عبر الوسائل الإلكترونية بقصد المساس بسلامة أنظمة الحاسوب وشبكات الاتصالات والبيانات الرقمية، من خلال تعطيل وظائفها أو الإخلال بها والتلاعب بمحتواها أو اتلافها.<sup>4</sup>

---

<sup>1</sup> - منى عبد الله السمحان، "متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية"، مجلة كلية التربية، العدد 111، جامعة المنصورة، مصر، 2020، ص 11.

<sup>2</sup> - محمد كمال، الإرهاب السيبراني، ط1، دار كلیم للطباعة والنشر والتوزيع، القاهرة، مصر، 2022، ص12.

<sup>3</sup> - كريمة صمودي، سمر برقي، الأمن السيبراني في الجزائر، مذكرة ماستر في قانون أعمال، كلية الحقوق والعلوم السياسية، جامعة 08 ماي 1945، قالمة، الجزائر، 2024-2025، ص 13.

<sup>4</sup> - شادي عبد الوهاب منصور، حروب الجيل الخامس: أساليب التحفيز من الداخل على الساحة الدولية، ط1، العربي للنشر والتوزيع، القاهرة، مصر، 2019، ص99.

### المطلب الثاني: مجالات الأمن السيبراني وأهميته

إن التهديدات الرقمية المتزايدة في الفضاء الإلكتروني، نجدها تلمس مختلف المجالات، منها السياسية، والعسكرية، والاقتصادية، والاجتماعية، وهو الأمر الذي جعل ضرورة ملحة لما له من توفير الحماية القانونية وتعزيز أمن البيئة الرقمية، وكذلك على مختلف أنواع الأمن الرقمي، وانطلاقاً من ذلك سنتطرق في هذا المطلب إلى ما يأتي: الفرع الأول: مجالات الأمن السيبراني، والفرع الثاني: أهمية الأمن السيبراني.

### الفرع الأول: مجالات الأمن السيبراني

يشمل الأمن السيبراني أنواعاً وأبعاداً متعددة، حيث أنها تهدف إلى حماية الأنظمة والبيانات باعتبارها تقوم على الجمع بين الجوانب التقنية، والقانونية والبشرية، وذلك لضمان سرية المعلومات وسلامتها وتوافرها، في مواجهة هذا النوع من التهديدات الرقمية.

### أولاً: أنواع الأمن السيبراني

إن الأمن الرقمي يتناول مختلف الأصناف، وذلك تبعاً لتنوع الاعتداءات الرقمية التي تستهدف كل صنف، ومن أهمها:

أ/ **أسلوب التعافي:** يطبق هذا المفهوم باعتبار أن آلياته تختلف وتتغير حسب نشاط المؤسسات والشركات، وعلى هذا الأساس فإنه يتم من خلاله إعداد برنامج منظم يهدف إلى استرجاع تطبيق الخدمات بصورة تدريجية، إذ يضمن استمرار أداء المهام لمستعملي الخدمة، وعليه فإن هذا التوجه يقوم على تنظيم سير العمليات التي تكون بعد الاضرار أو الاضطرابات باعتبارها تلمس ضوابط المعطيات، وذلك ضمن إعادة النظر في العودة إلى الوضع الطبيعي وهذا طبقاً لحالات الخطيرة الرقمية.<sup>1</sup>

<sup>1</sup> - علي بن طراز، "الأمن السيبراني: المدلول والمهامة"، مجلة البحوث والدراسات المعاصرة، المجلد 02، العدد 01، مديرية الخدمات الجامعية، قالمة، 2024، ص ص 65-66

ب/ أمن الهاتف المحمول: يعتبر الدخول الغير مرخص له من أحد أبرز الاعتداءات التي تمس أمن المعلومات، وبطبيعة الحال فإنه يتيح لأشخاص غير مخولين من امكانية الدخول إلى المعطيات، وهو ما يفرض ضرورة تعزيز آليات الحماية، حيث تجدر الإشارة إلى أن الأجهزة الذكية باعتبارها تواجه مجموعة من المخاطر المتنوعة، من أهمها البرمجيات الخبيثة التي تؤدي إلى تسريب المعطيات أو إتلافها، بالإضافة إلى احتمالية إضاعة الجهاز أو تم نهبه، وفي مقابل ذلك فإنه يترتب عنه وصول الغير مشروع إلى المعطيات المخزنة وفي هذا السياق نفسه، فإنه لا بد من حماية المعطيات ذات الطابع الشخصي والنظامي في مجال الأمن السيبراني، نظرا للأجهزة الذكية باعتبارها جزءا منه في حين تشكل البرامج الخطيرة تهديدا مباشرا للشركات من خلال قدرتها على التجسس أو سرقة المعلومات أو التسبب في إتلافها.<sup>1</sup>

ج/ الأمن التشغيلي: إن هذا الأمن يقوم على فهم الاعتداءات وتحليل الثغرات من أجل تحديد نقاط الضعف والتعامل معها بطريقة وقائية، كما يعتمد على تنظيم طريقة تسيير الأنظمة، وتحديد صلاحيات الولوج بشكل محدود للعاملين، بالإضافة استخدام وسائل الحماية مثل: المصادقة الثنائية والمراقبة المستمرة، وعلى هذا النحو فإنه يهدف إلى حماية المعلومات الحساسة من أي اعتداء، وذلك من خلال رفع مستوى الانتباه، والتفكير في أساليب الهجوم المحتملة.<sup>2</sup>

د/ أمن المعلومات والبيانات: إن هذا الأمن يقوم بمتابعة السلوكيات ذات الطابع الضار، مع الحرص على تأمين القرائن عند الضرورة، بالإضافة إلى معالجة التهديدات المحتملة والتدخل في حالة وقوع الحوادث. وعلى هذا الأساس فإنه يفهم على أنه يشكل منظومة من التدابير التقنية والتنظيمية التي تعتمد بغرض تقييد الوصول إلى الأنظمة حصرا على الجهات المخولة، وذلك وفق ضوابط واجراءات المعمول بها، لضمان حماية المعلومات من الاطلاع او التغيير الغير المصرح به، وتوفيرها عند الحاجة وذلك من خلال حمايتها من أي الإيقاف أو تلف قد يطالها.<sup>3</sup>

<sup>1</sup> خولة مسراقي، "محاضرات في الهجمات السيبرانية وأمن المعلومات"، مقياس اليقظة الرقمية، أقيمت على طلبة السنة أولى ماستر،

قسم علوم التسيير، كلية الحقوق والعلوم السياسية، جامعة بليدة 2 لونيبي علي، 2024-2025، ص 50

<sup>2</sup> - المرجع نفسه، ص 50

<sup>3</sup> - علي بن طراز، المرجع السابق، ص 66.

هـ/ أمن البنية التحتية: يعد هذا التأمين من الالتزامات التي تفرض على المؤسسات من خلال اعتماد تدابير والإجراءات الوقائية اللازمة. بما يضمن عدم تعرض أنظمتها لأي اعتداء تكون غير مشروعة من قبل المعتدين. وعليه يعرف الأمن باعتباره جانبا تقنيا ذا صلة بالمعطيات، حيث يهدف إلى الحد من الاعتداءات التي تكون ناجمة ضده، وعليه لابد من وضع اجراءات ووسائل تسعى إلى حماية الأنظمة الحيوية، بما في ذلك مقرات المعطيات والأنظمة من أي تهديد.<sup>1</sup>

و/ أمن التطبيقات: يساهم الأمن السيبراني من خلال اعتماد مجموعة من الوسائل التقنية كجدار الحماية، وبرامج التصدي لتهديدات ضارة، بالإضافة إلى تقنيات التأمين في المعطيات التي تكون سرية، وفي هذا الإطار، تعزز وظيفته الأساسية المتمثلة في الحد من أضرار الهجمات الإلكترونية المحتملة. لذلك فإنها تستهدف كيانات بما يضمن رفع مستوى الحماية والوقاية المعلوماتية. وعليه فإن هذه البرامج تكون معرضة لمخاطر الاعتداءات الرقمية، نظرا لكونها متصلة بالبيئة الرقمية.<sup>2</sup>

### ثانيا: أبعاد الأمن السيبراني:

إن الأمن السيبراني لا يكفي فقط بحماية الأجهزة والتطبيقات، بل تمتد هذه الحماية لتشمل: الدولة، والمجتمع، والاقتصاد، والقانون، ومن أبرز أبعاد الأمن السيبراني المتمثل كآلي:  
أ/ الأبعاد الاقتصادية: لقد أدى استعمال الحاسوب والشبكة المعلوماتية إلى تقدم وسائل الإنتاج، وعليه فإنه أسهم في تنشيط الحركة ذات الطابع الاقتصادي، ومعاينة مختلف التعاملات الإنتاجية والاقتصادية، لذلك برزت الحاجة إلى ضرورة تحقيق الأمن الفضائي، وذلك لضمان سلامة البيانات. وقد أصبح من المسلم به أن المعطيات ووسائل التقنية تعتبر عنصرا من العناصر المحورية التي تعد قاعدة مرتكز عليها هذا التطور الاقتصادي، كما أصبح هذا المجال الرقمي محفزا لمختلف مجالات الوسط الاجتماعي، ومن هذا المنطلق، جاءت المعرفة من أهم عوامل دعم الاقتصاد والتطور الإنتاجي، وهو ما نجم عنه مؤخرا تزايد الاعتماد على الإنتاج الرقمي والسيطرة عليه من قبل الفاعلين في المجال الإنتاجي.<sup>3</sup>

1 - خولة مسراتي، المرجع السابق، 49

2 - علي بن طراز، المرجع السابق، ص 65.

3 - حمزة لعباشي، محمد الأمين قعفر، الأمن السيبراني وحماية البيانات الرقمية في الجزائر، مذكرة ماستر، في قانون الإعلام الآلي وأنترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي - برج بوعرييج، الجزائر، 2023-2024، ص 23.

ب/ الأبعاد العسكرية: يؤدي إيقاف أجهزة الحماية والرقابة الرقمية إلى عرقلة قدرتها على التحكم في التشكيلات العسكرية، وعلى هذا الأساس فإنها تعتبر خطرا خاصة إذا كانت هذه الشبكات الرقمية المستعملة غير مصونة من أي اقتحام أو من جهة تكون غير خارجية، ومن بين هذه الاعتداءات ما يمس بالأمن الدفاعي للأمم، إضافة إلى إيقاف امكانية الدولة على التوزيع الفوري لقدراتها وقواتها، أو العمل على وقف وسائل التواصل بين العناصر الدفاعية والشبكات الحاسوبية، وعلاوة على ذلك تمتلك السلطة السيبرانية امكانية ربط العناصر العسكرية ببعضها، وذلك عبر الشبكات الدفاعية في ظل البيئة الرقمية، مع نقل توجيهات دفاعية وتسيير المساعي عن بعد، غير أن هذه الأنظمة قد تستعرض بدورها إلى التعطيل أو اتلافها.<sup>1</sup>

ج/ الأبعاد القانونية: إن الجريمة الرقمية تتجاوز النطاق الوطني، وهو الأمر الذي يتطلب فرض ضرورة تفعيل التعاون والدعم الدولي، وذلك للتصدي لها، ويرجع ذلك إلى الطبيعة الخاصة لهذه الأفعال الإجرامية، نظرا لعسر اشكالية تحديد فاعلو هذه السلوكيات، فضلا عن التطور المستمر للمفاهيم التي تكون هذه الأخيرة متصلة بتقنيات المعطيات، ومن جهة أخرى لاتزال بعض التشريعات تعاني قصور في وضع أحكام صارمة تتلاءم مع الجرائم الرقمية، ويرجع هذا لكون أن وسائل التقنية والتشريع علاقة متبادلة، تسعى من خلالها القواعد التشريعية إلى التأقلم مع التطورات المتسارعة، وذلك عن طريق وضع منظومة تشريعية تنظم الأفعال المصرح بها، حيث تجرم التصرفات الغير مشروعة.<sup>2</sup>

1 - فتيحة بوعلام، الأمن السيبراني في الجزائر، مذكرة ماستر في قانون خاص، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، 22 جوان 2020، ص ص 39-40.

2 - سليمان قطاف، عبد الحليم بوقرين، "الأمن السيبراني والمضامين المفاهيمية المرتبطة به"، مجلة وطنية للدراسات العلمية الأكاديمية، المجلد 05، العدد 02، جامعة الأغواط، الجزائر، 2022، ص 47.

د/ الأبعاد الاجتماعية: إن الضرورة تكمن في إتاحة التعلم والتدريب، وذلك في المجال التقني المرتبط بالمراسلات والبيانات، ولا يقتصر ذلك فقط على الإجراءات الأمنية والردعية فحسب، بل يستوجب الأمر ترسيخ الوعي الأمني ضمن الثقافات التكنولوجية المعلوماتية، إلى جانب تنمية سلوكيات منظمة وآمنة لدى الأفراد في البيئة الرقمية، وبالتالي فإنه يتم الموافقة عليها والالتزام بها من طرف جميع العاملين في النطاق الرقمي. كما يعد نشر الوعي بين مختلف الأطراف عبر المنصات والبيانات الدولية، عنصرا أساسيا في تعزيز الإدراك السليم لأساليب الوقاية، ومن بين هذه الإجراءات الوقائية الداعمة لرفع مستوى الأمن الرقمي، تحرر بدقة دون غموض، مع حسن تدبيرها لتغطية مختلف العوائق والتهديدات ذات الطابع الأمني الوقائي والردعي، وعليه فإنه يفرض على المجتمع المعطيات تبني مبادرات في مجال الإعلام والتربية المدنية، وذلك بهدف توعية المواطنين وتبصيرهم بواجباتهم الوقائية، بالإضافة إلى تعزيز الالتزام الشخصي بالإجراءات الدفاعية، فضلا عن بيان الآثار الجزائية المترتبة عن عدم احترام التعهدات الأمنية المقررة.<sup>1</sup>

### الفرع الثاني: أهمية الأمن السيبراني

للاأمن السيبراني أهمية كبيرة في كافة المجالات تتمثل فيما يلي:

- الحفاظ على المعلومات وسلامتها وتجانسها وذلك بكف الأيدي من العبث بها.<sup>2</sup>
- تعزيز حماية أنظمة تقنية المعلومات لتكون المرجع الوطني في شؤون تخصصها، تهدف إلى حماية مصالح الوطن الحيوية وأمنه والبنى التحتية الحساسة فيه، ومراعاة الأهمية الحيوية المتزايدة لتخصصه.
- استكشاف نقاط الضعف والثغرات في الأنظمة ومعالجتها.
- ضمان توافر استمرارية عمل نظم المعلومات.<sup>3</sup>

<sup>1</sup> - سليمان قطاف، عبد الحليم بوقرين، المرجع السابق، ص 47

<sup>2</sup> - فارس محمد العمارات، ابراهيم محمد الحمامصة، المرجع السابق، ص 35-36

<sup>3</sup> - حمزة لعباشي، محمد الأمين قعفر، المرجع السابق، ص ص 19-20

- يساهم في تعزيز إنتاجية المؤسسات والأفراد من خلال فحص الفيروسات وتفعيل جدران الحماية، والقيام بالنسخ الاحتياطية بمخاطر الاختيار عن طريق البريد الإلكتروني والروابط المشبوهة.
- الحفاظ على سلامة عمل قطاعات الدولة الإلكترونية من أي اختراق.<sup>1</sup>

---

<sup>1</sup> - شيماء مساط، عائشة بوطيبة، تأثير الجريمة الإلكترونية على الأمن السيبراني في الجزائر، مذكرة ماستر في قانون جنائي، معهد الحقوق، المركز الجامعي عبد الحفيظ بوصوف ميلة، 2024-2025، ص46.

## المبحث الثاني: الجرائم السيبرانية ودوافع ارتكابها

إن وسائل التقنية المعاصرة أصبحت معيارا جوهريا، وذلك في مختلف المجالات، وبالرغم من مزاياها المتعددة، إلا أن لها جانبا سلبيا يتمثل في انتشار السلوكيات الإجرامية المرتبطة بها، وهو الأمر الذي أدى إلى بروز ما يعرف بالجريمة السيبرانية، وعليه فإن هذه الجريمة ترتبط ارتباطا وثيقا بالتكنولوجيا الحديثة، ومن هذا المنطلق، لقد اختلف الفقهاء فيما بينهم حول وضع مفهوم دقيق وموحد للجريمة الرقمية.

حيث تعد هذه الجريمة من الجرائم العابرة للحدود الوطنية، وذلك بالنظر إلى طبيعتها وسماحتها، فضلا عن تعدد صورها وأسباب ارتكابها.

وعليه سنتناول هذا المبحث فيما يلي:

### المطلب الأول: مفهوم الجريمة السيبرانية

تعد الجريمة الرقمية من المفاهيم الحديثة المرتبطة بالتطور التقني، لذا فإن الفقه اختلفوا فيما بينهم حول وضع تعريف موحد لها، نظرا لتعدد صورها وأساليب ارتكابها، ولإحاطة بهذا المفهوم سيتم التطرق إلى الفرع الأول: تعريف الجريمة السيبرانية الفرع الثاني: خصائص الجريمة السيبرانية الفرع الثالث: أركان الجريمة السيبرانية.

### الفرع الأول: تعريف الجريمة السيبرانية

"نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة على الحساب والتي تحول عن طريقه"<sup>1</sup>

"كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية، ينشأ عنه خسارة تلحق بالمجني عليه أو كسب يحققه الجاني".<sup>2</sup>

<sup>1</sup> - سليمة سعيدي، بلال حجاز، جرائم المعلومات والشبكات في العصر الرقمي، ط1، دار الفكر الجامعي، الإسكندرية، مصر، 2017، ص ص 55-56.

<sup>2</sup> - حنان مهداوي، "التنظيم القانوني للجريمة الإلكترونية في التشريع الجزائري"، مجلة الفكر القانوني والسياسي، المجلد 06، العدد 02، كلية الحقوق والعلوم السياسية، جامعة محمد لمين دباغين، سطيف، 2022، ص ص 1060-1061.

## التعريف القانوني للجريمة الإلكترونية:

بالنظر إلى صعوبة المجال الرقمي وتعقيده، واستحالة ضبطه ضمن تعريف ثابت ودقيق لأنظمة المعلوماتية، على هذا الأساس نجد أن بعض القوانين قد وضعت تعريفا خاصا بالنظام المعلوماتي من الناحية القانونية. وعليه عسر تحديد المقصود بأنظمة البيانات التلقائية تشريعا، فقد فوض المشرعون مهمة ذلك إلى الفقه والقضاء.<sup>1</sup>

القانون الجزائري: المادة 02 من القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال و مكافحتها : "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو بنظام الاتصالات الإلكترونية". "على خلاف المشرع الفرنسي الذي لم يعطي تعريفا للجريمة الإلكترونية"<sup>2</sup>

### أولا: الاتجاه الضيق من تعريف الجريمة الإلكترونية.

عرف أنصار الاتجاه الضيق الجريمة الإلكترونية بأنها: "كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازم لارتكابه من ناحية، ملاحقة تحقيقه من ناحية أخرى"، ومن بين التعريفات أيضا تعريف الفقيه Merwe الجريمة المعلوماتية هي: "الفعل الغير المشروع الذي يتورط في ارتكابه الحاسب الآلي أو هو الفعل الإجرامي الذي يستخدم في اقتوافه الحاسب الآلي كأداة رئيسية"<sup>3</sup> وعرفها Rosen Blat بأنها: "كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف، أو الوصول إلى المعلومات المخزنة داخل الحاسب، والتي تحول عن طريقه"<sup>4</sup>

1 - راضية عيمور، "الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري"، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد 06، العدد 01، جامعة الأغواط، 2022، ص ص 92-93.

2 - اسمهان بوضياف، "الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 11، جامعة محمد بوضياف-المسيلة، سبتمبر 2018، ص 352.

3 - وهيبه سالمى، "الجريمة الإلكترونية: دراسة في المفهوم والمظاهر"، مجلة قضايا معرفية، المجلد 02، العدد 03، جامعة الجلفة، سبتمبر 2022، ص 317.

4 - مونة مقلاتي، راضية مشري، "الجريمة الإلكترونية دلالة المفهوم وفعالية المعالجة القانونية"، مجلة أبحاث قانونية وسياسية، المجلد 06، العدد 01، جامعة 08 ماي 1945، جوان 2021، ص 493.

وعليه فإن جانب آخر يشترط لقيام الجريمة الرقمية أن ينصب محل الاعتداء على الأجهزة الإلكترونية أو نظم البيانات ذاتها، بحيث يكون الفعل الإجرامي موجها مباشرة إلى الأنظمة المعلوماتية، وبناء على ذلك يضيق هذا الاتجاه من نطاق الجريمة الرقمية، إذ لا يمتد إلى كل سلوك تستعمل فيه الحاسوب أو الوسائل الإلكترونية لتحقيق الفعل الغير مشروع، وإنما يقتصر هذا الاعتداء المباشر على هذه الأنظمة.

وعليه تم تعريف هذه الجريمة على أنها، "نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي أو تلك التي يتم تحويلها عن طريقه".<sup>1</sup>

### ثانيا: الاتجاه الموسع من تعريف الجريمة الإلكترونية

على عكس الاتجاه السابق يرى فريق آخر من الفقهاء<sup>2</sup> "خبراء منظمة التعاون الاقتصادي والتنمية بأنها كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها".<sup>3</sup>

"وأیضا كل استخدام في صورة فعل أو امتناع من شأنه الاعتداء على أي مصلحة مشروعة، سواء كانت مادية أو معنوية، يكون ناتج بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية ومعاقب عليها قانونا أيا كان غرض الجاني".<sup>4</sup>

<sup>1</sup> - سفيان سوير، محمد بن عمار، جرائم معلوماتية، رسالة ماجستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بالقائد، تلمسان، ص13.

<sup>2</sup> - موني مقلاتي، محمد بن عمار، المرجع سابق، ص 449.

<sup>3</sup> - سليمة سعیدی، بلال حجاز، المرجع السابق، ص56.

<sup>4</sup> - عماد دمان ذبيح، سمیه بھلول، "الآليات العقابية لمكافحة الجريمة الإلكترونية في التشريع الجزائري"، العدد13، جامعة عباس لغرور خنشلة، جامعة محمد لمين دباغين سطيف2، جانفي 2020، ص140.

## الفرع الثاني : خصائص الجريمة السيبرانية

إن الجريمة السيبرانية تختلف عن الجرائم التقليدية ، كونها ترتكب بوسائط إلكترونية وأنظمة معلوماتية، وذلك بالنظر إلى طبيعتها التقنية المرتبطة باستخدام الحواسيب والشبكات الرقمية. كما تتسم هذه الجريمة بالطابع العابر للحدود الإقليمية اثر سرعة تطبيقها، مع امكانية امتداد آثارها إلى نطاق جغرافي واسع، وهو الأمر الذي يعقد اجراءات اكتشافها وبالتالي يصعب تحديد هوية مرتكبيها وملاحقتهم. حيث يقتضي ارتكاب هذا النوع من الجرائم توافر قدر من المهارات والخبرات التقنية لدى الجاني، بما يمكنه من استغلال الوسائل المعلوماتية والتكنولوجية في تحقيق هذا الفعل الغير مشروع. وانطلاقا من ذلك، سيتم التطرق إلى أبرز خصائص الجريمة السيبرانية والمتمثلة فيما يلي:

### أولا: عالمية الانتشار(عابرة للدول)

إن التطور الرقمي لم يعد يشكل عائق أمام المجرمين ، بل أصبح وسيلة تمكنهم من ارتكاب أفعالهم الغير المشروعة عن بعد، وذلك دون الحاجة إلى التواجد المادي في مكان وقوع الجريمة. وعليه فقد تمتد آثار هذه الأفعال إلى عدة دول. ومن هذا المنطلق، يرجع ذلك إلى الانتشار الواسع للتقنيات الحديثة وشبكات المراسلات، التي سهلت بدورها في انتقال هذه السلوكيات المخالفة للقانون بين مختلف الدول، وهو الأمر الذي يؤكد أن هذا النوع من الجرائم لا تخضع للحدود الإقليمية التقليدية.<sup>1</sup>

### ثانيا: الجريمة الإلكترونية جريمة مستحدثة

لقد شهد الكون خلال الفترات الضئيلة الفائتة، تطورا تكنولوجيا متسارعا، مما جعل منه فضاءا مرتبطا أشبه بقرية صغيرة، وهو ما ساهم في بروز الجرائم الرقمية باعتبارها من الجرائم الحديثة التي تكون مرتبطة بالتطور التقني وعليه، فقد تجاوز هذا التطور قدرات أجهزة الضبط والآليات التقليدية المعتمدة في مكافحتها، وهو الأمر الذي أثر على فعالية التدخلات التشريعية والأمنية، جعل هذه الجرائم تشكل تهديدا حقيقيا لأمن الدول وسلامة الأفراد، وعلى هذا الأساس، أصبحت الجرائم الرقمية من أخطر صور الإجرام المعاصر خاصة في ظل الانفتاح العالمي والتوسع المستمر في استخدام الوسائل التكنولوجية.<sup>2</sup>

<sup>1</sup> -خضار فايذة، محاضرات في " مفهوم الجريمة المعلوماتية"، 2024، ص14.

<sup>2</sup> -ابتسام بوبعابة، التحقيق في الجريمة الإلكترونية، مذكرة ماستر في قانون الإعلام الآلي والأنترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعرييج، ص18.

### ثالثا: صعوبة اكتشاف وإثبات الجريمة السيبرانية

تتميز الجريمة الرقمية بأنها ترتكب ضمن بيئة رقمية، وفي الغالب لا تخلف آثار مادية واضحة، وعليه يمكن معاينتها مباشرة بعد ارتكابها. كما أن ما قد ينشأ عنه آثار رقمية يظل عرضة للزوال أو التغيير، وهو الأمر الذي يجعل عملية الحفاظ عليها وإثباتها من الناحية التقنية مسألة دقيقة ومعقدة، كونها تتطلب وسائل متخصصة.<sup>1</sup> كما يرجع ضعف التبليغ عن الجرائم الرقمية إلى خوف كثير من الأشخاص، وذلك إلى التعرض للتشهير أو المساس بسمعتهم، وهو ما يجعلهم يترددون في الإبلاغ عنها رغم وقوعها.<sup>2</sup> لذلك فإن التطور التكنولوجي المتسارع أدى إلى بروز أنماط إجرامية مستحدثة لم تكن معروفة سابقا، وهو الأمر الذي كشف محدودية القواعد التشريعية التقليدية رغم كفايتها لمواجهة هذا النوع من الجرائم، لاسيما في ظل عجزها عن مسايرة التحولات التقنية المتلاحقة، وأيضا أساليب إرتكاب هذه الجريمة المتطورة.<sup>3</sup>

### رابعا: وقوعها في بيئة المعالج الآلية للمعطيات

إن الجريمة المعلوماتية المتعلقة بالاعتداء على نظام المعالجة الآلية للبيانات تقوم متى وقع عليها الفعل وذلك أثناء معالجة المعطيات والبيانات داخل النظام المعلوماتي، باعتبار أن هذا الشرط يعد أساسا لقيام أركانها القانونية، أما من ناحية عدم توافره، فإن وصف الجريمة المعلوماتية ينتفي لعدم اكتمال عناصرها.<sup>4</sup>

1 - سليم مزبود، "الجرائم المعلوماتية واقعها في الجزائر وآلية مكافحتها"، المجلة الجزائرية للإقتصاد والمالية، العدد 1، جامعة المدية، أفريل 2014، ص ص 97-98.

2 - عائشة عبد الحميد، "الجرائم المعلوماتية وكيفية مكافحتها"، مجلة الإناسة وعلوم المجتمع، العدد 07، جامعة الشاذلي بن جديد الطارف، الجزائر، جويلية 2020، ص 130.

3 - مليكة بقاح، اشكالية الجرائم الإلكترونية في التشريع الجزائري، رسالة دكتوراه في علوم الإعلام والاتصال، كلية علوم الإعلام والاتصال، جامعة الجزائر 3، ص 25.

4 - ريمة بن عميروش، "عن خصوصية الجريمة المعلوماتية"، مجلة الفقه القانوني والسياسي، المجلد 2، العدد 2، جامعة محمد الصديق بن يحيى، جيجل، أكتوبر 2024، ص 79.

### الفرع الثالث: أركان الجريمة السيبرانية

إن الجريمة الرقمية تتحقق بتوافر الركن الشرعي، والركن المادي، والركن المعنوي، وعليه سنتناول في هذا الفرع أبرز أركان الجريمة الرقمية على النحو التالي:

#### أولاً: الركن الشرعي(القانوني)

يعد الركن الشرعي للجريمة السند القانوني الذي يحدد القواعد الجزائية، وذلك من حيث تحديد الأفعال المجرمة، مع بيان العقوبات المقررة لها، باعتباره الإطار الجوهري الذي تبنى عليه أي جريمة. أما فيما يخص الجريمة الإلكترونية فإن هذا الركن يخضع بدوره لمبدأ الشرعية الجزائية، وعليه فإنه يستند أساساً ابتداءً من المادة الأولى لا ادانته إلا بمقتضى قانون صادر قبل ارتكاب الفعل المجرم من المادة الأولى من قانون العقوبات وعليه لا جريمة ولا عقوبة ولا تدبير أمن بغير قانون<sup>1</sup>، وبالتالي فإن القاضي الجنائي لا يجوز له إلحاق فعل غير قانوني بفعل آخر غير مشروع لمجرد وجود تشابه بينهما وعليه فإنه لا ينشئ للقاضي تجريمًا خارج حدود النص وعلى هذا الأساس فإن المشرع في مجال التجريم يقوم على مبدأ قانون عقابي وهو الأمر الذي يقتضي عدم امكانية ايقاع العقاب إلا على الأفعال التي ورد بشأنها النص القانوني الصريح دون سواه.<sup>2</sup>

#### ثانياً: الركن المادي للجريمة المعلوماتية

إن هذا الركن يترتب عنه حدوث اعتداءات على الالتزامات ضمن نطاق الحماية التي يقررها القانون وعليه فإن هذا النشاط يصدر عن شخص يتمتع بالإدراك سواء تمثل في امتناع سلبى أو فعل ايجابي، حيث تم تصنيف هذه الجريمة إلى ركائز منها السلوك الإجرامي والعلاقة السببية بين الفعل والنتيجة وهذا راجع إلى تصنيف الدكتور فرح رضا في تجزئة هذه الأفعال.<sup>3</sup>

<sup>1</sup> - حسام بن ميسا، عبد المولى حملاوي، آليات مكافحة الجريمة الإلكترونية في التشريع الجزائري، رسالة ماستر في القانون الجنائي، قسم الحقوق، المركز الجامعي، عبد الحفيظ بوالصوف - ميلة، 2014، ص ص 19-20.

<sup>2</sup> - سهام بوشاقور، المسؤولية الجزائية عن الجريمة الإلكترونية، مذكرة ماستر في قانون جنائي، قسم القانون العام، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم، جوان 2023، ص 24.

<sup>3</sup> - عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماستر في إدارة التحقيقات الاقتصادية والعلوم التجارية والمالية، قسم علوم التسيير، كلية علوم التسيير، 2 جويلية 2019، ص 14.

### ثالثا: الركن المعنوي للجريمة المعلوماتية

يتخذ الركن المعنوي في أغلب الجرائم بصفة عامة، صور القصد الجنائي والذي يتحقق بتوافر إرادة لدى الجاني لارتكاب الفعل الغير المشروع، مع علمه بأن هذا الفعل يجرمه القانون كما ينطبق هذا الأمر نفسه على الجريمة المعلوماتية، إذ يقوم ركنها المعنوي على توافر الإرادة الإجرامية لدى الفاعل، وهو ما يتجلى من خلال استعمال المشرع الجزائري لعبارات "الغش" و"العمد" و"الإعداد للجريمة من قانون العقوبات، وهذا ما يؤكد أن الجريمة المعلوماتية تعد جريمة عمدية بامتياز، ولا يفترض فيه عنصر الخطأ.<sup>1</sup>

### المطلب الثاني: صور الجريمة السيبرانية ودوافع ارتكابها

في ظل التطور التكنولوجي المتسارع والتحول الرقمي الذي يشهده العالم في مختلف المجالات، أصبحت التكنولوجيا جزءا لا يتجزأ من الحياة اليومية، سواء على المستوى الفردي أو المؤسسي، ومع هذا التوسع والتقدم الكبير في مجال استخدام الحواسيب ظهرت صور وأنواع جديدة لجرائم لم تكن من قبل وهذا ما سنتناوله في الفرع الأول، أما الفرع الثاني خصصناه لمعرفة دوافع ارتكاب هاته الجرائم.

### الفرع الأول: صور الجريمة السيبرانية

تشمل الجريمة السيبرانية طائفة واسعة من الجرائم لذا قسمنا ، أولا الجرائم المالية الإلكترونية، ثانيا: الجرائم المرتبطة بالبيانات الشخصية.

#### أولا: الجرائم المالية الإلكترونية(الاحتيال الإلكتروني، غسل الأموال):

وهي الجرائم التي ترتكب باستخدام الوسائل الالكترونية أو عبر الشبكات الرقمية، بهدف تحقيق مكاسب مالية غير مشروعة، وتتعدد هذه الجرائم ويمكن استخلاصها فيما يلي:

<sup>1</sup> حمزة خضري، حمزة غشاش، "خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري"، مجلة الدراسات القانونية، المجلد 06، العدد 02، جامعة محمد بوضياف المسيلة، 2020، ص ص 174-175.

**1-مبدأ عمل الفيروسات يختلف بناء على أسلوب تصميمها:** فمنها ما يبدأ بالعمل بمجرد فتح الرسالة التي تحتوي عليها الفيروسات، ومنها ما ينشط بمجرد تشغيل البرنامج الذي تحمله، وتعد من اخطر وأكثر الجرائم الإلكترونية انتشارا، حيث يعود تاريخ ظهور الفيروسات إلى أربعينيات القرن الماضي عندما تحدث عنها العالم الرياضي "جون فون نيومان" في سياق الحوسبة دون الاتصال بشبكة الأنترنت.<sup>1</sup>

**2-جرائم الاختراقات:** تعرف عملية الاختراق بأنها دخول غير مصرح به إلى أجهزة الكمبيوتر أو الشبكات دون اذن، يقوم بها أفراد ذو خبرة تقنية عالية يستخدمون أدوات متطورة لتجاوز اجراءات الأمان، وتتنوع الدوافع باختلاف أهداف المخترقين من الفضول إلى تحقيق مكاسب مالية، وهذا هو الهدف الأكثر انتشارا يتمثل في سرقة البيانات الحساسة وبيعها.<sup>2</sup>

**3-جريمة الاستلاء والنصب والاحتيال:** فيعتمد الاحتيال الإلكتروني على خداع الأفراد، والمؤسسات باستخدام تقنيات رقمية بهدف الحصول على أموال بطرق غير قانونية كالتصيد الاحتيالي، والتزوير الرقمي.<sup>3</sup>

ويكون الاستيلاء إما لنفسه أو لغيره على مال منقول أو على سند، أو توقيع هذا السند، وذلك عن طريق الاحتيال واتخاذ اسم كاذب، أو انتحال صفة غير صحيحة.<sup>4</sup>

**4-جريمة الاعتداء على حقوق الملكية الفكرية :** يكون بالاعتداء على الإعلانات التجارية وبراءات الاختراع، وكذلك نسخ وتقليد البرامج وإعادة انتاجها وصنعها دون ترخيص، فهو اعتداء على الحقوق المالية والحقوق الأدبية<sup>5</sup>

1 - كريمة صمودي، سمر برقعي، المرجع السابق، ص 41.

2 - المرجع نفسه، ص ص 41-42

3- محمد شايب، المرجع السابق، ص 51.

4- فارس محمد العمارات، ابراهيم الحمامصة، المرجع السابق، ص 83.

5- المرجع نفسه، ص 83

ونرى أن هاته الجريمة هي فعل غير مشروع يقوم به الفرد من خلال الاستغلال دون ترخيص قانوني، وهذا ما يمس بالحماية القانونية المقررة للإبداع والابتكار.

**5- جريمة تعطيل الأجهزة والشبكات:** تؤدي هذه الجريمة إلى تعطيل أجهزة الحاسوب عن طريق استهداف برامجها، مما قد يسبب أعطالا فنية تؤثر على المكونات الإلكترونية لأجهزة وتوقف عملها.<sup>1</sup> فيمكننا القول أن هذا الفعل يرتكب عمدا بهدف إعاقة عمل الأنظمة الإلكترونية أو إيقافها كلياً أو جزئياً، مما يؤدي إلى الإضرار بكفاءة الخدمات وتعطيلها.

**ثانياً: الجرائم المرتبطة بالبيانات الشخصية (سرقة الهوية، انتهاك الخصوصية)**

وهي الجرائم السيبرانية التي تستهدف البيانات الشخصية للأفراد، واستغلالها للأضرار بهم أو انتهاك خصوصياتهم، ومن أكثر هذه الجرائم شيوعاً نذكر ما يلي:

**1- جريمة انتحال الشخصية:** بمرور الزمن والتطورات التكنولوجية تحولت هذه الجريمة من أساليبها التقليدية إلى صور مستحدثة عبر الفضاء السيبراني، فيستغل المجرمون البيانات الشخصية للضحايا مثل العنوان ، تاريخ الميلاد وبعض التفاصيل الخاصة لإجراء معاملات احتيالية بما في ذلك الحصول على بطاقات الائتمان والقيام بعمليات أخرى، فتتيح لهم هاته الهوية المسروقة إخفاء هويتهم الحقيقية والعمل تحت اسم مستعار، وغالباً ما يتم جمع هذه المعلومات من خلال الإعلانات المتاحة على الإنترنت.<sup>2</sup>

**2- جريمة المضايقة والملاحقة:** ترتكب جرائم المضايقة والملاحقة الإلكترونية عبر شبكة الأنترنت باستعمال البريد الإلكتروني، أو مختلف وسائل الاتصال الأخرى، وذلك من أجل توجيه رسائل تتضمن التهديد والتخويف، وتتفق هذه الجرائم مع صور الملاحقة التقليدية من حيث الغاية الإجرامية والمتمثلة في فرض السيطرة والتحكم في الضحية، وتتميز عنها في سهولة إمكانية إخفاء هوية الجاني، وتعدد

<sup>1</sup> - كريمة صمودي، سمر برقي، المرجع السابق، ص 42.

<sup>2</sup> - المرجع نفسه، ص 43.

رسائل الاتصال بسرعة استخدامها، وهذا هو الأمر الذي يساعد في اتساع نطاق انتشارها وتزايد خطورتها.<sup>1</sup>

**3- جرائم الابتزاز:** وذلك باستخدام أساليب عدة، وعادة ما يكون الضحية من قليلي الخبرة والمعرفة الإلكترونية أو من الأطفال والنساء، واستخدام مواقع المواعدة على الأنترنت للتعرف وتكوين علاقات.<sup>2</sup>

فنستنتج أن هذه الجريمة تقوم على الخداع والتلاعب بالضحية من أجل استدراجها لفعل ما وابتزازها وتحقيق أهداف غير قانونية، كما يمكننا قول أن أخطر ما يميز هاته الجريمة أنها لا تعرف حدودا سياسية أو اجتماعية.

**4- جرائم التشهير وتشويه السمعة:** تتمثل في قيام الجاني بنشر معلومات قد تكون سرية أو كاذبة أو مضللة تمس بسمعة الضحية، سواء كان فردا أو جماعة أو مؤسسة تجارية أو سياسية وحتى دينية، وتعدد الوسائل المستعملة في ارتكاب هذه الجرائم، وفي مقدمتها انشاء مواقع إلكترونية أو استعمال شبكات الأنترنت لنشر وتداول تلك المعلومات.

كما يشمل هذا النوع من الجرائم نشر الشائعات والأخبار الكاذبة والزائفة بقصد الإساءة وتحقيق أغراض غير مشروعة كالا ابتزاز والتأثير على الرأي العام.<sup>3</sup>

<sup>1</sup> - صفيان بخدة، ناصر وقاص، الطبيعة القانونية للجرائم المستحدثة ووسائل ارتكابها جريمة الأنترنت كنموذج، مجلة البحوث القانونية والسياسية، المجلد 03، العدد 16، جامعة مولاي الطاهر، سعيدة، الجزائر، أبريل 2021، ص ص 135-136.

<sup>2</sup> - محمد بلقاسم بوفاتح، الجريمة الإلكترونية، دراسة سوسيو قانونية، كلية الحقوق والعلوم السياسية، جامعة الجلفة، ص، 62.

<sup>3</sup> - صفيان بخدة، ناصر وقاص، المرجع السابق، ص ص 136-137.

5- الجرائم المخلة بالأخلاق والاداب العامة : شهدت الأنترنت تطورا واضحا في شتى المجالات ولاسيما تلك المتعلقة بالصفحات والمواقع الموجودة فيها، وقد أدى ذلك إلى انتشار مواقع تحريض على ممارسة الجنس للكبار والأطفال، وتقوم هذه المواقع بنشر صور فاضحة لهم.<sup>1</sup>

### الفرع الثاني: دوافع ارتكاب الجريمة السيبرانية

تتعدد الأسباب التي تدفع بالمجرم السيبراني لإرتكاب الجريمة السيبرانية وتختلف أهدافه وغاياته لذلك سنقوم بذكر أهم الدوافع.

1-تحقيق مكاسب وأرباح مادية: إن الهدف من الجرائم الإلكترونية قد يكون لأسباب مادية محضة أين يسعى مرتكب هذه الجريمة إلى الحصول على أموال معينة أين يكون الربح المادي هو الهدف الأساسي من ارتكاب مثل هذه الجرائم.<sup>2</sup>

ويعد هذا الدافع أكثر الدوافع تحريكا للجنة لاقترافهم هذه الجرائم خاصة ذوي الخبرة والمحترفين، وما يبرز ويبين هذا الدافع هو حجم الربح الممكن تحقيقه وبالنظر كذلك إلى خصائص الجرائم الإلكترونية.<sup>3</sup>

2- قهر النظام واثبات التفوق على تطور الوسائل التقنية: في بعض الأحيان يكون الدافع وراء ارتكاب هذه الجرائم هو قهر النظام والرغبة في إثبات الذات وإظهار التفوق التقني في القدرة على تحدي أي تطور جديد، وهي ظاهرة منتشرة أكثر بين فئات الشباب.<sup>4</sup>

<sup>1</sup> - محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام الغير مشروع لشبكة الأنترنت دراسة مقارنة، ط2، دار النهضة العربية، القاهرة، 2009، ص 146.

<sup>2</sup> - صابر بحري، منى خرموش، أهم الدوافع السيكلوجية وراء الجريمة الإلكترونية، مجلة دراسات في سيكلوجية الانحراف، المجلد 06، العدد 01، جامعة محمد لمين دباغين، جامعة سطيف 02، الجزائر، ماي 2021، ص 48.

<sup>3</sup> - محمود أحمد طه، المواجهة التشريعية لجرائم الكمبيوتر والأنترنت، دراسة مقارنة، دار الفكر والقانون، 2016-2017، ص 16.

<sup>4</sup> - محمد الدام، المرجع السابق، ص 33

**3- دافع التعلم:** يعد هذا الدافع من بين الدوافع التي تؤدي إلى ارتكاب هذه الجريمة، حيث يسعى بعض الأفراد إلى اختراق الأنظمة المعلوماتية بدافع اكتساب المعرفة التقنية، أو الاطلاع على المعلومات المخزنة داخل الحواسيب والشبكات الإلكترونية، اعتقاداً بأن لهم الأحقية في جمع والحصول على هاته المعلومات، وغالباً ما يبرر موقفهم بهدفهم في التعلم وتطوير المهارات، دون قصد الإضرار بالغير ويشكلون مجموعات يتقاسمون ويتبادلون المعلومات والخبرات المكتسبة، من عمليات الاختراق ويستفيدون منها في أنشطة مختلفة ولو بطرق غير شرعية.<sup>1</sup>

**4- دافع الانتقام:** يعد هذا الدافع من أخطر الدوافع المؤدية إلى ارتكاب الجريمة السيبرانية، إذ غالباً ما يكون الجاني شخصاً يمتلك معلومات وبيانات مهمة عن الشركة التي يعمل بها، ويرتبط هذا الدافع في الغالب بالحياة المهنية، كالشعور بالظلم أو الحرمان، من بعض الحقوق المهنية أو التعرض للفصل من العمل، الأمر الذي يدفع الجاني إلى السعي للانتقام من صاحب العمل من خلال استغلال المعلومات أو الوسائل الإلكترونية.<sup>2</sup>

فيتضح أن الموظف يكون قد تعرض للإهانة والإساءة من طرف رب العمل فيقوم بالحقده عليه وهذا ما يتولد عنه الانتقام.

**5- دافع سياسي أو عقائدي:** يتم من طرف المجرمين المعادين للحكومات وذلك عبر تخريب المواقع الحكومية واختراق الحسابات عبر منصات التواصل الاجتماعي مثل تويتر وفيسبوك لنشر معلومات كاذبة والفتنة بين الأفراد.<sup>3</sup>

ويعتبر كذلك محرك أنشطة الإرهاب الإلكتروني وحروب المعلومات الدوافع السياسية والإيديولوجية، كما قد تحركه دوافع المنافسة فيسعى إلى الاستيلاء على الأسرار التجارية.<sup>4</sup>

1 - محمد الدام ، المرجع السابق، ص33

2 - صابر بحري ،منى خرموش، المرجع السابق، ص52

3 - محمد الدام، المرجع السابق، ص33

4 - محمود أحمد طه، المرجع السابق، ص16.

**6- دافع التسلية واللهو:** يعد هذا الدافع من بين الدوافع التي قد تؤدي إلى ارتكاب الجريمة الإلكترونية، حيث يقدم بعض الأفراد على القيام بأفعال غير مشروعة عبر الوسائط الإلكترونية بقصد المزاح والترفيه فقط دون توافر نية إجرامية، غير أنه قد يترتب عنها نتائج خطيرة مما يكسبها وصفا إجراميا، ويلاحظ أنه العديد من مرتكبي الجرائم تكون بدايتهم بدافع الفضول والتسلية ومع مرور الوقت ومع اكتسابهم التدريجي للخبرة والمهارات يتحولون من مجرد أشخاص عاديين إلى محترفين في ارتكاب هذا النوع من الجرائم.<sup>1</sup>

<sup>1</sup> - صابر بحري، منى خرموش، المرجع السابق، ص 50.

## خلاصة الفصل الأول

يعد الأمن السيبراني منظومة متكاملة من الآليات والإجراءات المنظمة، باعتبارها تسعى إلى حماية الأجهزة والتقنيات الحديثة، بما في ذلك المعطيات والبيانات المتداولة عبر الفضاء الرقمي، وذلك لمواجهة مختلف أشكال التهديدات والاعتداءات الإلكترونية، حيث أن هذه الحماية لا تقتصر فقط على تأمين الأجهزة، بل تمتد لتشمل حماية البنية التحتية الرقمية والشبكات، التطبيقات، البيانات، إلى جانب أبعاده والعسكرية، القانونية والاجتماعية، وهو ما يعكس اتساع مفهوم الأمن السيبراني وتشعب مجالاته.

ومع التطور المتسارع للتكنولوجيا والاعتماد المتزايد على الأنظمة المعلوماتية، برزت الحاجة إلى ضبط المفاهيم المتصلة بالأمن السيبراني خاصة في ظل تنوع المخاطر التي يشهدها الفضاء الرقمي، ومن هذا المنطلق أصبح الأمن القومي يرتبط ارتباطا وثيقا بحماية الأفراد والدول والمؤسسات من التهديدات المتزايدة الناتجة عن الاستخدام المكثف للتقنيات الحديثة.

وفي هذا السياق، تعد الجريمة السيبرانية من أبرز التحديات التي تواجه الأمن السيبراني، باعتبارها كل نشاط غير مشروع يستهدف أنظمة البيانات أو البرامج المعلوماتية عبر الوسائط الإلكترونية، حيث تمتاز هذه الجريمة بطابعها العابر للحدود نظرا لإمكانية ارتكابها بسهولة دون التقيد بحدود مكانية أو زمنية، الأمر الذي يزيد من خطورتها ويجعل مكافحتها أكثر تعقيدا، كون أن هذا الفعل الغير القانوني لا يتحقق إلا بتوافر أركانها الأساسية، المتمثلة في الركن المادي الذي يشمل السلوك الإجرامي والنتيجة المترتبة عنه والعلاقة السببية بينهما، إلى جانب الركن المعنوي القائم على اتجاه إرادة الجاني في القيام بالنشاط المجرم، فضلا عن الركن الشرعي الذي يستند إلى وجود نصوص قانونية تجرم هذه الأفعال، كما ترتبط هذه الجرائم بدوافع متعددة قد تكون مالية أو انتقامية أو سياسية وغيرها، حيث تستهدف مختلف صور الاعتداء على الأنظمة المعلوماتية والمعطيات الرقمية.

وعليه، فإن هذا الفصل يوضح الأمن الرقمي وما قد ينجم عنه من انتهاكات رقمية، مما يمهد للانتقال للفصل الثاني لمواجهة هذا النوع من التهديدات.

## الفصل الثاني: المواجهة التشريعية لحماية الأمن السيبراني.

### تمهيد:

بعد التطرق في الفصل الأول الى الإطار المفاهيمي للأمن السيبراني والجريمة السيبرانية من خلال تحديد مفهومها وخصائصهما، يتضح أن هذا المجال لم يعد مجرد موضوع تقني مرتبط بتكنولوجيا المعلومات، بل أصبح يشكل تحدياً قانونياً وأمنياً متصاعداً يفرض على الدول إعادة النظر في آليات الحماية والمواجهة المعتمدة.

ويهدف هذا الفصل الى تحليل مختلف الوسائل والآليات القانونية والتقنية التي تعتمد عليها الدول لمواجهة الجرائم السيبرانية والحد من آثارها.

ثم ننتقل في الفصل الثاني الى تسليط الضوء على الإطار التطبيقي والعلمي للأمن السيبراني وذلك من خلال تحليل مختلف الوسائل والآليات التي تعتمد عليها الدول لمواجهة الجرائم السيبرانية، سواء من خلال أنظمة الحماية المعلوماتية أو من خلال القواعد القانونية والتنظيمية التي تضعها السلطات المختصة لضمان أمن الفضاء الرقمي.

كما اقتضى الأمر إنشاء وتكليف جهات وهيئات مختصة تتولى مهام الوقاية والكشف والمتابعة والمكافحة، بما يضمن ذلك مواجهة فعالة للجرائم السيبرانية وحماية جميع الأنظمة والبيانات.

ومن جهة أخرى لم يكتف المشرع بوضع تدابير وقائية وتنظيمية، بل أقر منظومة عقابية تتضمن عقوبات عامة وأخرى خاصة تتناسب مع طبيعة الجرائم المرتكبة وخطورتها، بهدف تحقيق الردع وحماية المصالح والحقوق التي كفلها القانون. غير أن فعالية هذه المنظومة القانونية تبقى مرتبطة بقدرتها على التكيف ومواكبة التطورات المتسارعة التي يشهدها الفضاء الرقمي، خاصة مع تطور أساليب ارتكاب الجرائم السيبرانية. الأمر الذي يطرح العديد من التحديات أمام المشرع والجهات المختصة سواء على المستويين الوطني أو الدولي، ومن هذا المنطلق تم تقسيم هذا الفصل الى مبحثين كالآتي:

- المبحث الأول: آليات حماية الأمن السيبراني و الهيئات المختصة لمكافحته
- المبحث الثاني: جزاء الاخلال بالأمن السيبراني و التحديات التي تواجهه

## المبحث الأول: آليات حماية الامن السيبراني و الهيئات المختصة لمكافحته

نظرا لتنامي الجريمة الرقمية وما تسببه من تهديد مباشر الواقع على أمن الأفراد واستقرار المؤسسات وسلامة المعطيات، وعليه فإن الجزائر سارعت إلى تبني تدابير وقائية، وذلك لتعزيز الأمن الرقمي، وكذلك حماية الأنظمة المعلوماتية من مختلف أشكال الاعتداء الرقمي، وعلى هذا الأساس تم دعم هذه الجهود كإنشاء هيئات وطنية متخصصة، بحيث تتولى الوقاية ومكافحة هذا الفرع من الجرائم، مع تعزيز التعاون الدولي لمواجهة طبيعتها العابرة للحدود، وهو ضمان فعالية التصدي لها بما يضمن ذلك تحقيق حماية تكون فعالة للفضاء السيبراني على المستويين الوطني والدولي، وعليه سنتطرق في هذا المبحث إلى:

- المطلب الأول: الآليات المتبعة لمكافحة الجريمة

- المطلب الثاني: الهيئات المختصة للتصدي للجريمة السيبرانية.

## المطلب الأول: الآليات المتبعة لمكافحة الجريمة

يعد الأمن السيبراني وسيلة أساسية لحماية الفضاء الرقمي وذلك من المخاطر التي تكون محتملة، وأيضا ضمان سلامته ولهذا الغرض فلقد تم اعتماد مجموعة من آليات الوقائية والردعية للحد من الأضرار قبل وقوعها وهذا ما سوف نتناوله في هذا المطلب.

## الفرع الأول: الآليات الوقائية لمكافحة الجريمة السيبرانية:

تعد التدابير الوقائية من الوسائل المعتمدة للحد من هذه الجريمة، وذلك من خلال تعزيز فعالية الكشف عنها وهذا ما سوف يتم تناوله في هذا الفرع:

## أولا: مراقبة الاتصالات الالكترونية:

تتعلق إجراءات المراقبة، وذلك طبقا لما أورده التشريع ، بالاتصالات الإلكترونية، حيث يراد بهذه الاتصالات، في إطار مفهوم هذا القانون،<sup>1</sup> طبقا لنص المادة 2 من قانون 09-04 بند (و): "كل

<sup>1</sup> دنيا زاد ثابت، مراقبة الاتصالات الإلكترونية والحق في حرمة الحياة الخاصة في القانون الجزائري، مجلة العلوم الاجتماعية والإنسانية، العدد السادس، جامعة تبسة، ص207.

تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية."

كما تعتبر المراقبة من بين أهم الوسائل الوقائية وذلك في مواجهة الجرائم الرقمية، حيث تتيح مراقبة الاتصالات الرقمية، بالإضافة إلى جمع محتواها وتسجيله أثناء حدوثها، ويكون ذلك في الحالات الآتية:<sup>1</sup>

"للوفاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة تأمين الدولة.

- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني".<sup>2</sup>

"لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.

- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة".<sup>3</sup>

كما تجدر الإشارة إلى أن المشرع قد اشترط عدم الشروع في عمليات المراقبة المنصوص عليها في المادة 4 من القانون 04/09، وذلك إلا بعد الحصول على إذن كتابي يكون من قبل السلطة القضائية المختصة.<sup>4</sup>

### ثانيا: الاستعانة بمزودي الخدمات.

لقد فرض المشرع على مزودي خدمات الاتصال جملة من الالتزامات التي تهدف إلى دعم عمل السلطات القضائية، وذلك في مجال مكافحة الجرائم الإلكترونية، إذ يتعين عليهم المساهمة في جمع المعطيات المرتبطة بحركة الاتصالات وتسجيلها وحفظها، كبيانات التعريف ووسائل الاتصال التي تكون مستعملة زمنيا، بالإضافة إلى الجهة المواجهة إليها، مع وضع هذه المعلومات تحت تصرف الجهات

<sup>1</sup> عبد الصديق شيخ، الوقاية من الجرائم الإلكترونية في ظل قانون رقم 04/ 09 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، مجلة معالم للدراسات القانونية والسياسية، المجلد 4، العدد 1، جامعة يحي فارس بالمدينة، الجزائر، 2020، ص198.

<sup>2</sup> إسماعيل بن يحي، التعريف بمراقبة الاتصالات الإلكترونية كإجراء من إجراءات جمع الأدلة في الجريمة الإلكترونية، مجلة صوت القانون، المجلد 8، العدد 2، المركز الجامعي علي كافي، تندوف، الجزائر، 2022، ص 1070.

<sup>3</sup> كريمة مرزوقي، مراقبة الاتصالات الإلكترونية وحق الفرد في الخصوصية المعلوماتية، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 5، العدد 2، جامعة مولود معمري، تيزي وزو، 2020، ص1371.

<sup>4</sup> عبد الصديق شيخ، المرجع السابق، ص 198.

المختصة عند الضرورة، كما أوجب عليهم اتخاذ التدابير اللازمة لإزالة المحتوى الغير المشروع أو تقييد الوصول إليه متى صدر بشأنه طلب من السلطات المختصة.<sup>1</sup>

#### أ. الالتزام بمساعدة سلطات الضبط القضائي.

كما أوجب المشرع على مقدمي خدمات الإعلام والاتصال، بما في ذلك مزود وخدمات الأنترنت، وضع المعطيات المخزنة لديهم، وذلك تحت تصرف سلطات الضبط القضائي متى اقتضت ضرورة التحقيق ذلك.<sup>2</sup> حيث يلزم على مقدمي الخدمات بحفظ مختلف المعطيات التي تكون مرتبطة بهوية مستخدمي الخدمات، بما يشمل المعطيات المتعلقة بمضمون الاتصالات والمواقع التي يتم الولوج إليها، إضافة إلى جانب سائر المعلومات التي من شأنها المساهمة في تسهيل إجراءات التحري والتحقيق، كما ألزمهم باحترام السرية التامة الخاصة بالعمليات المنجزة، وذلك بناء على طلب الجهات المختصة بالتحقيق، تحت طائلة العقوبات المقررة قانونا في حالة إفشاء أسرار التحري والتحقيق.<sup>3</sup>

#### ب. الالتزام بحفظ المعطيات المتعلقة بحركة السير.

لقد أوجب المشرع الجزائري مزودي خدمات الأنترنت والاتصالات بالاحتفاظ، خلال مدة يحددها القانون، بالمعطيات ذات الصلة بالمستخدمين والبيانات وحركة السير الخاصة بالاتصالات الإلكترونية، وذلك بهدف تمكين السلطات المختصة من تعقب الجرائم الإلكترونية والكشف عن مرتكبيها، بالإضافة إلى تسهيل إجراءات البحث والتحري عند الاقتضاء.<sup>4</sup>

<sup>1</sup>سفيان ملوكي، عمر جيلالي، السياسة العامة الأمنية الجزائرية في ضوء التحديات السيبرانية المعاصرة، مجلة الفكر القانوني والسياسي، المجلد 9، العدد 2، جامعة عمار ثليجي، الأغواط، 2025، ص221.

<sup>2</sup> محمد بعجي، التزامات مقدمي الخدمة عبر الأنترنت، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 4، العدد 1، جامعة الجزائر 1، 2019، ص32.

<sup>3</sup> وداد بن سالم، عبد الله شيباني، النظم القانوني لمقدمي خدمة الأنترنت في ظل القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد 13، العدد 1، جامعة محمد لمين دباغين، سطيف 2، 2024، ص 65.

<sup>4</sup> رضوان علي، رزق الله العربي بن مهدي، المكافحة المؤسسية للجريمة الإلكترونية في التشريع الجزائري، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد 9، العدد 2، جامعة عمار ثليجي، الأغواط، 2025، ص 1394.

## الفرع الثاني: الآليات الردعية لمكافحة الجريمة السيبرانية:

تستدعي مكافحة هذه الجريمة الاعتماد على اليات ردعية تمكن السلطات المختصة من جمع الأدلة الرقمية وضبطها بما يضمن فعالية إجراءات المتابعة والتحقيق وهذا ما سيتم دراسته في هذا الفرع

**أولاً: التفتيش الإلكتروني.**

يقصد بالتفتيش الرقمي أو الدخول إلى أنظمة المعلومات، على أنه إجراء قانوني تتولاه الجهات المختصة، الذي يهدف إلى جمع إثباتات التي تكون متعلقة بالجريمة وذلك داخل الأجهزة والأنظمة المعلوماتية، وعليه فإن هذا الإجراء يقوم بالاطلاع على المعطيات الرقمية المتداولة والمحفوظة، بالإضافة إلى كشف مختلف البيانات ذات الصلة بالفعل الإجرامي، كالمعطيات الرقمية داخل الأجهزة الرقمية والتطبيقات خارج الإطار القانوني، وكذلك بيانات توثق عمليات الاتصال، وعليه فإن هذا التفتيش الرقمي يساهم في جمع القرائن الرقمية وتحليلها، بما يساعد على إعادة بناء وقائع الجريمة، وذلك لتحديد ظروف ارتكابها، والوصول إلى الحقيقة بغرض إثباتها<sup>1</sup> وعليه فإن الجرائم الإلكترونية لا تنحصر في نطاق مادي فقط، بل تمتد إلى بيئة رقمية بما تتضمنه بيانات تكون رقمية ذات الصلة بالجريمة.

في حين أن تحديد محل التفتيش في الجرائم التقليدية لا يطرح إشكالا كبيرا، نظرا أن آثارها تكون عادة موجودة في أماكن مادية واضحة بحيث يمكن معاينتها على نحو مباشر<sup>2</sup> وعليه فإنه يفترض في القائم بعملية التفتيش أن يكون ملما بدرجة معتبرة بعلوم الإعلام الآلي .

وذلك بما يسمح له الإحاطة بنظم الحاسوب محل التفتيش وفهم خصائصها التقنية، كما يمكنه أن يستعين بخبراء النظام عند الاقتضاء للمساهمة في تنفيذ إجراءات التفتيش، لاسيما فيما يتعلق بإمكانية الوصول إلى النظام والحصول على كلمات المرور الخاصة به فضلا عن تحديد المكان المناسب، وذلك لإجراء التحليل التقني المتعلق بأنظمة الحاسوب الآلي محل التفتيش<sup>3</sup>، وعليه فلقد وسع المشرع الجزائري

<sup>1</sup> نسمة بطيحة، محاضرات في مقياس الوقاية من الجرائم الإلكترونية، القيت على طلبة سنة الثانية ماستر، قسم الحقوق، كلية الحقوق و العلوم

السياسية، جامعة محمد لمين دباغين سطيف - 2، 2021-2022، ص ص 29،30

<sup>2</sup> فتية خليف، محمد صالح مهداوي، خصوصية التفتيش في البيئة الرقمية، المجلة الجزائرية للقانون المقارن، المجلد 5، العدد 9، جامعة بلحاج بوشعيب بعين تموشنت، الجزائر، 2022، ص 6.

<sup>3</sup> نجية عراب ثاني، الآليات الوقائية من جرائم تكنولوجيا الإعلام والاتصال ومكافحتها في القانون الجزائري، مجلة البحوث في الحقوق والعلوم السياسية، المجلد 8، العدد 1، جامعة أبو بكر بالقائد، تلمسان، الجزائر، 2022، ص 470.

من نطاق التفتيش عن بعد ليشمل أيضا الحالات التي تتجاوز حدود الإقليم الوطني، وذلك عندما تتوفر مؤشرات جدية تدل على احتمال وجود المعطيات محل البحث، وعليه فإن مثل هذه الحالات يمكن الولوج إلى البيانات، وذلك سواء من خلال نظام معلوماتي كامل أو جزء منه، أو حتى إذا كانت مخزنة خارج البلاد، كما يحق للسلطات القضائية المختصة وضباط الشرطة القضائية الحصول على هذه المعطيات في وفق إطار التعاون والمساعدة القضائية مع السلطات الأجنبية، وطبقا للإجراءات القانونية التي تكون سارية<sup>1</sup>، وذلك في إطار ما تقرره الاتفاقيات الدولية، إضافة إلى جانب تطبيق مبدأ المعاملة بالمثل بين الدول، ومن هذا الأساس يجوز للجهات المختصة الاستعانة بأهل الخبرة والمختصين في الأنظمة والمعلوماتية، نظرا لما تتطلبه هذه العمليات من معرفة تقنية دقيقة بكيفية عمل المنظمات الرقمية، حيث أنه لا يتم إجراء التفتيش، إلا بتوافر جملة من الشروط القانونية من بينها وجود جريمة إلكترونية قائمة تبرز اتخاذ هذا الإجراء، إضافة إلى تحديد محل التفتيش والجهة المختصة بمباشرة، كذلك إلى صدور إذن قانوني من قبل السلطة المختصة، مع مراعاة حضور الأشخاص الذين يحدددهم القانون أثناء تنفيذ التفتيش، فضلا عن التقيد بمدة زمنية مقرر لإجرائه<sup>2</sup>، وعليه فإن التوجه نحو تحديث مختلف المرافق والاعتماد المكثف على تقنية المعلوماتية .

نجد أن المشرع الجزائري أقر بصورة إستثنائية إمكانية القيام بالتفتيش الرقمي قبل تحقق الفعل الإجرامي، وذلك في نطاق جرائم معينة التي حددها القانون حصرا، كما أن هذا الإجراء يجد مبرره في الطبيعة الحساسة لبعض المجالات، لاسيما المرتبطة بالدفاع والأمن، والتي تفرض إخضاعها لتدابير رقابية إستباقية لحمايتها، حيث يعد هذا الإجراء من إختصاصات<sup>3</sup>، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال<sup>4</sup>.

<sup>1</sup> رجا أو مدور، فرشة كمال، التفتيش الجزئي في البيئة الرقمية، مجلة صوت القانون، المجلد 7، العدد 1، جامعة محمد البشير الإبراهيمي، برج بوعريش، الجزائر، ماي 2020، ص، ص983، 984.

<sup>2</sup> عبد العالي حاحة، سمية قلات، المكافحة الإجرائية للجرائم الإلكترونية، دراسة حالة الجزائر، مجلة المفكر، المجلد 13، العدد 2، جامعة محمد خيضر بسكرة، جافني، 2018، ص، ص231، 222.

<sup>3</sup> كمال حفصاوي، عمر مخلوف، التفتيش الإلكتروني بين ضرورة التحقيق والحق في سرية المراسلات والاتصالات، مجلة الباحث للدراسات الأكاديمية، المجلد 11، العدد 1، جامعة سطيف 2، جامعة غليزان، 2024، ص332.

<sup>4</sup> سهيلة بوزيرة، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بين سرية المعطيات الشخصية الإلكترونية ومكافحة الجرائم الإلكترونية، المجلة النقدية للقانون والعلوم السياسية، المجلد 17، العدد 2، جامعة تيزي وزو، جامعة محمد الصديق بن يحي جيجل، الجزائر، 2022، ص563.

## ثانيا: الحجز الالكتروني:

كما تباشر عملية حجز<sup>1</sup> البيانات المخزنة داخل الأنظمة المعلوماتية، كلما كانت ذات فائدة في الكشف عن الجرائم أو تحديد فاعليها، وذلك ضمن ما تفرضه مقتضيات البحث والتحقيق.<sup>2</sup>

### أ. حجز المعطيات والبيانات الآلية:

يمتد نطاق الحجز كل ماهو ذو طبيعة مادية، إضافة إلى البيانات التي تتم معالجتها، وذلك بوسائل إلكترونية، أما فيما يتعلق بتحديد محل الحجز، فإنه يمكن أن يمتد ليطال كافة المعطيات المخزنة التي يكون من شأنها الإسهام في كشف الجريمة أو تحديد مرتكبيها، غير أنه يمكن إستثناء الإقتصار على الحجز الجزئي، بحيث يقتصر الإجراء على المحتوى الذي يكون مرتبط مباشرة بالشخص المشتبه فيه دون غيره.<sup>3</sup>

### ب. الحجز عن طريق منع وصول المعطيات

لقد نص المشرع في القانون 09-04 المادة 7 على إخفاء حماية على المعطيات التي يتم إكتشافها أثناء عمليات التفتيش، وعليه فإنه منح للجهات المختصة صلاحية إصدار أوامر تحفظية بشأنها، وذلك بهدف منع محوها أو إتلافها، وكذلك ضمان عدم الولوج إليها بصورة غير مشروعة، كما لم يجز اللجوء إلى إجراء الحجز عن طريق منع الوصول إلى هذه المعطيات إلا في حالة واحدة، والتي تتمثل في تعذر حجزها فعليا، وفي السياق ذاته، حول المادة 8 من ذات القانون للسلطات القائمة على التفتيش إمكانية الإستعانة بأي شخص مختص ومؤهل تقنيا لإستعمال الوسائل المناسبة التي من شأنها منع الإطلاع على المعطيات، بإعتبارها قد تتضمن محتواها أفعالا مجرمة، وذلك طبقا لأحكام التشريع.<sup>4</sup>

<sup>1</sup> يزيد بوحيط، تفتيش المنظومة المعلوماتية وحجز المعطيات في التشريع الجزائري، التواصل في الإقتصاد والإدارة والقانون، العدد 48، جامعة باجي مختار عنابة، ديسمبر 2016، ص91.

<sup>2</sup> رضا هميسي، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، العدد 5، جامعة ورقلة، جامعة الوادي، الجزائر، جوان 2012، ص 175.

<sup>3</sup> عبد القادر فلاح، حجز وحفظ المعطيات في الجريمة الإلكترونية، مجلة صوت القانون، المجلد الثامن، العدد 1، جامعة الجبالي بونعامة الخميس مليانة، 2021، ص181.

<sup>4</sup> فاطيمة حايطي، نبيلة هبة هروال، الحماية الإجرائية للحق في الخصوصية الرقمية في مواجهة الجريمة المعلوماتية، مجلة الدراسات القانونية، المجلد 7، العدد 2، جامعة ابن خلدون، تيارت، الجزائر، جوان 2021، ص 139.

## المطلب الثاني: الهيئات المختصة للتصدي للجريمة السيبرانية.

مع إتساع إستخدام الفضاء الرقمي في الحياة اليومية، فإنه لم تعد الجريمة السيبرانية مجرد احتمال، بل واقع يفرض معيقات تكون مستمرة، ومن هذا السياق برزت الحاجة إلى إعتماد هيئات وطنية تتولى الحماية الداخلية، بالإضافة إلى تعزيز التعاون الدولي التي تسعى إلى توحيد الجهود ومواجهة هذا النوع من الجرائم التي لا تعترف بالحدود، وهو ما سنتناوله في هذا المطلب، الفرع الأول: على المستوى الوطني والفرع الثاني: على المستوى الدولي.

### الفرع الأول: على المستوى الوطني.

لقد أصبح الأمن الرقمي مجالا يتعدد فيه أشكال الإعتداءات التي تمس أمن المعلومات، وسلامة المعطيات لذلك تعمل سلطات المختصة على المستوى الوطني وضع تدابير تنظيمية . لتحقيق الأمن، وكذلك حماية المستخدمين.

### أولا: على المستوى الدرك الوطني.

#### أ/- مركز الوقاية من جرائم الإعلام الآلي وجرائم المعلوماتية للدرك الوطني.

إن هذه المؤسسة تبأشر طائفة من الوظائف وذلك لمكافحة الجرائم السيبرانية بإعتبار أنها تقوم بتأمين الرقابة التي تكون بشكل متواصل من خلال المنصة الرقمية، بالإضافة أن تتولى رقابة المراسلات الرقمية لصالح قوات الدرك الوطني المؤمن، ويكون هذا في نطاق ما يخول به التشريع، وعليه فلقد تم تأسيس هذه المؤسسة لمكافحة الجرائم التكنولوجية لنظم المعلوماتية،<sup>1</sup> طبقا للمرسوم الرئاسي رقم 261-15، حيث يوجد مكانه ببئر مراد راييس وفق القانون 04/09 المادة 14 السابق الذكر.<sup>2</sup>

<sup>1</sup> عبد القادر فلاح، عبد المالك نادية أيت، التحقيق الجنائي لجرائم الإلكترونية وإثباتها في التشريع الجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 4، العدد 2، جامعة الجبالي بنعامة، خميس مليانة، 2019، ص 1696.

<sup>2</sup> المرسوم الرئاسي، رقم 15 - 261 المؤرخ في 24 ذي الحجة 1436 الموافق لـ 8 أكتوبر 2015، الذي يحدد تشكيلة و تنظيم و كفاءات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكفحتها، ج. ر.ج. ج، العدد 53، الصادر في 18 أكتوبر 2015

## ب/- المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني.

ان هذا المعهد يتولى جملة من المهام التي تستجيب لطلبات السلطة القضائية وضباط الشرطة القضائية، وأيضا الجهات المخولة قانونيا، وهذا خاصة في إطار معالجة القضايا ذات الطابع المعقد.<sup>1</sup> كما من شأنه تأمين القيام بالأعمال المكلفة له على نحو دقيق.

باعتباره يضم مجموعة من الفروع والجهات التي تكون ذات الاختصاص، منها قسم السيارات: حيث يتولى تعقب التعدي التي قد تكون في تزوير أعدادها ومعرفة المسروق منها، أما مصلحة الوثائق: وذلك بإيضاح الأموال التي تم تحريفها، بالإضافة إلى إثبات سلامة المستندات والتوقيعات، وأيضا المستندات الخصوصية التي تكون ذات طابع الشخصي.<sup>2</sup>

## ثانيا: على المستوى الأمن الوطني.

أ/- المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني: في جانفي 2015 أدرجت ضمن البنية الهيكلية المديرية للأمن الوطني القضائي، أما في سنة 2023 في الجزائر العاصمة فقط تتم إفتتاح موقعها المستجد، وعليه فإن المعينات التي تكون متصلة بالإعتداءات الإلكترونية والإجرام التقني قد نتج عنه نزاعات النمط الخامس، لذلك فإن هذه الوظيفة تعمل على إدراج تقنيات معاصرة وجديدة، وذلك من أجل تحسين النشاط الأمني، كما أن هذه الهيئة ذات كفاءة مهنية، وهذا راجع لتطبيق نشاطها دوليا ووطنيا، كما أنها مزودة بآليات تكنولوجية معاصرة، وعلاوة على هذا فإنها تضم أشخاصا ذوي قدرات مرتفعة متخصصين في مجالاتهم التقنية.<sup>3</sup>

<sup>1</sup> إدريس بن عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، كلية الحقوق والعلوم السياسية، جامعة العربي تبسي - تبسة، الجزائر، ص 113.

<sup>2</sup> سميحة بلقاسم، حميد بوشوشة، الجريمة الإلكترونية بعد جديد للإجرام في الجزائر واقعها وآليات مجابهتها، مجلة العلوم الإنسانية أم البواقي، المجلد 10، العدد 1، جامعة 8 ماي 1945، جامعة قسنطينة 3، جوان 2023، ص، ص 550، 551.

<sup>3</sup> محمد جواد بمراح، رفيقة زبدة، إستراتيجية الدفاع الجزائرية لمواجهة التهديدات السيبرانية، مجلة الرسالة للدراسات والبحوث الإنسانية، المجلد 10، العدد 1، جامعة أبي بكر بالقائد، جامعة الجلفة، الجزائر، 2025، ص 881.

ب/- **المديرية التقنية:** إن هذه المديرية التقنية تتولى بصفة خاصة بالقيام بمهام المراقبة الوقائية للإتصالات الرقمية، وذلك بهدف الحد من الجرائم ذات الطابع الإرهابي، وكل أشكال الإعتداء التي تمس أمن الدولة، كما أنها تساهم في دعم السلطات القضائية، وذلك تحت إطار الجهود الرامية إلى التصدي لمختلف الجرائم التي تكون مرتبطة بتكنولوجيا الإعلام والاتصال.<sup>1</sup>

**ثالثا: على المستوى الجيش الوطني الشعبي.**

أ/- **مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة:** أنشأت بتاريخ 11 جوان 2015 على مستوى دائرة الإستعمال والتحضير لأركان الجيش الوطني، لذلك فقد كلفت بمهمة تأمين وحماية المنظومات والمنشآت الحيوية للبلاد من مختلف أشكال الجريمة الرقمية.<sup>2</sup>

حيث تعد هذه المصلحة على أنها تابعة لقيادة الجيش الوطني الشعبي على مستوى دائرة الإستعمال والتحضير، لذا فإن هدفها تكمن في حماية وتأمين المنشآت الحيوية الخاصة بالقوات المسلحة الجزائرية من أي تهديد سيبراني محتمل، وعلاوة على هذا فإنها تتولى تنفيذ السياسة العامة للدفاع الرقمي وذلك داخل الجيش الوطني الشعبي، إضافة إلى تعزيز وتقييم أمن الأنظمة المستغلة، وكذلك تنظيم التسيير في هذا المجال بإعتبارها فاعلا أساسيا ضمن العمليات العسكرية.<sup>3</sup>

**رابعا: على مستوى وزراء العدل.**

أ/- **الأقطاب القضائية المتخصصة :** لقد تم توسيع الأقطاب الجزائية المتخصصة إلى أربعة جهات قضائية والمتمثلة في وهران، قسنطينة، ورقلة، سيدي محمد. لذا فإن التشريعات السابقة تبقى نافذة من أمر 66-155 من قانون الإجراءات الجزائية، أما حسب المادة 889-2 من نفس القانون 25 - 14<sup>4</sup>، وفق المواد المرحلية والنهائية، لذلك فإنه يبقى العمل بالتشريعات السابقة إلى حد إفراز التشريعات

<sup>1</sup> حكمة بوكحيل، سامية بن عديد، الهيئة الوطنية للوقاية من جرائم الإعلام والتكنولوجيا الإتصال ودورها في تفتيش نظم المعلوماتية، مجلة الدراسات القانونية المقارنة، المجلد 7، العدد 1، جامعة محمد الشريف مساعدي سوق أهراس، 2021، ص 1545.

<sup>2</sup> جمال زمورة، ليلي بن عيسى، أهمية حكومة الأمن السيبراني لضمان تحول رقمي آمن للخدمات العمومية في الجزائر، مجلة البحوث الاقتصادية المتقدمة، المجلد 7، العدد 2، جامعة محمد خيضر بسكرة، الجزائر، 2022، ص 424.

<sup>3</sup> عبد الله جعفري، التهديدات السيبرانية وتأثيرها على الأمن القومي الجزائري، المجلة الأفريقية للدراسات القانونية والسياسية، المجلد 6، العدد 2، جامعة أحمد دراية أدرار، الجزائر، 2022، ص 252.

<sup>4</sup> القانون رقم 25-14 مؤرخ في 3 غشت سنة 2025، المعدل والمتمم المتضمن قانون إجراءات الجزائية، ج.ر.ح، العدد 54، الصادر في 13 غشت سنة 2025.

التنفيذية الحديثة، وعليه أن قاضي التحقيق ووكيل الجمهورية وقاضي الحكم يتوسع إختصاصهم في الأفعال الإجرامية المعنية إلى خارج إطارهم الترابي، ويتم هذا بواسطة توسيع التخصص في بعض الجهات القضائية ليضم جهات قضائية مختلفة، وعليه فإن التشريع الحديث للإجراءات الجزائية سنة 2025 بإعتباره مختص بالأقطاب الجزائية والمنسق في النصوص 310 إلى غاية 314 منه على أنه يتولى الإطلاع في الأفعال المجرمة التي تكون معينة منها: المواد المخدرة، النقل الغير القانوني، المتاجرة بالبشر، المتاجرة بأجساد الإنسان، تهريب المهاجرين، الخطف، التلاعب، الممارسات التجارية الغير المشروعة.<sup>1</sup>

## ب/- القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال:

**1- الإختصاص النوعي:** يتأسس الإختصاص النوعي للمحاكم، وذلك حسب طبيعة الفعل الجرمي والتي هي تستخلص من العقوبة المقررة لها في قانون العقوبات أو القوانين المكملة، حيث يقتضي ذلك أن يقوم بتكييف الواقعة وربطها كالنموذج التشريعي الذي يكون مناسباً، ومن ثم تحديد نوع الجريمة الذي يكون على أساس مقدار العقوبة لتعيين الجهة القضائية المختصة.<sup>2</sup> فإن المشرع ذكر الجرائم التي تكون محددة قانونياً وكذلك الجرائم المرتبطة بها، ينعقد الإختصاص الحصري لهذا القطب في هذا المجال في:<sup>3</sup> " بجرائم نشر وترويج أخبار كاذبة بين الجمهور من شأنها المساس بالأمن أو السكينة العامة أو إستقرار المجتمع، جرائم المساس بأنظمة المعالجة الآلية للمعطيات المتعلقة بالإدارات والمؤسسات العمومية، جرائم نشر وترويج أنباء معرضة تمس بالنظام والأمن العموميين ذات الطابع المنظم أو العابر للحدود الوطنية، جرائم التمييز وخطاب الكراهية جرم الإتجار بالأشخاص أو بالأعضاء البشرية أو تهريب المهاجرين بأمن الدولة أو بالدفاع الوطني".<sup>4</sup>

<sup>1</sup> فريد روابح، محاضرات في قانون الإجراءات الجزائية، أقيمت على طلبة السنة الثانية ليسانس، كلية الحقوق والعلوم السياسية، جامعة محمد لمين دباغين، سطيف 2، 2026 ص 17.

<sup>2</sup> جمال الدين بوقرة، جمال الدين عنان، القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 7، العدد 1، جامعة محمد بوضياف، المسيلة، جوان 2022، ص 1684.

<sup>3</sup> زهرة سعيد بن، بلقاسم بالعربي، القطب الجزائي الوطني المتخصص في مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، دراسة في المفهوم والإختصاص، مجلة الدراسات القانونية والإقتصادية، المجلد 8، العدد 2، جامعة يحي فارس، المدية، الجزائر، 2025، ص 611.

<sup>4</sup> سلمى عبد النبي، دور القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال في مواجهة الإعتداءات الواقعة على المعطيات المعلوماتية، مجلة الحقوق والعلوم السياسية، المجلد 11، العدد 2، جامعة خنشلة، جامعة باتنة، 2024، ص 22.

## 2- الإختصاص الإقليمي:

القانون 25- 14 المادة 336 من قانون الإجراءات الجزائية: "يمارس وكيل الجمهورية لدى القطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وقاضي التحقيق ورئيس ذات القطب صلاحياتهم في كل كامل الإقليم الوطني".

وعليه يفهم من هذا النص أن المشرع خول القطب الجزائري إختصاصا إقليميا، كون أنه يمتد إلى كامل التراب الوطني، وذلك نظرا لطبيعة الخاصة للجرائم المتصلة بتكنولوجيا الإعلام والاتصال، التي غالبا ما تتميز بإتساع في نطاق إرتكابها، وكذلك تعدد الأشخاص المتورطين فيها، فضلا عن تعقيدها وخطورتها<sup>1</sup>.

### الفرع الثاني: على المستوى الدولي.

أمام التطور السريع للتكنولوجيات الإعلام والاتصال وإزدياد الجرائم الإلكترونية أصبحت الدولة لوحدها غير قادرة على مواجهة المخاطر السيبرانية، مما أوجب على الدول التعاون فيما بينها لحصر هذا الإجرام المستحدث والقضاء عليها نهائيا، وعليه سنتطرق أولا: إلى التعاون الأمني الدولي، ثانيا: التعاون القضائي الدولي، وثالثا: التعاون الدولي من خلال تسليم المجرمين.

### أولا: التعاون الأمني الدولي.

تقتضي طبيعة العلاقات الدولية وإستمرار الدول في التعايش فيما بينها توفير حد أدنى من الأمن والإستقرار والنظام العام، وتعد الجريمة إحدى القضايا المهمة التي تحظى بإهتمام السلطات العمومية والباحثين والأفراد، لما لها من آثار تمس أمن المجتمع وإستقراره، فلا تستطيع الدولة بمجهودها المنفردة القضاء على الجريمة لاسيما في ظل التطور المتسارع الذي شاهده مجالات الإتصالات وتكنولوجيات المعلومات، ونلاحظ أنه مع الإنتشار الواسع لشبكة الأنترنت برزت أنماط مستحدثة من الجرائم من بينها والجرائم المرتبطة بالفضاء الإلكتروني، بإعتبارها أحد صور الجرائم المعلوماتية التي تمس بسرية الأنظمة المعلوماتية وسلامتها.

<sup>1</sup> أمينة عمورة، إلهام بوحلايس، القطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، مجلة البحوث في العقود وقانون الأعمال، المجلد 7، العدد 1، جامعة الإخوة منتوري، قسنطينة 1، الجزائر، 2022، ص 74.

كما إمتدت آثارها لتشكل تهديدا للمصالح الحيوية والأمن السياسي للدول.<sup>1</sup>

ولمكافحة هذه الظاهرة هناك عدة منظمات أهمها مايلي:

**1. المنظمة الدولية للشرطة الجنائية " الإنتربول "** : تتمثل أهداف هذه المنظمة في تدعيم وتنمية أوجه التعاون المشترك بين سلطات الشرطة الجنائية بمختلف الدول، في حدود القوانين الوطنية السارية، بما ينسجم مع مبادئ الإعلان العالمي لحقوق الإنسان، فضلا عن السعي إلى إنشاء وتطوير الهيئات والمؤسسات القادرة على الإسهام بفعالية في الوقاية من جرائم القانون العام ومكافحتها.<sup>2</sup>

**2. منظمة الشرطة الجنائية الإفريقية " الأفريبول "** : تعتبر هذه المنظمة أكبر منظمة شرطة في القارة الإفريقية، وهي مكونة من قوات الشرطة لواحد وأربعين دولة، مقرها الرئيسي في الجزائر العاصمة تهتم بتسهيل تبادل المعلومات بين قوات الشرطة الوطنية بخصوص الجريمة الدولية والإرهاب والمخدرات والإتجار بالأسلحة في إفريقيا .

ومن أهم أهدافها إلزام المؤسسات الشرطة الإفريقية على إيجاد حلول إفريقية خالصة، وكفيلة بمعالجة كل قضاياها وإنشغالاتها الأمنية .<sup>3</sup>

يمكننا القول أنه على الرغم من حداثة هذه المنظمة إلا أن الجزائر تسعى إلى الإسهام بفعالية في مكافحة الجريمة المنظمة من خلال دعم وتنسيق آليات التعاون الأمني خاصة مع آلية التعاون الشرطي الإفريقي " الأفريبول "، وتبرز أهمية هذا التعاون في ظل تصاعد الجريمة المنظمة والإرهاب، مما يستدعي تعزيز تبادل الخبرات وتطوير القدرات وتكثيف التنسيق الأمني لمواجهة الجريمة العابرة للحدود والحد منها.<sup>4</sup>

<sup>1</sup> فريد ناشف، آليات التعاون الدولي في مكافحة الجرائم الإلكترونية، مجلة البحوث في الحقوق والعلوم السياسية، المجلد 8، العدد 1، جامعة البليدة 2، الجزائر، 2022، ص، ص 437، 438.

<sup>2</sup> آسيا لعمراني، التعاون الدولي في مواجهة الجرائم السيبرانية "الجزائر نموذجا"، المجلة الجزائرية للعلوم السياسية والعلاقات الدولية المجلد 3، العدد 2، كلية العلوم السياسية والعلاقات الدولية، جامعة الجزائر 2، الجزائر، ديسمبر 2012، ص 84.

<sup>3</sup> المرجع نفسه، ص 87.

<sup>4</sup> المرجع نفسه، ص 88.

حيث تقوم العلاقة بين " الأنتربول " و " الأفريبول " على التعاون في مكافحة الجرائم الإلكترونية التي تهدد الأمن الدولي عبر إستهداف الأنظمة الدفاعية والبيانات الحساسة للدول والشركات الكبرى، لذلك أصبح الإجرام الإلكتروني من أهم مجالات إهتمام المنظمات، من خلال التنسيق الأمني وتبادل الأدلة الإلكترونية والمعلومات التقنية لمواكبة تطورات الجريمة السيبرانية.<sup>1</sup>

**3. منظمة الشرطة الأوروبية " الأوروبول ":** في الحقيقة إن إنشاء منظمة الشرطة الجنائية الأوروبية بموجب إتفاق دولي قد جعل مسار تطورها يتسم بالتعقيد، حيث إستلزم ذلك فترة زمنية طويلة من أجل تعديل وتطوير الأسس القانونية الكفيلة بتكليفها مع المهام المستحدثة، كما أن مركزها القانوني لم يكن محددًا بدقة بإعتبارها هيئة أوروبية ذات أساس مستمد من قواعد القانون الدولي العام، وهو ما تمت معالجته سنة 2009 عندما يتم المجلس قرارا يقضي بإعادة تنظيمها وتحويلها إلى هيئة أوروبية ذات إطار قانوني أكبر وضوح ويرى أنه قد منح الإتحاد الأوروبي جهاز "الأوروبول" صلاحيات تهدف إلى تعزيز التعاون بين السلطات الوطنية مع إحترام سيادة الدول خاصة في مجال مكافحة الجريمة المنظمة، من خلال تنسيق إجراءات التحقيق الشرطي والجمركي والقضائي، كما يتيح له الإطار القانوني طلب تدخل الدول الأعضاء والمشاركة في التحقيقات، إضافة إلى تحليل المعلومات المتعلقة بمختلف أشكال الجريمة المنظمة.<sup>2</sup>

### ثانيا: التعاون القضائي الدولي.

إن مواجهة الجرائم الدولية والقضاء عليها يقتضي وجود عمل مشترك بين الدول، الأمر الذي جعل من تكريس مبدأ التعاون القضائي الدولي أمرا حتميا ولا بد منه، وهذا التعاون يلعب دورا كبيرا في تحقيق العدالة الجنائية وذلك من خلال آلياته الفعالة، ويشمل التعاون القضائي عدة أشكال تتمثل فيمايلي:

<sup>1</sup> عبد العزيز لزعر، رشيد زباني، آلية الإتحاد الإفريقي للتعاون " الأفريبول " ودورها في مكافحة الجريمة الإلكترونية، مجلة متون، جامعة مولاي الطاهر، سعيدة، الجزائر، 2021، ص، ص 258، 289.

<sup>2</sup> أمين ودرار، الشرطة الجنائية الإفريقية "الأفريبول"، حوليات جامعة الجزائر 1، المجلد 34، العدد 1، الجزائر، مارس، 2020، ص 145.

**1. تبادل المعلومات:** يتجسد ذلك في قيام الدول بتزويد السلطات القضائية الأجنبية بما تطلبه من بيانات ووثائق وأدلة وقراءة تتعلق بجرمة محل تحقيق أو متابعة، موجهة إلى أحد رعاياها خارج إقليم الدولة، مع بيان الإجراءات المتخذة بشأنه، كما قد يمتد هذا التعاون إلى تبادل السوابق القضائية الخاصة بالمتابعين في مثل هذه الجرائم، وقد كرست الفقرة الثانية من المادة 1 من معاهدة الأمم المتحدة النموذجية للمساعدة المتبادلة في المسائل الجنائية هذا المبدأ، كما أكدت المادة الأولى من إتفاقية الرياض للتعاون القضائي العربي على ضرورة تبادل المعلومات بين الدول الأطراف والتنسيق بين الأنظمة القضائية.<sup>1</sup>

**2. نقل الإجراءات:** تتمثل هذه الصورة من التعاون في قيام دولة ما بناء على إتفاقية أو معاهدة دولية بإتخاذ ومباشرة إجراءات المتابعة وتحقيق بشأن جريمة وقعت في إقليم دولة أخرى ولصالحها، بشرط توافر عدد من الضوابط القانونية، في مقدمتها شرط التجريم المزدوج وأن تساهم الإجراءات المتخذة بصورة فعالة في الوصول إلى الحقيقة وتحقيق العدالة الجنائية.

وقد برزت هذه الصورة العديد من الإتفاقيات الدولية، من بينها المعاهدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية، وإتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لسنة 2020، لاسيما المادة 21 منها. إضافة إلى معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي لسنة 1999 في مادتها 9، وكذا المادة 16 من النموذج الإسترشادي لإتفاقية التعاون القانوني والقضائي الصادرة عن مجلس التعاون الخليجي سنة 2003.<sup>2</sup>

**3. الإنابة القضائية:** يقصد بها طلب قيام دولة ما بإتخاذ إجراء من إجراءات الدعوى العمومية بناء على طلب صادر عن دولة أخرى، عندما يتعذر على السلطات القضائية مباشرة هذا الإجراء بنفسها، وذلك لضرورته في الفصل في نزاع أو قضية معروضة أمامها.

وتهدف هذه الآلية إلى تسهيل الإجراءات الجنائية بين الدول بما يضمن إجراء التحقيقات اللازمة وتقديم المتهمين للمحاكمة، مع تجاوز القيود المرتبطة بمبدأ السيادة الإقليمية الذي يمنع السلطات الأجنبية من ممارسة بعض الأعمال القضائية داخل إقليم دولة أخرى، كسماع الشهود أو إجراء التفتيش وغيرها .

<sup>1</sup> آسيا لعمراني، المرجع السابق، ص 82.

<sup>2</sup> فريد ناشف، المرجع السابق، ص 441.

كما يلاحظ أن العديد من المعاهدات والإتفاقيات المتعلقة بالمساعدة القضائية الدولية إتجهت إلى إلزام الدول الأطراف بتعيين سلطة مركزية غالبا ما تكون وزارة العدل، تتولى إستقبال وإرسال ضباط الإنابة القضائية مباشرة وذلك بهدف تسريع الإجراءات وتحقيق فعالية أكبر في التعاون القضائي الدولي.<sup>1</sup>

### ثالثا: التعاون الدولي من خلال تسليم المجرمين.

يعد تسليم المجرمين أهم مظاهر التعاون القضائي الدولي في مجال العدالة الجنائية، إذ يهدف إلى عدم إفلات الجناة من العقاب بمجرد هروبهم من دولتهم التي إرتكبوا فيها الجريمة لجوءهم إلى دولة أخرى، كما يسهم هذا الإجراء في منع المجرمين من إستغلال إختلاف الأنظمة القانونية بين الدول العثور على مكان أمن يقيهم من المتابعة والعقاب.<sup>2</sup>

ونلاحظ من الفقرة السابقة أن تسليم المجرمين يعتبر أحد أهم صور التعاون القضائي الدولي من خلال قيام الدولة بتسليم شخص موجود في إقليمها إلى دولة أخرى، قصد متابعته جزائيا.

وكانت هذه المسألة في مجال مكافحة الجرائم الإلكترونية موضوع العديد من الإتفاقيات والمعاهدات الدولية أهمها: معاهدة بودابست لمكافحة جرائم الأنترنت من خلال المواد 12، 23، 24 و 25 منها، وتوصيات المجلس الأوروبي بشأن مشاكل الإجراءات الجنائية المتعلقة بالتكنولوجية المعلومات من خلال التوصية (95 / 13) بتاريخ 11 سبتمبر 1995.<sup>3</sup>

### - الإتفاقيات والمعاهدات في مجال مكافحة الجرائم الإلكترونية:

1. إتفاقية بودابست لمكافحة الجريمة السيبرانية:<sup>4</sup> تعد أول معاهدة دولية متخصصة في مواجهة جرائم الأنترنت، وقد تم إعدادها في إطار مجلس أوروبا بالعاصمة المجرية بودابست في أواخر سنة 2001، وقد أبرمت في 8 نوفمبر 2001 وتم المصادقة عليها في 23 نوفمبر 2001، وهدفت إلى وضع إطار

<sup>1</sup> حيلالي شويرب، فائزة مراد، الآليات الدولية والوطنية لمكافحة الجريمة السيبرانية، مجلة الدراسات القانونية والسياسية، المجلد 9، العدد 2، جوان، 2023، ص 166

<sup>2</sup> إيمان بن عثمان، ليلي بن بغيلة، التعاون القضائي الدولي ركيزة أساسية لتحقيق العدالة الجنائية الدولية، مجلة الشهاب، المجلد 11، العدد 1، جامعة الأمير عبد القادر للعلوم الإسلامية، الجزائر، 2025، ص 485.

<sup>3</sup> فريد ناشف، المرجع السابق، ص 442.

<sup>4</sup> إتفاقية مجلس أوروبا المتعلقة بالجريمة المعلوماتية ( إتفاقية بودابست)، اعتمدت بتاريخ 23 نوفمبر 2001 بالعاصمة بودابست، دخلت حيز التنفيذ 01 جويلية 2014.

قانوني دولي موحد لمكافحة الجريمة السيبرانية من خلال إلزام الدول المصادقة بتجريم عدد من الأفعال في تشريعاتها الداخلية.

ويمكننا القول أن هذه الجرائم تشمل الإرهاب الإلكتروني، تزوير بطاقات الائتمان، وإستغلال الأطفال في الدعارة عبر الأنترنت وغيرها من الجرائم المعلوماتية، كما تهدف الإتفاقية إلى تنسيق التشريعات الوطنية بين الدول وتعزيز التعاون الدولي في مجال مكافحة الجرائم الإلكترونية، وقد جاءت نتيجة مشاورات طويلة بين الحكومات وأجهزة الشرطة وخبراء قطاع التكنولوجيا المعلومات بمشاركة عدة دول من بينها الولايات المتحدة الأمريكية.<sup>1</sup>

لقد صادقت على هذه الإتفاقية العديد من الدول، من بينها دول الأعضاء في مجلس أوروبا إضافة إلى دول أخرى مثل: كندا، اليابان، وجنوب إفريقيا، وتنص على إمكانية إنضمام دول أخرى غير الدول الإتحاد الأوروبي، وهذا ما يعكس طبيعتها الدولية الواسعة إستنادا لنص المادة 48 منه.

فيتضح أنه تعد هاته الإتفاقية مرجعا أساسيا في مجال مكافحة الجرائم السيبرانية سواء بالنسبة للإتفاقيات اللاحقة أو التشريعات الوطنية الخاصة بالدول.<sup>2</sup>

## 2. الإتفاقية العربية لمكافحة جرائم تقنية المعلومات:<sup>3</sup>

تم إعتماؤها بتاريخ 21 ديسمبر 2010 إطارا قانونيا إقليميا يهدف إلى تعزيز التعاون بين الدول العربية في مجال مكافحة الجرائم المعلوماتية، وقد نصت الإتفاقية في مادتها الأولى ضمن الفصل الأول على ضرورة تعزيز وتدعيم التعاون العربي المشترك في مواجهة جرائم تقنية المعلومات، بما يضمن الحد من مخاطرها وحماية أمن الدول العربية، ويتضح أنها أقرت مجموعة من الآليات من بينها: التعاون القضائي، تبادل المعلومات، تحديد الاختصاص القضائي، تسليم المجرمين، والمساعدة القضائية المتبادلة.

وأصبحت سارية المفعول بعد التصديق عليها في مصر عام 2015 بعد إنضمام عدد من الدول<sup>4</sup>

<sup>1</sup> سليمان قطاف، عبد الحليم بوقرين، مواجهة الجرائم السيبرانية في ضوء الإتفاقيات الدولية، مجال البحوث القانونية والاقتصادية، المجلد 5، العدد 2، كلية حقوق العلوم السياسية، جامعة عمار تليجي الأغواط، الجزائر، 2022، ص 79.

<sup>2</sup> فريد ناشف، المرجع السابق، ص 343.

<sup>3</sup> المرسوم الرئاسي 14 - 2052، المؤرخ في 08 سبتمبر 2014، المتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، ج.ر.ج، العدد 57.

<sup>4</sup> أسيا لعمراني، المرجع السابق، ص 79.

## المبحث الثاني: جزاء الاخلال بالامن السيبراني و التحديات التي تواجهه

أصبحت الجريمة السيبرانية من أبرز التحديات التي تواجه المجتمعات الحديثة في ظل التطور المتسارع لتكنولوجيا المعلومات والاتصال، لما تسببه من أضرار تمس الأفراد والمؤسسات والدول على حد سواء وقد فرضت هذه الجرائم أنماطا جديدة من المخاطر يصعب التصدي لها بالوسائل التقليدية، مما استدعى وضع أطر قانونية خاصة لمكافحتها، ورغم الجهود التشريعية المبذولة، لا تزال هناك العديد من التحديات القانونية المرتبطة بطبيعة الفضاء الرقمي وتطور أساليب الجريمة الإلكترونية.

وسوف يتم دراسة الجزاءات المقررة لجرائم الفضاء السيبراني في المطلب الأول، أما بالنسبة للمطلب الثاني فتم عنوانته بالتحديات التي تواجه الامن السيبراني

### المطلب الأول: الجزاءات المقررة لجرائم الامن السيبراني .

في ظل توسع إستخدام الفضاء الرقمي، إعتد المشرع الجزائري تدابير تشريعية لتصدي للجريمة الإلكترونية، وذلك سواء ضمن القوانين العامة أو الخاصة، وهذا ما سنتطرق إليه في هذا المطلب:

### الفرع الأول: مكافحة الجريمة السيبرانية بموجب القوانين العامة.

إن الفعل المشبوه الغير القانوني يرى بأنه يشكل أحد مظاهر تدخل الدولة، وذلك بضمان حماية النظام العام و صون الحقوق والحريات في البيئة الرقمية وفق نصوص قانونية.

### أولاً: الدستور.

إن الدستور إلزم بضمان حماية خصوصية ذات الطابع الشخصي، ومنع أي شكل من أشكال المساس بحياتهم الشخصية وفق المادتين من قانون الدستور 38- 140<sup>1</sup>، حيث تعد من صور هذا المساس كل فعل يسيء بسمعة الفرد، أو إلتقاط صورة أو تسجيلهم، وتوجيه الإهانة أو الإتهام الباطل له، كما يضمن الدستور هذه الضمانات ويكفل بصونها تشريعيا، وعليه أنه تم إستحداث مواد تشريعية التي تسعى هذه الأخيرة إلى تحقيق الأمن والتصدي للإعتداءات، خاصة في ظل تزايد المنازعات ضمنها،

<sup>1</sup> الجمهورية الجزائرية الديمقراطية الشعبية مرسوم الرئاسي رقم-442، الموافق 30 ديسمبر سنة 2020، يتعلق بإصدار التعديل الدستوري، المصادق عليه في استفتاء اول نوفمبر سنة 2020، العدد 12

لذا فإن هذه الحماية تواكب الحريات المستحدثة وتتماشى مع الحياة المعاصرة، لاسيما في مجالات الملكية الفكرية وضمانات المصنف، والفنية، ومن هذا المنطلق خاص الدستور هذه الأسس المكفولة تحت إطار تشريعي مستقل يضمن حمايتها، كما يتيح هذا الإطار الفرض له الإمكانية في الولوج إلى المعطيات مع التمتع بالخصوصية، وذلك في انسجام مع توجهات السلطة الجزائرية ومعايير إتفاقيات بين الدول التي تهدف إلى حماية الضمانات الإنسان والحريات الأساسية، وبناء عليه تتجسد هذه الضمانات وفق عدة تشريعات من قانون الدستور.<sup>1</sup>

- القانون الدستور المادة 38: " الحق في الحياة يصنف بالإنسان يحميه القانون ولا يمكن أن يجرم أحد منه إلا في الحالات التي يحددها القانون."

- المادة 40 من قانون الدستور: " تحمي الدولة المرأة من كل أشكال العنف في كل الأماكن والظروف في الفضاء العمومي وفي المجالين المهني والخاص ويضمن القانون الإستفادة الضحايا من هياكل الإستقبال ومن أنظمة التكفل ومن مساعدة قضائية".

### ثانيا: الجريمة الإلكترونية بموجب القانون المدني الجزائري .

يتناول القانون المدني بصفة عامة صور الإعتداء على الحياة الخاصة وما قد ينجم عنه المساس بالحقوق الشخصية المتعلقة بالفرد، من بينها الحق في الخصوصية، وفي نفس السياق يتميز هذا الإعتداء بإقرار حق المتضرر، وذلك في التعويض عن الأضرار الناتجة المتمثل في إنتهاك حياته الخاصة، وبناء على هذا فإن المسؤولية المدنية تعد الأساس القانوني للمطالبة بهذا التعويض.<sup>2</sup> القانون المدني 05-07 المادة 124: " للفعل أي كان يرتكبه الشخص بخطئه ويسبب ضرر للغير من كان سببا في حدوثه بالتعويض".<sup>3</sup>

<sup>1</sup> فاطمة خرفش، سميرة لزار، الإطار المفاهيمي والقانوني لمواجهة الجرائم السيبرانية، مجلة سوسيوولوجيا الجريمة للبحوث والدراسات العلمية في الظواهر الإجرامية، جامعة علي لونيسي، البلدة 2، ص 66.  
<sup>2</sup> أسماء بن لعربي، مديحة الفحلة، مكافحة الجريمة الإلكترونية رؤية تشريعية وإستراتيجيات عملية، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد التاسع، كلية الحقوق العلوم السياسية، 2025، ص 1245.  
<sup>3</sup> القانون رقم 05-07 مؤرخ في 13 مايو سنة 2007، المعدل والمتمم الأمر رقم 75-58، المتضمن القانون المدني، ج ر ج ج، العدد 3، مايو سنة 2007.

### ثالثا: تعديل قانون الإجراءات الجزائية.

في إطار إجراءات التحقيق يستخدم بعض أدوات الخاصة التي تندرج وفق وسائل، كتقنية التسلسل وتوثيق الأصوات وأخذ الصور ومراقبة الاتصالات، حيث يقيد هذه الإجراءات وفق نص تشريعي، أي أنه لا يجوز الولوج إليها إلا بعد نيل الترخيص المسبق وذلك من قبل الجهة المختصة للتأكد من خطورة هذه الجرائم، كما يفرض على المسؤولون بهذه الإجراءات بعدم إفشاء معطيات تكون خاضعة للجانب المهني، مع فرض الضابط الشرطي القضائي المكلف بإعداد تقرير، تقرير يوضح فيه الخطوات التنفيذية، وذلك تحت إطار مراحل التحقيقات والتحريات وفق فئة من الإعتداءات خاصة التي تستهدف نظم المعالجة الرقمية للمعطيات، ويأتي ذلك وفق ما نص عليه المشرع الجزائري للإتصال للجرائم الإلكترونية المعاصرة، طبقا لقانون الإجراءات الجزائية.<sup>1</sup> المادة 124 من قانون 14-25.<sup>2</sup>

### رابعا: مكافحة الجريمة الإلكترونية من خلال قانون العقوبات .

إن المشرع الجزائري، خصص ضمن قانون العقوبات قسما خاصا (قسم السابع مكرر)، حيث يتناول هذا الفرع تنظيم المعطيات التي تمس بالنظم المعالجة الآلية للمعطيات، بإعتبار أن هذا الفرع يسعى إلى معاقبة السلوكيات الغير قانونية التي تستهدف نظم المعلوماتية ذات الصلة بها، مما أقر لها عقوبات تتناسب مع هذه الأفعال المحرمة، وذلك تحت إطار تشريعي في سياق جهود الجزائر لتصدي لمثل هذا النوع من الجرائم الإلكترونية من خلال سن تشريعات خاصة منها.<sup>3</sup> قانون رقم 04-14 المادة 394 مكرر إلى 394 مكرر 7.<sup>4</sup>

<sup>1</sup> أسيا السبتي، عمر بوقريط، الجرائم السيبرانية مفهومها وآليات مكافاتها، مجالات الحقوق والعلوم السياسية، المجلد 18، العدد 1، جامعة الإخوة منتوري، قسنطينة 1، 2025، ص 215.

<sup>2</sup> المادة 124 من القانون 14-25 المتعلق بقانون إجراءات الجزائية

<sup>3</sup> مباركة حنان كركوري، التأصيل القانوني لجرائم السيبرانية المرتكبة عبر الوسائط الرقمية، المجلة الإفريقية للدراسات القانونية والسياسية، المجلد 7، العدد 1، جامعة أحمد دراية، جامعة الجزائر، جوان، 2023، ص 130.

<sup>4</sup> قانون رقم 6/26 مؤرخ في 28 أبريل سنة 2024، المعدل المتمم لأمر 66-155 المتضمن قانون العقوبات، ج ر ج ح، العدد 30، الصادر في 8 يونيو سنة 1966.

من خلال المادة 394 مكرر 1، حيث جرم المشرع في هذه المادة الإعتداء على المعلومات التي يحتويها النظام، وبطبيعة الحال تعد جزء منه، عن طريق الإدخال بالإضافة معطيات غير صحيحة، وإما المحو، وذلك بإزالة معطيات تكون مسجلة، أو أي تغيير البيانات التي تكون موجودة داخل النظام، أو التعديل أو إستبدالها ببيانات أخرى.<sup>1</sup>

" - العقوبات الأصلية": إن تطبيق العقوبة بالنسبة للشخص المعنوي،<sup>2</sup> المادة 394 مكرر من قانون العقوبات، بالحبس من ستة أشهر إلى سنتين، وبغرامة من 60,000 إلى 20,000 دج.

- المادة 394 مكرر 4: " يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي."

- العقوبات التكميلية: " وهذا طبقا لنص المادة 18 من قانون العقوبات.

- المادة 394 مكرر 7، حيث جرم المشرع الإشتراك سواء صدر عن شخص طبيعي أو معنوي في جماعة تسعى إلى التحضير لتحقيق إرتكاب هذه الجريمة، وذلك بإعتبارها تمس بالأنظمة المعلوماتية، لاسيما إذ إقترن هذا الإشتراك بأفعال مادية تجسد هذا التحضير.<sup>3</sup>

## الفرع الثاني: مكافحة الجريمة السيبرانية بموجب القوانين الخاصة .

أمام التزايد المستمر لتهديدات والهجمات الإلكترونية، أصبح من الضروري الإعتماد على قوانين خاصة تهدف إلى تعزيز الأمن السيبراني وحماية الأنظمة المعلوماتية والبيانات الرقمية من مختلف أشكال الإعتداء والإستغلال غير المشروع، حيث سعى المشرع الجزائري إلى وضع إطار قانوني ينظم إستخدام القضاء ويحدد العقوبات اللازمة، وهذا ما سيتم تناوله في هذا الفرع .

<sup>1</sup> سعاد رابح، ضوابط مكافحة الجريمة المعلوماتية، مجلة القانون العام الجزائري والمقارن، المجلد 7، العدد 1، جامعة جيلالي ليايس، سيدي بلعباس، الجزائر، جوان، 2021، ص 270.

<sup>2</sup> عماد دمان ذبيح، سمية بهلول، الآليات العقابية لمكافحة الجريمة الإلكترونية في التشريع الجزائري العدد 13، جامعة عباس لغرور خنشلة، جامعة محمد لمين دباغين، سطيف 2، جانفي، 2020، ص 149.

<sup>3</sup> خيرة عناصر إلهام شهرة زاد روايح، الجريمة الإلكترونية في ظل 04-09 بين الواقع والمأمور، مجلة البحوث القانونية والإقتصادية، المجلد 8، العدد 2، جامعة لونييسي علي البلدية 2، الجزائر، 2025، ص 751.

أولاً: مكافحة الإجرام السيبراني بموجب القانونية 09-04 المتعلق بوقاية من تكنولوجيات الإعلام والاتصال ومكافحتها: وإن كان تجسيدا لبنوده على أرض الواقع ما زال ضعيفا إلى حد الساعة نتيجة إهمال الجوانب التقنية الكفيلة بتصنيف هذه الجرائم وفي تحديد العقوبة المناسبة في حق مرتكبيها، ففي معظم الأحيان تختصر العقوبات على الغرامة المالية فقط<sup>1</sup>

ثانياً: مكافحة الإجرام السيبراني بموجب القانون 18/4 المتعلم القواعد العامة للبريد والاتصالات الإلكترونية: حيث جاء فيه عدم إستعمال شبكات وخدمات إتصال إلكترونية لخرق الحياة الخاصة بالأفراد وفي حالة المخالفة تعتبر جريمة يعاقب عليها القانون،<sup>2</sup> حيث إستحدث هذا القانون مجموعة من الآليات القانونية من أجل التصدي إلى الجرائم المرتبطة بالعالم الافتراضي، من بينها إنشاء سلطة الضبط التي خولت لها مهمة السهر على ضمان إحترام متعاملي البريد والاتصالات الإلكترونية للأحكام التنظيم المتعلقة بها،<sup>3</sup> وذلك وفقا لما نصت عليه المادة 13 من القانون 18-04.

كما جرم إنتهاك سرية المراسلات المرسله عن طريق البريد أو الإتصالات الإلكترونية أو إفشاء مضمونها أو نشرها وإستعمالها بدون ترخيص من المراسل أو المرسل إليه، كذلك جرم محاولة فتح وتحويل المراسلات الصادرة عن طريق البريد الإلكتروني بعقوبة الحبس من سنة إلى خمس سنوات وغرامة مالية من 500,000 إلى 100,000 دج. وهذا لإستنادا لنص المادة 164 من نفس القانون.<sup>4</sup>

ثالثاً: مكافحة الإجرام السيبراني بموجب القانون 18-05 المتعلق بالتجارة الإلكترونية: نص المشرع الجزائري في المادة 3 منه على ما يلي: تمارس التجارة الإلكترونية في إطار التشريع والتنظيم المعمول بها.

غير أنه تمنع كل معاملة عن طريق الإتصالات الإلكترونية تتعلق بمايلي:

- المنتجات التي تمس بحقوق الملكية الفكرية أو الصناعية أو التجارية.

<sup>1</sup> رضا مهدي، الجرائم السيبرانية واليات مكافحتها في التشريع الجزائري، مجلة اليزا للبحوث و الدراسات، المجلد 6، العدد 2، جامعة محمد بوضياف، المسيلة، الجزائر، 2021، ص 118

<sup>2</sup> سعاد واجعوط، مكافحة الجريمة السيبرانية على المستوى الوطني، دفاثر البحوث العلمية، المجلد 06، العدد 2، معاهد الحقوق و العلوم السياسية، المركز الجامعي، تيبازة، الجزائر، 2024، ص 427.

<sup>3</sup> رضا مهدي، المرجع السابق، ص 121

<sup>4</sup> سعاد واجعوط، المرجع السابق، ص 427.

- كل سلعة أو خدمة محظورة بموجب التشريع المعمول به...<sup>1</sup>

وعليه فقد قام هذا القانون بتجريم هاته المخالفات التي تمس النشاط التجاري عبر الأنترنت، ورتب عليها عقوبات مذكورة في نصوص المواد من 37 إلى 48 من هذا القانون وتم تقديرها بغرامة مالية من 200,000 إلى 100,000 دج، كما يمكن للقاضي أن يأمر بغلق الموقع الإلكتروني لمدة تتراوح من شهر إلى ستة أشهر، وهذا إستنادا لما جاء في المادة 37.

\* رابعا: مكافحة الإجرام السيبراني بموجب القانون 15 - 04 المتعلق بالتوقيع والتصديق الإلكترونيين:<sup>2</sup> حيث نص هذا القانون على تجريم الأفعال المرتبطة بالبيانات والمعلومات ذات الطابع الشخصي مثل جريمة إفشاء البيانات الشخصية أو إساءة إستعمالها أنه يعاقب عليها بالحبس من ثلاثة أشهر إلى ثلاث سنوات، وب عقوبة تكميلية غرامة من مليون إلى 5 مليون أو بإحدى العقوبتين فقط، وهذا حسب ما جاء في المادة 68.<sup>3</sup>

وكذلك جريمة جمع البيانات الشخصية للمعني دون موافقته وهذا مائص عليه صراحة المادة 43 حيث أقرت أنه يعاقب الحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 200,000 دج إلى 100,000 دج أو بإحدى العقوبتين.<sup>4</sup>

خامسا: مكافحة الإجرام السيبراني بموجب القانون 25 / 11 المعدل والمتمم بقانون 7/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي:<sup>5</sup> جاء من أجل حماية الحياة الخاصة للأفراد والمعطيات، حيث فرض عقوبات صارمة لبعض الأفعال التي تمس البيانات الشخصية وذلك دون الإخلال بالعقوبات الأشد والمنصوص عليها الساري المفعول.

<sup>1</sup> قانون 5/18 المؤرخ في 10 ماي 2018، المتعلق بالتجارة الإلكترونية، ج ر ج ج، العدد 28 الصادر بتاريخ 16 ماي 2018.  
<sup>2</sup> قانون رقم 15 - 04 المؤرخ في 1 فيفري 2015، تحدد القواعد العام المتعلقة بالتوقيع والتصديق الإلكترونيين، ج ر ج ج، العدد 6، الصادر بتاريخ 2015.

<sup>3</sup> سعاد واجعوط، المرجع السابق، ص ص 426 427.

<sup>4</sup> المرجع نفسه، ص 427

<sup>5</sup> قانون رقم 18 - 7 المؤرخ في 10 يونيو 2018، المعدل والمتمم بالقانون 11/25 المؤرخ في 24 يوليو 2025، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج ر ج ج، العدد 48، الصادر في 24 يونيو 2025.

كما جاء القانون 07/18 في المادة 54 منه، بعقوبة الحبس من سنتين إلى خمس سنوات بغرامة من 200,000 دج إلى 500,000 دج كل شخص يخالف أحكام المادة الثانية من هذا القانون.<sup>1</sup>

ويعاقب بالحبس من سنة إلى ثلاث سنوات بغرامة من 100,000 دج إلى 300,000 دج كل من قام بجمع معطيات ذات طابع شخصي بطريقة تدليسية أو غير نزيهة وغير مشروعة، حسب ما جاء في نص المادة 59 من 07/18.

حيث ادخل المشرع الجزائري بموجب القانون 11/25 المعدل والمتمم من القانون 07/18 مجموعه من الاحكام الاجرائية المستحدثة توائم بين حماية الحقوق والحريات الفردية ، وبين مقتضيات الامن العام والتعاون الدولي . وتتمحور هذه الاحكام حول الوقاية من الجرائم والتحري عنها ، اضافه الى المتابعة الجزائية وتنفيذ العقوبات، حيث تم اقرار اطار قانون صارم لنقل المعطيات نحو الخارج يخضع الرقابة المسبقة وضمان الحماية الامنية الكافية<sup>2</sup>.

واستنادا للمادة 45 مكرر 08 منه فإنه : "في حالة حدوث خرق للمعطيات ذات الطابع الشخصي، يجب على المسؤول عن معالجة اخطار السلطة الوطنية في أجل لا يتجاوز خمسة (05) ايام من علمه بذلك

### المطلب الثاني: تحديات الأمن السيبراني

يعتبر الأمن الرقمي من المجالات التي تواجه في الوقت الحالي ضغطا متزايدا، وذلك نتيجة تعدد مصادر الخطر وتشابكها، وهو الأمر الذي جعل التعامل معها أكثر تعقيدا من السابق كما أن طبيعة هذه التهديدات لم تعد ثابتة، بل أصبحت تتغير باستمرار نظرا لإستهداف مختلف جوانب الأنظمة الرقمية والبنى الأساسية، وهو ما يفرض مقاربة شاملة لفهم هذه الإشكاليات والتعامل معها بفعالية، وهو ما سوف نتناوله في هذا المطلب : الفرع الأول: تحديات الأمن السيبراني في عصر الذكاء الاصطناعي. والفرع الثاني: إستهداف البنية التحتية، الفرع الثالث: مهددات التقنية

<sup>1</sup> نادية لاکلي، الجريمة السيبرانية في الجزائر والعقوبات المقررة لها، مجلة الإجهاد القضائي، المجلد 15، العدد 1، مخبر أثر الإجهاد القضائي على حركة التشريع، جامعة محمد خيضر، بسكرة، الجزائر، 2023، ص 268.

<sup>2</sup> بسمة فوغالي، مستجدات حماية المعطيات ذات الطابع الشخصي في ظل القانون 11/25 ، مجلة البحوث في العقود وقانون الاعمال، المجلد 11، العدد 01 ، جامعة محمد لمين دباغين، سطيف 02، الجزائر ، 2026 ، ص 650.

## الفرع الأول: تحديات الأمن السيبراني في عصر الذكاء الاصطناعي

لقد أصبح تأمين الفضاء الرقمي في ظل توسيع استخدام تقنيات الذكاء الاصطناعي أكثر تعقيدا مما كان عليه سابقا، إذ أنه لم تعد المخاطر واضحة أو سهلة التوقع، وأمام هذا الواقع أفرز تحديات جديدة تتطلب وعيا أكبر وأساليب أكثر دقة ومرونة في التعامل معها ومن بين أهم هذه التحديات والمتمثلة فيما يلي:

### أولا: أضرار عرضية

قد يترتب على المؤسسة نتائج خطيرة تتمثل في إتخاذ إجراءات تمييزية وذلك تجاه بعض الأفراد أو الفئات، وذلك وفق الاعتماد على البيانات وخوارزميات تكون متحيزة في مجال الأمن الرقمي، وهو الأمر الذي يؤدي الى حدوث أضرار ، بالإضافة الى إختلالات التقنية، وهذا راجع للإستناد الى تكنولوجيا الأنظمة الذكية<sup>1</sup>

### ثانيا: التحيز في صنع القرار

إن توظيف تقنيات الذكاء الاصطناعي في مجال الأمن السيبراني قد ينتج عنه آثار سلبية، وذلك متى استندت هذه الأنظمة الى بيانات غير متوازنة أو الى آليات المعالجة التي تفتقر الى الحياد. وعلى هذا النحو، قد ينعكس هذا على طبيعة القرارات باعتبار أنها صادرة منها بصورة تمس فئات أو أشخاص دون غيرهم.<sup>2</sup>

### ثالثا: إنتهاك خصوصية البيانات

تستوجب هذه الوضعية مراجعة التشريع المعمول به قبل إطلاق برامج الأنظمة في مجال الأمن، وذلك لضمان احترام ضوابط السرية على نحو دقيق. ومن هذا المنطلق، يأتي ذلك نتيجة المخاوف التي تكون مرتبطة بحماية المعطيات التي تتعامل معها التقنيات الذكية، من خلال تحليلها ومعالجتها، خاصة أن هذه الأنظمة قد تتيح في بعض الحالات إمكانية الوصول الى تلك البيانات.<sup>3</sup>

<sup>1</sup> سارة بخوش، "الذكاء الاصطناعي والامن السيبراني: الوظائف والتحديات" المجلة الجزائرية للعلوم الإنسانية والاجتماعية، المجلد 09، العدد 01، جامعة قسنطينة 3 صالح بوبنيدر، الجزائر، 2025، ص 146.

<sup>2</sup> يحيى راوية، هاجر كرملاش، "الذكاء الاصطناعي نحو مواجهة التحديات السيبرانية" مجلة العلوم القانونية والاجتماعية، المجلد العاشر، العدد الأول، جامعة باتنة 1، الجزائر، مارس 2025، ص 261.

<sup>3</sup> المرجع نفسه، ص 261

#### رابعاً: الاستخدام الضار للخوارزميات

رغم ما تتميز به خوارزميات الذكاء الاصطناعي من قدرة على معالجة كميات كبيرة من البيانات، والكشف عن الأنماط في وقت وجيز، إلا أن هذه التقنيات يرى بأنها تستغل من قبل بعض الجهات الضارة، وذلك للوصول الى معلومات حساسة أو لإستهداف البنى التحتية، وهو الأمر الذي يثير جملة من المخاطر.<sup>1</sup>

#### خامساً: إساءة استخدام الذكاء الاصطناعي

لا تقتصر آثار الذكاء الاصطناعي على الاستخدامات المشروعة وحسب، بل قد تنعكس سلباً على الأمن السيبراني، وذلك متى جرى توظيفه لأغراض غير مشروعة، والذي قد يتمثل في إنتاج محتويات مضللة أو الترويج لدعايات سلبية.<sup>2</sup>

#### الفرع الثاني: إستهداف البنية التحتية

يعد استهداف البنية التحتية من أخطر التحديات في المجال الرقمي اليوم، وذلك ما ينجم عنه تعطل مباشر للخدمات الأساسية وما قد يترتب عنه من اضطرابات تمس مختلف القطاعات الحيوية، وهو ما تتسم دراسته في هذا الفرع كما يلي :

تواجه البنية التحتية للدول، منها العسكرية أو المدنية، لتهديدات إلكترونية خطيرة لإستهداف<sup>3</sup> قدرة الدولة على أداء مهامها الأساسية، خاصة عندما تتعرض مجموعة من الخدمات والوظائف الحيوية للتعطيل، أو التدمير، مما تمس بالصحة العامة، أو السلامة، أو الأمن القومي، أو جمعها معاً. وعلى هذا الأساس، فإن هذه قطاعات الاتصالات، والطاقة، وكذلك الاعمال المصرفية، والنقل، والصحة العامة، والزراعة والأغذية، المياه، المواد الكيميائية، إضافة الى الملاحة البحرية<sup>4</sup> ففي شهر رمضان من سنة 2012، نفذت مجموعة سيبرانية تطلق على نفسها إسم "سيف العدالة" هجوماً ما أدى الى

<sup>1</sup> فاطمة الزهراء بن أحمد، صحراوي بن شيحة، "الذكاء الاصطناعي وتحسين الأمن السيبراني للمنظمات: دراسة حالة شركة مايكروسوفت"، مجلة البشائر الاقتصادية، المجلد الحادي عشر، العدد 01، جامعة جيلالي اليابس سيدي بالعباس، الجزائر، أبريل 2025، ص 284.

<sup>2</sup> المرجع نفسه، ص 285

<sup>3</sup> سينا محمد، "التحديات الأمنية للدول في الفضاء السيبراني"، قضايا سياسية، العدد 80، ص 319.

<sup>4</sup> وداد بوطلاعة، منال بوكورو، "الهجمات السيبرانية على البنية التحتية الحرجة دراسة في ضوء القانون الدولي العام"، مجلة حقوق الإنسان والحريات العامة، المجلد 07 العدد 02، جامعة الأخوة منتوري قسنطينة1، 2022، ص 328-329.

استهداف الحواسيب المكتبية التابعة لشركة النفط السعودية أرامكو، وعلى الرغم من أن هذا الهجوم لم يوجه فقط نحو الأنظمة المرتبطة بالتشغيل التكنولوجي الخاص بالمنشآت النفطية، وهو ما نتج عنه تعطيل نحو 30000 حاسوب وإخراجها عن الخدمة. وعليه تم استخدام برنامج شمعون في تنفيذ هذه العملية. كما تجدر الإشارة أن هذه المجموعة ابرزت هذا السلوك بأنه أتى في سياق ردها على ما اعتبرته استخدام النظام الحاكم في السعودية لموارده المالية النفطية وذلك في تمويل انتهاكات في عدد من دول منطقة جنوب غرب آسيا<sup>1</sup>، كما شهدت كوريا الجنوبية، في ديسمبر 2014 هجوم الكتروني كبير على شركة الطاقة المائية والنووية، وعليه فلقد أثار مخاوف خاصة على المستوى العالمي وذلك بشأن مدى هشاشة البنى التحتية الحيوية أمام التهديدات السيبرانية. وفي الاتجاه ذاته فإن الولايات المتحدة لم تكن بمنأى عن هذه الهجمات، إذ تعرضت شبكات الكهرباء فيها، حسب سنة 2009، لهجمات واسعة مما أحدثت انقطاعات واسعة<sup>2</sup>.

كما تعد الهجمات السيبرانية، من منظور روسيا، إحدى الوسائل المستخدمة وذلك لبسط السيطرة على فضائها المعلوماتي. وعليه في المقابل هذا هو إضعاف الفضاء المعلوماتي لخصومها، وتحت هذا الإطار، لقد لجأت إلى استخدام برمجيات خبيثة مدمرة، سعياً لإستهداف أجزاء من البنية التحتية الوطنية الأوكرانية، ومن أبرز الأمثلة على ذلك ما وقع ديسمبر 2015، حيث استخدمت برمجيات خبيثة ماسحة ضد شركات توزيع الكهرباء في أوكرانيا، وهو الأمر الذي أدى إلى تخريب إمدادات الكهرباء لنحو ربع مليون مواطن أوكراني، وبعد عام من ذلك، لقد أعيد تنفيذ عملية مماثلة لكن تأثيرها كان أقل فعالية<sup>3</sup>.

<sup>1</sup> أنيس عبد الوهاب بن أحسن، "القوة السيبرانية الإيرانية وأثرها على الاستقرار الإقليمي"، مجلة السياسة العالمية، المجلد 6، العدد 2، جامعة الجزائر 3، الجزائر، 2022، ص738.

<sup>2</sup> سينا علي محمود، المرجع السابق، ص 319.

<sup>3</sup> بخدة خدة، "الصراعات الدولية في العصر الرقمي: دور المنصات الرقمية في صراع روسيا وأوكرانيا"، المجلة الجزائرية للحقوق والعلوم السياسية، المجلد 10، العدد 02، جامعة وهران 2 محمد بن أحمد، الجزائر، 2025، ص 09.

### الفرع الثالث: مهددات التقنية

إن التهديدات التكنولوجية تعد من أبرز المعوقات التي تواجه الأنظمة الرقمية في الوقت الحالي، وذلك خاصة مع سرعتها وتطورها المستمر وصعوبة التنبؤ بها، غير أن هذا الواقع يجعل التعامل معها أكثر تعقيدا، وهذا ما سنتطرق إليه في هذا الفرع المتمثل على النحو الآتي

إن غالبية المعاملات بين الشركات والأفراد والمنظمات تتم في الوقت الراهن، وذلك عبر الفضاء الافتراضي<sup>1</sup>، وعليه فإن عملية تحقيق الأمن الإلكتروني تواجه العديد من العوائق والتحديات، كما يمكن الإشارة الى أهمها فيما يلي<sup>2</sup>:

#### أولا: زيادة عدد المشتركين في شبكة الانترنت لأكثر من 10 ملايين مشترك بالجزائر

وعليه فإنه يتزايد هذا بشكل متوازن تبعا لحجم التحديات ، وعلاوة على ذلك فإن تزايد عدد المستخدمين يؤدي الى ارتفاع مستوى المخاطر، وهو الأمر الذي يجعل عملية تحديد هوية مرتكبي الجرائم الإلكترونية أكثر تعقيدا، نتيجة الصعوبة التي يفرضها عمليات البحث والتحري داخل هذا العدد الكبير والمتنامي باستمرار من قبل المستخدمين.<sup>3</sup>

#### ثانيا: التطور التكنولوجي وظهور الانترنت اللاسلكي

إن نتيجة هذه التقنيات، مرتكب الجريمة الرقمية لم يعد الى الحاجة في التواجد أمام حواسيب مرتبطة بشكل سلكي لشبكة الانترنت، وذلك لتنفيذ أفعاله الاجرامية، ومن هذا الأساس، فإنه يفرض على الجهات الأمنية ضرورة رفع مستوى الجاهزية، وتبني أحدث الوسائل التقنية من أجل مواكبة هذه التطورات، والتصدي لها بفعالية.<sup>4</sup>

<sup>1</sup> حورية بن سيدهم، رقية عواشيرة، "الأمن الفضائي -التحديات والحلول-" المجلة الجزائرية للأمن الإنساني، المجلد 05، العدد 02، جامعة سطيف 2، جامعة باتنة 1، 2020، ص 128.

<sup>2</sup> عادل بوعرعار " الآليات المسخرة لمواجهة تحديات الأمن السيبراني في الجزائر، مجلة سوسيولوجيا للبحوث والدراسات، المجلد 06، العدد الأول، جامعة المدينة، الجزائر، 2025، ص 97.

<sup>3</sup> سميرة بارة، " الأمن السيبراني (Cyber Security) في الجزائر السياسات والمؤسسات، المجلة الجزائرية للأمن الإنساني، العدد الرابع، جامعة قاصدي مرباح ورقلة، جويلية 2017، ص 275.

<sup>4</sup> عادل بوعرعار، المرجع السابق، ص 97.

## خلاصة الفصل الثاني

لقد أبرزت الدراسة أن حماية الفضاء الرقمي أصبح من الضروريات، خاصة في ظل الاعتماد المتزايد على الأنظمة المعلوماتية. وعليه ونظرا لانتشار الجرائم ضمن هذا الفضاء الإلكتروني، لابد من تصدي لهذه الجريمة وذلك بما يشمل تدابير وقائية تسعى الى الحد من وقوعها، بما يعزز من مستوى الحماية ويقلل من المخاطر المحتملة. وفي هذا السياق تبين أهمية تخصص مصالح أمنية وقضائية للتكفل بالجرائم المرتبطة بتكنولوجيا الاعلام والاتصال، بالنظر الى ما تتميز به من خصوصية تقنية تستدعي خبرات وتتلاءم مع طبيعتها. كما عملت الجزائر على تعزيز جهودها الوطنية من خلال استحداث هيئات متخصصة تتولى متابعة التهديدات السيبرانية والتصدي لها، بما يساهم في رفع فعالية الحماية. وإلى جانب ذلك تعزيز التعاون الدولي باعتباره يساعد في تتبع الجريمة الرقمية، خاصة عندما تتجاوز أثارها وإجراءات ارتكابها الحدود الوطنية، وهو ما تجسده مختلف الاتفاقيات الدولية التي انضمت إليها الجزائر في هذا المجال، ومن جانب آخر، يعكس إهتمام المشرع الجزائري بتنظيم مجال الأمن السيبراني من خلال نصوص قانونية تهدف الى تحقيق الأمن في هذا المجال والتصدي لمختلف الاعتداءات عليه. ورغم الجهود المبذولة، لا يزال الأمن السيبراني يواجه معوقات متزايدة مرتبطة بالتطور التقني إضافة الى المخاطر الناتجة عن سوء استخدام الذكاء الاصطناعي، وكذلك تدمير البنية التحتية الأساسية وما ينجم عنه خطورات بالغة.

الخاتمة

## الخاتمة:

من خلال دراستنا لموضوع " الأمن السيبراني تحدي جديد للقانون " خلصنا إلى أن تطورات التكنولوجيا المتسارعة وما صاحبها من توسع في استخدام الوسائل الرقمية، قد أفرزت واقعا جديدا فرض على الأنظمة القانونية ضرورة التكيف مع مختلف المخاطر والتهديدات الناشئة في الفضاء السيبراني، وهذا ما سعت إليه الدراسة من خلال تسليط الضوء على مفهوم الأمن السيبراني وبيان أهميته، باعتباره أحد أهم الركائز الأساسية في بناء مجتمع رقمي آمن ومتطور. حيث يرتبط ارتباطا وثيقا بمجموعة من المفاهيم المشابهة والمتمثلة في التهديد السيبراني، القوة السيبرانية، الإرهاب السيبراني والحرب السيبرانية. بالإضافة إلى تبيان الأنواع المتعلقة بالأمن السيبراني ألا وهي الأمن التشغيلي، أمن التطبيقات وصولا إلى أمن البنية التحتية وأمن المعلومات والبيانات.

وأثبتت الدراسة أن هذا الفضاء الرقمي تتداخل فيه عدة أبعاد فتتوزع بين البعد الذي يتعلق بحماية الطابع الرقمي، والبعد الإقتصادي، بالإضافة إلى البعد القانوني، البعد الاجتماعي وأخيرا البعد العسكري.

وتتكامل هذه الأبعاد والأنواع لتهدف إلى حماية المعلومات والبيانات والشبكات الإلكترونية من جميع الهجمات السيبرانية، كما يساهم أيضا في الحفاظ على سرية المعلومات وسلامتها وضمان توافرها للمستخدمين، وهذا ما يعزز الثقة في التعاملات والخدمات الرقمية.

وعلى الرغم من التطور المتسارع في تكنولوجيا المعلومات والاتصالات وما حققه من فوائد في مختلف المجالات، إلا أنه أدى إلى ظهور أنماط جديدة من الجرائم الإلكترونية والتي تتميز بسرعة انتشارها وصعوبة إكتشافها لكونها جريمة عابرة للحدود والقارات، وباعتبار أنها سهلة الإرتكاب ولا تحتاج إلى أي مجهود كبير، فإن قيام هذه الجريمة يستلزم توفر أركان أساسية تنحصر فيمايلي: الركن المادي، الركن المعنوي والركن الشرعي، من جهة أخرى كشفت الدراسة أهم صور هذه الجرائم السيبرانية، حيث تنقسم إلى جرائم مالية، وتشمل كل من جرائم الإختراقات، جرائم الإستيلاء والنصب والإحتيال، جرائم تعطيل الأجهزة والشبكات وغيرها، إضافة إلى ذلك الجرائم المرتبطة بالبيانات الشخصية مثل جريمة إنتحال

الشخصية، وسرقة الهوية، جريمة المضايقة والملاحقة، جرائم التشهير والجرائم المخلة بالأدب العامة، وكل هذه الجرائم تمس بالمصلحة الشخصية وإنتهاك الخصوصية .

ومن ناحية أخرى أظهرت هذه الدراسة تعدد دوافع إرتكاب الجريمة السيبرانية تبعا للإختلاف الحياة وأهدافهم فقد تكون دوافع مالية، كما قد ترتبط بدوافع سياسية عقادية، وعلاوة على ذلك قد تحدث هذه الجريمة بدافع الإنتقام أو بهدف التسلية واللهو.

كما أنه تم التطرق إلى مختلف الآليات القانونية المعتمدة في مجال الأمن السيبراني والتي تهدف إلى الوقاية من هذه الجرائم، إضافة إلى إبراز دور الجهات والهيئات المختصة المكلفة بحماية الفضاء السيبراني والمتمثلة في الهيئة الوطنية للوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام والاتصال ومكافحتها، مركز الوقاية من الجرائم في الإعلام الآلي والجرائم المعلوماتية التابع للدرك الوطني، فضلا عن الجهود الدولية المبذولة.

وقد بينت الدراسة أن مواجهة هذه الجرائم لا تقتصر على التدابير التقنية فحسب، وإنما تتطلب أيضا إطارا قانونيا فعالا وقادرا على مواكبة التطورات المتسارعة في مجال تكنولوجيا المعلومات والاتصال. وهو ما سعى إليه المشرع الجزائري من أجل توفير الحماية القانونية اللازمة ضد التهديدات السيبرانية، وذلك من خلال سن مجموعة من النصوص القانونية والتنظيمية الرامية إلى حماية الأنظمة المعلوماتية ومكافحة الجرائم، ومن أمثلة ذلك القانون 09 / 04 المتعلق بالوقاية من التكنولوجيات الإعلام والاتصال ومكافحتها، إضافة إلى القانون 04/18 المتعلق بالقواعد العامة للبريد والاتصالات الإلكترونية، والقانون 07/18 المعدل والمتمم بالقانون 11/25 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، وهذه بعض من القوانين التي تجرم هذا نوع من الجرائم إلى جانب إستحداث آليات ومؤسسات مختصة تظهر على تعزيز الأمن السيبراني والوقاية منه .

فيمكننا القول أن المشرع الجزائري قد وضع أسسا قانونية مهمة لتحقيق الأمن السيبراني إلا أن ضمان حماية فعالة وشاملة يظل مرهونا بالتطور المستمر للتشريعات والآليات بما يتناسب مع التحديات الرقمية المتجددة .

وأخيرا، ومن خلال ما سبق يمكننا التأكيد أن الأمن السيبراني لم يعد مجرد مجال تقني متخصص بل أصبح مسؤولية مشتركة وأحد ومقومات الأساسية لتحقيق التنمية الشامل وضمان المستقبل الرقمي للأجيال القادمة .

وفي ختام هذه الدراسة توصلنا إلى مجموعة من النتائج نذكر منها مايلي:

- معظم الجرائم السيبرانية تحدث نتيجة ضعف الوعي الأمني لدى المستخدمين وعدم وجود خطط شاملة للحماية .
- قصور القواعد القانونية التقليدية عن إستيعاب الجرائم السيبرانية المستحدثة بسبب طبيعتها الافتراضية.
- إعتداد البنية التحتية الإلكترونية بشكل متزايد على الأنظمة الرقمية، مما يجعلها عرضة للهجمات التي لها عواقب يمكن أن تمس بالمصلحة المادية والمعنوية للمستخدمين .
- الصعوبات التي تواجه الأجهزة القضائية والأمنية في جمع الأدلة وإثبات الجرائم السيبرانية، ومع صعوبة تتبع الأثر الإلكتروني العابر للحدود في مجال التحريات، وهذا نظرا لتطورها بشكل متسارع.
- الآثار الخطيرة التي تخلفها الجرائم السيبرانية لها أثر سلبي على الأفراد من خلال الإبتزاز المالي والإحتيال، التأثير النفسي، وعلى مستوى المؤسسات بفقدان ثقة بين العملاء وتسرب البيانات وكذلك سرقة الملكية الفكرية، أما على مستوى الدول عن طريق التهديدات الأمنية والإقتصادية.
- الحماية التشريعية المقررة في مجال الأمن السيبراني وأنظمة المعلومات متخذة من قوانين متفرقة يصعب التحكم في ضبط حماية فعالة ودقيقة في غياب نص قانوني خاص يقوم بتنظيم هذا المجال.
- للجرائم السيبرانية تأثير سلبي على الحريات وحرمة الحياة الخاصة في حال إستخدام تكنولوجيا إعلام والاتصال بشكل مخالف للقوانين والتنظيمات.

بناء على نتائج أعلاه نقترح مجموعة من التوصيات نستخلصها فيما يلي:

- تكثيف برامج التوعية والتثقيف حول مخاطر الجرائم السيبرانية وسبل الوقاية منها، وذلك من خلال الحملات التوعوية والملتقيات، مع إمكانية إدراج الأمن السيبراني في المنظمات التعليمية.
- الإسراع في تحديث المنظومة التشريعية، وذلك بسن نصوص قانونية خاصة ومستقلة تجرم هذه الجرائم السيبرانية.
- تحسين أمن البنية التحتية الإلكترونية من مختلف التهديدات، وذلك من خلال تطبيق روابط أمنية قوية وإنشاء مراكز للسلامة المعلوماتية، ووضع خطط للطوارئ.
- ضرورة وضع تدابير حمائية وإستباقية من قبل المؤسسات والدول نظرا للخسائر التي تخلفها الجرائم السيبرانية .
- ضرورة سن تقنين خاصة يعنى بالأمن السيبراني وحماية أمن المعلومات .
- تعزيز التعاون الدولي مع المنظمات والدول المتقدمة، وتبادل المعلومات والخبرات لمكافحة هذه الجرائم .
- وضع ميثاق دولي يلزم جميع الدول بالإنطواء تحته يهدف إلى حماية الحقوق والحريات وحرمة الحياة الخاصة ضد مخاطر الإجرام السيبراني .

## قائمة المصادر المراجع

## قائمة المصادر والمراجع:

أولا: المصادر:

### 1.الدساتير

- الجمهورية الجزائرية الديمقراطية الشعبية المرسوم الرئاسي رقم-442،الموافق 30ديسمبر سنة 2020 ،يتعلق بإصدار التعديل الدستوري ،المصادق عليه في استفتاء اول نوفمبر سنة 2020،العدد 12

### 2.القوانين:

- القانون رقم 05- 07 المؤرخ في 13 مايو سنة 2007، المعدل والمتمم الأمر رقم 75- 58، المتضمن القانون المدني، ج ر ج ج، العدد 3، مايو سنة 2007.
- قانون 04-09 المؤرخ في 5 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها، ج.ر.ج. ج، العدد 47 الصادر بتاريخ 16 اوت 2009.
- قانون رقم 15 - 04 المؤرخ في 1 فيفري 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج ر ج ج، العدد 6، الصادر بتاريخ 2015.
- القانون 18-04 المؤرخ في 10ماي2018، المتعلق بالقواعد المتعلقة بالبريد والاتصالات الإلكترونية، ج. ر. ج. ج، العدد27، الصادر في 31ماي2018.
- قانون 5/18 المؤرخ في 10 ماي 2018، المتعلق بالتجارة الإلكترونية، ج ر ج ج العدد 28 ،الصادر بتاريخ 16 ماي 2018.
- قانون رقم 18 - 07 المؤرخ في 10 يونيو 2018، المعدل والمتمم بالقانون 11/25 المؤرخ في 24 يوليو 2025، المتعلق بحماية الأشخاص الطبيعية في مجال معالجة المعطيات ذات الطابع الشخصي، ج ر ج ج، العدد 48، الصادر في 24 يونيو 2025.
- القانون رقم 25-14 مؤرخ في 3 غشت سنة 2025،المعدل والمتمم المتضمن قانون إجراءات الجزائية ،ح.ر.ج.ح،العدد54،الصادر في 13 غشت سنة 2025.
- قانون رقم 6/26 مؤرخ في 28 أبريل سنة 2024، المعدل والمتمم لأمر 66- 155 المتضمن قانون العقوبات، ج ر ج ج، العدد 30، الصادر في 8 يونيو سنة 1966.

3. المراسيم الرئاسية:

- المرسوم الرئاسي ، رقم 15 - 261 المؤرخ في 24 ذي الحجة 1436 الموافق لـ 8 أكتوبر 2015، الذي يحدد تشكيلة و تنظيم و كفاءات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها، ج .ر.ج. ج ، العدد 53، الصادر في 18 أكتوبر 2015

4. الاتفاقيات الدولية:

- إتفاقية مجلس اوروبا المتعلقة بالجريمة المعلوماتية (اتفاقية بودابست)، اعتمدت بتاريخ 23 نوفمبر 2001 بالعاصمة بودابست، دخلت حيز التنفيذ 01 جويلية 2014
- المرسوم الرئاسي 14 - 2052، المؤرخ في 08 سبتمبر 2014، المتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، ج.ر.ج.ج، العدد 57

5. المعجم :

- مجمع اللغة العربية، " المعجم الوسيط"، ط4، مكتبة الشروق الدولية، القاهرة، مصر، 2004

ثانيا: المراجع:

1. الكتب

- سليمة سعيدي، بلال حجاز، جرائم المعلومات والشبكات في العصر الرقمي، ط1، دار الفكر الجامعي، الإسكندرية، مصر، 2017.
- شادي عبد الوهاب منصور، حروب الجيل الخامس: أساليب التحفيز من الداخل على الساحة الدولية، ط1، العربي للنشر والتوزيع، القاهرة، مصر، 2019
- فارس محمد العمارات، ابراهيم الحمامصة، الأمن السيبراني: المفهوم وتحديات العصر، ط1، دار الخليج للنشر والتوزيع، الأردن، عمان، 2022
- فارس محمد العمارات، "جرائم العصر من الرقمية إلى السيبرانية"، ط1، دار الخليج للنشر والتوزيع، الأردن، عمان، 2023
- محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام الغير مشروع لشبكة الأنترنت دراسة مقارنة، ط2، دار النهضة العربية، القاهرة، 2009

- محمد كمال، الإرهاب السيبراني، ط1، دار كلیم للطباعة والنشر والتوزيع، القاهرة، مصر، 2022
- محمود أحمد طه، المواجهة التشريعية لجرائم الكمبيوتر والأنترنت، دراسة مقارنة، دار الفكر والقانون، 2016-2017.
- منى الأشقر جبور، "السيبرانية هاجس العصر"، المركز العربي للبحوث القانونية والقضائية، بيروت، لبنان، 2017

## 2. المقالات

- إدريس بن عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، كلية الحقوق والعلوم السياسية، جامعة العربي تبسي - تبسة، الجزائر
- اسلام مصطفى، جمعة مصطفى، "جريمة اختراق الأمن السيبراني وحماية استخدام البيانات والمعلومات في القانون المصري"، المجلة القانونية، 12، العدد 3، جامعة القاهرة، 2022
- أسماء بن لعربي، مديحة الفحلة، مكافحة الجريمة الإلكترونية رؤية تشريعية وإستراتيجيات عملية، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد التاسع، كلية الحقوق العلوم السياسية، 2025
- إسماعيل بن يحيى، التعريف بمراقبة الاتصالات الإلكترونية كإجراء من إجراءات جمع الأدلة في الجريمة الإلكترونية، مجلة صوت القانون، المجلد 8، العدد 2، المركز الجامعي علي كافي، تندوف، الجزائر، 2022
- اسمهان بوضياف، "الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 11، جامعة محمد بوضياف-المسيلة، سبتمبر 2018
- أسيا السبتي، عمر بوقريط، الجرائم السيبرانية مفهوما وآليات مكافحتها، مجالات الحقوق والعلوم السياسية، المجلد 18، العدد 1، جامعة الإخوة منتوري، قسنطينة 1، 2025
- آسيا لعمرائي، التعاون الدولي في مواجهة الجرائم السيبرانية "الجزائر نموذجا"، المجلة الجزائرية للعلوم السياسية والعلاقات الدولية المجلد 3، العدد 2، كلية العلوم السياسية والعلاقات الدولية، جامعة الجزائر 2، الجزائر، ديسمبر 2012
- أمين ودرار، الشرطة الجنائية الإفريقية "الأفريبول"، حوليات جامعة الجزائر 1، المجلد 34، العدد 1، الجزائر، مارس، 2020

- أمينة عمورة، إلهام بوحلايس، القطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، مجلة البحوث في العقود وقانون الأعمال، المجلد 7، العدد 1، جامعة الإخوة منتوري، قسنطينة 1، الجزائر، 2022
- أنيس عبد الوهاب بن أحسن، "القوة السيبرانية الإيرانية وأثرها على الاستقرار الإقليمي"، مجلة السياسة العالمية، المجلد 6، العدد 2، جامعة الجزائر 3، الجزائر، 2022
- إيمان بن عثمان، ليلي بن بغيلة، التعاون القضائي الدولي ركيزة أساسية لتحقيق العدالة الجنائية الدولية، مجلة الشهاب، المجلد 11، العدد 1، جامعة الأمير عبد القادر للعلوم الإسلامية، الجزائر، 2025
- بخدة خدة، "الصراعات الدولية في العصر الرقمي: دور المنصات الرقمية في صراع روسيا أوكرانيا"، المجلة الجزائرية للحقوق والعلوم السياسية، المجلد 10، العدد 02، جامعة وهران 2 محمد بن أحمد، الجزائر، 2025
- بسمه فوغالي، مستجدات حماية المعطيات ذات الطابع الشخصي في ظل القانون 11/25، مجلة البحوث في العقود وقانون الاعمال، المجلد 11، العدد 01، جامعة محمد لمين دباغين، سطيف 02، الجزائر، 2026
- جمال الدين بوقرة، جمال الدين عنان، القطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 7، العدد 1، جامعة محمد بوضياف، المسيلة، جوان 2022
- جمال زمورة، ليلي بن عيسى، أهمية حكومة الأمن السيبراني لضمان تحول رقمي آمن للخدمات العمومية في الجزائر، مجلة البحوث الاقتصادية المتقدمة، المجلد 7، العدد 2، جامعة محمد خيضر بسكرة، الجزائر، 2022
- حكيمة بوكحيل، سامية بن عديد، الهيئة الوطنية للوقاية من جرائم الإعلام والتكنولوجيا الاتصال ودورها في تفتيش نظم المعلوماتية، مجلة الدراسات القانونية المقارنة، المجلد 7، العدد 1، جامعة محمد الشريف مساعدي سوق أهراس، 2021
- حمزة خضري، حمزة غشاش، "خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري"، مجلة الدراسات القانونية، المجلد 06، العدد 02، جامعة محمد بوضياف المسيلة، 2020

- حنان مهداوي، "التنظيم القانوني للجريمة الإلكترونية في التشريع الجزائري"، مجلة الفكر القانوني والسياسي، المجلد 06، العدد 02، كلية الحقوق والعلوم السياسية، جامعة محمد لمين دباغين، سطيف، 2022
- حورية بن سيدهم، رقية عواشرية، "الأمن الفضائي - التحديات والحلول -" المجلة الجزائرية للأمن الإنساني، المجلد 05، العدد 02، جامعة سطيف 2، جامعة باتنة 1، 2020
- حيلالي شويرب، فايزة مراد، الآليات الدولية والوطنية لمكافحة الجريمة السيبرانية، مجلة الدراسات القانونية والسياسية، المجلد 9، العدد 2، جوان، 2023
- خيرة عناصر إلهام شهرة زاد روابح، الجريمة الإلكترونية في ظل 04-09 بين الواقع والمأمور، مجلة البحوث القانونية والإقتصادية، المجلد 8، العدد 2، جامعة لونيبي علي البليدة 2، الجزائر،
- دنيا زاد ثابت، مراقبة الاتصالات الإلكترونية والحقوق في حرمة الحياة الخاصة في القانون الجزائري، مجلة العلوم الإجتماعية والإنسانية، العدد السادس، جامعة تبسة
- راضية عيمور، "الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري"، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد 06، العدد 01، جامعة الأغواط، 2022
- رجاء أو مدور، فرشة كمال، التفتيش الجزئي في البيئة الرقمية، مجلة صوت القانون، المجلد 7، العدد 1، جامعة محمد البشير الإبراهيمي، برج بوعرييج، الجزائر، ماي 2020
- رضا مهدي، الجرائم السيبرانية واليات مكافحتها في التشريع الجزائري، مجلة اليزا للبحوث و الدراسات، المجلد 6، العدد 2، جامعة محمد بوضياف، المسيلة، الجزائر، 2021
- رضا هميسي، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، العدد 5، جامعة ورقلة، جامعة الوادي، الجزائر، جوان 2012
- رضوان علي، رزق الله العربي بن مهدي، المكافحة المؤسسية للجريمة الإلكترونية في التشريع الجزائري، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد 9، العدد 2، جامعة عمار ثليجي، الأغواط
- ريمة بن عميروش، "عن خصوصية الجريمة المعلوماتية"، مجلة الفقه القانوني والسياسي، المجلد 2، العدد 2، جامعة محمد الصديق بن يحيى، جيجل، أكتوبر 2024

- زهرة سعيد بن، بلقاسم بالعربي، القطب الجزائري الوطني المتخصص في مكافحة الجرائم المتصلة بالتكنولوجيا الإعلام والإتصال، دراسة في المفهوم والإختصاص، مجلة الدراسات القانونية والإقتصادية، المجلد 8، العدد 2، جامعة يحي فارس، المدية، الجزائر، 2025
- سارة بخوش، "الذكاء الاصطناعي والأمن السيبراني: الوظائف والتحديات" المجلة الجزائرية للعلوم الإنسانية والإجتماعية، المجلد 09، العدد 01، جامعة قسنطينة 3 صالح بوبنيدر، الجزائر، 2025
- ساعد بوقرص، الأمن السيبراني "مخاطر وتحديات وتطلّبات ممارسات وتوصيات واستراتيجيات خاصة"، مجلة الأبحاث في الحماية الإجتماعية، المجلد 03، العدد 01، الجزائر 2022
- سعاد رابح، ضوابط مكافحة الجريمة المعلوماتية، مجلة القانون العام الجزائري والمقارن، المجلد 7، العدد 1، جامعة جيلالي لياس، سيدي بلعباس، الجزائر، جوان، 2021
- سعاد واجعوط، مكافحة الجريمة السيبرانية على المستوى الوطني، دفاثر البحوث العلمية، المجلد 06، العدد 2، معاهد الحقوق و العلوم السياسية، المركز الجامعي، تيبازة، الجزائر، 2024
- سعيد محمودي، "الأمن السيبراني في الجزائر: بين المعالجة الأمنية والحماية القانونية"، مجلة الناقد للدراسات السياسية، المجلد 7، العدد 2، جامعة بشار، الجزائر، 31 أكتوبر 2023
- سفيان ملوكي، عمر جيلالي، السياسة العامة الأمنية الجزائرية في ضوء التحديات السيبرانية المعاصرة، مجلة الفكر القانوني والسياسي، المجلد 9، العدد 2، جامعة عمار ثليجي، الأغواط، 2025
- سلمى عبد النبي، دور القطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال في مواجهة الاعتداءات الواقعة على المعطيات المعلوماتية، مجلة الحقوق والعلوم السياسية، المجلد 11، العدد 2، جامعة خنشلة، جامعة باتنة، 2024
- سليم مزبود، "الجرائم المعلوماتية واقعها في الجزائر وآلية مكافحتها"، المجلة الجزائرية للاقتصاد والمالية، العدد 1، جامعة المدية، أفريل 2014
- سليمان قطاف، عبد الحليم بوقرين، مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية، مجال البحوث القانونية والاقتصادية، المجلد 5، العدد 2، كلية حقوق العلوم السياسية، جامعة عمار ثليجي الأغواط، الجزائر، 2022
- \_\_\_\_\_، "الأمن السيبراني والمضامين المفاهيمية المرتبطة به"، مجلة وطنية للدراسات العلمية الأكاديمية، المجلد 05، العدد 02، جامعة الأغواط، الجزائر، 2022

- سميحة بلقاسم، حميد بوشوشة، الجريمة الإلكترونية بعد جديد للإجرام في الجزائر واقعها وآليات مجابقتها، مجلة العلوم الإنسانية أم البواقي، المجلد 10، العدد 1، جامعة 8 ماي 1945، جامعة قسنطينة 3، جوان 2023
- سميرة بارة، "الأمن السيبراني (Cyber Security) في الجزائر السياسات والمؤسسات، المجلة الجزائرية للأمن الإنساني، العدد الرابع، جامعة قاصدي مرباح ورقلة، جويلية 2017
- سهيلة بوزيرة، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بين سرية المعطيات الشخصية الإلكترونية ومكافحة الجرائم الإلكترونية، المجلة النقدية للقانون والعلوم السياسية، المجلد 17، العدد 2، جامعة تيزي وزو، جامعة محمد الصديق بن يحيى جيجل، الجزائر، 2022
- سينا محمد، "التحديات الأمنية للدول في الفضاء السيبراني"، قضايا سياسية، العدد 80
- صابر بحري، منى خرموش، أهم الدوافع السيكلوجية وراء الجريمة الإلكترونية، مجلة دراسات في سيكلوجية الانحراف، المجلد 06، العدد 01، جامعة محمد لمين دباغين، جامعة سطيف 02، الجزائر، ماي 2021
- صفيان بخدة، ناصر وقاص، الطبيعة القانونية للجرائم المستحدثة ووسائل ارتكابها جريمة الأنترنت كنموذج، مجلة البحوث القانونية والسياسية، المجلد 03، العدد 16، جامعة مولاي الطاهر، سعيدة، الجزائر، أفريل 2021
- عادل بوعرعار "الآليات المسخرة لمواجهة تحديات الأمن السيبراني في الجزائر، مجلة سوسيولوجيا للبحوث والدراسات، المجلد 06، العدد الأول، جامعة المدية، الجزائر، 2025
- عائشة عبد الحميد، "الجرائم المعلوماتية وكيفية مكافحتها"، مجلة الإناسة وعلوم المجتمع، العدد 07، جامعة الشاذلي بن جديد الطارف، الجزائر، جويلية 2020
- عبد الصديق شيخ، الوقاية من الجرائم الإلكترونية في ظل قانون رقم 09/ 04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، مجلة معالم للدراسات القانونية والسياسية، المجلد 4، العدد 1، جامعة يحيى فارس بالمدية، الجزائر، 2020
- عبد العالي حاحة، سميرة قلات، المكافحة الإجرائية للجرائم الإلكترونية، دراسة حالة الجزائر، مجلة المفكر، المجلد 13، العدد 2، جامعة محمد خيضر بسكرة، جانفي، 2018

- عبد العزيز بن فهد ،بن محمد بن داود، "الجرائم السيبرانية : دراسة تأصيلية مقارنة"، مجلة الإجتهد للدراسات القانونية والاقتصادية، المجلد 09، العدد 03، جامعة تمنراست، 2020
- عبد العزيز لزعر ،رشيد زباني، آلية الاتحاد الإفريقي للتعاون " الأفربول " ودورها في مكافحة الجريمة الإلكترونية، مجلة متون، جامعة مولاي الطاهر، سعيدة، الجزائر، 2021
- عبد القادر فلاح، حجز وحفظ المعطيات في الجريمة الإلكترونية، مجلة صوت القانون، المجلد الثامن، العدد 1، جامعة الجيلالي بونعامة الخميس مليانة، 2021
- عبد القادر فلاح، عبد المالك نادية أيت، التحقيق الجنائي لجرائم الإلكترونية وإثباتها في التشريع الجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 4، العدد 2، جامعة الجيلالي بونعامة ،خميس مليانة، 2019
- عبد الله جعفري، التهديدات السيبرانية وتأثيرها على الأمن القومي الجزائري، المجلة الأفريقية للدراسات القانونية والسياسية، المجلد 6، العدد 2، جامعة أحمد دراية أدرار، الجزائر، 2022
- علاء الدين فرحات، الفضاء السيبراني: "تشكيل ساحة المعركة في القرن الحادي والعشرين"، مجلة العلوم القانونية والسياسية، المجلد 10، العدد 03، ديسمبر 2019
- علي بن طراز، "الأمن السيبراني: المدلول والماهية"، مجلة البحوث والدراسات المعاصرة، المجلد 02، العدد 01، مديرية الخدمات الجامعية، قالمة، 2024
- عماد دمان ذبيح، سمية بهلل، "الآليات العقابية لمكافحة الجريمة الإلكترونية في التشريع الجزائري"، العدد 13، جامعة عباس لغرور خنشلة، جامعة محمد لمين دباغين سطيف 2، جانفي 2020
- عماد دمان ذبيح، سمية بهلل، الآليات العقابية لمكافحة الجريمة الإلكترونية في التشريع الجزائري العدد 13، جامعة عباس لغرور خنشلة، جامعة محمد لمين دباغين، سطيف 2، جانفي، 2020
- فاطمة الزهراء بن أحمد، صحراوي بن شيحة، "الذكاء الاصطناعي وتحسين الأمن السيبراني للمنظمات: دراسة حالة شركة مايكروسوفت"، مجلة البشائر الاقتصادية، المجلد الحادي عشر، العدد 01، جامعة جيلالي اليابس سيدي بالعباس، الجزائر، أبريل 2025
- فاطمة خرشف، سميرة لزار، الإطار المفاهيمي والقانوني لمواجهة الجرائم السيبرانية، مجلة سوسيولوجيا الجريمة للبحوث والدراسات العلمية في الظواهر الإجرامية، جامعة علي لونيبي، البليدة 2

- فاطيمة حايطي، نبيلة هبة هروال، الحماية الإجرائية للحق في الخصوصية الرقمية في مواجهة الجريمة المعلوماتية، مجلة الدراسات القانونية، المجلد 7، العدد 2، جامعة ابن خلدون، تيارت، الجزائر، جوان 2021
- فتيحة خليف، محمد صالح مهداوي، خصوصية التفتيش في البيئة الرقمية، المجلة الجزائرية للقانون المقارن، المجلد 5، العدد 9، جامعة بلحاج بوشعيب بعين تموشنت، الجزائر، 2022
- فريد ناشف، آليات التعاون الدولي في مكافحة الجرائم الإلكترونية، مجلة البحوث في الحقوق والعلوم السياسية، المجلد 8، العدد 1، جامعة البليدة 2، الجزائر، 2022
- كريمة مزروقي، مراقبة الاتصالات الإلكترونية وحقوق الفرد في الخصوصية المعلوماتية، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 5، العدد 2، جامعة مولود معمري، تيزي وزو، 2020
- كمال حفصاوي، عمر مخلوف، التفتيش الإلكتروني بين ضرورة التحقيق والحقوق في سرية المراسلات والاتصالات، مجلة الباحث للدراسات الأكاديمية، المجلد 11، العدد 1، جامعة سطيف 2، جامعة غليزان، 2024
- لبنى خميس مهدي، صفاء تغريد، أثر السيبرانية في تطور القوة، مجلة حمورابي، المجلد 8، العدد 33-34، العراق، 2020
- مباركة حنان كركوري، التأصيل القانوني لجرائم السيبرانية المرتكبة عبر الوسائط الرقمية، المجلة الإفريقية للدراسات القانونية والسياسية، المجلد 7، العدد 1، جامعة أحمد دراية، جامعة الجزائر، جوان، 2023
- محمد بعجي، التزامات مقدمي الخدمة عبر الأنترنت، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 4، العدد 1، جامعة الجزائر 1، 2019
- محمد بلقاسم بوفاتح، الجريمة الإلكترونية، دراسة سوسيو قانونية، كلية الحقوق والعلوم السياسية، جامعة الجلفة
- محمد جواد بمراح، رفيقة زبدة، إستراتيجية الدفاع الجزائرية لمواجهة التهديدات السيبرانية، مجلة الرسالة للدراسات والبحوث الإنسانية، المجلد 10، العدد 1، جامعة أبي بكر بالقائد، جامعة الجلفة، الجزائر، 2025
- منى عبد الله السمحان، "متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية"، مجلة كلية التربية، العدد 111، جامعة المنصورة، مصر، 2020

- مونة مقلاتي، راضية مشري، "الجريمة الإلكترونية دلالة المفهوم وفعالية المعالجة القانونية"، مجلة أبحاث قانونية وسياسية، المجلد 06، العدد 01، جامعة 08 ماي 1945، جوان 2021
- نادية لاکلي، الجريمة السيبرانية في الجزائر والعقوبات المقررة لها، مجلة الإجهاد القضائي، المجلد 15، العدد 1، مخبر أثر الاجتهاد القضائي على حركة التشريع، جامعة محمد خيضر، بسكرة، الجزائر، 2023
- نجية عراب ثاني، الآليات الوقائية من جرائم تكنولوجيا الإعلام والاتصال ومكافحتها في القانون الجزائري، مجلة البحوث في الحقوق والعلوم السياسية، المجلد 8، العدد 1، جامعة أبو بكر بالقائد، تلمسان، الجزائر، 2022
- وداد بن سالم، عبد الله شيباني، النظم القانوني لمقدمي خدمة الأنترنت في ظل القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد 13، العدد 01، جامعة محمد لمين دباغين، سطيف 2، 2024
- وداد بوطلاعة، منال بوكورو، "الهجمات السيبرانية على البنية التحتية الحرجة دراسة في ضوء القانون الدولي العام"، مجلة حقوق الإنسان والحريات العامة، المجلد 07 ن العدد 02، جامعة الأخوة منتوري قسنطينة 1، 2022
- وهيبة سامي، "الجريمة الإلكترونية: دراسة في المفهوم والمظاهر"، مجلة قضايا معرفية، المجلد 02، العدد 03، جامعة الجلفة، سبتمبر 2022
- يحيى راوية، هاجر كرماش، "الذكاء الاصطناعي نحو مواجهة التحديات السيبرانية" مجلة العلوم القانونية والاجتماعية، المجلد العاشر، العدد الأول، جامعة باتنة 1، الجزائر، مارس 2025
- يزيد بوحليط، تفتيش المنظومة المعلوماتية وحجز المعطيات في التشريع الجزائري، التواصل في الاقتصاد والإدارة والقانون، العدد 48، جامعة باجي مختار عنابة، ديسمبر 2016

### 3. الرسائل العلمية

أ. أطروحة دكتوراه:

ملیكة بقاح، إشكالية الجرائم الإلكترونية في التشريع الجزائري، رسالة دكتوراه في علوم الإعلام والاتصال، كلية علوم الإعلام والاتصال، جامعة الجزائر 3

### ب. رسالة ماجستير:

سفيان سوير، محمد بن عمار، جرائم معلوماتية، رسالة ماجستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بالقائد، تلمسان

### ج. مذكرات ماستر:

- ابتسام بوبعابة، التحقيق في الجريمة الإلكترونية، مذكرة ماستر في قانون الإعلام الآلي والأنترنيت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعرييج
- حمزة لعباشي، محمد الأمين قعفر، الأمن السيبراني وحماية البيانات الرقمية في الجزائر، مذكرة ماستر، في قانون الإعلام الآلي وأنترنيت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي - برج بوعرييج، الجزائر، 2023-2024.
- حسام بن ميسا، عبد المولى حملاوي، آليات مكافحة الجريمة الإلكترونية في التشريع الجزائري، رسالة ماستر في القانون الجنائي، قسم الحقوق، المركز الجامعي، عبد الحفيظ بوالصوف - ميله، 2014.
- سهام بوشاقور، المسؤولية الجزائية عن الجريمة الإلكترونية، مذكرة ماستر في قانون جنائي، قسم القانون العام، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم، جوان 2023
- شيماء مساط، عائشة بوطيبة، تأثير الجريمة الإلكترونية على الأمن السيبراني في الجزائر، مذكرة ماستر في قانون جنائي، معهد الحقوق، المركز الجامعي عبد الحفيظ بوالصوف ميله، 2024-2025
- عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماستر في إدارة التحقيقات الاقتصادية والعلوم التجارية والمالية، قسم علوم التسيير، كلية علوم التسيير، 2 جويلية 2019
- كريمة صمودي، سمر برقعي، الأمن السيبراني في الجزائر، مذكرة ماستر في قانون أعمال، كلية الحقوق والعلوم السياسية، جامعة 08 ماي 1945، قالمة، الجزائر، 2024-2025
- محمد الدام، الأمن السيبراني، مذكرة ماستر في جريمة وأمن، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمة لخضر، جامعة الواد، 2022-2023
- محمد شايب، تأثير التهديدات السيبرانية على الأمن المجتمعي الجزائري، مذكرة ماستر تخصص علاقات دولية، المدرسة الوطنية العليا للعلوم السياسية، قسم العلاقات الدولية، الجزائر، 2024-2025

- وائل خليل الرحمان بوطمين، البعد السيبراني للأمن القومي الجزائري: دراسة مقارنة لنماذج دولية رائدة، مذكرة ماستر، تخصص علاقات دولية، المدرسة الوطنية العليا للعلوم السياسية، الشهيد دور محمد ابراهيم القاسم، الجزائر، 2024-2025
- فتيحة بوعلام، الأمن السيبراني في الجزائر، مذكرة ماستر في قانون خاص، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، 22 جوان 2020

#### 4. المطبوعات و المحاضرات الجامعية

- خضار فايزة، محاضرات في " مفهوم الجريمة المعلوماتية"، 2024
- خولة مسراتي، "محاضرات في الهجمات السيبرانية وأمن المعلومات"، مقياس اليقظة الرقمية، أقيمت على طلبة السنة أولى ماستر، قسم علوم التسيير، كلية الحقوق والعلوم السياسية، جامعة بليدة 2 لونيبي علي، 2024-2025
- فريد روابح، محاضرات في قانون الإجراءات الجزائية، أقيمت على طلبة السنة الثانية ليسانس، كلية الحقوق والعلوم السياسية، جامعة محمد لمين دباغين، سطيف 2، 2026
- نسمة بطيحة، محاضرات في مقياس الوقاية من الجرائم الالكترونية، القيت على طلبة سنة الثانية ماستر، قسم الحقوق، كلية الحقوق و العلوم السياسية ، جامعة محمد لمين دباغين سطيف – 2، 2021-2022

## فهرس المحتويات

فهرس المحتويات

|    |                                                   |
|----|---------------------------------------------------|
| خ  | قائمة المختصرات:                                  |
| 1  | مقدمة                                             |
| 7  | الفصل الأول: الأمن السيبراني والجريمة السيبرانية  |
| 8  | تمهيد                                             |
| 9  | المبحث الأول: ماهية الأمن السيبراني               |
| 9  | المطلب الأول: مفهوم الأمن السيبراني               |
| 9  | الفرع الأول: نشأة الأمن السيبراني                 |
| 11 | الفرع الثاني: تعريف الأمن السيبراني               |
| 13 | الفرع الثالث: المفاهيم المرتبطة بالأمن السيبراني  |
| 16 | المطلب الثاني: مجالات الأمن السيبراني وأهميته     |
| 16 | الفرع الأول: مجالات الأمن السيبراني               |
| 20 | الفرع الثاني: أهمية الأمن السيبراني               |
| 22 | المبحث الثاني: الجرائم السيبرانية ودوافع ارتكابها |
| 22 | المطلب الأول: مفهوم الجريمة السيبرانية            |
| 22 | الفرع الأول: تعريف الجريمة السيبرانية             |
| 22 | الفرع الثاني : خصائص الجريمة السيبرانية           |

|    |                                                                            |
|----|----------------------------------------------------------------------------|
| 27 | الفرع الثالث: أركان الجريمة السيبرانية .....                               |
| 28 | المطلب الثاني: صور الجريمة السيبرانية ودوافع ارتكابها .....                |
| 28 | الفرع الأول: صور الجريمة السيبرانية .....                                  |
| 32 | الفرع الثاني: دوافع إرتكاب الجريمة السيبرانية .....                        |
| 35 | خلاصة الفصل الأول .....                                                    |
| 36 | الفصل الثاني: المواجهة التشريعية لحماية الأمن السيبراني .....              |
| 37 | تمهيد: .....                                                               |
| 38 | المبحث الأول: آليات حماية الامن السيبراني و الهيئات المختصة لمكافحته ..... |
| 38 | المطلب الأول: آليات المتبعة لمكافحة الجريمة .....                          |
| 38 | الفرع الأول: الآليات الوقائية لمكافحة الجريمة السيبرانية: .....            |
| 41 | الفرع الثاني: الآليات الردعية لمكافحة الجريمة السيبرانية: .....            |
| 44 | المطلب الثاني: الهيئات المختصة للتصدي للجريمة السيبرانية. ....             |
| 44 | الفرع الأول: على المستوى الوطني. ....                                      |
| 48 | الفرع الثاني: على المستوى الدولي .....                                     |
| 54 | المبحث الثاني: جزاء الاخلال بالامن السيبراني و التحديات التي تواجهه .....  |
| 54 | المطلب الأول: الجزاءات المقررة لجرائم الامن السيبراني. ....                |
| 54 | الفرع الأول: مكافحة الجريمة السيبرانية بموجب القوانين العامة. ....         |
| 57 | الفرع الثاني: مكافحة الجريمة السيبرانية بموجب القوانين الخاصة. ....        |

|    |                                                             |
|----|-------------------------------------------------------------|
| 60 | المطلب الثاني: تحديات الأمن السيبراني                       |
| 61 | الفرع الأول: تحديات الأمن السيبراني في عصر الذكاء الاصطناعي |
| 62 | الفرع الثاني: استهداف البنية التحتية                        |
| 64 | الفرع الثالث: مهددات التقنية                                |
| 65 | خلاصة الفصل الثاني                                          |
| 66 | الخاتمة                                                     |
| 72 | قائمة المصادر المراجع                                       |
| 85 | فهرس المحتويات                                              |
| 90 | الملخص                                                      |
|    |                                                             |
|    |                                                             |

## الملخص

## الملخص:

باعتبار أن الأمن السيبراني مصطلح يفرض نفسه بقوة في مجال الأنظمة الرقمية، فإنه لا يمكن للدول تجاهله خاصة في ظل التهديدات المتزايدة التي تمس بالمصلحة المادية والجسدية والمعنوية، وعليه فقد أصبح هذا النوع من الإعتداءات يشكل تحديا حقيقيا أمام مختلف العالم وهو ما دفع المشرع الجزائري إلى إدراك هذه الإشكالية حيث سعى إلى إرساء العديد من القوانين، من أجل توفير الحماية اللازمة لمستخدمي الفضاء الرقمي، ومع ذلك ورغم الجهود المبذولة إلا أنها لا تزال تحقق الحماية المطلوبة، نظرا لخصوصية هذا النوع من الأخطار الرقمية.

الكلمات المفتاحية:

الأمن السيبراني، الجريمة السيبرانية، حماية المعطيات الرقمية، التهديدات السيبرانية.

## Abstract:

As cybersecurity has become an increasingly significant concept in the field of digital systems, it can no longer be ignored by states, especially in light of the growing threats that affect material, physical, and moral interests. Consequently, cyberattacks have emerged as a real challenge facing countries worldwide. This situation has prompted the Algerian legislator to recognize the seriousness of the issue and to establish several laws aimed at providing the necessary protection for users of the digital space. However, despite the efforts made, the desired level of protection has not yet been fully achieved due to the specific and evolving nature of digital threats.

## Keywords:

Cybersecurity, Cybercrime, Digital Data Protection, Cyber Threats.