وزارة التعليم العالي والبحث العلمي

Ministry of higher education and scientific research

جامعة محمد البشير الابراهيمي –برج بوعريريج–

University of mohamed al-bachir al-ibrahimi –bba-

كلية الحقوق والعلوم السياسية

Faculty of law and political sciences

مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر اكاديمي في الحقوق

تخصص: قانون الإعلام الآلي والأنترنت

الموسمة بـ:

الأمن السيبراني وحماية البيانات الرقمية في الجزائر

إعداد الطالبين:

– لعباشي حمزة

– قعفر محمد الامين

إشراف الاستاذ:

د. صحراوي شهرزاد

رمضانى مريم	استاذ محاضر ب	رئيسا
صحراوي شهرزاد	استاذ محاضر أ	مشرفا ومقررا
بلقمرى ناهد	استاذ محاضر أ	ممتحنا

السنة الجامعية: 2023– 2024

الجمهورية الجزائرية الديمقراطية الشعبية
People's democratic republic of Algeria
وزارة التعليم العالي والبحث العلمي
Ministry of higher education and scientific research
جامعة محمد البشير الإبراهيمي – برج بوعريريج
University Of Mohamed Al-Bashir Al-Ibrahimi - BBA
كلية الحقوق والعلوم السياسية
Faculty of Law and Political Sciences

إذن بالإيـــداع

أنا الممضي أسفله الأستاذ : ..... صحراوي بشير .....

الرتبة : ..... استاذ محاضر أ .....

المشرف على مذكرة الماستر الموسومة بـ : ..... الحماية الجزائية للبيانات الرقمية في التشريع الجزائري .....

.....

من إعـــداد :

الطالب الأول : ..... عبابنة حمزة .....

الطالب الثاني : ..... قحفر محمد الأمين .....

أوافق على إيداع الطالب (الطالبين) لمذكرة التخرج لدى الإدارة من أجل برمجتها للمناقشة.

إمضاء الأستاذ المشرف

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

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي
الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

(الطالب الأول)

أنا الممضي أسفله،
السيد(ة): لعباشي حمزة الصفة: طالب، أستاذ، باحث طالب
الحامل(ة) لبطاقة التعريف الوطنية رقم 103758460 والصادرة بتاريخ 2022/11/25
المسجل(ة) بكلية / معهد الحقوق والعلوم السياسية قسم ماستر قانون إعلام آلي وانترنت
والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج، مذكرة ماستر، مذكرة ماجستير، أطروحة دكتوراه)،
عنوانها: الأمن المعلوماتي وحماية البيانات الرقمية في الجزائر

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

التاريخ: .....

توقيع المعني (ة)

30 جوان 2024

عن رئيس المجلس الشعبي البلدي
و بتفويض منه عون الإدارة الإقليمية
العباشي عبد الكريم

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

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي
الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

(الطالب الثاني)

أنا الممضي أسفله،

السيد(ة): قعفر محمد الأمين ..... الصفة: طالب، أستاذ، باحث ..... طالب .....

الحامل(ة) لبطاقة التعريف الوطنية رقم 119044088 والصادرة بتاريخ 2020/11/28 .....

المسجل(ة) بكلية / معهد الحقوق والعلوم السياسية ..... قسم ماستر قانون إعلام آلي وأنترنت .....

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

عنوانها: الأمن السيبراني وحماية البيانات الرقمية في الجزائر .

.....

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

التاريخ: .....

توقيع المعني (ة)

30 جوان 2024

عن رئيس المجلس الشعبي البلدي
و بتفويض منه - عن الأمين العام
هداجي عبد الكريم

بسم الله الرحمن الرحيم

شكر وتقدير

الحمد لله وحده والصلاة والسلام على من لا نبي بعده.

في المقام الأول نشكر المولى عز وجل على توفيقه لنا ومنه علينا بإتمام هذا البحث ونسأله مزيدا من النجاح والتوفيق في مشوارنا الدراسي.

ويسرنا أن نتقدم بأسمى عبارات الشكر للأستاذة الفاضلة المشرفة " صحراوي شهرزاد" التي أشرفت على هذا البحث ولم تبخل علينا بتوجيهاتها وآرائها.

كما نتقدم بالشكر الجزيل لكل من ساعدنا في هذا العمل.

كما لا يفوتنا أن نتقدم بشكرنا الخالص مع فائق التقدير والاحترام لأساتذتنا الكرام الذين كانوا عونا لنا طيلة مشوارنا الدراسي والجامعي.

كما نتقدم بالشكر إلى كل من مد لنا يد العون في إتمام هذا البحث، وإلى كل من ساهم فيه من قريب أو بعيد.

الإهداء:

أهدي عملي هذا إلى من قال فيهما الله:

" وأخفض لهما جناح الذل من الرحمة وقل ربي أرحمهما كما ربياني صغيرا "

سورة الإسراء الاية 24

إلى والداي الكريمين حفضهما الله وأطال في عمرهما.

إلى إخوتي الأعزاء ولكل الأهل.

إلى أصدقائي.

و إلى من رفعو ريات العلم والتعليم أساتذتي الأفاضل.

و إلى كل من ساهم معي في إنجاح هذه المذكرة.

لعباشي حمزة

الإهداء

اهدي ثمرة هذا العمل المتواضع الى:

من أسقوني حنان لا ينتهي وأعطوني الحب الدائم وربوني على

العلم والأخلاق لأصل الى هذا المستوى

والدتي ووالدي الغاليين

الى الإخوة الأكارم.

والى من حملتهم ذاكرتي ولم تحملهم مذكرتي.

اليكم جميعا أهدي ثمرة هذا الجهد.

قعفر محمد الأمين

مقدمة

مع تزايد الاعتماد على التكنولوجيا الرقمية في مختلف مجالات الحياة، أصبح الأمن السيبراني وحماية البيانات الرقمية موضوع حيوي يحتاج إلى اهتمام متزايد، إن التطورات السريعة في تكنولوجيا المعلومات والاتصالات قد جلبت فوائد كبيرة للمجتمع الجزائري، لكنها في الوقت نفسه تسببت في ظهور تحديات جديدة تتعلق بأمن المعلومات وحماية البيانات الشخصية والمالية.

الأمن السيبراني يشمل مجموعة من الاستراتيجيات والإجراءات التي تهدف إلى حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية. في الجزائر، كما هو الحال في معظم دول العالم، يواجه قطاع الأمن السيبراني تحديات متعددة، بما في ذلك الهجمات الإلكترونية المتزايدة، ونقص الوعي الأمني لدى المستخدمين، ونقص التشريعات والسياسات الفعالة في هذا المجال.

تعتمد الجزائر على مجموعة من التشريعات والقوانين التي تهدف إلى مكافحة الجرائم السيبرانية وحماية خصوصية الأفراد، من بين هذه التشريعات، يأتي قانون 09-04، الذي يحدد إطارًا قانونيًا للوقاية من الجرائم المرتبطة بتكنولوجيا المعلومات ومكافحتها، وعلى المستوى المؤسسي، تعمل الجزائر على إنشاء وتطوير هيئات متخصصة لتعزيز الأمن السيبراني، مثل الوكالة الوطنية للأمن السيبراني، التي تهدف إلى تنسيق الجهود الوطنية لمكافحة التهديدات السيبرانية وتعزيز الوعي بأهمية الأمن السيبراني.

I. اهمية الموضوع:

تبرز أهمية هذا الموضوع في الحاجة إلى حماية البيانات الشخصية والخصوصية للمواطنين، وضمان استمرارية الخدمات الحيوية التي تعتمد على الأنظمة الرقمية، مثل الطاقة، الصحة، والاتصالات. بالإضافة إلى ذلك، يعزز الأمن السيبراني بيئة آمنة للاقتصاد الرقمي، مما يسهم في جذب الاستثمارات الأجنبية وتشجيع الابتكار المحلي، إن تطوير إطار قانوني ومؤسسي قوي لمكافحة الجرائم السيبرانية وتنسيق الجهود الوطنية

والدولية لمواجهة هذه التهديدات هو أمر أساسي لضمان أمن واستقرار الجزائر في العصر الرقمي.

II. اهداف الموضوع:

الهدف من بحثنا الوصول إلى إجابات كافية على من خلال:

- التعرف على مخاطر التحول الرقمي وحوكمة المؤسسات والهيئات الحساسة للدولة الجزائرية على أمنها الداخلي ومنظومتها المعلوماتية.
- كشف طبيعة وحجم التهديدات التي تستهدف الجزائر وأمنها السيبراني الداخلي.
- معرفة التحديات التي تواجهها الجزائر أمام تنفيذها سياسات وآليات حماية البيانات والأنظمة المعلوماتية، والوقوف في وجه الهجمات السيبرانية التي تستهدفها.
- التعرف على أهم التقنيات الحديثة التي توظف في تنفيذ الهجمات السيبرانية.

III. أسباب اختيار الموضوع:

تتعدد اسباب اختيارنا لموضوع هذه الدراسة وتشمل مايلي:

1- أسباب موضوعية:

يتمحور ذلك حول طبيعة الموضوع وأهميته الكبيرة حيث أنه يفرض نفسه على الساحة البحثية في جميع المجالات، التقنية أو الاقتصادية، أو القانونية، أو الإعلامية، وغيرها، حيث أصبح موضوع الأمن السيبراني وحماية البيانات الرقمية في الجزائر ضرورة حتمية، فالجزائر مثل غيرها من الدول، تعاني من تهديدات سيبرانية متزايدة ومعقدة تستهدف البنية التحتية الحيوية والمعلومات الحساسة، مما تستلزم مكافحة الجرائم السيبرانية وتنسيق الجهود الوطنية والدولية لمواجهة هذه التهديدات هو أمر أساسي لضمان أمن واستقرار الجزائر في العصر الرقمي.

2- اسباب ذاتية:

ترجع أسباب اختيار الموضوع أسباب اختيار الموضوع إلى نظراً لأهميته الشخصية بالنسبة لي كمواطن يعيش في عصر رقمي متسارع. تتزايد اعتمادي واعتماد المجتمع على التكنولوجيا والإنترنت في الحياة اليومية، سواء في التواصل أو العمل أو الخدمات المصرفية، ومع ذلك، تزايدت المخاطر السيبرانية التي تهدد خصوصيتنا وسلامة معلوماتنا الشخصية، حيث شعرت بالحاجة إلى فهم أعمق لكيفية حماية نفسي وعائلتي من هذه التهديدات، وكذلك كيف يمكن لبلدنا تطوير بنية تحتية سيبرانية قوية تحمي المواطنين وتضمن استمرارية الخدمات الحيوية، إن اختيار هذا الموضوع ينبع من رغبتي في المساهمة في نشر الوعي وتعزيز الأمن السيبراني، مما يعزز الثقة في استخدام التكنولوجيا ويسهم في بناء مجتمع رقمي آمن ومستقر.

I. الدراسات السابقة:

اخترنا من بين أهم الدراسات التى تناولت موضوع الأمن السيبيراني وحماية البيانات الرقمية في الجزائر ثلاث نتطرق اليها كما يلى:

الدراسة الاولى:

دراسة بارة سمير: الدفاع الوطني والسياسات الوطنية للأمن السيبراني في الجزائر – الدور والتحديات المجلة الجزائرية للأمن الإنساني، جامعة باتنة 1، الجزائر، المجلد 2، العدد 2، 2017،

تمحورت هده الدراسة حول تقديم أساسيات عن الأمن السيبراني والجريمة السيبرانية، وأهم مؤسسات الدفاع الوطني وسياسات تحقيق الأمن السيبراني في الجزائر، مع التطرق للعوائق المتعددة التي تعيق تحقيق الأمن السيبراني في ظل التحديات الآنية والمستقبلية، وقد خلصت هده الدراسة إلى إعطاء مجموعة من النتائج ولعل أهمها:

- إلتزام قرارات الصادرة عن الأمم المتحدة وعن القمة العالمية لمجتمع المعلومات بشقيها، والداعية إلى نشر ثقافة الأمن السيبراني.
- وضع إطار تعاون يضمن تبادل المعلومات ونقل الممارسات الفضلى في مجال الأمن السيبراني.
- تأمين إنسجام الأنظمة القانونية، المكافحة للجرائم السيبرانية، بما يمنع نشوء جنات رقمية.

إلا أن هذه الدراسة ركزت على الأمن السيبيراني من ناحية الدفاع الوطني والسياسات الوطنية ولم تتناول جانب حماية البيانات الرقمية في الجزائر.

الدراسة الثانية:

دراسة للدكتور جمال بوازدية بعنوان الإستراتيجية الجزائرية في مواجهة الجرائم السيبرانية " التحديات والآفاق " منشورة بتاريخ 13/02/2018

وجاء في هذه الدراسة " أصبح من الصعب جدا على الدول توفير الحماية لأنظمتها المعلوماتية خاصتا وأن عملية الإستعمال المتزايد والمفرط لتكنولوجيات الإعلام والإتصال، فاقت كل اتقديرات فهذا العالم الغريب والمتجدد، جعل من القابلية للعطب إحدى الهواجس التي تعاني منها الدولة، فالجرائم المستحدثة في الفضاء السيبراني من شأنها المساس بالأمن القومي إن لم تفعل اليقضة المعلوماتية وذالك عن طريق المراقبة المستمرة لهذا الميدان حتى يتم الإستباق في وضع الآلية الكفيلة للتأقلم مع التحديات التي تفرزها التطورات التكنولوجية.

وفي هذا الإطار توجهت الجزائر إلى طرح تصورات ورسم سياسة أمنية مزدوجة – الأمن السيبراني – للتحكم في أنظمة المراقبة لحماية المنظومة المعلوماتية للمؤسسات والمواطنين من جهة، ومواجهة الأخطار من جهة ثانية، ولتدارك النقائص تجتهد الجزائر في الجهة الخارجية من خلال التعاون المتعدد التخصصات للإستفادة من تجارب غيرها من الدول ".

وقد خلصت هذه الدراسة إلى مجموعة من النتائج ولعل أهمها:

1-الجريمة السيبرانية جعلت من كل الأنظمة المعلوماتية للمؤسسات السيادية والشركات الكبرى والمراكز المالية والحسابات الخاصة للأفراد عرضة للإختراق والتهديد من أجل الإبتزاز المساومة والتجسس رغم ما توفره الدولة من وسائل مادية وتقنية وبشرية للحماية.

2-الصراعات الدولية أصبحت حافز رئيسي لطغيان الجريمة السيبرانية على جميع مجالات الحياة لدرجة أن المخاطر الآنية والمستقبلية قد بلغت مستويات من شأنها المساس بالأمن الوطني القومي والعالمي مما يستدعي إطلاق صفارات الإنذار لإعادة النظر في المنظومة الأمنية.

إلا أن هذه الدراسة ركزت على الإستراتيجية الجزائرية من ناحية مواجهة الجرائم السيبرانية ولم تتناول جانب حماية البيانات الرقمية في الجزائر.

الدراسة الثالثة:

دراسة الدكتور إدريس عطية بعنوان مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، منشورة في سنة 2019.

وقد تمحورت هذه الدراسة حول التصورات الجزائرية في مجابهة المخاطر والتحديات السيبرانية من خلال تكييف المنظومة الأمنية مع التحولات الجيو إستراتيجية العالمية .

إلا أن هذه الدراسة ركزت على مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري ولم تتناول جانب حماية البيانات الرقمية في الجزائر.

II. الاشكالية:

انطلاقا مما سبق يمكن طرح الاشكالية التالية:

كيف كرس المشرع الجزائري الامن السيبرانى و حمى البيانات الرقمية في الجزائر ؟

III. **الاسئلة الفرعية:**

للإحاطة أكثر بموضوع الدراسة، سنحاول طرح بعض الأسئلة الفرعية التالية:

- كيغ حمى المشرع الجزائري الأمن السيبراني في الجزائر؟
- ما هو واقع حماية البيانات الرقمية في الجزائر؟

IV. **الاطار المنهجي:**

تعتمد الدراسة على منهج وصفي يسمح لنا بتغطية جميع جوانب الموضوع من خلال تناول الإطار المفاهيمى للامن السيرانى والبيانات الرقمية، ومن ثم وصف الإطار القانونى الذي وضعه المشرع الجزائري لحماية الامن السيبرانى والبيانات الرقمية في الجزائر.

V. **خطة البحث:**

انتهجنا في هذا البحث الى خطة مقسمة الى مقدمة وفصلين، الأول يتضمن الأمن السيبراني في الجزائر، مقسم الى مبحثين، المبحث الأول نتناول فيه ماهية الأمن السيبراني، أما المبحث الثاني نعرض فيه التدابير القانونية والمؤسسية والتقنية لتحقيق الأمن السيبراني في الجزائر.

– أما فيما يخص الفصل الثاني، فنتناول حماية البيانات الرقمية في الجزائر، مقسم الى مبحثين، المبحث الأول نتحدث فيه عن ماهية البيانات الرقمية، والمبحث الثاني المتضمن الاطار القانوني لحماية البيانات الرقمية في الجزائر.

الفصل الأول:

الأمن السيبراني في الجزائر

مع التطور الهائل في التكنولوجيا الرقمية وانتشار استخدام الإنترنت في كافة مجالات الحياة اليومية، أصبحت الحاجة إلى الأمن السيبراني وحماية البيانات الرقمية في الجزائر أكثر إلحاحاً من أي وقت مضى، تواجه الجزائر تحديات متزايدة في التصدي للتهديدات السيبرانية التي تستهدف البنية التحتية الحيوية والمعلومات الحساسة، مما يفرض ضرورة تطوير استراتيجية شاملة للأمن السيبراني.

يتضمن هذا الفصل استعراضاً لمفهوم الأمن السيبراني وأهميته، ويحلل الوضع الحالي للأمن السيبراني في الجزائر، بما في ذلك التشريعات والسياسات المعمول بها، وكذلك الجهود المؤسسية المبذولة لتعزيز أمن المعلومات وحماية البيانات الرقمية، سنستعرض أيضاً التحديات التي تواجه الجزائر في هذا المجال ونقترح سبل تحقيق الأمن السيبراني الجزائري، لضمان حماية الأفراد والمؤسسات من التهديدات السيبرانية المتزايدة وضمان استمرارية التطور الرقمي الآمن.

وعليه ينقسم هذا الفصل إلى:

- **المبحث الاول: مفهوم الأمن السيبراني**
- **المبحث الثاني: التدابير القانونية والمؤسسية والتقنية لتحقيق الأمن السيبراني في الجزائر**

المبحث الأول: مفهوم الأمن السيبراني

خلال المؤتمر العالمي للاتصالات 2017 بجنيف، خرج المشاركين في هذا المؤتمر بتوصيات أهمها ضرورة إنشاء اتفاقيات دولية للعمل المشترك في مجال تحقيق الأمن السيبراني، بحكم أن الجميع معرض للهجمات الإلكترونية، التي تنجم عنها خسائر اقتصادية كبيرة، لدرجة تحطيم البنى التحتية للدول، فأبدت مختلف الدول رغبتها في تبادل الخبرات والمعلومات في هذا المجال، ومنها الجزائر التي تسعى لتحقيق أعلى درجات من الامن السيبراني.

وعليه سنتناول في هذا المبحث تعريف الأمن السيبراني والمصطلحات ذات العلاقة به (المطلب الأول)، ثم أهمية الأمن الاستبراني، أهدافه، أنواعه وأبعاده (المطلب الثاني)، تليها التحديات التي تواجهها الجزائر أمام تطبيق الأمن السيبراني والتهديدات السيبرانية (المذطلب الثالث)

المطلب الأول: تعريف الامن السيبراني والمصطلحات ذات العلاقة به

تعددت التعاريف المحددة للأمن السيبراني،لذا سيتناول الفرع عددا منها لتحديد تعريف الامن السيبرانى (الفرع الأول)، كما سنتطرق من خلال المطلب الى بعض المفاهيم المرتبطة والمقاربة للأمن السيبراني (الفرع الثاني).

الفرع الأول: تعريف الأمن السيبراني

اولا- التعريف اللغوى:الأمن السيبراني مكوّن من لفظتين ": الأمن "، و" السيبراني "

- **الأمن:** هو نقيض الخوف، أي بمعنى السلامة والأمن مصدر الفعل أمن أمناً وأماناً وأَمَنَةً أي اطمئنان النفس وسكون القلب وزوال الخوف، ويقال: أمن من الشر، أي سلم منه.[1]
- **السيبراني:** مصطلح السيبرانية الآن هو واحد من أكثر المصطلحات تردداً في معجم

[1] منى عبد الله السمحان، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية، العدد 111، جامعة المنصورة، المملكة العربية السعودية، 2020 ، ص9

الأمن الدولي، وكلمة " cyber " لفظة يونانية الأصل مشتقة من كلمة "kybernetes " بمعنى الشخص الذي يدير دفة السفينة،حيث تستخدم مجازاً للمتحكم governor .[1]

وأشار بعض المؤرخين الي أن أصلها يرجع إلى عالم الرياضيات الأمريكي (Norbert Wieners 1894–1964) وذلك للتعبير عن التحكم الآلي.

ثانيا – التعريف الاصطلاحي:

هناك العديد من التعاريف التي قدمت لمفهوم الأمن السيبراني، حيث يُعرف بأنه " مجموعة من الإجراءات المتخذة في مجال الدفاع ضد الهجمات السيبرانية ونتائجها التي تشمل تنفيذ التدابير المضادة المطلوبة".[2]

والأمن السيبراني هو"ممارسة الدفاع عن أجهزة الكومبيوتر والأجهزة المحمولة والأنظمة الالكترونية، والشبكات، والبيانات من الهجمات الخبيثة،كما يرد بمعنى أمن الشبكات والأنظمة المعلوماتية والبيانات والمعلومات، والأجهزة المتصلة بالانترنيت، وعليه فهو المجال الذي يتعلق بإجراءات ومعايير الحماية المفروض اتخاذها،أو الالتزام بها،لمواجهة التهديدات، ومنع الهجمات، أو على الأقل الحد من آثارها.

وقد عرفته وزارة الدفاع الأمريكي Pintagon أنه "كافة الإجراءات التنظيمية التي تأمن الحماية الكافية للمعلومات بجميع أنواعها وأشكالها، سواء كانت الكترونية أو مادية، من مختلف المخاطر والهجمات والجرائم وأفعال التخريب والتجسس والحوادث،بينما أدرج الإعلان الأوروبي، الأمن السيبراني بمعنى " قدرة النظام المعلوماتي على مقاومة محاولات الاختراق أو الحوادث غير المتوقعة التي تستهدف البيانات ". [3]

[1] المرجع نفسه ، ص9

[2] المرجع نفسه، ص ص9-10.

[3] ليلى بن برغوث، الأمن السيبراني وحماية خصوصية البيانات الرقمية في الجزائر في عصر التحول الرقمي والذكاء الاصطناعي، التهديدات، التقنيات، التحديات وآليات التصدي، المجلة الدولية للاتصال الاجتماعي، المجلد 10، العدد 01، جامعة عبد الحميد بن باديس، مستغانم، 2023، ص447.

الأمن السيبراني هو "عبارة عن مجموعة من الوسائل التقنية والإدارية التي يتم استخدامها لمنع الاستخدام من قبل غير المصرّح له على شبكات الكمبيوتر، أو سوء الاستغلال واستعادة المعلومات الإلكترونية التي تحتويها بهدف ضمان واستمرارية عمل نظم المعلومات وتأمين حماية وسرية وخصوصية البيانات الخاصة بفواعل الفضاء السيبراني، وعليه فهو المجال المتعلق بالإجراءات ومقاييس ومعايير الحماية المفروض اتخاذها، أو الالتزام بها لمواجهة التهديدات، ومنع التعديات، أو للحد من آثارها في أقصى وأسوأ الأحوال ".[1]

والأمن السيبراني هو "مجموعة من الأدوات والسياسات والمفاهيم الأمنية،والضمانات الأمنية، والمبادئ التوجيهية،من المخاطر المحدقة بالمعلومات ومعالجتها، والإجراءات، والتدريب، وأفضل الممارسات، وضمان التقنيات التي يمكن أن استخدامها لحماية البيئة الإلكترونية وتنظيم أصول المستخدم ".[2]

مما سبق يتضح أن الأمن السيبراني هو "مجموع الآليات والأطر القانونية والهياكل التنظيمية وجهود خلايا الدفاعية والأمنية الوطنية والدولية التي من شأنها العمل على حماية مصالح الفواعل الدولية وغير الدولية من المخاطر والتهديدات والجرائم السيبرانية التي تفتك بالفضاء السيبراني والحد منها، والتي تشكل خطرا ليس على أنظمة المعلومات فحسب بل على الأمن القومي والدولي ".

ولا شك بأن الوصول إلى تعريف يتصف بالشمولية للأمن السيبراني يستدعي منا الوقوف عند مجموعة من العناصر تعد الفاعلة والمتحكمة في تحقيقه وهي التكنولوجيا – الأحداث – الاستراتيجيات والعمليات والأساليب – الإنسان – المرجع الأمني.

وبالتمعن في هذه العناصر نتوصل إلى أن الأمن السيبراني يجب أن يتميز بـ:

[1] جيلالي دلالي، يعقوب بلبشير، رهانات الأمن السيبراني الوطني في ظل التحول الرقمي، قراءة في التأصيل المعرفي واستراتيجية المواجهة التشريعية، مجلة كلية القانون الكويتية العالمية، السنة العاشرة، العدد 1، جامعة حسيبة بن بوعلي، الشلف، 2021، ص ص536-537.

[2] سمير بارة، الأمن السيبراني في الجزائر، السياسات والمؤسسات، المجلة الجزائرية للأمن الإنساني، العدد 04، جامعة قاصدي مرباح، ورقلة، ص258.

- طابع متعدد التخصصات الاجتماعية والتقنية.
- كونه شبكة خالية من الحجم، والتي قدرات الفاعلين يمكن أن تكون مماثلة على نطاق واسع.
- درجة عالية من التغيير والترابط، وسرعة التفاعل.[1]

الفرع الثاني: المصطلحات ذات العلاقة بأمن السيبراني

هناك العديد من المفاهيم المرتبطة بالأمن السيبراني، ومن أهمها ما يلي:

1-الفضاء السيبراني:

يمكن إعطاء توجه مفاهيمي للفضاء السيبراني بأنه " ذلك العالم الافتراضي المتشابك مع عالمنا المادي، عن طريق الاعتماد المتبادل بالتأثير بين العالمين بالنظرة التفاعلية التكاملية والتي تنعكس بالمخاطر والمزايا اللامتناهية "[2].

وقد ظهر مصطلح الفضاء السيبيراني في ثمانينيات القرن الماضي في إحدى روايات الخيال العلمي للكاتب الأمريكي – الكندي المشهور **وليام جيبسون**، حيث يعتمد هذا المجال الإفتراضي على نظم الكمبيوتر وشبكات الأنترنيت ومخزون هائل من المعلومات والبيانات، فيتم التواصل بالشبكات عبر الهواتف وأجهزة الحواسيب وغيرها من دون التقيد بالحدود الجغرافية.[3]

فالفضاء السيبراني هو عبارة عن " بيئة إلكترونية غير ملموسة معقدة التفاعل يتم فيها بناء نماذج لظواهر أو صور إلكترونية لظواهر شبه حقيقية في التفاعلات والتعاملات البعيدة فالسيبرة عملية انعكاسية نشطة يعكس فيها مدخلات التفاعلات الإلكترونية في بيئة

[1] المرجع نفسه ، ص258.
[2] يوسف بوغرارة، الأمن السيبراني: الاستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبراني، مجلة الدراسات الافريقية وحوض النيل، المجلد 1، العدد 3، المركز الديمقراطي العربي ، جامعة مستغانم، 2018، ص103.
[3] المرجع نفسه، ص103.

لا يستطيع الإنسان إدراكها، وبصورة أخرى هي عبارة عن شبكة إلكترونية لمجموعة من الخوادم الإلكترونية حيث تتفاعل هذه الشبكات التي تتوفر فيها قاعدة بيانات فيما بينها باستخدام وسيلة تواصل افتراضية متجاوزة كل الحواجز الجغرافية والسياسية، سعيا وراء تحسين قدرة الاتصال والتعامل الإلكتروني، كما أنها محاكاة حاسوبية عادة ما تكون في صورة بيئة افتراضية لمستخدمي العالم الافتراضي.[1]

ومنه نستنتج أن الفضاء السيبراني هو استخدام تقنيات التكنولوجيا وكل ما يتعلق بها من ذكاء صناعي من طرف الدول أو الوكلاء لتحقيق السيطرة على فضاء القوة السيبرانية، فبه يتم التحكم في كل ما يتعلق بالحياة المدنية والعسكرية،وبذلك يعتبر المجال الخامس لفضاء القوة الاستراتيجية.

2-الجوسسة السيبرانية:

يعتبر التجسس السيبراني تلك المحاولات المتعمدة لاختراق أجهزة الكمبيوتر والمواقع الإلكترونية التابعة للدولة المناوئة أو الخصم بهدف سرقة معلومات سرية.[2]

تعتبر هذه الجريمة من أخطر الجرائم السيبرانية فهي نتاج ما أسفر عنه التقدم العلمي والتكنولوجي الحديث في شأن أجهزة التنصت الحديثة ذات القدرة الفائقة والدقة البالغة في أعمال التجسس حيث تهدف إلى جمع المعلومات العسكرية أو السياسية أو حتى جمع المعلومات غير العسكرية كجمع تلك المتعلقة بالمجال الاقتصادي والتجاري أو المجال الثقافي.

والتجسس قد يهدف إلى تعطيل عمل الشبكات العنكبوتية وحواسيبها، وأنظمتها بهدف سرقة معلومات سرية سياسية، أو عسكرية أو مالية من دولة ونقلها إلى دولة أخرى.[1]

[1] علي زياد علي الصراع والأمن الجيوسيبراني في الساحة الدولية: دراسة في استراتيجيات الاشتباك الرقمي، دار أمجد للنشر والتوزيع، عمان، 2020، ص ص. 53 - 54.

[2] شادي عبد الوهاب منصور، حروب الجيل الخامس: أساليب " التفجير من الداخل " على الساحة الدولية، العربي للنشر والتوزيع، القاهرة، 2019، ص 106.

ويتمثل أحد الأمثلة على التجسس العسكري في قيام " هاكرز " بالتسلل إلى جهاز أحد المتعاقدين مع الجيش الأمريكي وسرقة آلاف الملفات الخاصة بالمقاتلة أف 35، وتتمثل المعلومات الاقتصادية التي يتم عادة استهدافها في براءات الاختراع وحقوق الملكية الفكرية، أو المواقف التفاوضية للدول.[2]

3-الجريمة السيبرانية:

تتكون الجريمة الالكترونية أو الافتراضية " Cyber Crime " من مقطعين هما الجريمة " Crime"" و" Cyber" أي الالكترونية، ويستخدم مصطلح الالكترونية لوصف فكرة جزء من الحاسب أو للإشارة إلى عصر المعلومات،أما الجريمة فهي السلوكيات والأفعال الخارجة عن القانون ؛والجرائم الالكترونية: هي المخالفات التي ترتكب ضد الأفراد أو مجموعات من الأفراد بدافع الجريمة وبقصد إيذاء سمعة، الضحية أو إلحاق أي أذى مادي أو عقلي للضحية سواء كان مباشر أو غير مباشر، باستخدام شبكات الاتصالات مثل الانترنت غرف الدردشة والبريد الالكتروني.[3]

وتتشابه الجريمة الإلكترونية مع الجريمة التقليدية من ناحية وجود دافع لدى المجرم لارتكاب الجريمة ووجود ضحية، إضافة إلى أداة ومكان الجريمة، لكن الاختلاف الحقيقي بين نوعي الجريمة، يكمن في أن الأداة في الجريمة الإلكترونية ذات تقنية عالية، كما أن مكان الجريمة لا يتطلب انتقال الجاني إليه انتقالا فيزيائيا. وبالتالي فهي كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات.[4]

[1] أميرة عبد العظيم، محمد عبد الجواد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، العدد 35، الجزء3، القاهرة، 2020، ص415.

[2] شادي عبد الوهاب منصور، مرجع سبق ذكره، ص 106

[3] حاتم بن عزوز، مناني حليمة، الأمن السيبراني والجريمة الالكترونية في الدول مابعد الحداثية: الولايات المتحدة الامريكية –نموذجا-، مجلة الرسالة للدراسات الإعلامية، المجلد 6، العدد 2، الجزائر، 2022، ص582.

[4] المرجع نفسه ، ص582.

وقد عرفها " سولاز " " Artar Solaz " على أنها: أي نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كانت مرتبطة بتقنية المعلومات، وعرفها كل من "هلدر " و" جايشنكار Halder & k.Jaishankar " بأنها الجرائم التي ترتكب ضد أفراد أو مجموعات من الأفراد مع وجود دافع إجرامي لإلحاق الضرر عمدا بسمعة الضحية، أو التسبب في ضرر مباشر أو غير مباشر للضحية، وتسمى أيضا بجرائم الحاسوب حيث يتم استخدام جهاز الكمبيوتر كأداة لزيادة المعاملات غير القانونية كالاحتيال والإتجار في المواد الإباحية والملكية الفكرية وسرقة الهويات وانتهاك الخصوصية. [1]

وعليه نستنتج أن جريمة سيبرانية هي كل فعل يأخذ وصف الجريمة في القانون الجزائي العام يرتكب في الفضاء السيبراني من قبل أشخاص، أو جماعات، أو منظمات،أو دول بواسطة أجهزة الحاسوب وبرامج الإعلام الآلي وشبكة الإنترنت،أو الاعتداء عليها أو بها، مما يهدد حق الأفراد في الخصوصية وقواعد البيانات الخاصة وأنظمة المعلومات والاتصالات،وقد يأخذ بعداً آخر أمنياً وعسكرياً حينما يتعلق الأمر بأنظمة الدفاع الإلكتروني وسياسات الجوسسة والجوسسة المضادة وبرامج التسلح.

ويمكننا إيجاز خصائص الجريمة الإلكترونية فيما يلي: [2]

- مسرح الجريمة لا يظهر في الواقع بل هو الفضاء الإلكتروني بأسره.
- في الجريمة الإلكترونية المجرم والضحية لا يشترط أن يكونا في مكان واحد أو دولة واحدة، عكس الجرائم العادية كالمخدرات أو القتل ويكون لها مسرح جريمة ثابت للمعاينة فهي جرائم ترتكب عن بعد.
- مبدأ إقليمية النص الجنائي ومدى إمكانية تطبيق القوانين الوطنية على الجرائم الواقعة بالأنترنت.

[1] المرجع نفسه ، ص582.
[2] المرجع نفسه ، ص ص583-584.

- الجرائم المعلوماتية قابلة للتوسع والابتكار، فهي مرتبطة في الأساس بالتقدم التقني والمعلوماتي فكلما ظهرت تقنية جديدة ظهرت معها جرائم جديدة.
- تتسم الجرائم المتعلقة بشبكة الأنترنت بالخطورة البالغة، فهي ترتكب من طرف فئات متعددة مما يصعب معرفة من هو مرتكب الجريمة، هذا ما يجعل مكتب التحقيقات الفيدرالي الأمريكي يطلق عليها وصف الوباء "Epidemics ".
- تتصف هذه الجريمة بالخفاء، أي عدم وجود آثار مادية يمكن متابعتها فهي صعبة الاكتشاف، وكذا صعوبة الاحتفاظ بدليل الجريمة المعلوماتية في أقل من ثانية أن يمحو أو يحرف أو يغير البيانات والمعلومات في زمن محدود، فضلا عن سهولة تهربه عن مسؤولية هذا العمل بإرجاعها إلى خطأ في نظام الكومبيوتر على سبيل المثال.
- عدم وجود مفهوم مشترك لماهية الجريمة المعلوماتية، وعدم وجود تعريف قانوني موحد لها، ولعل السبب في ذلك يرجع إلى عدم وجود تنسيق دولي في مجال الجريمة المعلوماتية، ذلك لغياب معاهدات دولية ثنائية أو جماعية لمواجهتها، أو لاختلاف مفهومها تبعا لاختلاف النظم القانونية.[1]

المطلب الثاني: أهمية الأمن الاستبراني، أهدافه، أنواعه وأبعاده

في عالمنا المتصل رقمياً بشكل متزايد، تبرز أهمية الأمن السيبراني كضرورة حيوية لحماية المعلومات والأنظمة من التهديدات السيبرانية المتنامية،حيث أن الأمن السيبراني يهدف إلى حماية البيانات الحساسة والشبكات والأنظمة من الهجمات الضارة التي يمكن أن تؤدي إلى سرقة المعلومات أو تدميرها أو التلاعب بها.

وسنتطرق من خلال هذا المطلب الى أهمية الأمن السيبراني وأهدافه (الفرع الأول)، ثم الى أنواع وأبعاد الأمن السيبراني (الفرع الثاني).

[1] المرجع نفسه ، ص ص583-584.

الفرع الأول: أهمية الأمن الاستبراني وأهدافه

أصبح الأمن السيبراني أمرًا حيويًا لضمان سلامة المعلومات والبنية التحتية الرقمية، مع الاعتماد المتزايد على الإنترنت في جميع جوانب الحياة الشخصية والعملية، وتظهر أهمية الامن السيبراني وأهدافه من خلال مايلي:

أولا: أهمية الأمن السيبراني

في عالمنا المترابط بواسطة الشبكة، يستفيد الجميع من برامج الدفاع السيبراني. فمثلاً على المستوى الفردي يمكن أن يؤدي هجوم الأمن السيبراني إلى سرقة الهوية أو محاولات الابتزاز، أو فقدان البيانات المهمة مثل الصور العائلية.

كما تعتمد المجتمعات على البنية التحتية الحيوية، مثل محطات الطاقة والمستشفيات، وشركات الخدمات المالية، لذا فإن تأمين هذه المنظمات وغيرها أمر ضروري للحفاظ على عمل مجتمعنا بطريقة آمنة وطبيعية. [1]

كما تتمثل أهمية الأمن السيبراني فيما يلى:

- الحفاظ على المعلومات وسلامتها وتجانسها، وذلك بكف الأيادي من العبث بها تحقيق وفرة البيانات وجاهزيتها عند الحاجة إليها.
- حماية الأجهزة والشبكات ككل من الاختراقات لتكون درع واق للبيانات والمعلومات.
- استكشاف نقاط الضعف والثغرات في الأنظمة ومعالجتها.
- استخدام الأدوات الخاصة بالمصادر المفتوحة وتطويرها لتحقيق مبادئ الأمن السيبراني.
- توفير بيئة عمل آمنة جدًا خلال العمل عبر الشبكة العنكبوتية.[2]
- ضمان توافر استمرارية عمل نظم المعلومات.

[1] منى عبد الله السمحان، مرجع سبق ذكره، ص12.
[2] المرجع نفسه ، ص12.

- تعزيز حماية وسرية وخصوصية البيانات الشخصية اللازمة لحماية المواطنين والمستهلكين على حدٍ سواء من المخاطر المحتملة.
- اتخاذ جميع التدابير في مختلف مجالات استخدام الإنترنت.
- التأسيس لصناعة وطنية في مجال الأمن السيبراني لتحقيق الريادة في هذا المجال.
- تعزيز حماية أنظمة تقنية المعلومات، لتكون المرجع الوطني في شؤون تخصصها، بهدف حماية مصالح الوطن الحيوية وأمنه والبني التحتية الحساسة فيه ومراعاة الأهمية الحيوية المتزايدة لتخصصه.[1]

ثانيا: أهداف الأمن السيبراني

لتعزيز حماية أنظمة التقنيات التشغيلية على كافة الأصعدة، بما في ذلك الأجهزة والبرمجيات والخدمات والبيانات، يجب التركيز على التصدي لهجمات وحوادث أمن المعلومات التي تستهدف الأجهزة الحكومية ومؤسسات القطاعين العام والخاص. كذلك، يتطلب توفير بيئة آمنة وموثوقة للتعاملات في مجتمع المعلومات ضمان صمود البنية التحتية الحساسة أمام الهجمات الإلكترونية. تحقيق هذه الأهداف يستلزم تبني استراتيجيات دفاعية متقدمة وتطوير بنية تحتية قوية للأمن السيبراني لضمان استمرارية الأعمال وحماية المعلومات الحساسة من التهديدات المتزايدة.

لتوفير المتطلبات اللازمة للحد من المخاطر والجرائم الإلكترونية التي تستهدف المستخدمين، يجب القضاء على نقاط الضعف في أنظمة الحاسب الآلي والأجهزة المحمولة بمختلف أنواعها، وسد الثغرات في أنظمة أمن المعلومات. بالإضافة إلى ذلك، ينبغي مقاومة البرمجيات الخبيثة التي تهدف إلى إحداث أضرار جسيمة للمستخدمين. تحقيق هذه الأهداف يتطلب تبني استراتيجيات شاملة لتعزيز الأمان الرقمي وحماية المستخدمين من التهديدات السيبرانية المتزايدة.

[1] وريدة خيلية، إشكالية المواطنة في ظل قيم التكنولوجيا الحديثة بين حرية المواطن والأمن السيبراني، حوليات جامعة الجزائر،ص813.

للحد من التجسس والتخريب الإلكتروني على مستوى الحكومة والأفراد، يجب اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر المحتملة في مختلف مجالات استخدام الإنترنت. يتضمن ذلك تدريب الأفراد على آليات وإجراءات جديدة لمواجهة التحديات الخاصة باختراق أجهزتهم التقنية بهدف الإضرار بمعلوماتهم الشخصية، سواء بالإتلاف أو السرقة. تحقيق هذه الأهداف يتطلب تنفيذ سياسات شاملة وتوفير التدريب اللازم لتعزيز الأمان الرقمي وحماية البيانات الشخصية من التهديدات السيبرانية المتزايدة. [1]

الفرع الثاني: أنواع وأبعاد الأمن السيبراني

لقد صنف الأمن السيبراني الى عدة أنواع، وذلك لخصوصيته التي تحتم على المتصارعين الالتزام باستراتيجيات وتقنيات تعتمد على القوة التكنولوجية، والكفاءة البشرية المتمكنة في المجال مع توفر عنصر السرعة والمباغتة، فلابد من وضح خطط استباقية لرصد مختلف التهديدات المحتملة، وكذا تحديد الابعاد التي يمكن أن تحتاجها مختلف الهجمات السيبرانية للعدو.

[1] منى عبد الله السمحان، مرجع سبق ذكره، ص12.

أولا: أنواع الأمن السيبراني

ينطبق هذا المصطلح على مجموعة متنوعة من السياقات، بدءًا من قطاع الأعمال، وصولًا إلى الحوسبة المتنقلة، وبالإمكان عمومًا تقسيمها إلى عدة فئات شائعة كما يلي:

1- **أمن الشبكات:** هو ممارسة تأمين شبكة الكمبيوتر من العناصر المتطفلة والانتهازية سواء المهاجمين المستهدفين، أو البرامج الضارة.

2-**أمن التطبيقات:** يركز على الحفاظ على البرامج والأجهزة خالية من التهديدات، إذ يمكن أن يوفر التطبيق المخترق الوصول إلى البيانات المصممة للحماية، وإن تطبيق مفهوم الأمان الناجح يبدأ في مرحلة التصميم الأولي قبل نشر البرنامج أو الجهاز.

3-**أمن المعلومات:** سلامة وخصوصية البيانات، سواء في مرحلة التخزين يحمي أو التناقل.

4-الأمن التشغيلي: يشمل العمليات والقرارات التي تتعامل مع أصول البيانات، وتكفل حمايتها.[1]

ثانيا: أبعاد الأمن السيبراني

1-**البعد العسكري:** لقد كانت بدايات الانترنت في بيئة عسكرية، بشكل أساسي، لتنتقل فيما بعد إلى الأوساط العلمية والأكاديمية، تمثلت في أبحاث تخدم القدرات العسكرية وتطورها والانجازات العلمية التي تسهم في تفوق بلد على آخر، حيث كان التنافس على أشده، بين الاتحاد السوفياتي والولايات المتحدة الأميركية، في مجال الوصول إلى الفضاء الخارجي، وتطوير الأسلحة النووية.[2]

وتتراكم الأمثلة الموضحة لذلك، نذكر منها مثلا ما حصل في جورجيا، واستونيا، وكوريا الجنوبية، وإيران، كمثال على بعض الهجمات والاختراقات التي ترجمت ماديا، سواء باندلاع

[1] المرجع نفسه ، ص14.
[2] سمير بارة، مرجع سبق ذكره، ص260.

صراع مسلح لاحق، كذلك الذي وقع، بين روسيا وجورجيا، أو بانقطاع الاتصال بالانترنت في استونيا، بين الدولة والمواطنين والتشويش على الإدارات الحكومية. [1]

كذلك اختراقات أنظمة المنشآت النووية، في إيران وتحقق إمكانات التلاعب بها، مع ما يعنيه هذا من تعرض الأمن القومي للدولة المعنية.

وتكمن الميزة النسبية للقوة السيبرانية في قدرتها على ربط الوحدات العسكرية ببعضها البعض عبر الشبكات العسكرية في الفضاء الالكتروني، بما يسمح بسهولة تبادل المعلومات وتدفقها، وسرعة اتخاذ القرارات العسكرية، ومن ثمة تحقيق الأهداف عن بعد ومن دون شك فإن عدم استغلال هذه التقنية والتسلح بها، أو تأمينها بشكل جيد من أي اختراق خارجي، سيؤدي بالضرورة إلى شن هجمات إلكترونية مضادة على شبكات القوات العسكرية، ومن ثم تدمير قواعد البيانات، وما يلحقه من مخاطر. [2]

2-**البعد الاقتصادي:** لقد أصبح الفضاء الإلكتروني جاذباً لقطاعات المجتمع كافة، وباتت المعرفة محرك الانتاج والنمو الاقتصادي، كما أيقن الجميع أن مبدأ التركيز على المعلومات والتكنولوجيا يعد عاملا من العوامل الأساسية للنهوض بالاقتصاد، وهو ما دفع بالدول في الآونة الأخيرة تزيد من استثمارها في المعرفة وأصبحت عصرنة الاقتصاد مرتبطة بالتحكم في الاقتصاد الرقمي من طرف مختلف الفاعلين الاقتصاديين والاجتماعيين، كما أن استخدام الكمبيوتر وشبكة الانترنت في تطوير الصناعات وتحريك الاقتصاد ومعالجة كل المعاملات الاقتصادية والمالية زاد من أهمية ضرورة توفير الأمن السيبراني لضمان حماية هذه المعلومات. [3]

3-**البعد الاجتماعي:** من الضروري تعميم المفهوم الصحيح والسليم للأمن إلى كل

[1] المرجع نفسه، ص 260.
[2] سمير بارة، مرجع سبق ذكره، ص261.
[3] المرجع نفسه، ص 261.

المشتركين في الشبكة الدولية للمعلومات، إذ تعتبر من الخطوات الأساسية التي تقوي مستوى الأمن إذا ما صيغت بطريقة واضحة وعُرفت ونفذت بذكاء، ولذلك يعتبر تنظيم الحملات الإعلامية والتثقيف المدني لأجل مجتمع معلومات مسؤول من الضرورة بمكان بحيث تغطي التحديات والمخاطر وتدابير الأمن والوقائية والرادعة لأجل تثقيف جميع الأفراد السيبرانيين للتعاطي مع عملية الأمن.

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

ينبغي جعل الشبكة الدولية للمعلومات شعاعا مفتوحا للجميع بحيث يمكن لجميع المتعاملين السيبرانيين أن يستفيدوا من البنى التحتية والخدمات المتاحة لهم دون تحمل مخاطر أمنية زائدة ويحتاج الأمر إلى بلورة مدونة أخلاقيات الأمن، تكون مقبولة ومحترمة من جانب جميع العاملين في الفضاء السيبراني.[1]

4-**البعد القانوني:** يترتب على النشاط الفردي والمؤسساتي والحكومي، في الفضاء السيبراني، نتائج قانونية وموجبات تستدعي اهتماما خاص، لحل النزاعات التي يمكن أن تنشأ عنها وهو ما يستدعي مواكبة التحولات التي رافقت ظهور مجتمع المعلومات فظهرت حقوق أخرى، كحق النفاذ إلى الشبكة العالمية للمعلومات، وتوسعت بعض المفاهيم، لتشمل أساليب الممارسة الجديدة باستخدام تقنيات المعلومات والاتصالات كالحق في إنشاء المدونات الالكترونية، والحق في إنشاء التجمعات على الانترنت والحق في حماية ملكية البرامج المعلوماتية. كما ظهرت موجبات جديدة، ذات انعكاسات

[1] المرجع نفسه ، ص 262

اقتصادية مثل: موجب الاحتفاظ ببيانات الاتصالات، وموجب الإبلاغ عن مخالفات وجرائم خاصة بالمحتوى.

كل هذه التغيرات والتحولات تستدعي وجود ترسانة قانونية تنسجم مع التطورات الحاصلة، إن على مستوى الحقوق، أو على مستوى البيئات والعمليات.[1]

5-**البعد السياسي:** هناك أمثلة كثيرة تدفع نحو الاهتمام بالبعد السياسي للأمن السيبراني، كالتسريبات المختلفة للوثائق الحساسة، التي تؤدي إلى مشكلات عويصة جدا، على المستوى الخارجي والدولي، كما أنه لا ينكر أحد الدور المتعاظم الشبكات التواصل الاجتماعي على المستوى السياسي (حملات انتخابية، تظاهرات افتراضية، حركات احتجاجية الكترونية، كما يتم استغلال هذه المواقع من طرف العديد من الحكومات لتمرير سياساتها).

وفي سياق آخر يجب ألا نغفل عن استخدام هذه المواقع من طرف الحركات الإرهابية لتجنيد أفرادها وجمع التمويل لعملياتها، وآلية للاتصال بينها كأفراد وكجماعات، وهو ما استوجب على الدول العمل على حماية أمنها من التهديدات والمخاطر التي قد تتعرض لها من خلال شبكة الانترنت.[2]

المبحث الثاني: التدابير القانونية والمؤسسية والتقنية لتحقيق الأمن السيبراني في الجزائر

في ظل التزايد السريع للتكنولوجيا الرقمية وانتشار الإنترنت، تواجه الجزائر كغيرها من الدول تحديات كبيرة في مجال الأمن السيبراني، تبرز الحاجة إلى وضع تدابير قانونية ومؤسسية فعالة لحماية البنية التحتية الرقمية والمعلومات الحساسة من التهديدات السيبرانية المتنوعة.

[1] المرجع نفسه، ص ص 262-263.
[2] محمد مختار، "هل يمكن أن تتجنب الدول مخاطر الهجمات الالكترونية؟"، مجلة اتجاهات الاحداث، العدد 6، 2015، ص7.

وعليه سيتناول هذا المبحث مطلبين الاول تحت عنوان إجراءات مواجهة الجريمة الالكترونية في التشريع الجزائري وسبل تحقيق الأمن السيبراني الجزائري، اما الثانى فتحت عنوان الاليات والجهود الامنية الجزائرية لمواجهة التهديدات السيبرانية.

المطلب الاول: إجراءات مواجهة الجريمة الالكترونية في التشريع الجزائري وسبل تحقيق الأمن السيبراني الجزائري

تعد مسألة حماية وتحقيق الأمن السيبراني من المسائل المهمة والمعقدة والتي باتت تشغل كل أجهزة الدولة الأمنية والسياسية والاقتصادية وغيرها من الميادين الحساسة والمؤثرة في قوة الدولة، حيث بات الخطر السيبراني يشكل أكبر تهديد لأمن الدولة، ويعود ذلك لقدرة الفواعل الخارجية المهددة من التسلل، وتمكنها من التكنولوجيا لتحقيق أهدافها بكل سلاسة، وبالتالي وضع التشريع الجزائري عدة إجراءات لمواجهة الجريمة الالكترونية و تحقيق الأمن السيبراني الجزائري.

الفرع الأول: إجراءات مواجهة الجريمة الالكترونية في التشريع الجزائري

لقد أخص المشرع الجزائري تنظيم الجرائم الإلكترونية بقوانين عامة وخاصة، حيث تمثلت القوانين حوض النيل العامة في: [1]

أ- **الدستور الجزائري:** كفل دستور 1996 وكذا التعديل الطارئ عليه 2016، حماية الحقوق الأساسية والحريات الفردية وذلك عن طريق أهم المبادئ الدستورية في مواده:

- المادة 38: الحريات الأساسية وحقوق الإنسان والمواطن مضمونة.
- المادة 44: حرية الإبتكار الفكري والفني والعلمي مضمونة للمواطن.
- حقوق المؤلف بحميها القانون.

[1] يوسف بوغرارة، مرجع سبق ذكره، ص ص109-110.

- لا يجوز حجز أي مطبوع أو تسجيل أو أية وسيلة أخرى من وسائل التبليغ والإعلام إلا بمقتضى أمر قضائي.
- الحريات الأكاديمية وحرية البحث العلمي مضمونة وتمارس في إطار القانون.
- تعمل الدولة على ترقية البحث العلمي وتثمينه خدمة للتنمية المستدامة للأمة.

ب- **قانون العقوبات:** لقد استدرك المشرع الجزائري في السنوات الأخيرة الفراغ القانوني في مجال الجريمة الإلكترونية نسبيا، حيث تمخض عنه إصدار القانون 15-04 المتضمن تعديل قانون العقوبات؛ وذلك بتخصيص الفصل السابع مكرر للمساس بأنظمة المعالجة الآلية للمعطيات، وفي عام 2006 أدخل المشرع تعديل بموجب قانون رقم 2306 المؤرخ في 20 ديسمبر 2006، ليصدر في 2009 القانون رقم 09-04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

ت- **قانون الإجراءات الجزائية:** تتابع الجريمة الإلكترونية بنفس إجراءات تتبع الجريمة التقليدية) التفتيش المعاينة الاستعمال الضبط، التسرب الشهادة الخبرة...)، مع زيادة تمديد الاختصاص المحلي لوكيل الجمهورية في الجرائم الإلكترونية في المادة 37 من قانون الإجراءات الجزائية.[1]

تتمثل القوانين الخاصة التي أقرها المشرع الجزائري في مجال الجريمة الإلكترونية:

أ- **قانون البريد والاتصالات السلكية واللاسلكية:** حيث نصت عدة مواد منه فيما يخص المجال السيبراني ؛المادة 87، والتي نصت على سهولة إجراء التحويلات المالية إلكترونيا، والمادة 84/2 على استعمال حوالات الدفع العادية والإلكترونية، كما نصت المادة 105 على احترام المراسلات، أما المادة 127 بجزاء كل من يفتح أو يخرب بريد.

[1] المرجع نفسه ، ص 109.

ب- **قانون التأمينات:** وقد نص هذا القانون على تنظيم الجريمة الإلكترونية من خلال مؤسسات وهيئات الضمان الاجتماعي، وذلك في عدة نصوص تخص البطاقة الإلكترونية.

ت- **القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها:** حيث جاء هذا القانون منظما للجرائم المتصلة بتكنولوجيا الإعلام والاتصال وكل ما له علاقة بالمنظومة المعلوماتية.[1]

الفرع الثانى: الاطار المؤسسي لمواجهة التهديدات السيبرانية

ويتعلق ذلك بمجمل النشطات التي قامت بها الدولة الجزائرية في سبيل تعزيز الأمن السيبراني، إلا أن هناك أجهزة عملياتية عمدت الدولة إلى إنشائها لغرض مواجهة الجريمة الالكترونية، وتتمثل في:[2]

- مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني.
- المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني.
- المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني.

الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

المطلب الثاني: الاليات والجهود الامنية الجزائرية لمواجهة التهديدات السيبرانية

تولي الدولة الجزائرية الأولوية القصوى للأمن السيبراني ضمن الإستراتيجية الأمنية العامة للدولة، من حيث تسخير التدابير اللازمة؛ التي من شأنها توفير أكبر درجة حماية لبنيتها المعلوماتية التحتية وتحقيق أمنا سيبرانيا مناسبا للتحولات الرقمية الجارية وعملية عصرنة قطاعات الدولة، التي تفرض تحديات كبيرة أمام تحقيق الأمن اللازم لمختلف أجهزة الدولة ومواطنيها، ويتأتى ذلك بمجموع الآليات والاستراتيجيات التي سخرتها الدولة والتي أقر بها العديد من الفاعلين والمسؤولين، خاصة مسؤولي الأمن السيبراني على مستوى جهاز

[1] المرجع نفسه ، ص ص109-110.
[2] سمير بارة، مرجع سبق ذكره، ص ص428-429

الجيش الوطني الجزائري وبعض الأشخاص المختصين في مجال الأمن والجريمة الالكترونية.

الفرع الأول: آليات تصدي الجزائر للتهديدات السيبرانية

كشف العميد **تيتوش** عن مجموعة من الآليات التي عملت الجزائر على تفعيلها ومن بينها يذكر: [1]

- تزود مخابر " دائرة الإشارة وأنظمة المعلومات والحرب الإلكترونية " والضباط العاملين بـ أحدث الوسائل والأجهزة التعليمية المعتمدة في محال التكوين، من بينها محاكيات متخصصة بمعايير دولية لاستعمال واستخدام وسائل الحرب الالكترونية.
- تعزيز المدرسة العليا للإشارة بأكاديمية " سيسكو "، التي تقدم حاليا تكوينا عالي المستوى في تسيير وتأمين الشبكات.
- تجهيز الدائرة العسكرية بـ " وسائل وتجهيزات جد متطورة تستجيب للمعايير الدولية، مما يؤهلها اليوم إلى إنتاج كميات معتبرة من المعدات التي من شأنها تلبية بشكل فعال احتياجات المستخدمين.
- توفير ورشتين ميكانيكيتين مجهزتين بآلات تحكم رقمية عالية الدقة، تُستخدم لتصنيع الأجزاء وقطع الغيار الميكانيكية اللازمة في مجال التصليح والصيانة.
- ومن المرتقب – بحسب المسؤول ذاته – إبرام دائرة الحرب الإلكترونية بالجيش الجزائري عقود تطوير بالشراكة مع كبرى الشركات العالمية في مجال تكنولوجيا الإعلام والاتصال.
- ومع نهاية 2021، تعززت قدرات الردع للجيش الجزائري بنوع آخر، بحسب ما ذكره موقع " مينا ديفينس " المختص في أخبار التسلح، إذ كشف عن حصول الجيش الجزائري على نظام حرب إلكتروني حديث وصفه بـ " المتكامل في الحرب الإلكترونية "، استوردته

[1] ليلى بن برغوث، مرجع سبق ذكره، ص ص 452-453.

الجزائر من الصين من قبل شركتين صينيتين وهما " ELLNC " و" CEIC ". ونبه إلى أن المعلومات المتوفرة حول هذا النظام الإلكتروني الدقيق " قليلة جدا، لكنه لفت إلى عدم الخلط بينه وبين نظام التشويش المضاد للطائرات المعروف باسم " CHL – 903"، ومن بين الميزات المتوفرة في هذه المنظومة الإلكترونية الجديدة و" المعقدة " التي سردها " المصدر " كشف رادارات العدو لمسافة 600 كليومتر وتحديد المواقع وتصنيف تحركات العدو على هذه المسافات، وحماية الرادارات والأنظمة المضادة للطائرات من الصواريخ المضادة للإشعاع من خلال تغطية ترددات الرادار " وكذا " منع الاتصالات لمسافة 300 كيلومتر، ومنع العدو في الجو والبحر والبر من استخدام أنظمة تحديد المواقع عبر الأقمار الصناعية لمسافة 300 كيلومتر. [1]

أما بالنسبة لوزير الاتصال عمار بلحيمر، فقد أفاد في تصريح له لقناة الشروق اونلاين أن سبل التصدي للتهديدات السيبرانية، التي تنتهجها الجزائر، تتمثل في:

- إنتاج محتوى وطني نوعي على المواقع الالكترونية الإعلامية والأرضيات العلمية.
- تامين الشبكة تكريسا لسيادة الدولة على مجال الرقمنة.
- اشتراط التوطين الرقمي في نطاق DZ، بالنسبة للمواقع الالكترونية الناشطة في إطار المرسوم التنفيذي المستحدث، والمتعلق بنشاط الإعلام عبر الانترنيت وحق الرد والتصحيح.
- وبالنسبة لأدوات تأمين المواقع أشار الوزير إلى أن أبرزها شهادة SSL أو شهادة المفتاح العمومي، التي هي وعبارة عن بطاقة هوية رقمية، تسمح بالتحقق من هوية الشخص أو المنظمة، أو الموقع الالكتروني.

كما أشار السيد عبد العزيز مجاهد، مدير المعهد الوطني للدراسات الاستراتيجية الشاملة في حوار له على قناة النهار، أن الاستراتيجية الجزائرية للأمن السيبراني تتمثل في إجراءات

[1] المرجع نفسه ، ص ص 452-453.

احترازية وأخرى للمعالجة وتشمل التدابير الاحترازية كل فئات ومؤسسات الدولة، بداية من توعية المواطن ومرورا بكل هياكل ومؤسسات الدولة ومؤسسة الجيش مسؤوليها.:[1]

بالإضافة إلى التظاهرات والملتقيات والأيام الدراسية، التي نظمتها مؤسسات الدولة، مؤسسة الجيش حول الأمن السيبراني والتهديدات الأمنية، والفعاليات التعاونية بين الدول الأعضاء.

والمراسيم الرئاسية الخاصة بالأمن السيبراني خير دليل على اهتمام الدولة بالموضوع، حيث وقع رئيس الجمهورية السيد عبد المجيد تبون خلال سنة 2020، على مرسوم يقضي بإرساء استراتيجية للأمن السيبراني، وإنشاء مجلس ووكالة للأمن السيبراني، واعتماد نظام يقضة شامل بهدف التصدي للتهديدات الجديدة، وفي أوت 2021، تم استحداث قطب جزائي جديد مكلف بمتابعة الجرائم السيبرانية ومكافحتها، وعلى مستوى الجيش الوطني استحدثت مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة في نوفمبر 2021.

كما اهتمت مؤسسة الجيش بمسألة الذكاء الاصطناعي AT وحروب الجيل الخامس G5، حيث سلطت جريدة الجيش الضوء على فعاليته في مجال الدفاع السيبراني والتنبؤ بالهجمات وحجمها وأنواعها بالإضافة إلى الوسائل والتقنيات التي تستخدم في حروب الجيل الخامس، مثل الذبابات الصغيرة التي تسير، الصواريخ والروبوتات التي تقتحم ميادين المعارك، وغيرها، وأيضا تنويهها إلى المخاطر التي يفرضها هذه النوع من التقنيات الحديثة على منظومات الأمن الدولية. [2]

وحسب البروفيسور " **سعدي سلامي** " عملت الجزائر مؤخرا، ضمن برنامج رئيس الجمهورية من خلال السياسة الجديدة، الذي أعطى اهتماما بالغا لجانب الأمن السيبراني، خاصة بالنسبة للتكوين العالي وذلك من خلال:

1-إصدار مراسيم رئاسية تتضمن إنشاء مدارس عليا لتكوين إطارات في المجال.

[1] سمير بارة، مرجع سبق ذكره، ص ص428-429

[2] ليلى بن برغوث، مرجع سبق ذكره، ص ص 453-454.

2-إنشاء مركز عملياتي ذو محتوى وطني للأمن السيبراني في الجزائر، يقدم خدمات في مجال الهجمات السيبرانية، للعديد من المؤسسات والهيئات.

3-تحيين برامج التكوين والبحث العلمي في مجال الالكترونيات والإعلام الآلي، بما يتلاءم مع التكنولوجيات الحديثة، من أجل مواكبة الانتقال من الجيل الرابع إلى الجيل الخامس.

4-تركز الدولة الجزائرية في عملية تطبيق استراتيجيات وآليات التصدي للتهديدات السيبرانية، على أن ذلك من مهام ومسؤوليات جميع فئات وأجهزة الدولة الجزائرية وذلك من خلال استراتيجية وطنية شاملة للأمن السيبراني، تبدأ من المواطن من خلال وعيه بالمخاطر الموجودة على الفضاء السيبراني، وتقيده الصارم بالإجراءات السليمة، عند استخدامه للوسائط التكنولوجية، ثم المختصين في مجال الأمن السيبراني، ثم المسؤولين على كافة المؤسسات الفاعلة في الدولة.

5-تحرص الدولة الجزائرية دائما على التكيف مع التحولات السريعة للفضاء السيبراني.

6-توفر الدولة الجزائرية من خلال أجهزة الأمن ومكافحة الجريمة الالكترونية، على توفير الحلول، سواء كانت استباقية، أو علاجية، لحماية الرصيد المعلوماتي.

7-اهتمام مؤسسة الجيش باستدعاء الفاعلين في القطاعات الحساسة للدولة، إلى كافة المحافل والمناسبات المخصصة للبحث في المجال الأمني السيبراني بغرض الوصول إلى حلول عملية فعالة، وإشراك مسؤولي هذه القطاعات في تنفيذ استراتيجيات الأمن وحماية المعلومات، وهذا ما حدث خلال الملتقى الذي نظمته مؤسسة الجيش بعنوان الأمن السيبراني والدفاع السيبراني. كما أشرنا أنفا؛ حيث حضره كل من وزراء الداخلية والجماعات المحلية والتهيئة العمرانية والاتصال، والتعليم العالي والبحث العلمي والرقمنة والإحصائيات والبريد والاتصالات السلكية واللاسلكية والمدير العام للمعهد الوطني للدراسات الإستراتيجية الشاملة والأمين العام لوزارة الدفاع الوطني بالنيابة، بالإضافة إلى

قادة القوات والدرك الوطني، ومنهم قائد الناحية العسكرية الأولى، ورؤساء دوائر ومدراء ورؤساء مصالح مركزية.[1]

الفرع الثاني: الجهود الأمنية لمكافحة التهديدات السيبرانية

منذ أحداث الحادي عشر من سبتمبر عام 2001 أولت الجزائر في استراتيجيتها الأمنية والدفاعية اهتماما بالغا بالإرهاب السيبراني، خاصة أنها عانت طويلا من الحركات الإرهابية وتهديدها لأمنها القومي، فبات تأمين الفضاء السيبراني من خطر تطرف هذه الحركات إحدى المهمات التي أوكلت لجهاز الدفاع، وهذا ما أكده اللواء مناد نوبة القائد العام للدرك الوطني في كلمته بمناسبة افتتاح الندوة الدولية حول " الأمن السيبراني "، قائلا: " إن الإرهاب الإلكتروني بات من أخطر الجرائم التي تستهدف الجزائر، من خلال تنامي مظاهر الترويج لكل أشكال العنف والإرهاب والتطرف باستعمال أحدث التقنيات التكنولوجية خاصة شبكات التواصل الاجتماعي والمنتديات الالكترونية...،

وقد تحدث " جاك دريدا "عن الحرب الجديدة، ودور الحركات الإرهابية فيها بالقول لقد تحول الإرهاب إلى خطر مجهول ويهدد الجميع لقدرته الفائقة على التدمير، فلم يعد عن طريق القنابل والتفجيرات وإنما أصبح يتم على الصعيد الرقمي بالهجوم الالكتروني واختراق أنظمة المعلومات والتشويش.[2]

وفي هذا السياق، طالبت الجزائر بصياغة ميثاق دولي يضبط ويقنن النشر في وسائل التواصل الاجتماعي حتى لا يستخدمها الإرهابيون كمنبر لنشر أفكارهم، بسبب سهولة سيطرة تلك الحركات المتطرفة والإرهابية على الفضاء السيبراني، كما سعت إلى تطوير قدرات جهاز الشرطة في مجال مراقبة التكنولوجيا الرقمية والانترنت، بتدريب فرق متخصصة

[1] المرجع نفسه ، ص ص 452-455.

[2] نجمة شريط، الامن السيبراني في العقيدة الدفاعية الجزائرية: الفرص والقيود، المجلة الجزائرية للسياسة والأمن، المجلد 2، العدد 2، جامعة وهران 2، الجزائر، 2023، ص84

لملاحقة المتطرفين على الشبكة ومراقبة كل ما ينشر من بيانات ومعلومات يمكن أن توجه الرأي العام من الشباب، واعتمدت مصالح الأمن الوطني في دفاعها السيبراني على استراتيجية متكاملة بين الوحدات العسكرية والأمنية: فتوجهت الاستراتيجية العسكرية الجزائرية لتحقيق الأمن السيبراني بتكثيفها لأجهزة مراقبة الأنظمة لتحمي الدولة من كافة التهديدات، ومتابعة حالة تقدم نشاطات لتجسيد السياسة الشاملة للدفاع السيبراني الرامية لضمان فعالية الحماية ضد التهديدات السيبرانية التي تستهدف أنظمة المعلومات ومنظومات الاتصال وكذا منظومة أسلحة الجيش.

تبنت الاستراتيجية الدفاعية الجزائرية تنشيط الدفاع الوقائي الالكتروني من خلال:

- الكشف المبكر عن الهجمات في وقتها الحقيقي والهجوم الالكتروني الاستباقي.
- استراتيجية التضليل والإخفاء والخداع.
- مبادرة الجزائر للمشاركة في فعاليات المؤتمرات والاجتماعات والملتقيات الدولية القائمة على تجنيب ومنع استعمال الفضاء الالكتروني ووسائله للإرهاب والدعاية له بغية تبادل الخبرات والتقنيات الدولية.

فبالرغم من محاولة تطوير الآليات الدفاعية لمواجهة الإرهاب السيبراني إلا أنه ليس التهديد الوحيد الذي تعاني منه المنظومة الأمنية الدفاعية الجزائرية، ففي دراسة لشركة "McAfee " الخاصة بأمن المعلومات لعام 2018، احتلت الجزائر صدارة الدول العربية، فجاءت في المركز 14 عالميا، وقد أحبطت " KASPERSKY " فيها 95 ألف هجمة الكترونية، وقد سبق وصنفتها الشركة أكثر بلد مهدد سيبرانيا حول العالم بنسبة هجمات طالت 44 بالمئة من المستخدمين "، فعام 2018 كان حافلا بالجرائم الالكترونية، بسبب ازدياد اعتماد الحكومة الجزائرية على الفضاء السيبراني في تسيير معاملاتها الدولية وميادينها الحيوية، وتربص قراصنة المعلوماتية بها باستخدام أدوات أكثر فتكا، والتي قد

تهدف للتلاعب بالرأي العام وإثارة الكراهية العرقية والدينية وكذلك لسرقة معلومات وبيانات مهمة وتوقيف المرافق الحيوية للبلد.[1]

[1] المرجع نفسه ، ص ص84-86.

خلاصة واستنتاجات

بناءً على ما سبق ، يمكن الوصول إلى الاستنتاجات التالية :

- تشهد الجزائر تزايدًا في التهديدات السيبرانية بما في ذلك الهجمات على أنظمة الحكومة والشركات والمواطنين، مما يستدعي استجابة فعالة وشاملة.
- يتطلب الوضع الحالي تعزيز البنى التحتية للأمن السيبراني وتبني استراتيجيات دفاعية متقدمة للحد من التهديدات والحفاظ على سلامة البيانات والمعلومات الحساسة.
- من أجل مكافحة الهجمات السيبرانية بفعالية، يجب تعزيز التوعية وتوفير التدريب المستمر للأفراد والمؤسسات حول مخاطر الأمن السيبراني وكيفية التعامل معها.
- يعد التعاون المستمر بين القطاع الحكومي والقطاع الخاص، بالإضافة إلى التعاون الدولي، أساسيًا لمكافحة التهديدات السيبرانية المعقدة والمتطورة.
- ينبغي للجزائر الاستثمار في البنية التحتية التكنولوجية وتحديث استراتيجيات الأمن السيبراني باستمرار، مع التركيز على تطوير القدرات المحلية في هذا المجال.

وبالتالي واقع الأمن السيبراني في الجزائر يتميز بتحديات كبيرة تتطلب استجابة شاملة ومستمرة، تعزيز البنية التحتية، وزيادة الوعي والتدريب، وتحسين التعاون الوطني والدولي، والاستثمار في التقنيات المتقدمة هي خطوات أساسية لضمان بيئة رقمية آمنة ومستدامة في الجزائر.

الفصل الثاني:

حماية البيانات الرقمية

في الجزائ

مع تزايد الاعتماد على التكنولوجيا الرقمية في جميع جوانب الحياة، أصبحت حماية البيانات الرقمية موضوعاً بالغ الأهمية على الصعيدين الوطني والدولي، في الجزائر ومع التوسع السريع في استخدام الإنترنت والخدمات الرقمية، برزت الحاجة الماسة إلى تعزيز حماية البيانات الرقمية لضمان سلامة المعلومات الشخصية والمالية للمواطنين، وحماية البنية التحتية الرقمية للمؤسسات الحكومية والخاصة.

تشمل حماية البيانات الرقمية مجموعة واسعة من الإجراءات والتدابير الأمنية التي تهدف إلى حماية المعلومات من الوصول غير المصرح به، والسرقة، والتلف، في الجزائر تتزايد التهديدات السيبرانية التي تستهدف البيانات الحساسة، مما يضع ضغوطاً إضافية على الجهات المسؤولة لتطوير سياسات فعالة وتعزيز الوعي الأمني بين المستخدمين.

استجابة لهذه التحديات، تبذل الجزائر جهوداً مكثفة لتعزيز البنية التحتية للأمن السيبراني، وتحديث التشريعات المتعلقة بحماية البيانات، وتطبيق أفضل الممارسات العالمية في هذا المجال، يهدف هذا النهج إلى خلق بيئة رقمية آمنة تتيح الاستفادة من التكنولوجيا بشكل آمن ومسؤول، وتحافظ على حقوق الأفراد والشركات في عصر المعلومات المتسارع.

لذا سوف نتطرق في هذا الفصل إلى المباحث التالية:

- المبحث الاول: مفهوم البيانات الرقمية
- المبحث الثاني: الاطار القانوني لحماية البيانات الرقمية في الجزائر

المبحث الاول: مفهوم البيانات الرقمية

يبرز مفهوم البيانات الرقمية كعنصر أساسي لضمان استدامة التطور التكنولوجي، وتحقيق التوازن بين الفوائد الاقتصادية والاجتماعية للتكنولوجيا من جهة، ومتطلبات الأمن والخصوصية من جهة أخرى.

المطلب الأول: تعريف قواعد البيانات الرقمية وخصوصيتها

يتضمن هذا المطلب تعريف قواعد البيانات الرقمية (الفرع الأول)، خصوصية قواعد البيانات الرقمية (الفرع الثاني).

الفرع الأول: تعريف قواعد البيانات الرقمية

يمكن تعريف قواعد البيانات الرقمية من خلال اربع اتجاهات، كما يلى:

- ✓ **التعريف الفقهي:**

كما عرفها جانب آخر من الفقه على أنها: " تجميع مميز للبيانات يتوافر فيه عنصر الابتكار أو الترتيب أو التبويب عبر مجهود شخصي بأية لغة أو رمز، ويكون مخزنا بواسطة الحاسوب ويمكن استرجاعه بواسطته أيضا.[1]"

- ✓ **التعريف التقنى:**

تعتبر قواعد البيانات وليدة تقنية المعلومات، ولذلك فهي تعرف من الناحية التقنية على أنّها عبارة عن مجموع بطاقات (fichiers) تشمل ومنظمة تسمح باقتطاع البيانات حسب على بيانات معدلة المستعمل"[2].

[1] سمية بومعزة،حقوق المؤلف في النطاقين التقليدي والرقمي في ظل التشريع الجزائري. مذكرة ماجستير في الحقوق ، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، 2015-2016، ص.120

[2] صغيري- ميلود، دور قواعد بيانات النظام الوطني للتوثيق على الخط S.N.D.L بالمكتبات الجامعية في دعم وتطوير البحث العلمي (دراسة ميدانية بجامعة المسيلة) ،مذكرة ماجستير في علم المكتبات والعلوم الوثائقية، كلية العلوم الإنسانية والحضارة الإسلامية ، جامعة أحمد بن بلة، وهران، 2014 2015، ص 23

كما تعرف قواعد البيانات أيضا بمعناها التقني على أنها: " الملفات والعلاقات الموجودة في وعاء افتراضي إلكتروني يطلق عليه وعلى الأوساط الحاسوبية التي تستخدم لتخزين الملفات في إطار نظام المعلومات بقاعدة البيانات".[1]

- ✓ **تعريف من ناحية اتفاقية لقواعد البيانات**

يتميز القالب الاتفاقي في تعريف قواعد البيانات بالوحدة وفي نفس الوقت بالتنوع، بحيث تنص اتفاقية برن المتعلقة بحماية المصنفات الأدبية والفنية بموجب المادة الثانية الفقرة الخامسة على أنّه " تتمتع مجموعات المصنفات الأدبية والفنية لدوائر المعارف والمختارات الأدبية التي تعتبر ابتكارا فكريا،بسبب اختيار وترتيب محتوياتها بالحماية بهذه الصفة وذلك دون المساس بحقوق المؤلفين فيما يختص بكلّ مصنف يشكل جزءا من هذه المجموعات"[2].

- ✓ **التعريف القانونى:**

عرفت المادة الأولى الفقرة الثانية من قرار التوجيه الاوروبي قواعد البيانات على أنها: "تجميع أعمال أو بيانات أو أية مواد أخرى، منتجة بشكل مستقل، متى كانت مرتبة بطريقة نظامية، ومنهجية، ويمكن الوصول إليها فرديا سواء بوسيلة إلكترونية أو بأي طريقة أخرى".[3]

حيث يتضح من نص المادة أعلاه أن القرار التوجيهي الأوروبي قد عرف قاعدة البيانات من خلال النمط والطريقة المنهجية لتجميع البيانات الخاص بها، وهو الشيء الكفيل بإضفاء الحماية القانونية لها.

ويتعين الإشارة إلى أنه قد ورد تعريف آخر لقواعد البيانات في التشريع الفرنسي، وذلك بموجب ملحق المرسوم رقم 240-95 المؤرخ في 1995/03/03 المتعلق

[1] ايمان آيت مهدي ، نظم إدارة قواعد البيانات العلائقية ودورها في تشغيل نظم مساندة القرار ،مجلة شعاع للدراسات الاقتصادية ،المجلد 3 العدد 1، مارس 2019، ص 311

[2] المادة 02/05 من اتفاقية برن لحماية المصنفات الأدبية والفنية المؤرخة في 09 سبتمبر سنة 1886 والمتممة بباريس في 04 مايو سنة 1896 والمعدلة ببرلين في 13 نوفمبر سنة 1908، والمتممة ببرن في 20 مارس سنة 1914 والمعدلة بروما في 02 يونيو سنة 1928 وبروكسل في 26 يونيو سنة 1948 واستوكهولم في 14 يوليو سنة 1967 وباريس في 24 يوليو سنة 1971 والمعدلة في 28 سبتمبر سنة 1979 والتي صادقت عليها الجزائر بموجب الأمر الرئاسي 97-341 المؤرخ في جر العدد 61، الصادرة بتاريخ 14/09/1997.

[3] المادة الأولى، الفقرة الثانية، قرار التوجيه الأوروبي.

بمصطلحات المعلوماتية والمنفذ للقانون رقم: 665- 94 المؤرخ في 1994/08/04 المتعلق باللغة الفرنسية، حيث عرف هذا الملحق قواعد البيانات على أنها " مجموعة معطيات منظمة بقصد استعمالها بواسطة برامج مرتبطة بتطبيقات مميزة وبشكل يسهل الحركة المستقلة لهذه المعطيات وتلك البرامج".[1]

الفرع الثاني: خصوصية قواعد البيانات الرقمية

يعود الفضل في صياغة مفهوم خصوصية المعلومات الالكترونية أو البيانات الرقمية، كمفهوم مستقل عن باقي مفاهيم الخصوصية إلى المؤلفين الأمريكيين westin alan و milar في مؤلفهما الخصوصية والحرية، وفي كتاب الاعتداء على الخصوصية، ويمكن القول أن مفهومي الخصوصية والخصوصية المعلوماتية أو الرقمية مترادفان وما يفرقهما هو فقط أن الخصوصية المعلوماتية برزت في ظل ظهور الانترنيت وتقنيات الاتصال الحديثة والفضاءات الرقمية، بينما الخصوصية عامة موجودة منذ القدم، انطلاقا من ضبط الحياة والسلوكيات الفردية في إطار الجماعة وأحقية الآخرين عليه في احترام خصوصياتهم ولا يجوز لأي شخص التعدي عليها بأي شكل من الأشكال، ومن هنا فالخصوصية المعلوماتية (الرقمية) هي حق الفرد في أن يضبط عملية جمع المعلومات الشخصية عنه وعملية معاملتها آليا وحفظها وتوزيعها واستخدامها في صنع القرار الخاص بالمؤثر فيه.[2]

المطلب الثاني: خصائص قواعد البيانات الرقمية

تمتاز قاعدة البيانات بجملة من الخصائص تتعلق أساسا بجانبها التقني من حيث تجميعها المنطقي للبيانات، أو الاسترجاع المنظم لها، وكذا كيانها المادي، وإلى استقلالية

[1] محمد عطية علي ، محمد الرازي ،الحماية القانونية لقواعد البيانات في القانون المصري والتشريعات المقارنة، دار الجامعة الجديدة للنشر الإسكندرية، 2013، ص 86.
[2] ليلى بن برغوث، مرجع سبق ذكره، ص447.

بياناتها عن هيكل قاعدة البيانات إضافة إلى خصائص أخرى تتعلق بالجانب القانوني فهي نتاج فكري محمي قانونا ينتمي إلى بيئة المصنفات الرقمية.[1]

ويتناول هذا المطلب الخصائص التقنية لقواعد البيانات الرقمية (الفرع الأول)، الخصائص القانونية لقواعد البيانات الرقمية (الفرع الثاني).

الفرع الأول: الخصائص التقنية لقواعد البيانات الرقمية

تتمثل في ما يلي:

- **التجميع المنطقي للبيانات:** من خلال هذه الخاصية يظهر لنا الفرق بين قاعدة البيانات ومختلف التجميعات الأخرى التي قد تتشابه معها في بعض الخصائص؛ إذ أن قاعدة البيانات الرقمية تعتمد في عملها على تجميع منطقي للبيانات التي تحتويها على عكس مختلف التجميعات العشوائية التي لا تشكل قاعدة بيانات.[2]

وإضافة لذلك تعتمد قاعدة البيانات الرقمية من خلال هذه الخاصية على الحد من تكرار البيانات المتاحة على قاعدة البيانات، وذلك لتجنب الأخطاء المحتملة والتي قد تصل إلى عدة نتائج مكررة، كما تجنب هذه الخاصية الأخطاء والخسارة في مساحة الذاكرة الخاصة بقاعدة البيانات.

- **التطور والتحديث والاسترجاع المنظم للبيانات:** إذ يمكن لمستخدم قاعدة البيانات الرقمية استرجاع المعلومات والبيانات التي يحتاجها فقط دون باقي البيانات الأخرى التي تحتويها قاعدة البيانات الرقمية، ويعتمد الاسترجاع المنظم على تصفية البيانات، مما يساهم في تقليص حجم عرض البيانات المتاحة، وذلك عن طريق اختيار تحديد لعرض النتائج حسب الطلب.

[1] عبد الله قيبوعة، الاليات القانونية لحماية قواعد البيانات في ظل البيئة الرقمية –دراسة مقارنة–، أطروحة مقدمة لنيل شهادة دكتوراه الطور الثالث في الحقوق، تخصص القانون الخاص المعمق، كلية الحقوق والعلوم السياسية، الجامعة الافريقية أحمد دراية أدرار، 2022 ، ص29

[2] محمد سلطان ، ماجد على محاسنة،تكنولوجيا قواعد البيانات وأثرها في اختيار الاستراتيجية التنافسية لشركات الدواء الأردنية ،أطروحة دكتوراه فلسفة في الإدارة كلية الدراسات الإدارية والمالية العليا ، جامعة عمان العربية للدراسات العليا، 2007، ص37.

كما تجدر الإشارة إلى أنّ خاصية الاسترجاع المنظم تعتمد على تناسق البيانات، بحيث يظهر لكل مستخدم المعطيات بصورة متناسقة وواضحة وبعيدة عن البيانات غير المرغوب فيها، خصوصا إذا تزامن ذلك مع تواجد مستخدم أخر يقوم بعملية البحث على قاعدة البيانات[1].

- **الكيان المادي لقواعد البيانات الرقمية:** تتمتع قواعد البيانات الرقمية بكيان مادي محسوس وذلك نظرا لتجسيدها على دعامة مادية أو الحامل الإلكتروني أو جهاز الحاسب الآلي أو شبكات الإنترنت وهو المفهوم الذي يمكن من خلاله التفرقة بين قواعد البيانات الإلكترونية التي يتم تثبيتها على قرص صلب أو جهاز الحاسب الآلي وبين قواعد البيانات على الخط التي يتم تثبيتها على شبكات الإنترنت وكذا قواعد البيانات التي تعتمد في تثبيتها على دعامة ورقية[2].
- **استقلالية البيانات عن هيكل قاعدة البيانات الرقمية:** يقصد بهذه الخاصية " تحقيق استقلالية هياكل التخزين عن هياكل البيانات الواقعية"، بحيث تتكون قاعدة البيانات من مجموعة البيانات والمعطيات التي تكون منتجة مسبقا وبشكل مستقل، إذ تعتمد أغلب قواعد البيانات على الفصل بين هذه البيانات التي تشكل محتوى قاعدة البيانات وبين شكلها. [3]

الفرع الثاني: الخصائص القانونية لقواعد البيانات الرقمية

تتميز قاعدة البيانات بعدة خصائص قانونية فهي مصنف رقمي ونتاج فكري محمي قانونا:

[1] عبد الله قيبوعة، مرجع سبق ذكره ، ص 29.
[2] المرجع نفسه، ص29.
[3] عبد الله قيبوعة، مرجع سبق ذكره، ص ص29-30.

- **قاعدة البيانات مصنف رقمي:**

يعتبر المصنف الرقمي عبارة عن: " مصنف إبداعي عقلي ينتمي إلى بيئة تقنية المعلومات، إذ يضم برامج الحاسوب وقواعد البيانات والدوائر المتكاملة وأسماء النطاقات ومواقع الإنترنت...الخ"

حيث تنتمي قواعد البيانات إلى بيئة المصنفات الرقمية التي تعتبر أحد أهم مظاهر عصر الرقمنة وهو ما دفع أغلب التشريعات المقارنة إلى البحث في سبيل توفير الحماية القانونية لها، لاسيما أن قواعد البيانات قد أصبحت تساهم بشكل كبير في عملية التطور الاقتصادي والعلمي وشتى مجالات الحياة العامة.[1]

- **قاعدة البيانات الرقمية نتاج فكري محمي قانونا:**

تعتبر قواعد البيانات نتاج فكري معترف به قانونا، تحميه مختلف التشريعات المقارنة، حيث خولت أغلب هذه التشريعات للمؤلف حق الاستئثار بنتاجه الفكري أو الذهني، وهو ما ينتج عنه بالضرورة عدة حقوق مادية وأدبية، تحميها مختلف التشريعات الداخلية والدولية أيضا.[2]

المطلب الثالث: تمييز قواعد البيانات عن غيرها من المصنفات الرقمية

إن تحديد مفهوم قواعد البيانات وإزالة اللبس في معناها الذي قد يتشابه أو يختلط ببعض المفاهيم أو المصنفات، وهو ما يقتضي منا التطرق إلى مفهوم بعض هذه المصنفات كبرامج الحاسوب والوسائط المتعددة، مع محاولة التفرقة بينها وبين قواعد البيانات.

الفرع الأول: تمييز قواعد البيانات عن برامج الحاسوب

[1]. المرجع نفسه ، ص 31
[2] المرجع نفسه ، نفس الصفحة.

هناك من يعرف برامج الحاسوب على أنها " مجموعة من التعليمات والأوامر التي يمكن استعمالها عن طريق جهاز الحاسوب بغرض الحصول على نتائج معينة"[1].

وعلى الرغم من أن قواعد البيانات وبرامج الحاسوب يتشابهان بكونهما مصنفات رقمية محمية بموجب قانون حقوق المؤلف في معظم التشريعات المقارنة إلا أنّهما يختلفان في عدة نقاط أهمها:

- **من حيث الجانب التقني:** تعتمد قواعد البيانات في عملها أساسا على ما يصطلح عليه بنظام إدارة قواعد البيانات، إذ يقوم هذا النظام بمهمة فتح قاعدة البيانات والوصول إلى مختلف البيانات المتاحة عليها عن طريق توجيهات المستخدم، أما عن برامج الحاسوب فإن التعامل معها يكون بصفة مباشرة عن طريق لوحة مفاتيح جهاز الكمبيوتر.
- **من حيث الفائدة:** إذ تختلف قاعدة البيانات عن برامج الحاسوب من حيث الفائدة المرجوة من كليهما، فإذا كانت قواعد البيانات تقوم على مسألة ترتيب منطقي ومنهجي لمجموعة من البيانات قصد تسهيل الوصول إليها عند الحاجة، فإن برامج الحاسوب هي عبارة عن مجموعة من التعليمات والأوامر التي توجه إلى الآلة من أجل القيام بإنجاز مهام محددة اعتمادا على هذه التعليمات والأوامر. [2]
- **من حيث الأنواع:** هناك ثلاثة معايير يعتمد عليها في تقسيم أنواع قواعد البيانات، فالمعيار الأول خاص بهيكلة البناء وتقسم حسبه قواعد البيانات إلى قواعد بيانات هرمية، وقواعد بيانات شبكية وأخرى علائقية، أما المعيار الثاني فهو معيار خاص بالوظيفة ويقسم قواعد البيانات إلى قواعد بيانات فردية وقواعد بيانات متشاركة وأخرى موزعة، إضافة إلى قواعد بيانات جماهيرية، أما عن المعيار الثالث فهو معيار خاص بالمحتوى يقسم قواعد البيانات إلى قواعد بيانات بيبليوجرافية وقواعد بيانات مرجعية وقواعد بيانات

[1] المرجع نفسه ، ص32.
[2] كوثر مازوني، الشبكة الرقمية وعلاقتها بالملكية الفكرية، دار هومة للنشر ،الجزائر 2008، ص 116.

النصوص الكاملة، وذلك على خلاف برامج الحاسوب التي تنقسم حسب وظيفتها إلى برامج تشغيلية وأخرى تطبيقية.[1]

- **من حيث الهدف:** تهدف قواعد البيانات في مجملها إلى تسهيل الوصول إلى معلومة ما عن طريق خصائص عملها المميزة، وذلك على عكس برامج الحاسوب التي تهدف إلى الوصول لحل أو معالجة مسألة معينة.[2]

الفرع الثاني: تمييز قواعد البيانات عن قواعد المعلومات

يقصد بالبيانات أنها: " مجموعة من الحقائق التي تعبر عن مواقف وأفعال معينة حدثت في الماضي أو الحاضر أو ستحدث في المستقبل سواء كان التعبير بالكلمات ؛ أو الأشكال؛ أو الرموز "[3].

أما عن مصطلح المعلومات فتعرف: "نتائج عمليات النماذج، التكوين، التنظيم، أو تحويل البيانات بطريقة تؤدي الى زيادة مستوى المعرفة للمستقبل"[4].

وبناء على ذلك يمكن استخلاص تعريف لكل من قاعدة البيانات وقاعدة المعلومات على النحو التالي: " قاعدة البيانات عبارة عن خوارزم ورموز رياضية، تكون مقسمة إلى ملفات وسجلات وحقول، تتمتع بأداء وظيفي متميز ناتج عن جهد فكري جاد أما قاعدة المعلومات هي عبارة عن خوارزم ورموز رياضية تقوم بمعالجة البيانات التي تظهر فيها البصمة الشخصية بشكل ينم عن وجود جهد فكري متميز "[5].

[1] المرج نفسه ، ص116.
[2] المرجع نفسه، ص116.
[3] أيمن عبد الله فكري، الجرائم المعلوماتية (دراسة مقارنة في التشريعات العربية والأجنبية مكتبة القانون والاقتصاد، الطبعة الأولى، الرياض، 2014، ص 39.
[4] أمينة قدابفة، استراتيجية أمن المعلومات، مجلة أبعاد اقتصادية، المجلد 6، العدد1، 2016، ص164.
[5] كوثر مازوني، مرجع سبق ذكره، ص118.

الفرع الثالث: تمييز قواعد البيانات عن المصنفات المتعددة الوسائط

يعرف هذا النوع من المصنفات على أنه " ناقل معلوماتي جديد يجمع في الوقت ذاته الصوت والنص والصورة الثابتة أو المتحركة والبيانات القادمة بدورها من وسائط مختلفة ".[1]

حيث يتضح أنه يتشابه مع مصنف قواعد البيانات من حيث كونهما مصنفات رقمية يمتازان بلمسة خاصة من مؤلفهما في اختيار وجمع موادهما، إلا أن ذلك لا ينفي وجود عدة اختلافات تتمثل أساسا في:

- **من حيث عملية الدمج والترتيب:** إن كان مصنف قواعد البيانات يعتمد في عملية تجميعه للبيانات على ترتيبها بطريقة نظامية ومنهجية فقط دون عملية دمجها، فإن مصنف الوسائط المتعددة يتضمن تفاعل وعملية دمج بين عدة مؤثرات كالصوت والصورة والكتابة والنص.[2]
- **من حيث استقلالية البيانات:** هناك من يرى أن شرط استقلال البيانات الذي تتضمنه قاعدة البيانات غير متوفر في مصنف الوسائط المتعددة لاسيما ألعاب الفيديو باعتبارها مصنفا متعدد الوسائط.
- **من حيث الوصول الفردي للبيانات:** يظهر من جهة أخرى أنه وإن كان بالإمكان الوصول إلى بيانات قواعد المعطيات بصفة فردية سواء بوسيلة الكترونية أو بأي طريقة أخرى، فإن ذلك لا يتصور في مصنف الوسائط المتعددة الذي تترابط محتوياته بصورة تمنع الوصول إلى بيناته بصفة فردية.[3]

[1] فتيحة حواس، حماية المصنفات الرقمية وأسماء النطاقات على شبكة الانترنت، مكتبة الوفاء القانونية، الطبعة الأولى، الإسكندرية 2017، ص64.

[2] أحمد محمد الإمام، الملكية الفكرية لقواعد البيانات في القانون السوري والمقارن، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية المجلد، 29، العدد الثاني 2013، ص 346

[3] كمال دعاس، حق المؤلف في ميدان المصنفات الرقمية أطروحة دكتوراه في القانون، كلية الحقوق سعيد حمدين ،جامعة الجزائر 1، 2018 ص 229.

المبحث الثاني: الاطار القانوني لحماية البيانات الرقمية في الجزائر

في ظل التطور السريع لتكنولوجيا المعلومات والاتصالات، أصبحت حماية البيانات الرقمية ضرورة ملحة لضمان سلامة وأمان المعلومات الشخصية والتجارية والحكومية، حيث تسعى الجزائر كجزء من التزامها بحماية بيانات مواطنيها ومؤسساتها، إلى تطوير إطار قانوني ومؤسسي شامل يهدف إلى مواجهة التهديدات السيبرانية وضمان حماية البيانات الرقمية.

وعليه قسم هذا المبحث الى حماية قواعد البيانات الرقمية وفقا لقواعد المسؤولية المدنية (المطلب الأول) تليها الحماية الجزائية لقواعد البيانات الرقمية في التشريع الجزائري (المطلب الثاني) ثم الجزاء الجنائي المقرر لجنح تقليد مصنف قاعدة البيانات الرقمية (المطلب الثالث).

المطلب الأول: حماية قواعد البيانات الرقمية وفقا لقواعد المسؤولية المدنية

إن دراسة موضوع حماية قواعد البيانات الرقمية وفقا لقواعد المسؤولية المدنية يقتضي منا التطرق إلى أساس المسؤولية المدنية، فيما إذا كان الضرر الذي أصاب مؤلّف قاعدة البيانات ناتج عن التزام عقدي، إذ تطبق بشأنه أحكام وقواعد المسؤولية العقدية (الفرع الاول) أو ناتج عن التزام غير عقدي، والذي تطبق بشأنه قواعد المسؤولية التقصيرية (الفرع الثاني).

الفرع الأول: حماية قواعد البيانات الرقمية بموجب أحكام المسؤولية العقدية

إن إنشاء أي عقد يترتب عليه بالضرورة التزامات تقع على طرفيه، إذ أن القوة الملزمة للعقد تفيد قيام كل طرف بتنفيذ التزامه وفي حالة عدم قيام أحد الطرفين بتنفيذ هذا الالتزام عينا، وقام الدائن بطلبه أجبر المدين على تنفيذه، وهو أصل الالتزام أما إذا إستحال التنفيذ العيني حكم القاضي بالتعويض للدائن إذا طلبه هذا الأخير، وتوفرت شروطه المتمثلة

في الخطأ العقدي، والضرر، والعلاقة السببية بين الخطأ والضرر كما يشترط أن يكون العقد صحيحا بين أطرافه، وذلك بغض النظر عن نوعه، فيما إذا كان يتضمن عقدا في استغلال قاعدة البيانات، أو غيرها من العقود المتعلقة بها.[1]

أولا: الخطأ العقدي

ويقصد به عدم قيام المدين أو تأخره في تنفيذ التزامه التعاقدي، سواء كان هذا التأخير أو عدم التنفيذ قد وقع عن عنت من المدين، أو عن إهمال منه[2]، وينشأ الخطأ العقدي بالنسبة لموضوع الدراسة أي قاعدة البيانات الرقمية، إذا نكل مثلا مستخدم قاعدة البيانات بالتزامه التعاقدي مع مؤلف أو مصنع قاعدة البيانات، أو تأخر في تنفيذ هذا الالتزام.[3]

وقد تثار أيضا مسألة قيام الخطأ العقدي بين مؤلف قاعدة البيانات، وبين الناشر أو الموزع أو المنتج لها نتيجة إخلال أحد أطراف العلاقة بالتزامه التعاقدي، كأن يقوم الناشر بنشر المصنف على شبكة الإنترنت في غير الحالة التي تسلمها عليها من قبل المؤلّف، سواء بالتعديل عليها أو بغيرها من الأفعال المخالفة لبنود العقد المبرم بينهما.

ويقوم الخطأ أيضا في حالة عدم احترام مقدم خدمات الإنترنت لبنود العقد المتضمنة أخذ الاحتياطات اللازمة لمنع الدخول إلى المصنف، ولم يقم بتأمين الحراسة اللازمة لمضمون الموزعات المفتوحة للمشتركين.[4]

ويقع عبء إثبات الخطأ العقدي على عاتق الدائن، فإذا كان محل هذا الالتزام هو تحقيق نتيجة فعلى الدائن إثبات أن هذه النتيجة لم تتحقق، وإذا كان محل الالتزام هو بذل عناية وجب على الدائن في هذه الحالة إثبات عدم قيام المدين ببذل عناية الرجل العادي.[5]

[1] محمد صبري السعدي، الواضح في شرح القانون المدني الجزائري النظرية العامة للإلتزامات، مصادر الالتزام العقد والإرادة المنفردة، الجزء الأول، دار الهدى، الطبعة 4 ، الجزائر، 2006-2007 ، ص ص 310-311

[2] المرجع نفسه ، ص 311

[3] فتيحة حواس، مرجع سبق ذكره، ص 156

[4] المرجع نفسه ، ص 156

[5] محمد صبري السعدي، مرجع سبق ذكره، ص 314

ثانيا: الضرر

يعرف الأستاذ محمد صبري السعدي الضرر على أنّه: " الأذى الذي يصيب الشخص نتيجة المساس بمصلحة مشروعة له أو بحق من حقوقه، والمصلحة المشروعة إما أنا تكون مادية أو أدبية "، كما يرى هذا الأخير أن الضرر هو ركن من أركان قيام المسؤولية العقدية، إذ يجب أن يترتب على قيام الخطأ حدوث الضرر الذي يصيب الدائن نتيجة عدم قيام المدين بتنفيذ إلزامه التعاقدي أو التأخر فيه سواءا كان هذا الضرر ماديا أو أدبيا، حالا أو محقق الوقوع مسقبلا[1].

يتحقق الضرر بالنسبة إلى مؤلفي قاعدة البيانات إذا أخل المدين بالتزامه التعاقدي مما قد يسبب للدائن ضررا ماديا يمس حقوقه المالية أو معنويا، يلتزم هذا الأخير أي الدائن بإثباته.

ثالثا: العلاقة السببية بين الخطأ والضرر

مفاد هذا الركن أن يكون الضرر الذي أصاب الدائن (مؤلف قاعدة البيانات) ناتجا عن خطأ المدين (مستخدم الشبكة متعهد الإيواء، مورد المحتوى المعلوماتي...) أو بمعنى آخر أن يكون الخطأ الصادر من المدين هو السبب في الإضرار بالدائن.

ويقع عبء إثبات العلاقة السببية بين الخطأ والضرر على عاتق الدائن، ويجوز للمدين نفيه إذا أثبت أن الضرر وقع بسبب أجنبي أو بخطأ الدائن.[2]

وبذلك يستطيع مؤلّف قاعدة البيانات إذا أصابه ضرر ناتج عن الإخلال بالتزام عقدي بينه وبين مستخدم قاعدة البيانات، أو بينه وبين مقدم خدمات الأنترنت أن يثبت العلاقة السببية بين الخطأ العقدي الذي تسبب فيه المستخدم أو مقدم خدمات الإنترنت، وبين الضرر

[1] المرجع نفسه، ص ص 318 -319
[2] المرجع نفسه ،ص ص 318 -319

المادي أو / والمعنوي الذي أصابه، للحصول على تعويض عادل شريطة أن يكون هذا الضرر ناتج عن خطأ هذا الأخير.[1]

الفرع الثاني: حماية قواعد البيانات الرقمية بموجب أحكام المسؤولية التقصيرية

يقوم هذا النوع من المسؤولية في حالة غياب العقد الذي يربط بين مؤلف قاعدة البيانات، وبين غيره من المستخدمين الغير شرعيين لقاعدة البيانات، فإذا كانت المسؤولية العقدية هي نتاج أو جزاء عدم الالتزام بالعقد فإن المسؤولية التقصيرية هي نتاج أو جزاء الفعل الغير مشروع.

وتنص المادة 1240 من القانون المدني الفرنسي على أنه: " كل فعل أيا كان يقع من الإنسان ويحدث ضررا للغير يلزم من أوقع هذا الفعل الضار بخطئه بتعويض هذا الضرر".

كما تنص المادة 124 من القانون المدني الجزائري في نفس السياق على أنه: " الفعل أيا كان يرتكبه الشخص بخطئه، ويسبب ضررا للغير يلزم من كان سببا في حدوثة بالتعويض".[2]

أما المشرع المصري فقد نص هو الآخر بموجب المادة 163 من القانون المدني على أنه: " كل خطا سبب ضررا للغير، يلزم من ارتكبه بالتعويض".[3]

حيث قررت محكمة النقض المصرية في مسألة المسؤولية التقصيرية أن: " المقرر في قضاء هذه المحكمة أن المسئولية التقصيرية لا تقوم إلا بتوافر أركانها الثلاثة من خطأ ثابت في جانب المسئول إلى ضرر واقع في حق المضرور وعلاقة سببية تربط بينهما بحيث يثبت أن الضرر قد نشأ عن ذلك الخطأ ونتيجة لحدوثه "[4] ويتضح من ذلك أن المسؤولية

[1] المرجع نفسه، ص319.
[2] الجمهورية الجزائرية الديمقراطية الشعبية ، الأمر رقم: 75/58 المؤرخ في 26 سبتمبر 1975 والمتضمن القانون المدني، المعدل والمتمم الصادر في الجريدة الرسمية بتاريخ 30 أكتوبر 1975، العدد 81
[3] الجمهورية الجزائرية الديمقراطية الشعبية ، القانون رقم 131 لسنة 1948 المتضمن إصدار القانون المدني، المعدل بتاريخ 16 جويلية 2011
[4] محمد عطية على محمد الرزازي، مرجع سابق ذكره ، ص 436

التقصيرية تقوم على ثلاثة أركان أساسية وهي: الخطأ الضرر العلاقة السببية بين الخطأ والضرر.

أولا: طبيعة الخطأ في مجال حماية قواعد البيانات

المسؤولية التقصيرية هو: " إخلال بالتزام قانوني الذي يعتبر الإخلال به خطأ في المسؤولية التقصيرية فهو دائما التزام ببذل عناية، وهو أن يصطنع الشخص في سلوكه اليقظة والتبصر حتى لا يضر بالغير، فإذا انحرف عن هذا السلوك الواجب، وكان من القدرة على التمييز بحيث يدرك أنه قد انحرف، كان هذا الانحراف خطأ يستوجب مسؤولية تقصيرية ".[1]

أو هو حسب مفهوم آخر: " الانحراف عن سلوك الرجل المعتاد مع إدراك الشخص لذلك، وبعبارة أخرى هو الإخلال بالالتزام القانوني الذي يفرض على كل شخص بعدم الإضرار بالغير وأن يراعي في سلوكه الحيطة والتبصر حتى لا يضر بغيره، وهذا الالتزام هو التزام ببذل عناية وليس بتحقيق نتيجة وبالتالي إذا انحرف عن هذا السلوك أعتبر مخطئا واستلزم ذلك قيام مسؤوليته[2].

ويشترط لقيامه توفر عنصرين عنصر مادي، ويتمثل في التعدي البين على سلوك الشخص المتبصر الحازم لشؤونه، وعنصر معنوي يتمثل في الإدارك أو النية، إذ لا يمكن نسبة الخطأ إلى شخص فاقد للتمييز.[3]

ويقوم الخطأ في مصنف قاعدة البيانات، بالتعدي على أحد الحقوق الأدبية أو المادية لمؤلفها، كالدخول الغير مرخص لقاعدة البيانات، أو القيام باستنساخها أو استعمالها في غير الحالات الاستثنائية المرخصة لذلك، أو القيام بإعادة نشرها بدون ترخيص.

[1] عبد الرزاق أحمد السنهوري، الوسيط في شرح القانون المدني الجديد نظرية الالتزام بوجه عام ، الجزء 1 ،دار أحياء التراث العربي، بدون طبعة، بيروت ، 1952، ص ص 778.779

[2] محمد المهدي بكراوي ، مليكة جامعي ، المسؤولية التقصيرية مداخلة ملقاة بمناسبة اليوم الدراسي بعنوان: الإتجاهات الحديثة في نظرية المسؤولية المدنية كلية الحقوق والعلوم السياسية، جامعة أدرار، يوم 23 ماي 2013، ص 27

[3] سمية، بومعزة، حقوق المؤلف في النطاقين التقليدي والرقمي في ظل التشريع الجزائري، مذكرة ماجستير في الحقوق والعلوم السياسية جامعة باتنة ، ص 158

ثانيا: الضرر

ويقصد بالضرر " تفويت كسب مادي مشروع للمؤلف أو المساس بسمعته وتشويه، مصنفه، وهذا الضرر يجب على المؤلف إثباته"، وكما سبق الإشارة إليه فإن الضرر نوعان، ضرر مادي وهو الإخلال بمصلحة للمضرور ذات قيمة مالية، ويتمثل في الأذى الذي يلحق بمؤلف مصنف قاعدة البيانات ويتمثل هذا الضرر في المبلغ الذي كان سيدفعه المعتدى على قاعدة البيانات إذا استغلها بصفة قانونية وبمقابل، ويشترط في هذا الضرر أن يكون محققا، إذ أنه لا تعويض عن الأضرار المحتملة حتى يتحقق الضرر فعلا، وضرر معنوي أو أدبي ومجاله الأضرار الغير مالية، وهو الذي يصيب مؤلف قاعدة البيانات في شرفه واعتباره.[1]

ثالثا: العلاقة السببية

وتعتبر العلاقة السببية هي الرابطة بين الخطأ التقصيري، والضرر الذي أصاب مؤلف مصنف قاعدة البيانت، إذ يستلزم على هذا الأخير إثبات هذه العلاقة لقيام المسؤولية التقصيرية للشخص الماس بحق من الحقوق المادية أو الأدبية لمؤلف قاعدة البيانات.

ويتعين الإشارة إلى أنّ إثبات قيام العلاقة السببية في مجال قواعد البيانات على الخط بصفة خاصة، أو في مجال النشر الإلكتروني بصفة عامة، مسألة جد معقدة، وذلك نظرا لتعقد الظاهرة الالكترونية وتشعبها، فقد يعود سبب الضرر الذي يصيب مؤلف مصنف قاعدة البيانات إلى عدة أسباب أخرى ترجع إلى الأجهزة المستعملة، أو مزود خدمة الإنترنت أو مقدمها، وهو ما يستحيل معه تحديد السبب الرئيسي في الضرر.[2]

[1] عبد الله قيبوعة، مرجع سبق ذكره، ص ص199-200.
[2] المرجع نفسه ، ص ص199-200.

المطلب الثاني: الجرائم الماسة بمصنف قاعدة البيانات الرقمية

بالرجوع إلى الأحكام الجزائية التي تضمنها قانون حقوق المؤلف والحقوق المجاورة في التشريع الجزائري يتضح أن هذا الأخير قد أعطى وصفا وحيدا لهذه الجرائم، أين أدخلها تحت وصف جنحة التقليد.

حيث تقوم جنحة تقليد مصنف قاعدة البيانات على ثلاثة أركان أساسية، ركن شرعي (الفرع الأول)، وهو أساس أي متابعة جزائية وركن مادي (الفرع الثاني)، ويتشكل من عدة صور للاعتداء على قاعدة البيانات وركن معنوي (الفرع الثالث)، يعبر عن النية الإجرامية للمعتدي على قاعدة البيانات.

الفرع الاول: الركن الشرعي لجرائم التقليد الماسة بقواعد البيانات الرقمية

تنص المادة الأولى من قانون العقوبات الجزائري على أنه: " لا جريمة ولا عقوبة أو تدابير أمن بغير قانون"[1] ويستفاد من هذا النص أنه لا يمكن متابعة أي شخص ما لم تكن الأفعال التي قام بها هذا الأخير تشكل جريمة يعاقب عليها القانون.

ويتمثل الركن الشرعي للجرائم الماسة بمصنف قاعدة البيانات في التشريع الجزائري في ما نصت عليه أحكام المواد 151 و155 من الأمر 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة وتنص هاته المواد على عدة صور لجنحة التقليد.

و تنص المادة 151 على أنّه: يعد مرتكبا لجنحة التقليد كل من يقوم بالأعمال الأتية:

- الكشف غير المشروع للمصنف أو المساس بسلامة مصنف أو أداء لفنان مؤد أو عازف.
- استنساخ مصنف أو أداء بأي أسلوب من الأساليب في شكل نسخ مقلدة.
- استيراد أو تصدير نسخ مقلدة من مصنف أو أداء.

[1] الأمر رقم: 66-156 المؤرخ في 08/06/1966 المتضمن قانون العقوبات المعدل والمتمم.

- بيع نسخ مقلدة لمصنف أو أداء.
- تأجير أو وضع رهن التداول لنسخ مقلدة لمصنف أو أداء".

وتنص المادة 152 على أنّه: " يعد مرتكبا لجنحة التقليد كل من ينتهك الحقوق المحمية بموجب هذا الأمر فيبلغ المصنف أو الأداء عن طريق التمثيل أو الأداء العلني، أو البث الإذاعي السمعي أو السمعي البصري، أو التوزيع بواسطة الكبل أو بأية وسيلة نقل أخرى لإشارات تحمل أصواتا أو صورا وأصواتا أو بأي منظومة معالجة معلوماتية ".

أما المادة 155 فقد نصت على أنّه: يعد مرتكبا لجنحة التقليد... كل من يرفض عمدا دفع المكافأة المستحقة للمؤلف أو لأي مالك حقوق مجاورة آخر خرقا للحقوق المعترف بها بموجب الحقوق المنصوص عليها في هذا الأمر".[1]

ويتضح من ذلك أن المشرع الجزائري قد جرم كل شكل من أشكال التعدي على المصنفات بصفة عامة سواء كانت مصنفات رقمية أو غيرها من المصنفات الأخرى التي نص عليها من خلال الفصل الأول من الباب الأول بموجب المادة الثالثة وما يليها من الأمر رقم: 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة، بما فيها مصنف قاعدة البيانات التي نص عليها في المادة الخامسة من نفس الأمر، وبالتالي فإن أي مساس بقاعدة البيانات على الشكل الذي حدد بمفهوم المواد أعلاه يعد جنحة ويستوجب العقاب.

الفرع الثاني: الركن المادي لجرائم التقليد الماسة بقواعد البيانات الرقمية

يقصد بالركن المادي الفعل أو العمل الخارجي الذي يعبر عن النية الجنائية أو الخطأ الجزائي[2] فالقانون يعاقب على الأفعال المادية، ولا يعاقب على النوايا المجردة من الفعل أو العمل الخارجي لها.

[1] 151 و152 و155 من الأمر 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة

[2] فاطمة شعران، حماية المصنفات الرقمية في التشريع الجزائري والتشريعات المقارنة مجلة الدراسات القانونية المقارنة، جامعة حسيبة بن بوعلي الشلف المجلد 02، العدد 02 ديسمبر 2016، ص..119

ويقوم الركن المادي لجنحة التقليد على السلوك الإجرامي المتمثل في قيام الجاني بإحدى الأفعال المنصوص عليها بالمواد 151 و152 و155 من الأمر 03-05، والتي تؤدي إلى المساس بمصنف محمي قانونا كمصنف قاعدة البيانات الرقمية، وذلك بوجود علاقة سببية بين الفعل المجرم والنتيجة.

1-السلوك الإجرامي الماس بمصنف قاعدة البيانات الرقمية:

ويقصد به: " السلوك المادي الصادر عن الإنسان والذي يتعارض مع القانون، فالجريمة هي في المقام الأول، فعل آدمي أي سلوك صادر عن إنسان، فالفعل هو جوهر الجريمة ولهذا قيل: " لا جريمة دون فعل ".

والفعل يشمل الإيجاب كما يشمل السلب، فمن يأمره القانون بالعمل فيمتنع عن أدائه يكون قد خالف القانون مثله مثل من يأمره القانون بالامتناع عن الفعل فيفعل سواء بسواء، ففي كلتا الحالتين هناك مخالفة لأوامر القانون".[1]

ويقوم السلوك الإجرامي لجنح التقليد على اقتراف الجاني لهذا الجرم متخذا إحدى الصور المنصوص عليها في المواد 151 و152 و155 من الأمر.05-03

وتجدر الإشارة إلى أن هناك من يقسم هذه الصور إلى جنح التقليد المباشر كالكشف غير المشروع للمصنف، أو المساس بسلامة المصنف أو استنساخه، إضافة إلى تبليغ المصنف عن طريق التمثيل أو البث أو التوزيع وإلى جنح مشابهة لجنح التقليد تتمثل في التعامل في هذه المصنفات عن طريق الاستيراد والتصدير أو البيع أو التأجير أو الوضع رهن التداول لنسخ مقلدة لهذه المصنفات، وكذا كل رفض عمدي لدفع مكافأة مستحقة للمؤلف أو لمالك الحقوق المجاورة.[2]

[1] عبد الله سليمان ، شرح قانون العقوبات الجزائري القسم العام، الجزء 1 ، ديوان المطبوعات الجامعية ، الجزائر، 1996، ص 147

[2] حليمة بن دريس ،حماية حقوق الملكية الفكرية في التشريع الجزائري، أطروحة دكتوراه في القانون الخاص ، كلية الحقوق والعلوم السياسية جامعة تلمسان، 2013- 2014، ص ص 151-152

ويمكن تقسيم هذه الصور إلى نوعين رئيسيين، جرائم تتعلق بالمساس بالحق المعنوي لمؤلف قاعدة البيانات الرقمية، وجرائم أخرى تتعلق بالمساس بالحق المالي أو المادي لمؤلف قاعدة البيانات الرقمية.

أ- صور جرائم التقليد الماسة بالحق المعنوي لمؤلف قاعدة البيانات الرقمية

تشمل هذه الجرائم كل مساس بالحقوق الفكرية أو المعنوية لمؤلف قاعدة البيانات، وتتمثل في نوعين أساسيين: جريمة الكشف الغير مشروع لمصنف قاعدة البيانات الرقمية وجريمة المساس بسلامة مصنف قاعدة البيانات الرقمية.

- **جريمة الكشف الغير مشروع لمصنف قاعدة البيانات:** إذ أنه من حق أي مؤلف لمصنف أدبي محمي قانونا بما في ذلك مصنف قواعد البيانات أن يستأثر بمصنفه الفكري، كما له الحق أيضا في الكشف عن مصنفه في أي وقت كان وبأي طريقة كانت، وبذلك فإن أي كشف غير مشروع لقاعدة البيانات يعد جنحة من جنح التقليد يعاقب مرتكبها جزائيا[1].
- **جريمة المساس بسلامة مصنف قاعدة البيانات:** وهي أيضا صورة من صور الجرائم الماسة بالحق المعنوي لمؤلف قاعدة البيانات، حيث اعتبر المشرع الجزائري أن كل مساس بسلامة المصنفات الأدبية بشكل عام، عن طريق إحدى صور الحذف أو التعديل أو التصوير أو الإضافة من دون الرجوع إلى المؤلف شرطا لقيام المسؤولية الجزائية في هذه الصورة.[2]

وبالتالي فإن أي مساس بحق مؤلف قاعدة البيانات على مؤلفه، عن طريق حذف جزء من قاعدة البيانات أو القيام بتعديلات عليها، أو التصوير، أو الإضافة فيها، بغض النظر

[1] عبد الله قيبوعة، مرجع سبق ذكره، ص215
[2] المرجع نفسه ، ص215

عن نوع وطريقة هذه الإضافة، يعد مرتكبها مسؤولا جزائيا عن جنحة التقليد، عن طريق المساس بسلامة مصنف قاعدة البيانات.[1]

ب- **صور جرائم التقليد الماسة بالحق المالي لمؤلف قاعدة البيانات**

وتشمل هذه الجرائم كل مساس بالحق المادي الذي يتحصل عليه مؤلف قاعدة البيانات كمقابل إبداعه الفكري، كجريمة القيام باستنساخ قاعدة البيانات بغض النظر عن الأسلوب المعتمد في الاستنساخ، وجريمة استيراد أو تصدير نسخ مقلدة لمصنف قاعدة البيانات وجريمة بيع نسخ مقلدة من هذه المصنفات، وجريمة تأجير نسخ مقلدة منها، إضافة إلى جريمة الوضع رهن التداول لنسخ مقلدة لمصنف قاعدة البيانات وجريمة تبليغ المصنف الرقمي بأي منظومة معالجة معلوماتية وجريمة الرفض العمدي لدفع المكافأة المستحقة لمؤلف مصنف قاعدة البيانات. [2]

- **جريمة استنساخ مصنف قاعدة البيانات بأي أسلوب من الأساليب في شكل نسخ مقلدة:** يعتبر الحق في الإستنساح من أهم الحقوق التي يستأثر بها المؤلف وأبرزها وبأي وسيلة كانت، وبغض النظر عن الكمية أو الكيفية سواء كان المصنف كبيرا أم صغيرا، ذو قيمة أو دونها، أو كان هذا الإستنساخ كاملا أو بعضا من أجزائه أو جزء واحد منه فقط.[3]

ولذلك فإن أي استنساخ لقاعدة البيانات دون إذن من المؤلف يعد جريمة يعاقب عليها القانون بغض النظر عن الطريقة أو الكيفية التي يتم بها ذلك، سواء كان في جزء منها أو كلها.

وقد يتخذ الفعل الإجرامي للاستنساخ عدة صور كاستنساخ قاعدة البيانات المتاحة على الخط على دعامة مادية خارج الخط، أو استنساخ قاعدة البيانات المتاحة على

[1] المرجع نفسه ، ص215
[2] عبد الرحمان خلفي، الحماية الجزائية لحقوق المؤلف والحقوق المجاورة، منشورات الحلبي الحقوقية، ط1 ، لبنان، 2007، ص 151
[3] المرجع نفسه، ص 151

الخط على موقع آخر متاح هو الأخر على الخط، فكلتا الصورتين تشكلان جنحة تقليد مصنف قاعدة البيانات.[1]

- **جريمة استيراد أو تصدير نسخ مقلدة لمصنف قاعدة البيانات:** يتحقق الفعل المادي لهذه الجرائم بأي سلوك من شأنه عبور مصنف قاعدة البيانات الحدود الإقليمية للدولة، سواء عن طريق خروجه منها، وهو فعل التصدير، أو دخوله إليها وهو فعل الاستيراد.

ولا يشترط القانون أن يكون الشخص القائم بالفعل المادي أعلاه للجريمة جزائري الجنسية تطبيقا لمبدأ الإقليمية إلا أن الإشكال يثار حول مسألة الاختصاص في حالة ما إذا ارتكب الفعل المادي خارج التراب الوطني، وتم إدخال المصنف عبر الحدود الإقليمية، إذ لا يؤول الاختصاص في هذه الحالة للمحاكم الجزائرية طبقا للقواعد العامة فقط، بل أيضا على أساس ارتكاب الفعل الإجرامي الذي يبدأ في دولة أجنبية ويستمر داخل الحدود الوطنية.[2]

- **جريمة بيع نسخ مقلدة لمصنف قاعدة البيانات:** وهي أيضا صورة من صور جرائم التقليد، إذ جرم المشرع الجزائري كل بيع لمصنفات مقلدة أي نقل حق الاستغلال مقابل ثمن معين، بحيث لا يشترط في هذه العملية التكرار لثبوت الجريمة.[3]

وتقوم هذه الصورة عن طريق قيام الجاني بالفعل المادي المتضمن التصرف عن طريق البيع في مصنف قاعدة البيانات، وبالتالي يعد هذا الأخير مرتكبا لجريمة تقليد مصنف أدبي، ويعاقب على هذا الفعل المجرم طبقا للقانون.

- **جريمة تأجير نسخ مقلدة لمصنف قاعدة البيانات:** يقصد بالتأجير التمكين من حق الانتفاع لفترة معينة، دون اشتراط مدة محددة، إذ يكفي أن يكون الاستئجار لمرة واحدة، ولا يمكن الأخذ بمسألة العود في حالة تكرر العملية، إلا إذا صدر حكم نهائي يقضي بإدانة الشخص بالتقليد وأعاد هذا الأخير نفس الفعل المجرم.[4]

[1] المرجع نفسه ، ص 176.
[2] المرجع نفسه، ص 176
[3] سمية، بومعزة، مرجع سابق ذكره ، ص 175
[4] عبد الرحمان خلفي، مرجع سابق ذكره ، ص 181

حيث أضاف المشرع شكل آخر من أشكال التعدي على حقوق المؤلف وهو تأجير المصنف المقلد بطريقة غير شرعية، وبالتالي فإن أي منح لحق الانتفاع بمصنف قاعدة البيانات المقلد يعتبر جنحة ويستوجب العقاب.

- **جريمة الوضع رهن التداول لنسخ مقلدة لمصنف قاعدة البيانات:** فيعني عرضه قصد الانتفاع أو الاستعمال سواء بمقابل أو دون مقابل، فبمجرد قيام عملية العرض لمصنف مقلد تقوم جنحة التقليد حسب ما أورده المشرع الجزائري بالفقرة الأخيرة من المادة 151 من الامر المتعلق بحقوق المؤلف والحقوق المجاورة، كما نرى أن الفرق بين وضع المصنف المقلد رهن التداول وبين عملية البيع أو التأجير هو تحقق الغرض في الحالتين الأخيرتين، إذ أن عملية عرضه للبيع أو التأجير دون تحقق ذلك يجعلنا أمام الحالة الأولى وهي وضع المصنف المقلد رهن التداول وليس أمام عملية بيع أو تأجير.[1]
- **جريمة تبليغ المصنف الرقمي بأي منظومة معالجة معلوماتية:** تقوم جنحة التقليد المنصوص عليها بالمادة 152 من الأمر 03-05 بمجرد تبليغ المصنف الرقمي بواسطة نظام معالجة المعطيات أي إرسال المعلومات أو تبليغها بواسطة هذا النظام الالكتروني.

ولقد عرف المشرع الجزائري بموجب المادة الثانية من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها المنظومة المعلوماتية على أنها: أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين". [2]

- **جريمة الرفض العمدي لدفع المكافأة المستحقة لمؤلف مصنف قاعدة البيانات:** مفاد هذه الصورة هو استغلال المؤلف لحقه على قاعدة البيانات والتصرف فيها إما بالبيع أو

[1] المادة 151 من الامر المتعلق بحقوق المؤلف والحقوق المجاورة.

[2] الجمهورية الجزائرية الديمقراطية الشعبية ، القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها جريدة رسمية عدد، 47 الصادرة بتاريخ 16 أوت.2009.

الإيجار لشخص آخر هو المستفيد، وذلك بدفع مقابل مادي لهذا للاستغلال من قبل هذا الأخير إذ تتحقق هذه الصورة في، حالة رفض المستفيد دفع المقابل المادي المستحق لمؤلف قاعدة البيانات.

وبالتالي يعتبر المشرع الجزائري استنادا إلى أحكام المادة 155 من الأمر 2005-03 أن كل رفض عمدي لدفع مكافأة مستحقة لمؤلف المصنف صورة من صور جنح التقليد ويعاقب مرتكبها جزائيا.

2-وقوع الفعل المادي للإعتداء على مصنف قاعدة البيانات:

لقيام جنحة التقليد يشترط المشرع الجزائري أن يقع الفعل المجرم أو النشاط الإجرامي على مصنف محمي قانونا، كمصنف قاعدة البيانات كما يشترط أيضا أن يكون هذا المصنف يكتسي الشروط الخاصة لحمايته من أصالة وتجسيد مادي، إضافة إلى إيداعه لدى الجهات المختصة بالإيداع.

إضافة إلى هذه الشروط فإن توفير الحماية الجزائية لقاعدة البيانات مرهون بعدم وجود نزاع قضائي حول ملكية المصنف لم يفصل بعد، فإذا كان النزاع قائما سقطت الحماية إلى غاية الفصل النهائي بموجب حكم حائز لقوة الشيء المقضي فيه.[1]

3-عدم وجود ترخيص أو إذن من المؤلف (عدم موافقة المؤلف):

يعد هذا الشرط أحد عناصر الركن المادي لقيام جريمة التقليد، إذ لا يكفي لقيام جنحة التقليد قيام النشاط الإجرامي في أحد صوره التي سبق الإشارة إليها فقط، بل يجب أن يتم الفعل المادي لجريمة تقليد مصنف قاعدة البيانات بدون وجود ترخيص أو إذن من المؤلف، بحيث أن وجود الاذن يحول دون قيام الركن المادي للجريمة.

[1] عبد الرحمان خلفي، مرجع سبق ذكره ، ص 156

كما يتعين الإشارة إلى أنه يجب أن يكون الإذن أو الترخيص في حدود ما اتفق عليه، إذ أنه حتى في حالة وجود اتفاق على نسخ أحد المصنفات الرقمية يجب أن يلتزم الشخص بحدود النسخ المتفق على نسخها، ولذلك فإن جريمة التقليد تقوم بركنها المادي إذا تم نسخ عدد أكبر من العدد المتفق عليه.

ويتعين الإشارة إلى أن بعض الفقه قد اشترط أن يكون هذا الإذن كتابيا وصريحا أو ضمنيا لا يدع مجالا للشك في اتجاه نية مؤلف المصنف الرقمي بالترخيص لنسخ هذا المصنف.

إلا أنه وبالرجوع إلى الأمر المتعلق بحقوق المؤلّف والحقوق المجاورة نجد أن المشرع الجزائري قد أغفل إدراج نص صريح على وجوب كتابة الترخيص أو الإذن، ولذلك فإننا نرى وجوب تدارك المشرع الجزائري لهذه النقطة وذلك من خلال النص الصريح على أن يكون الترخيص كتابيا أو ضمنيا لا يدع مجالا للشك في قبول نسخ المصنفات الرقمية كشرط لقيام الركن المادي لجريمة التقليد. [1]

الفرع الثالث: الركن المعنوي لجنح تقليد مصنف قاعدة البيانات الرقمية

لقد اكتفى المشرع الجزائري بالإشارة إلى القصد الجنائي عن طريق اشتراطه لضرورة توافر العمد في ارتكاب الجريمة وذلك دون القيام بتعريفه، ولذلك يعرفه الأستاذ عبد الله سليمان على أنه: " العلم بعناصر الجريمة وإرادة ارتكابها.

حيث تعتبر جريمة تقليد مصنف قاعدة البيانات من الجرائم العمدية التي تقتضي توافر القصد الجنائي العام بعنصريه العلم بأن التقليد الذي يقع على مصنف قاعدة بيانات جريمة يعاقب عليها القانون واتجاه الإرادة الجاني إلى القيام بذلك الفعل.[2]

المطلب الثالث: الجزاء الجنائي المقرر لجنح تقليد مصنف قاعدة البيانات الرقمية

[1] عبد الله قيبوعة، مرجع سبق ذكره، ص221-223.
[2] المرجع نفسه ،ص221-223.

يعرف الجزاء الجنائي على أنّه رد الفعل الاجتماعي على انتهاك القاعدة الجنائية، ينص عليه القانون، ويأمر به القضاء، وتطبقه السلطات العامة ويتمثل في إهدار أو إنقاص أو تقييد محيط الحقوق الشخصية للمحكوم عليه المقرر بالقانون للناس كافة بهدف وقاية المجتمع من " الإجرام".[1]

ويمكن تقسيم الجزاء الجنائي الذي نص عليه المشرع الجزائري من خلال الأمر 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة إلى عقوبات جزائية أصلية تتمثل في تقييد حرية الجاني، أو الإنقاص من ذمته المالية (الفرع الاول) وعقوبات تكميلية تتمثل في غلق المؤسسة المستغلة في جنحة تقليد قواعد البيانات والمصادرة ونشر الحكم (الفرع الثاني).

الفرع الاول: العقوبة الأصلية لجنحة تقليد مصنف قاعدة البيانات الرقمية

لقد نص المشرع الجزائري من خلال المادة 04/2 من قانون العقوبات على أن: " العقوبات الأصلية هي تلك التي يجوز الحكم بها دون أن تقترن بها أية عقوبة أخرى " كما ينص بموجب المادة 05 أن: " العقوبات الأصلية في مادة الجنح هي:

- الحبس مدة تتجاوز شهرين إلى خمس سنوات ما عدا الحالات التي يقرر فيها القانون حدودا أخرى.
- الغرامة التي تتجاوز 20.000 دج ".

فالعقوبات الأصلية في مادة الجنح حسب القواعد العامة هي الحبس الذي تفوق الشهرين ولا تتجاوز الخمس سنوات، والغرامة التي تفوق 20.000 دج.

ولذلك فقد نص المشرع الجزائري من خلال المادة 153 من الأمر 03 05 المتعلق بحقوق المؤلّف والحقوق المجاورة على معاقبة كل مرتكب لجريمة من جرائم تقليد المصنفات في إحدى صورها المنصوص عليها في المواد 151 و.152 سواء حصل النشر في الجزائر

[1] عبد الله سليمان، شرح قانون العقوبات الجزائري ، القسم العام، الجزء الثاني الجزاء الجنائي، ديوان المطبوعات الجامعية ،الجزائر،1996، ص ص 406 407

أو في الخارج[1]، إضافة إلى الصورة المنصوص عليها بالمادة 155 من نفس الأمر بالعقوبات التالية:

- **عقوبة الحبس:** إذ يعاقب المشرع الجزائري بالحبس من 06 أشهر إلى 03 سنوات، كل من يقوم بتقليد المصنفات الأدبية والفنية بما فيها مصنف قاعدة البيانات.
- **عقوبة الغرامة:** حيث يعاقب أيضا مقلد المصنف الفكري حسب الحالات المنصوص عليها في المواد 151 و152 أعلاه بغرامة مالية من 500.000 دج إلى 1.000.000 دج.

ويتعين الإشارة إلى أن المشرع الجزائري يعاقب مرتكب جنحة التقليد بالعقوبتين معا استنادا إلى نص المادة 153 من الأمر 03-05، وذلك دون الإخلال بالسلطة التقديرية للقاضي في الحدود التي رسمها له القانون.

- **عقوبة الشريك في جريمة تقليد مصنف قاعدة البيانات:** حيث ينص المشرع الجزائري بموجب أحكام المادة 154 من الأمر 03-05 المتعلق بحقوق المؤلّف والحقوق المجاورة [2]على معاقبة الشريك الذي يشارك بعمله أو بالوسائل التي يحوزها للمساس بحقوق المؤلف عن طريق التقليد وفقا للأحكام المادة 151 من نفس الأمر بنفس العقوبة المقررة لهذه الجنحة أي الحبس من 06 أشهر إلى 03 سنوات، وبغرامة مالية من 500.000 دج إلى 1.000.000 دج.

ويفهم للوهلة الأولى من نص المادة 154 أعلاه أن جرائم المشاركة في جنحة التقليد تتعلق بالصور المذكورة بموجب المادة 151 فقط دون باقي الصور المذكورة في المادة 152 والمادة 155 من هذا الأمر.

[1] المواد 151 و152 من الأمر 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة
[2] المادة 154 من الأمر 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة.

- **عقوبة العود في جريمة تقليد مصنف قاعدة البيانات:** وهي العقوبة التي ينص عليها المشرع من خلال المادة 156 من الأمر 03-05 في حالة العود لارتكاب جنحة التقليد، عن طريق مضاعفتها، ويقصد بذلك مضاعفة عقوبة الحبس وعقوبة الغرامة معا.[1]

الفرع الثاني: العقوبات التكميلية لجنح تقليد مصنف قاعدة البيانات

عرف المشرع الجزائري العقوبات التكميلية من خلال المادة 04/3 من قانون العقوبات على أنها تلك التي لا يجوز الحكم بها مستقلة عن عقوبة أصلية، فيما عدا الحالات التي ينص عليها القانون، صراحة وهي إما إجبارية أو اختيارية ".

ويتعين الإشارة إلى أنّ العقوبات التكميلية في جرائم تقليد مصنف قاعدة البيانات تشمل حسب ما جاءت به أحكام المادة 156/2، والمادة 157 والمادة 158 من الأمر 08-2005 المتعلق بحقوق المؤلف والحقوق المجاورة غلق المؤسسة التي يباشر فيها تقليد المصنف المحمي، إضافة إلى مصادرة العتاد والمبالغ المكتسبة من عملية التقليد، إلى جانب نشر الحكم القاضي بالإدانة بجنحة التقليد.[2]

1-**غلق المؤسسة محل جنحة تقليد مصنف قاعدة البيانات:** لقد نص المشرع الجزائري على هذه العقوبة التكميلية من خلال المادة 156/2 من الأمر 03-05،حيث يخوّل المشرع الجزائري وبصفة جوازية للجهة القضائية المختصة أن تقرر غلق المؤسسة المستغلة في تقليد المصنفات وذلك بصفة مؤقتة لا تتجاوز 06 أشهر أو بصفة نهائية عند الاقتضاء من قبل الجهة القضائية المختصة.

2-**مصادرة العتاد والمبالغ المكتسبة من عملية تقليد مصنف قاعدة البيانات:**

تنص المادة 157 من الامر 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة على أنّه: " تقرر الجهة القضائية المختصة:

[1] المادة 156 من الأمر 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة.
[2] المادة 156/2، والمادة 157 والمادة 158 من الأمر 08-2005 المتعلق بحقوق المؤلف والحقوق المجاورة.

- مصادرة المبالغ التي تساوي مبلغ الإيرادات أو أقساط الإيرادات الناتجة عن الاستغلال غير الشرعي لمصنف أو أداء محمي.
- مصادرة وإتلاف كل عتاد أنشئ خصيصا لمباشرة النشاط غير المشروع وكل النسخ المقلدة.

كما نصت المادة 159 من نفس الأمر على أنه: " تأمر الجهة القضائية و152 من المختصة في جميع الحالات المنصوص عليها في المادتين 151 هذا الأمر، بتسليم العتاد أو النسخ المقلدة أو قيمة ذلك كله وكذلك الإيرادات أو أقساط الإيرادات موضوع المصادرة للمؤلف أو لأي مالك حقوق آخر أو ذوي حقوقهما لتكون عند الحاجة بمثابة تعويض عن الضرر اللاحق بهم.[1]

إذ يتضح من نص المادتين أعلاه أن المشرع الجزائري قد أخذ بإلزامية الحكم بمصادرة المبالغ المالية الناتجة عن الاستغلال الغير شرعي للمصنف الفكري، إضافة إلى القضاء بمصادرة وإتلاف العتاد المستعمل في جريمة التقليد، كما نص في نفس السياق على ضرورة الحكم بتسليم الإيرادات والعتاد والنسخ محل المصادرة للمؤلف أو مالك الحقوق أو ذويه كتعويض عن الضرر اللاحق بهم، وهي عقوبات تكميلية يحكم بها القاضي بصفة إلزامية حسب ما يفهم من نص المواد أعلاه.

3-**نشر الحكم القاضي بالإدانة بجنحة تقليد مصنف قاعدة البيانات:** وهو إبلاغ العامة بالجرم المرتكب في حق المؤلف على مصنفه الفكري، إذ يهدف هذا الإبلاغ أساسا إلى تنبيه العامة بهذه المصنفات المقلدة حتى لا يكون هناك حجة على التعامل بها.

حيث تنص المادة 158 من الأمر 08-05 على أنه: " يمكن للجهة القضائية المختصة بطلب من الطرف المدني، أن تأمر بنشر أحكام الإدانة كاملة أو مجزأة في الصحف التي تعينها وتعليق هذه الأحكام في الأماكن التي تحددها ومن ضمن ذلك على

[1] المادة 159 والمادة 151 و152 من الأمر 08-2005 المتعلق بحقوق المؤلف والحقوق المجاورة.

باب مسكن المحكوم عليه وكل مؤسسة أو قاعة حفلات يملكها على أن يكون ذلك على نفقة هذا الأخير شريطة أن لا تتعدى هذه المصاريف الغرامة المحكوم بها ".

يتضح من خلال هذه المادة أن أحكام النشر هي الأمور الجوازية التي تخضع للسلطة التقديرية لقاضي الحكم بناءا على طلب الطرف المدني، إلا أننا نرى أن نشر أحكام الإدانة من الأحكام التي يجب النص عليها بصفة إجبارية تفاديا لأي تحجج بالتعامل بالمصنفات المقلدة على أساس عدم العلم بذلك.[1]

[1] عبد الله قيبوعة، مرجع سبق ذكره، ص227

خلاصة واستنتاجات:

في عصر الرقمنة المتسارع، أصبحت حماية البيانات الرقمية أمراً بالغ الأهمية لضمان أمن المعلومات والحفاظ على الخصوصية.

الجزائر، مثل العديد من الدول الأخرى، تواجه تحديات كبيرة في مجال الأمن السيبراني نتيجة لتزايد الهجمات الإلكترونية والجرائم السيبرانية. تتطلب مواجهة هذه التحديات جهوداً مشتركة من الحكومة، القطاع الخاص، والمواطنين لتعزيز الأمن السيبراني وحماية البيانات الرقمية بفعالية.

وبناءً على ما سبق ، يمكن الوصول إلى الاستنتاجات التالية:

1- تواجه الجزائر تزايداً في التهديدات السيبرانية التي تستهدف البيانات الرقمية، مما يتطلب استجابة شاملة وفعالة لحماية هذه البيانات.
2- الحكومة الجزائرية تعمل على تطوير سياسات واستراتيجيات لتعزيز الأمن السيبراني، بما في ذلك تحديث التشريعات وتأسيس هيئات تنظيمية لمتابعة تنفيذها.
3- هناك حاجة ماسة لتعزيز الوعي بأهمية حماية البيانات الرقمية وتوفير برامج تدريبية للأفراد والعاملين في المؤسسات لمواجهة التهديدات السيبرانية بفعالية.
4- تحسين البنية التحتية التكنولوجية واعتماد تقنيات متقدمة للكشف عن الهجمات والاستجابة لها يعدان من الركائز الأساسية لحماية البيانات الرقمية.
5- تعزيز التعاون بين القطاعين العام والخاص داخل الجزائر، والتعاون مع المنظمات الدولية، يساهم في بناء دفاعات أقوى ضد التهديدات السيبرانية.
6- وجود خطط استجابة سريعة وفعالة للحوادث السيبرانية ضروري لتقليل الأضرار الناجمة عن الاختراقات والهجمات الإلكترونية.

فحماية البيانات الرقمية في الجزائر تتطلب مقاربة شاملة تتضمن تحسين التشريعات، تعزيز الوعي والتدريب، تطوير البنية التحتية التكنولوجية، وتشجيع التعاون المحلي والدولي،

والاستثمار في تكنولوجيا الأمن السيبراني. العلاقة الوثيقة بين حماية البيانات الرقمية والأمن السيبراني تفرض تبني استراتيجيات متكاملة لضمان بيئة رقمية آمنة وموثوقة، مما يساهم في حماية حقوق الأفراد والمؤسسات ويعزز الثقة في التحول الرقمي والتنمية المستدامة. من خلال هذه الجهود المتكاملة، يمكن للجزائر تعزيز موقعها في العالم الرقمي وضمان مستقبل آمن ومزدهر لمواطنيها.

وبالتالي فإن واقع حماية البيانات الرقمية في الجزائر يكشف عن تحديات كبيرة تتطلب استجابة شاملة ومستمرة. تحسين التشريعات، تعزيز الوعي والتدريب، تطوير البنية التحتية التكنولوجية، وتشجيع التعاون المحلي والدولي، والاستثمار في تقنيات الأمن السيبراني الحديثة هي خطوات أساسية لضمان حماية البيانات الرقمية وتعزيز الأمن السيبراني في البلاد. من خلال هذه الجهود، يمكن للجزائر بناء بيئة رقمية آمنة تدعم التنمية المستدامة وتحمي حقوق الأفراد والمؤسسات في العصر الرقمي.

خاتمة

في ختام هذه الدراسة يمكن القول أن الأمن السيبراني وحماية البيانات الرقمية في الجزائر يتطلبان جهداً مشتركاً من الحكومة و القطاع الخاص و المجتمع بأسره ، فتعزيز التشريعات و التوعية و التعاون المحلي و الدولي والاستثمار في التكنولوجيا هي خطوات أساسية لضمان بيئة رقمية آمنة ومستدامة ، من خلال هذه الجهود المتكاملة ، يمكن للجزائر أن تحقق مستوى عالياً من الأمن السيبراني ، مما يساهم في حماية حقوق الأفراد والمؤسسات ، و تعزيز الثقة في البنية التحتية الرقمية الوطنية ، ودفع عجلة التنمية المستدامة.

وبالتالي من الضروري توعية الأفراد بضرورة دراسة هذا المجال لأنه من أهم المجالات التي يجب أن نعطيها اتهتماما كبيرا من أجل حماية وسلامة البيانات الرقمية والحفاظ على مختلف الأجهزة التي تمس أمن البلاد و المواطنين .

واستنادا الى ما سبق يجب العمل لإيجاد آليات وسبل لتحقيق الأمن السيبراني ونقترح ما يلي:

- تكوين نخب وطنية مختصة بمجال الأمن السيبراني، وتكثيف الملتقيات الوطنية والدولية والتي من شأنها الاستفادة من تجارب الدولية وخبراتهم في مكافحة التهديدات السيبرانية.
- بناء قواعد قانونية تتناسب مع كل حالة من التهديدات السيبرانية، وتفعيلها على أرض الواقع وتطبيقها بصرامة حتى لا يفلت المنتهك من العقاب.
- بناء منظومة الكترونية دقيقة ومتطورة لمنع الهجمات الالكترونية التي تستهدف مفاصل الدولة المختلفة لاسيما المتعلقة بالأمن الوطني العسكرية منها والمدنية كالنشاط المصرفي والمالي والمؤسسات الأخرى.

مسايرة التطور التكنولوجي بتجديد التقنيات وامتلاك كل الأسلحة الالكترونية والتي من شأنها رصد التهديدات السيبرانية قبل وقوعها ومراقبة المنتهكين والمهددين لأمن الأفراد والمؤسسات والأمن القومي.

تحقيق الأمن الاكلتروني بتطلب ضرورة نشر الوعي المجتمعي بخطورة الجريمة الالكترونية وتشجيع التكوين العلمي والجامعي المتخصص في دراستها.

قائمة المراجع

أولا: قائمة المصادر

أ- نصوص تشريعية:

1. القانون رقم 131 لسنة 1948 المتضمن إصدار القانون المدني، المعدل بتاريخ 16 جويلية 2011
2. القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها جريدة رسمية عدد، 47 الصادرة بتاريخ 16 أوت 2009.
3. الأمر رقم: 75/58 المؤرخ في 26 سبتمبر 1975 والمتضمن القانون المدني، المعدل والمتمم الصادر في الجريدة الرسمية بتاريخ 30 أكتوبر 1975، العدد 81
4. الأمر رقم: 66-156 المؤرخ في 08/06/1966 المتضمن قانون العقوبات المعدل والمتمم.
5. الأمر 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة

ثانيا: قائمة المراجع:

أ- الكتب:

1-حواس فتيحة، حماية المصنفات الرقمية وأسماء النطاقات على شبكة الانترنت، مكتبة الوفاء القانونية، الطبعة الأولى، الإسكندرية 2017.

2-الرازي محمد عطية علي محمد، الحماية القانونية لقواعد البيانات في القانون المصري والتشريعات المقارنة، دار الجامعة الجديدة للنشر (بدون طبعة) الإسكندرية، 2013.

3-السعدي محمد صبري، الواضح في شرح القانون المدني الجزائري النظرية العامة للإلتزامات، مصادر الالتزام العقد والإرادة المنفردة، الجزء الأول، دار الهدى، الطبعة الرابعة الجزائر، 2006-2007.

4-سليمان عبد الله، شرح قانون العقوبات الجزائري القسم العام، الجزء الأول، الجريمة ديوان المطبوعات الجامعية بدون طبعة الجزائر، 1996.

5-السنهوري عبد الرزاق أحمد، الوسيط في شرح القانون المدني الجديد نظرية الالتزام بوجه عام الجزء الأول، مصادر الالتزام دار أحياء التراث العربي، بدون طبعة، بيروت، لبنان، 1952.

6-علي زياد علي، الصراع والأمن الجيوسيبراني في الساحة الدولية: دراسة في استراتيجيات الاشتباك الرقمي، دار أمجد للنشر والتوزيع، عمان، 2020.

7-فكري أيمن عبد الله، الجرائم المعلوماتية (دراسة مقارنة في التشريعات العربية والأجنبية مكتبة القانون والاقتصاد، الطبعة الأولى، الرياض، 2014.

8-مازوني كوثر، الشبكة الرقمية وعلاقتها بالملكية الفكرية، دار هومة للنشر (بدون طبعة) الجزائر 2008.

9-منصور شادي عبد الوهاب، حروب الجيل الخامس: أساليب " التفجير من الداخل " على الساحة الدولية، العربي للنشر والتوزيع، القاهرة، 2019.

ب- الاطروحات والرسائل (اطروحات الدكتوراه ثم رسائل الماجستير ثم الماستر)

❖ **أطروحات الدكتوراه:**

1-بن دريس حليمة، حماية حقوق الملكية الفكرية في التشريع الجزائري، أطروحة دكتوراه في القانون الخاص كلية الحقوق والعلوم السياسية جامعة تلمسان، 2013-2014.

2-دعاس كمال، حق المؤلف في ميدان المصنفات الرقمية أطروحة دكتوراه في القانون، كلية الحقوق سعيد حمدين جامعة الجزائر 1، 2018.

3-قيبوعة عبد الله، الاليات القانونية لحماية قواعد البيانات في ظل البيئة الرقمية -دراسة مقارنة-، أطروحة مقدمة لنيل شهادة دكتوراه الطور الثالث في الحقوق، تخصص القانون الخاص المعمق، كلية الحقوق والعلوم السياسية، الجامعة الافريقية أحمد دراية أدرار، 2022.

4-محاسنة محمد سلطان ماجد على، تكنولوجيا قواعد البيانات وأثرها في اختيار الاستراتيجية التنافسية لشركات الدواء الأردنية أطروحة دكتوراه فلسفة في الإدارة كلية الدراسات الإدارية والمالية العليا جامعة عمان العربية للدراسات العليا، 2007.

❖ **رسائل ماجيستير:**

5-سمية بومعزة، حقوق المؤلف في النطاقين التقليدي والرقمي في ظل التشريع الجزائري. مذكرة ماجستير في الحقوق كلية الحقوق والعلوم السياسية، جامعة باتنة 1، 2015-2016.

6-ميلود صغيري، دور قواعد بيانات النظام الوطني للتوثيق على الخط S.N.D.L بالمكتبات الجامعية في دعم وتطوير البحث العلمي (دراسة ميدانية بجامعة المسيلة) مذكرة ماجستير في علم المكتبات والعلوم الوثائقية، كلية العلوم الإنسانية والحضارة الإسلامية جامعة أحمد بن بلة، وهران، 2014 2015.

ث- **المقالات:**

1-الإمام أحمد محمد، الملكية الفكرية لقواعد البيانات في القانون السوري والمقارن، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية المجلد، 29، العدد الثاني 2013.

2-آيت مهدي ايمان، نظم إدارة قواعد البيانات العلائقية ودورها في تشغيل نظم مساندة القرار، مجلة شعاع للدراسات الاقتصادية المجلد الثالث العدد الأول، مارس 2019.

3-بارة سمير، الأمن السيبراني في الجزائر، السياسات والمؤسسات، المجلة الجزائرية للأمن الإنساني، العدد 04، جامعة قاصدي مرباح، ورقلة.

4-بكراوي محمد المهدي وجامعي مليكة، المسؤولية التقصيرية مداخلة ملقاة بمناسبة اليوم الدراسي بعنوان: الإتجاهات الحديثة في نظرية المسؤولية المدنية كلية الحقوق والعلوم السياسية، جامعة أدرار، يوم 23 ماي 2013.

5-بن برغوث ليلى، الأمن السيبراني وحماية خصوصية البيانات الرقمية في الجزائر في عصر التحول الرقمي والذكاء الاصطناعي، التهديدات، التقنيات، التحديات وآليات التصدي، المجلة الدولية للاتصال الاجتماعي، المجلد 10، العدد 01، جامعة عبد الحميد بن باديس، مستغانم، 2023.

6-بن عزوز حاتم، مناني حليمة، الأمن السيبراني والجريمة الالكترونية في الدول مابعد الحداثية: الولايات المتحدة الامريكية -نموذجا-، مجلة الرسالة للدراسات الإعلامية، المجلد 6، العدد 2، الجزائر، 2022.

7-بوغرارة يوسف، الأمن السيبراني: الاستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبراني، مجلة الدراسات الافريقية وحوض النيل، المركز الديمقراطي العربي، المجلد 1، العدد 3، جامعة مستغانم، الجزائر، 2018.

8-خيلية وريدة، إشكالية المواطنة في ظل قيم التكنولوجيا الحديثة بين حرية المواطن والأمن السيبراني، حوليات جامعة الجزائر 1، المجلد 35، العدد 02، 2021.

9-دلالي جيلالي، يعقوب بلبشير، رهانات الأمن السيبراني الوطني في ظل التحول الرقمي، قراءة في التأصيل المعرفي واستراتيجية المواجهة التشريعية، مجلة كلية القانون الكويتية العالمية، السنة العاشرة، العدد 1، جامعة حسيبة بن بوعلي، الشلف، الجزائر، 2021.

10- السمحان منى عبد الله، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية، العدد 111، جامعة المنصورة، المملكة العربية السعودية، 2020.

11- شريط نجمة، الامن السيبراني في العقيدة الدفاعية الجزائرية: الفرص والقيود، المجلة الجزائرية للسياسة والأمن، المجلد 2، العدد 2، جامعة وهران 2، الجزائر، 2023.

12- شعران فاطمة، حماية المصنفات الرقمية في التشريع الجزائري والتشريعات المقارنة مجلة الدراسات القانونية المقارنة، جامعة حسيبة بن بوعلي الشلف المجلد 02، العدد 02 ديسمبر 2016.

13- عبد العظيم أميرة، محمد عبد الجواد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، العدد 35، الجزء3، القاهرة، 2020.

14- قدايفة أمينة، استراتيجية أمن المعلومات، مجلة أبعاد اقتصادية، المجلد 6، العدد1، 2016.

15- كلاع شريفة، الأمن السيبراني وتحديات الجوسسة والاختراقات الالكترونية للدول عبر الفضاء السيبراني، مجلة الحقوق والعلوم الإنسانية، المجلد 15، العدد 01، جامعة الجزائر 3، 2022.

16- مختار محمد، "هل يمكن أن تتجنب الدول مخاطر الهجمات الالكترونية؟"، مجلة اتجاهات الاحداث، العدد 6، 2015

فهرس

المحتويات

فهرس المحتويات:

الملخص:

لقد أصبح موضوع الأمن السيبراني من المواضيع الهامة على المستوى الحكومي والفردي ، نظرا لاعتباره ركن أساسي في منظومة الأمن الحديث و المعاصر، و الجزائر كغيرها من الدّول تسعى جاهدة الى البحث و اللجوء الى معايير واجراءات لتحقيق الأمن السيبراني وحماية الأنظمة والبيانات الرقمية والتي اعتمدت على تطوير الإستراتيجيات الأمنية من خلال وضع خطط لتعزيز الأمن السيبراني وحماية الأنظمة الحيوية و الحساسة
و التعاون مع الجهات الدولية لتبادل المعلومات والخبرات في مجال الأمن السيبراني و تطوير البنية التحتية الرقمية، تعتبر الاستثمارات في الأمن السيبراني جزءا أساسيا من استراتيجية الدولة الجزائرية للحفاظ على سلامة البيانات والحد من التهديدات الإلكترونية حتى تتمكن الجزائر من تعزيز قدراتها على التصدي للتهديدات السيبرانية لضمان بيئة رقمية آمنة.

كلمات مفتاحية: الأمن السيبراني، حماية البيانات الرقمية، التهديدات السيبرانية (الالكترونية).

Abstract:

The issue of cybersecurity has become an important topic at the governmental and individual levels, given that it is considered a fundamental pillar of the modern and contemporary security system. Algeria, like other countries, is striving to research and resort to standards and procedures to achieve cybersecurity and protect digital systems and data, which has relied on developing strategies. Security by developing plans to enhance cybersecurity, protect vital and sensitive systems, and cooperate with international bodies to exchange information and expertise in the field of cybersecurity and develop digital infrastructure. Investments in cybersecurity are considered an essential part of the Algerian state’s strategy to maintain data integrity and reduce cyberthreats until... Algeria can strengthen its capabilities to confront cyber threats to ensure a secure digital environment.

Keywords: Cyber security, digital data protection, cyber threats.