Cybersecurity under Algerian legislation

Surya Nawaser
Faculty of Law and Political Science, Badji Mokhtar University - Algeria-

DOI: https://doi.org/10.31918/twejer.eli24.03
Published: 13/10/2024

Abstract

Technological development has brought about many transformations in various societies, including in the media; Different technologies are widely accepted by different age groups, which results in the birth of an illegitimate child; It is a cybercrime born from the womb of the illegal use of Internet networks.

Cybercrime has become a threat to natural and legal persons, it even threatens the internal security and economies of countries, which has required strengthening cyber security through legal mechanisms, first and foremost legislation.

According to these circumstances, countries have begun to include laws in their legislation that dedicate the prevention and control of cybercrime to the achievement of cyber security, which is one of the measures aimed at reducing security breaches, including Algerian legislation.

Keywords: *Security - Cyber - Legislation – Algerian.*

الأمن السيبراني في ظل التشريع الجزائري

أ. صورية نواصر
مكان العمل: كلية الحقوق والعلوم السياسية جامعة باجي مختار – الجزائر-
البريد الإلكتروني: nouacersoraya@yahoo.fr

الملخص:
أفرز التطور التكنلوجي و الرقمي العديد من التحولات في مختلف المجتمعات فشهدت الوسائط التكنلوجية المختلفة إقبالا غير معهود من مختلف الفئات العمرية، مما أسفر عنه إنجاب طفلا غير شرعي وهو الجريمة السيبرانية التي ولدت من رحم الاستعمال الغير مشروع لشبكات الإنترنيت.

لقد أضحت الجريمة السيبرانية تهدد الأشخاص الطبيعية و المعنوية، بل وتهدد أيضا الأمن الداخلي واقتصاديات الدول، مما أضحى لا مناص من تعزيز الأمن السيبراني بشتى الآليات القانونية وفي طليعتها التشريع.

من هذا المنطلق عكفت الدول على تضمين تشريعاتها قوانين تكرس الوقاية من الجريمة السيبرانية و مكافحتها بغية منها لتحقيق الأمن السيبراني الذي يعد من الإجراءات الهادفة للحد من الثغرات و الخروقات الأمنية مهما كان نوعها و من بينها التشريع الجزائري.

الكلمات المفتاحية : أمن – سيبراني- تشريع – جزائري

1. مقدمة

إن لكل تطور علمي وجها إيجابيا و آخر سلبيا و كذلك الشأن بالنسبة للتطور الذي شهده عالم الرقمنة فبفضل جانبها الإيجابي، تنوعت الخدمات و تيسرت الاتصالات و أصبحت في متناول الأشخاص الطبيعية والمعنوية، كما تيسرت المعاملات التجارية و المالية.

غير أن هذا التطور عرف تداعيات خطيرة وذلك على إثر الإقبال الواسع على البيئة الافتراضية والاستخدام الغير المحدود للوسائل الإلكترونية ، مما جعلها بؤرة من بؤر الجريمة المستحدثة ذات الصلة بالحاسب الآلي و الأنترنيت.

إن هذه الجرائم العابرة للحدود كشفت عن الجانب السلبي للتطور الرقمي و هذا ما يطلق عليه بالجرائم السيبرانية (cyber crime) التي أضحت تنخر في الاقتصاد الوطني فضلا عن الجانب الاجتماعي و الأمني .

و لعل أبرز ملامحها تلك الجرائم المرتكبة ضد المستهلك و النصب و الاحتيالي و تلك الماسة بالملكية الفكرية سواء الأدبية منها أو الصناعية و التجارية، وكذا الجرائم الماسة بالحياة الخاصة للأفراد و سرقة وتحويل الأموال و جرائم إعادة توجيه الخدمات المصرفية عبر الإنترانت بطرق احتيالية، وغيرها من الجرائم التي ينجر عنها خسائر مالية ضخمة.

إن هذا الاجرام الذي بات أبجدية من أبجديات التطور التكنلوجي لم تعد مختلف الدول بمنأى عنه، مما أصبح لا مناص من التصدي له و ذلك باستحداث تشريعات تضبط قواعد الاستخدام المشروع لهذه التكنلوجيا ، و إنشاء هيئات تسهر على تحقيق الأمن السيبراني ، وهذا ما عكف عليه المشرع الجزائري من خلال سنه لترسانة قانونية يصبو من خلالها تحقيق أمن سيبراني مستدام.

من هذا المنطلق فالإشكالية المطروحة على هذا المستوى تكمن في ما مدى نجاعة التشريع الجزائري في تحقيق الأمن السيبراني؟ و تنبثق عن هاته الإشكالية التساؤلات التالية :
- ما هو مفهوم الأمن السيبراني و ماهي المفاهيم المرتبطة به ؟
- ماهي أنواع الأمن السيبراني و أهدافه و أبعاده ؟
-ماهي التشريعات و الهيئات التي رصدها المشرع الجزائري لتحقيق الأمن السيبراني

و لتحليل موضوع الدراسة اعتمدنا على المنهجين الوصفي والتحليلي ، فاستندنا على الأول عند التطرق للمفاهيم و لعرض مختلف القوانين التي سنها المشرع الجزائري أما الثاني فكان لتحليل بعض النصوص القانونية للوقوف على فحواها وتوضيح الهدف الذي توخاه المشرع من سنها.

و للإجابة على الاشكالية المطروحة قسمنا هذه الورقة البحثية لثلاثة مطالب رئيسية سنتعرض إليها تبعا .

1. ماهية الأمن السيبراني

تعد الجريمة السيبرانية من الجرائم المستحدثة التي أفرزتها التكنلوجيا و الرقمنة و يسرها الإقبال المطرد على هذه التقنيات و القدرة على التحكم بها، فظهرت العديد من الجرائم الماسة بأمن الأشخاص و أمن الشركات و المؤسسات الاقتصادية، بل تعدى الأمر لأخطر من ذلك إذ أصبحت هذه الجرائم تمس بأمن الدول و اقتصادها الوطني .

إن هذه الجرائم التي عمادها تكنلوجيا الإعلام و الاتصال و تقنياته عرفت تنوعا بحسب محل الجريمة و أطرافها و اتساع نطاقها الذي يمتد خارج إقليم الدولة الواحدة، فخرجت بذلك عن تلك الجرائم المعهودة في الإجرام التقليدي.

بناء على ما تقدم أصبح تأمين الحاسوب أمرا حتميا و ذلك عن طريق تأمين المعلومات و البرامج ضد الهجمات الإلكترونية و غيرها من الاختراقات للأنظمة المعلوماتية، و هذا يمثل تحديا كبيرا يفرضه الواقع لوجود تسارع في الابتكارات التكنلوجية والتقنية ، التي من خلالها أصبح الجناة أسبق من التشريع بخطوة .

فضلا عن ما تقدم فإن التوجه السائد اليوم نحو الحكومة الإلكترونية، جعل العمل على تحقيق أمن سيبراني هو الحل الأمثل لحماية المؤسسات و مختلف الهيئات الحيوية في الدولة ، وهذا ما يؤدي للقول بأن الأمن السيبراني و الجريمة السيبرانية مرتبطان ترابطا طرديا.

وعليه و قبل الخوض في الموضوع لا بد من التطرق للمقصود من الأمن السيبراني و الجريمة السيبرانية و بعض المفاهيم المرتبطة به مع تحديد أهدافه وأبعاده وهذا ما سنتناوله بالتفصيل التالي:

1.2. مفهوم الأمن السيبراني

حضي مفهوم الآمن السيبراني باهتمام واسع وذلك بالنظر لأهميته فاختلفت **الرؤى** حول تحديد المقصود منه و ذلك لإختلاف الأسس المعتمد عليها في تعريفه، لذا سنقتصر على البعض منها و هذا ما سنبينها.

أولا: تعريف الأمن السيبراني بالنظر لأهدافه

اتخذ هذا الإتجاه من أهداف الأمن السيبراني تعريفا له فاعتبره نشاط يؤمن جملة من الموارد أهمها البشرية والمالية المرتبطة بتقنيات الاتصال والمعلومات، مما يجعله يحد من الأضرار و الخسائر الناجمة عن الجريمة السيبرانية مع العمل على اصلاح الخلل بحيث لا يؤدي ذلك للتوقف عن العمل أو الإنتاج. [1] (بارة ، 2017، ص 257)

ثانيا: التعريف التقني للأمن السيبراني

اعتبر فريق آخر من الفقه أن الأمن السيبراني يتحدد مدلوله من خلال الوسائل المستعملة لتحقيقه فذهب بالقول بأنه: " مجموعة من الوسائل التقنية و التكنلوجية و العمليات التي يتم استخدامها لحماية الشبكات و الأجهزة و البرامج و البيانات من الهجمات و التسلل الغير مسموح به ، و يعرف أيضا بأنه أمن تكنلوجيا المعلومات ." [2] (شويرب ; مراد 2023، ص 165)

ثالثا : تعريف الاتحاد الدولي للاتصالات و وزارة الدفاع الأمريكية

عرف الاتحاد الدولي للاتصالات الأمن السيبراني في تقريره الصادر بشأن الإصلاح في مجال الاتصالات سنة 2010-2011 بأنه :"مجموعة من المهمات مثل تجميع وسائل و سياسات و إجراءات أمنية و مبادئ توجيهية و مقاربات لإدارة المخاطر، و تدريبات و ممارسات فضلى و تقنيات يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين."

في حين اعتبرته وزارة الدفاع الأمريكية " جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية و الإلكترونية، من مختلف الجرائم : الهجمات ، التخريب ، التجسس و الحوادث. " [3] (السمحان ، 2010 ص 10)

2.2. المفاهيم المرتبطة بالأمن السيبراني

نظرا لارتباط الآمن السيبراني بجملة من المفاهيم كان لزاما علينا التعرض لها ويتعلق الأمر بالفضاء السيبراني و الجريمة السيبرانية و أمن المعلومات .

أولا : الفضاء السيبراني

عرف الفضاء السيبراني تعريفا تقنيا من طرف الوكالة الفرنسية لأمن أنظمة الإعلام على أنه: "فضاء التواصل المشكل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية ."

وقد عرفه الاتحاد الدولي للاتصالات بأنه " المجال المادي و الغير مادي الذي يتكون و ينتج عن عناصر هي: أجهزة الكمبيوتر ، الشبكات ،البرمجيات ، حوسبة المعلومات ، المحتوى ،معطيات النقل و التحكم ، و مستخدموا كل هذه العناصر ."[4] (زروقة 2019، ص 1017)

ثانيا : الجريمة السيبرانية

اختلف الفقه حول تحديد مدلول الجريمة السيبرانية و مرد ذلك حداثة المصطلح فتعددت المذاهب بشأنها نذكر منها: المادي ، التقني و القانوني وغيرها.

لقد ذهب الإتجاه المادي للقول بأن الجريمة السيبرانية تتمثل في كل سلوك غير قانوني يستخدم فيه أجهزة إلكترونية، يجني منها المجرم فوائد مادية أو معنوية مع تحميل الضحية خسارة مقابلة وغالبا ما يكون هدف الجاني هو القرصنة.[5] (بوضياف ، 2018،ص351)

أما الإتجاه التقني فقد عرفها بأنها كل عمل ضار يفترض فيه المعرفة الجيدة للتكنلوجيا من طرف الفاعل، و توظيف تقنيات الحاسوب للوصول إلى البيانات و البرامج من أجل الحذف ،النسخ ، التخريب، الحيازة أو التوزيع بصورة غير شرعية.[6] (بوازدية ،2019 ،ص 1268)

في حين اعتبرها الإتجاه الموضوعي بأنها " نشاط اجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود."[7] (الصحفي 2020،ص8)

و بالرجوع للتعريف التشريعي نجد أن المشرع عند تعديله لقانون العقوبات سنة 2004 بموجب القانون رقم 04-15 أطلق على الجرائم السيبرانية تسمية : الجرائم الماسة بأنظمة المعالجة الألية للمعطيات و ذلك وفقا لما ورد في القسم السابع مكرر منه، و تجدر الإشارة إلى أن المشرع الجزائري تبني في تعريفه للجريمة السيبرانية لما هو وارد بالاتفاقية الدولية للإجرام المعلوماتي .
وعند إصداره لقانون 09-04 اعتمد تسمية الجرائم المتصلة بتكنلوجيا الإعلام والاتصال و ذلك طبقا للمادة الثانية منه ".[8] (قانون 09-04،2009، ص 05)

و تنقسم الجريمة السيبرانية إلى نوعين: "الأول : موجه ضد جهاز الحاسوب أو أنظمة تقنية المعلومات و الاتصالات الأخرى بقصد إتلافها، أو تدميرها أو تعطيلها، و النوع الثاني: يشمل الجرائم التي يكون فيها الحاسب الآلي وسيلة إرتكاب جرائم الإحتيال وسرقة الهويات وبطاقات الائتمان والأرصدة المالية و التزوير و الإختلاس، وسرقة حقوق الملكية الفكرية."[9] (لعلوم الشرطة، 2016، ص9)

ثالثا : أمن المعلومات

يقصد بالأمن المعلوماتي أكاديميا "العلم الذي يبحث في نظريات و استراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها. ومن زاوية تقنية هو الوسائل و الأدوات و الإجراءات لضمان حماية المعلومات من الأخطار الداخلية و الخارجية، و من زاوية قانونية فإن أمن المعلومات هو محل دراسات و تدابير حماية سرية و سلامة محتوى توفر المعلومات ومكافحة أنشطة الاعتداء أو استغلال نظمها في ارتكاب الجريمة."[10](مريزق ، بوقلاشي، 2010، ص 8 و9)

وعرفت وكالة الأمن القومي في الولايات المتحدة في إحدى توصياتها أمن أنظمة المعلومات و الاتصالات بانها "حماية أنظمة المعلومات ضد أي وصول غير مرخص أو تعديل المعلومات أثناء حفظها ، معالجتها أو نقلها ، وضد إيقاف عمل الخدمة لصالح المستخدمين المخولين أو تقديم الخدمة لأشخاص غير مخولين، بما في ذلك جميع الإجراءات الضرورية لكشف ، توثيق و مواجهة هذه التهديدات ." [11] (الحديدي، 2022، ص 14) و يتميز أمن أنظمة المعلومات بخمسة خصائص و هي: السرية، التحقق من الهوية، الكمال، مكافحة الإنكار و التوفر.

3.2. أنواع الأمن السيبراني

لما كان الأمن السيبراني يصبو إلى مواجهة التحديات في المحال السيبراني عن طريق رفع القدرة و الكفاءة و الاحترافية المهنية، لإدارة المخاطر الإلكترونية في ظل عصر التحول الرقمي أين أصبحت كل القطاعات في الدولة سواء العامة منها أو الخاصة، فضلا عن الأشخاص و حاجتهم الملحة لتأمين معلوماتهم الشخصية فإن الأمن السيبراني أصبح أكثر من ضرورة ، وذلك بالنظر لازدياد المخاطر السيبرانية التي باتت الشبح الإلكتروني الذى يهدد المصالح الحيوية في عالم اتسم بالتطور التكنلوجي المستمر، لذا تعددت أنواعه سنتناولها في ما يلي :

أولا: أمن الشبكات

يتعلق أمن الشبكات بصفة أساسية بحماية جهاز الحاسوب فهو جزء فرعي من أمن المعلومات ، يهدف لحماية البنية التحتية للشبكة و ذلك من خلال تأمين الحماية اللازمة لكل المصادر و الموارد التي يمكن الوصول إليها عبر الشبكة عن طريق التهديدات كالفيروسات و برامج التجسس و غيرها، و يتكون أمن الشبكة من ثلاثة أنواع وهي مادية ، تقنية و إدارية . [12] (روبدين ، 2022) .

ثانيا: أمن البيانات

أمن البيانات هو عبارة عن عملية تصميم و نشر أدوات لحماية معلومات الأعمال الهامة من التدمير ، التعديل ، التعطيل و يستخدم لحماية المستخدمين المعتمدين أو التطبيقات أو الأنظمة من الوصول العمدي و العرضي الغير مرخص به. [13] (للتعلم ، 2023)

ثالثا : الأمن السحابي و أمان أنترنيت الأشياء

لما بات العالم اليوم يعتمد على الذكاء الاصطناعي بصورة كبيرة أصبح من اللازم حماية و تأمين السحابة الرقمية، و مرد ذلك هو احتواؤها على كمية هائلة من البيانات، و هناك شركات متخصصة في هذا المجال مثال: Microsoft Azureg و Google Cloud [14](بزنس ، 2023)

و بالنسبة لأمان أنترنيت الأشياء فهي ثورة تكنلوجية قائمة بحد ذاتها فمن خلال شبكة الأمان ، يقوم أمن أنترنيت الأشياء بتوفير أجهزة هامة من أجل تنزيل التحديثات بالنسبة للمستخدمين الذين يمتلكون أجهزة الكترونية القديمة و ذلك للحد من تعرضها للتهديدات الأمنية، و بالتالي فأمن أنترنيت الأشياء مهمته بحماية تلك الأجهزة باستكشافها و تصنيف المتصلة منها، و التجزئة التلقائية للتحكم في أنشطة الشبكة. [15](للتعلم ، 2023)

رابعا :الأمن التشغيلي

ينصرف هذا المصطلح إلى إدارة المخاطر المتعلقة بكافة مجالات الأمن السيبراني من طرف مسؤولي إدارة المخاطر، و ذلك عن طريق وضعهم لخطط بديلة في حالة تعرض البيانات لهجومات معينة، بالإضافة إلى ذلك يحوي الأمن التشغيلي على بيان توعوي للموظفين عن كيفية حماية المعلومات سواء التجارية أو الشخصية. [16] (خدماتك، 2022)

خامسا : أمن المستخدم النهائي و أمن البنية التحتية

يشير مصطلح أمن المستخدم النهائي إلي مجمل الممارسات التقنية التي تستخدم في حماية مختلف أجهزة المستخدمين من الهجمات السيبرانية الضارة بالأجهزة من بينها الفيروسات و غيرها، لذلك تسعى المؤسسات على حماية أجهزتها و تأمينها من المحاولات الخارجية الهادفة للوصول للشبكات و قواعد البيانات المخزنة. [17](بزنس، 2023)

و بخصوص أمن البنية التحتية فهذا النوع يعد إجراء أمني ذو أهمية بالغة لأنه يهدف لحماية البنية التحتية الحيوية كاتصالات الشبكة أو مركز البيانات أو الخادم أو مركز تكنلوجيا المعلومات، وجوهر هذا الإجراء هو الحد من نقاط ضعف هذه الأنظمة من الفساد أو التخريب أو الإرهاب، لذا يجب على أصحاب الأعمال و المنظمات و المؤسسات الحيوية التي تعتمد على البيئة التحتية الحيوية إدراك الالتزامات المتعلقة بهذا الإجراء.[18](للتعلم ، 2023)

4.2. أهداف الأمن السيبراني و أبعاده

يهدف الأمن السيبراني بصفة أساسية لحماية أنظمة البيانات و المعلومات من الهجمات السيبرانية و الاختراقات، مما يستدعي توفير آليات حماية فعالة و تختلف أبعاده باختلاف الميادين التي يهدف لحمايتها لذا سنتطرق لأهدافه و أبعاده .

أولا: أهداف الأمن السيبراني .

لما كان الأمن السيبراني قائم على التطور الدائم لبرامج الأمن فهو يهدف بذلك لديمومة استقرار الأنظمة، البيانات و مختلف الشبكات من التهديدات السيبرانية التي تشهد بدورها تطورا مستمرا، لذا كانت الحماية الشاملة أمرا لا مناص منه.

إن الأمن السيبراني يهدف لتعزيز أنظمة التقنيات التشغيلية و مكوناتها من أجهزة و برمجيات، و ما تقدمه من خدمات وما تحويه من بيانات، كما تهدف للتصدي للهجمات التي تستهدف المؤسسات في القطاع العام والخاص للوصول لبنى تحتية قوية، عن طريق سد الثغرات في أنظمة المعلومات و نقاط الضعف في مختلف أجهزة الحاسوب، و مقاومة الفيروسات والبرمجيات الخبيثة، كما تعمل على اتخاذ كل التدابير و الإجراءات اللازمة لحماية المستخدمين لشبكات الأنترنيت من التجسس و التخريب الإلكتروني . [19](السمحان، 2010 ،ص 12)

و تتحقق هذه الممارسة الأمنية للأمن السيبراني عن طريق أجهزة متخصصة تعمل على ما يلي:

- **الحفاظ على السرية** : إن العمل على الحفاظ علي البيانات أو المعلومات يتأتى عن طريق معايير و سياسات تعتمد على مراقبة كل عمليات الدخول و حضر تلك الغير مرخص بها، ومن تم تنحصر المعلومات على الفئة المخول لها ذلك دون غيرهم.

- **السلامة**: المقصود من السلامة موثوقية البيانات و تكاملها خلال دورة حياتها ، بحيث تبقى البيانات دون تغيير أثناء النقل و لا تتغير بواسطة كائنات غير مصرح بها، و يمكن استخدام خاصية التحكم

لمنع التغيرات الغير مقصودة بواسطة المستخدمين المصرح لهم و يجب أن تكون البرامج الاحتياطية متوافرة لاستعادة البيانات التالفة .[20](علي،2023 ، ص 12)

- **التوافر**: يقصد به التأمين الموثوق للبيانات و الخدمات و المعلومات المقدمة للمستخدمين المرخص لهم بذلك. [21] (الحديدي ، 2022، ص12)

ثانيا : أبعاد الأمن السيبراني

لما كان تحقيق الأمن السيبراني من المسائل الجوهرية و الأساسية للدولة، و ذلك بالنظر لأهميته في تحقيق الأمن الوطني في ظل تكنولوجيات العالم الحديث و ما فرضته الرقمنة من تحولات، لاسيما على مستوى الفضاء الافتراضي الذي عرف قفزة نوعية ، وما صاحب ذلك من مخاطر و تهديدات شملت كل الميادين ،هذا ما جعل السهر على تحقيق الأمن السيبراني ذو أبعاد متعددة ، لذا سنتعرض للبعض منها .

- البعد العسكري و السياسي

عرف القطاع العسكري الإنترنيت وما صاحبها من تطورات مند الوهلة الأولى و بصورة جلية، و انتقلت بعد ذلك إلى الأوساط الأكاديمية و العلمية، و يتميز البعد العسكري للأمن السيبراني في شق منه في قدرة القوة السيبرانية على ربط الوحدات العسكرية ببعضها البعض عبر العالم الافتراضي ، وهذا يسهل عملية تبادل المعلومات الذي ينعكس إيجابا على تحقيق الأهداف العسكرية.[22](قرة ، 2019)

و تعد على المستوى السياسي شبكات التواصل الاجتماعي منبرا لتبادل مختلف الأفكار بما فيها السياسية منها ، كما أصبحت وسيلة للانفتاح على مختلف المجتمعات، مما جعلها لنشر المعلومات و الآراء بصورة سريعة حيث تصل لملايين البشر في بضع لحظات، و يترتب عن ذلك العديد من الآثار السلبة إذا كانت المعلومات أو تلك الآراء و الأفكار تسعى لتهديم المجتمع و تغير معتقداته و أخلاقه ، أو تسعى لقلب نظام الحكم و إدخال البلاد في فوضى عارمة . لذا يقع على كاهل الدولة التصدي لهذه الأبعاد السياسية التي ترمي لزعزعة المجتمع و الأمن القومي في البلاد و ذلك عن طريق الهيئات و الأجهزة التي رصدت لتحقيق الأمن السيبراني، و سبيلها في ذلك تطبيق نصوص القانون المتعلقة بهذا الصدد .

-البعد الاقتصادي و الاجتماعي

يرتبط الأمن السيبراني ارتباطا وثيقا بالحفاظ على المصالح الاقتصادية التي تهدف كل الدول لتأمينها و العمل على تطويرها، و لتحقيق مسعها تعتمد على انتاج و تداول المعرفة و المعلومات، مما يبرز دور الأمن السيبراني في حماية الاقتصاد على مستوى عدة أصعدة، لا سيما و العالم اليوم عاكف على الاستثمار في مجال المعرفة معتمدا على المجال الرقمي، مما يؤكد على حقيقة الإرتباط الوثيق بين المجالين.[23] (السمحان،2010، ص 15)

و تعد حماية الملكية الصناعية و التجارية، و الملكية الأدبية و الفنية و حماية المستهلك من الإشهارات التضليلية و غيرها من بين مقاصد الأمن السيبراني، و ذلك للحفاظ على الاقتصاد و تأمين استقراره . أما على المستوى الاجتماعي فقد أصبحت المجتمعات في ظل زخم المعلومات ، لا سيما أمام المنحى التصاعدي و المستمر لمستعملي شبكات الأنترنيت و اتساع نطاق الرقمنة و تنوع الأجهزة الإلكترونية من حاسوب، هواتف ذكية و اللوحات الإلكترونية فتضاعفت المخاطر الاجتماعية و في مقدمتها الجريمة السيبرانية .

أمام هذا الوضع أصبح من الضروري تعميم المفهوم الصحيح للأمن ليمتد لكل المشاركين في الشبكة الدولية للمعلومات، لأن ذلك من شأنه تعزيز و تقوية مستوى الأمن إذا ما عرف ونفذ الأمر بذكاء، و لذلك يعد التثقيف المدني عن طريق إعداد حملات إعلامية توعوية يساعد على إعداد مجتمع المعلومات من أجل التعاطي مع عملية الأمن و ذلك من شأنه الحد من المخاطر السيبرانية ،و يرفع من مستوى التحديات الأمنية الوقائية والردعية.[24] (بارة، 2017، ص 430)

- البعد القانوني

إن العلاقة بين القانون و التكنلوجيا بكل أشكالها هي علاقة تكاملية، إذ تفرض هاته الأخيرة المواكبة القانونية لها، من خلال ضبط أطر تطبيقها و شروطها مع تحديد الأفعال محل التجريم و تقرير العقوبات المناسبة لها .

غير أن الوقت الراهن برهن أن الجريمة السيبرانية تفتقد للقوانين الصارمة للحد منها، و لعل ذلك يعود لعوامل عدة من بينها ، خصوصيتها من حيث صعوبة تحديد هوية مرتكبيها و مرونة التعريفات المرتبطة بتكنلوجيا المعلومات، إلى جانب طبيعة الجريمة كونها عابرة للحدود الأمر الذي يقتضي تفعيل التعاون الدولي المشترك لمكافحتها. [25](عطية 2019، ص 106)

وبالرغم من القصور المسجل على صعيد النصوص القانونية التي تعوزها الصرامة إلا أن البعد القانوني للأمن السيبراني سيظل يعكس آليات الوقاية والمكافحة ويكرس الحماية التشريعية و التنظيمية للوصول لأهداف الدولة المسطرة في مجال الأمن السيبراني.

1. التطور الموضوعي و الإجرائي للأمن السيبراني في التشريع الجزائري

نظرا للخطر الداهم الذي باتت تشكله الجريمة السيبرانية إذ نحت منحني خطير ليس على المستوى الوطني فحسب بل على الصعيد الدولى أيضا، و في هذا الصدد سجلت الفرقة المختصة بالأمن السيبراني بمصالح الدرك الوطني معالجة 2838 جريمة سيبرانية سنة 2001 لتقفز إلى4600 قضية سنة 2022 لتصل إلى 500 جريمة مند مطلع عام 2023 .[26] (تومیات ، 2023)

إن مرد ذلك هو ارتفاع نسبة مستخدمي ورواد الأنترنت إذ نشرت وكالة الاستشارات الدولية "DATAREPORTAL" في تقريرها السنوي حول الأنترنيت و شبكات التواصل لعام 2023، أن الجزائر عرفت ارتفاع في عدد مستخدمي الأنترنيت و الشبكات حيث سجلت 09, 32 مليون مستخدم في بداية عام 2023 بمعدل انتشار للأنترنيت بنسبة 70,9% من مجموع عدد السكان بعد أن كان في حدود 27 مليون مستخدم عام 2022. [27] (ب، 2023)

من هذا المنطلق عكف المشرع الجزائري على وضع منظومة قانونية تعزز الأمن السيبراني و ذلك على غرار باقي التشريعات للحد من تداعياته خطيرة و المتسارعة التي تلحق بالأشخاص و المؤسسات ، بل و بأمن الدولة واقتصادها، لذا قسمنا هذا المطلب لفرعين أساسيين :خصصنا الأول للقواعد الموضوعية للأمن السيبراني و الثاني للقواعد الإجرائية الهادفة لتحقيق الأمن السيبراني .

1.3. القواعد الموضوعية للأمن السيبراني

لقد كرست العديد من الدساتير الجزائرية حماية الحريات الأساسية و الفردية و حرمة الحياة الخاصة و ذلك بدء بدستور 1996 ثم 2016 وصولا لدستور 2020، حيث نصت المادة 34 فقرة 1 منه على: "تلزم الأحكام الدستورية ذات الصلة بالحقوق الأساسية و الحريات العامة وضماناتها، جميع

السلطات و الهيئات العمومية. " و قد أكدت على هذه الضمانة أيضا أحكام المادة 35فقرة 1 التي تنص: "تضمن الدولة الحقوق الأساسية و الحريات".

و في نفس السياق كرست المادة 47 حماية الحياة الخاصة، في حين نصت المادة 62 على حماية المستهلك حيث نصت: " تعمل السلطات العمومية على حماية المستهلكين، بشكل يضمن لهم الأمن و السلامة و الصحة و حقوقهم الاقتصادية." و نصت المادة 74 أيضا على حماية الإبداع الفكري فلا يمكن تقيده إلا عند المساس بكرامة الأشخاص أو بالمصالح العليا للأمة و الثوابت الوطنية .[28]
(دستور،2020، ص 11و12 و 13و18)

بناء عليه فلا بد من تعزيز هذه المبادئ بسن قوانين تفصيلية، لأنها الأداة التي تطبق من خلالها المبادئ الدستورية لذا سنتناول القواعد الموضوعية التي تكفل الأمن السيبراني في التشريع الجزائري .

أولا: القوانين المدنية الهادفة لتحقيق الأمن السيبراني

تعد المادة 124 من القانون المدني الجزائري أساس التعويض عن المسؤولية التقصيرية فهي مناط دعوى التعويض عن الضرر المادي اللاحق بالغير حيث تقضي بما يلي: "كل فعل أيا يرتكبه الشخص بخطئه و يسبب به ضررا للغير يلزم من كان سببا فيه بالتعويض." و قد نصت المادة 182 مكرر منه على وجوب التعويض عن الضرر المعنوي إذ قضت بما يلي: " يشمل التعويض كل مساس بالحرية أو الشرف أو السمعة."[29] (قانون 05-10، سنة 2005،ص 23 و24)

نلاحظ أن المشرع الجزائري جعل التعويض عن الضرر إحدى الآليات القانونية المدنية للحد من الأفعال الغير مشروعة بصفة عامة، ويعد الضرر الناتج عن مختلف صور الإجرام السيبراني من بين الأفعال الغير مشروعة المستحقة للتعويض هذا من جهة، و من جهة أخرى فإن الدعوى المدنية هي مناط جبر الضرر الناتج عن تلك الأفعال و من ثم تعد إحدى آليات تحقيق الأمن السيبراني .

و في ما يتعلق بالقوانين الخاصة فقد تضمن الأمر رقم 03-05 المتعلق بحقوق المؤلف و الحقوق المجاورة، حماية المصنفات مهما كان نوعها و مجابهة الاعتداءات الواردة عليها مدنيا وجزائيا.
حيث قضت المادة 159من الأمر المذكور أعلاه بتسليم محل المصادرة للمضرور عند الاقتضاء لتكون بمثابة تعويض عن الضرر حيث نصت على : "تأمر الجهة القضائية المختصة في جميع الحالات المنصوص عليها في المادتين 151 و 152من هذا الأمر، بتسليم العتاد أو النسخ المقلدة أو قيمة ذلك كله و كذلك الإرادات أو أقساط الإيرادات موضوع المصادرة للمؤلف أو لأي مالك حقوق آخر أو لذوي حقوقهما لتكون عند الحاجة بمثابة تعويض عن الضرر اللاحق بهم." [30](الأمر03-05،2023،ص21)
وفي هذا الصدد ننوه إلى أن هذا النص الخاص يقيد النص العام الوارد بموجب المادة 15من قانون الإجراءات الجزائية الذي تقضي بأن تؤول الأموال محل المصادرة للدولة.

من خلال هذه القواعد العامة الواردة في القانون المدني و القواعد الخاصة فإن المشرع يهدف لتعويض الضرر الناتج عن الفعل الغير مشروع مهما كان مصدره و نوعه بما في ذلك الهجمات السيبرانية و الجرائم السيبرانية .

ثانيا : قواعد الأمن السيبراني وفقا لقانون العقوبات

تعتبر القوانين الجزائية أكثر وقاية و صرامة وردعا، لذا حرص المشرع الجزائري على تعديل قانون العقوبات سنة 2004 بموجب القانون رقم 04-15 الذي تضمن قواعد موضوعية هامة تتعلق بالأمن السيبراني ، وذلك في إطار اصلاح العدالة، إذ خصص المشرع قواعد ردعية تتعلق بالإجرام

السيبراني و ذلك في القسم السابع مكرر من الفصل الثالث في ثمانية مواد بدء بالمادة 394مكرر إلى 394مكرر7. [31] (قانون04-2004، 15، ص 11 و12)

إن هذا الأمر يتعلق على وجه التحديد بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات التي تنقسم لثلاثة أصناف و هي:

-الأول يضم : الاعتداء على نظام المعالجة الآلية للمعطيات و ينطوي هذا الاعتداء على صورتين هما : جرمتي الدخول و البقاء الغير مرخص بهما في النظام المعلوماتي .[32] (براهيمي، 2016 ، ص 125)

و هو ما نصت عليه المادة 394مكرر من نفس القانون التي قضت : " يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50.000دج إلى 100.000دج كل من يدخل أو يبقي عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك."

وعزما من المشرع على حماية الأنظمة المعلوماتية و تحقيق الأمن السيبراني لجأ لمضاعفة العقوبة بالنظر للنتيجة المترتبة عن الفعل الغير مشروع طبقا لأحكام المادة 394 مكرر فقرة 2 من نفس القانون و التي قضت:"...تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة.

و إذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من 06 أشهر إلى سنتين و الغرامة من 50.000 دج إلى 150.000دج .

- الصنف الثاني يضم: الاعتداءات الواقعة على معطيات نظام المعالجة الآلية و سيرها و يهدف إلى إلحاق الضرر بالمعلومات التي يتضمنها جهاز الكمبيوتر أو وظائفه أو يعطل قدرة الأنظمة على أداء الوظيفة المنوطة بها ، و تتخذ بدورها صورتان هما: الاعتداء على المعطيات الداخلية للنظام والاعتداء على المعطيات الخارجية له. [33](براهيمي، ص 132)

لقد نص عليها المشرع على الصورة الأولى في أحكام المادة 394مكرر1 التي تقضي ب: "يعاقب بالحبس من 06 أشهر إلى 03 سنوات و بالغرامة من 500.000دج إلى2.000.000دج كل من أدخل بطريق الغش المعطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها."

أما الصورة الثانية فقد نصت عليها المادة 394مكرر2 من قانون العقوبات و التي قضت ب" يعاقب بالحبس من شهرين (2)إلى ثلاث(03)سنوات و بغرامة من 1.000.000دح إلي 5.000.000دج كل من يقوم عمدا أو عن طريق الغش بما يلي :

- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

-حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم ." [34] (قانون04-15،ص 12)

إن هذه القواعد الموضوعية سواء المدنية منها أو الجزائية لا يصبو من خلالها المشرع لمكافحة الجرائم السيبرانية فحسب، بل يصبومن خلالها أيضا لتحقيق أمن سيبراني مستدام.

ثالثا: الأمن السيبراني في طبقا للقوانين الخاصة

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

ومند مطلع سنة 2009 قام المشرع بسن العديد من القوانين الخاصة التي تتطلبها التحديات المعاصرة بالنظر لتطور الإجرام السيبراني و ما يتطلبه من مجابهة هذا من جهة، ومن جهة أخرى ترمي هذه القوانين لتحقيق الأمن السيبراني .

و تحقيقا لهذا المسعى أصدر المشرع القانون رقم 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنلوجيا الإعلام و الاتصال و مكافحتها، حيث نص على جملة من القواعد موضوعية و الإجرائية.

تضمن النوع الأول : التدابير الاحترازية ونصت عليها المادة 13 منه، وتتمثل في ضرورة إنشاء قطب وطني متخصص في الجرائم السيبرانية و حددت المادة 14 منه مهامه، كما تضمنت المادة 10 منه الالتزامات المفروضة على كل من :

- مقدمي الخدمات، يتوجب على هذه الفئة ، تقديم المساعدة للسلطات القضائية المكلفة بالتحريات لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها مع الحفاظ على السرية تحت طائلة العقوبات. و يتوجب عليهم أيضا حفظ لسنة واحدة تسري من تاريخ التسجيل ، المعطيات المتعلقة بحركة السير ويتعلق الأمر وفقا للمادة 11 من نفس القانون بالمعطيات التي تسمح بالتعرف على مستعملي الخدمة ، المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال ، المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة و مقدميها ، المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال و كذا عناوين المواقع المطلع عليها . و ما يتعلق بنشاطات الهاتف، يلتزم مقدم الخدمة بحفظ المعطيات التي تسمح بالتعرف على مستعمل الخدمة و مصدر الاتصال وتحديد مكانه.

- مقدمي خدمات الإنترنيت، فرض المشرع على هذه الفيئة وفقا للمادة 12من نفس القانون التدخل الفوري إما لسحب المحتويات التي تشكل جريمة بمجرد العلم بها وجعلها غير متاحة مع وجوب تخزينها ، بالإضافة إلي وجوب وضع ترتيبات تقنية لحصر إمكانيات الدخول للموزعات المخالفة للنظام والآداب العامة مع إشعار المشتركين بذلك، و يتوخى المشرع من فرضه تخزين المعلومات الحصول على الدليل المادي للقبض على الجناة.

في حين خص المشرع المادة 15 من نفس القانون للقواعد المتعلقة للإختصاص النوعي حيث نصت على : " زيادة على قواعد الإختصاص المنصوص عليها في قانون الإجراءات الجزائية ، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال المرتكبة خارج الإقليم الوطني ،عندما يكون مرتكبها أجنبيا و تستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني.

وحرصا من المشرع على تحقيق الأمن السيبراني و الحد من كل صور الإجرام المتعلقة به نص على التعاون الدولي وذلك في إطار المساعدات القضائية الدولية، تبادل جمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني، و في حالة الاستعجال يمكن قبول طلبات المساعدة القضائية الدولية الواردة عن طريق و سائل الاتصالات السريعة، مع مراعاة شروط الأمن الكافية للتأكد من صحة هذه الأخيرة، كل ذلك مع مراعاة الاتفاقيات الدولية و مبدأ المعاملة بالمثل و ذلك وفقا لمقتضيات المادة 16 من ذات القانون ، و يمتد التعاون الدولي لتبادل المعلومات و اتخاذ الإجراءات التحفظية وفقا للمادة 17 منه.

و تجدر الإشارة إلى وجوب مراعاة القيود الواردة على طلبات المساعدة القضائية الدولية الواردة في المادة 18 التي تنص: " يرفض تنفيذ طلبات المساعدة إذا كان من شأنه المساس بالسيادة الوطنية أو النظام العام، و يمكن أن تكون طلبات المساعدة مقيدة بشرط المحافظة على سرية المعلومات المبلغة أو بشرط عدم استعمالها في غير ما هو موضح في الطلب. " [35] (قانون09-04، 2009، ص 07و 08)

و يجب التنويه بأن الشق الإجرائي الذي تضمنه قانون 09-04 سنتطرق له في الفرع الثاني من هذا المطلب.

و في سنة 2018 قام المشرع بتعزيز الترسانة القانونية الهادفة لتحقيق الأمن السيبراني عن طريق سنه للقانون رقم 18-04 المؤرخ في 10 ماي سنة 2018 الذي يحدد العلاقات العامة المتعلقة بالبريد و الاتصالات الإلكترونية.

لقد جرم المشرع من خلال هذا القانون انتهاك سرية المراسلات الإلكترونية أو افشاء مضمونها أو نشرها أو استعمالها أو تخريبها دون ترخيص من المرسل أو المرسل إليه أو يخبر بوجودها أو يساعد في هذه الأفعال و ذلك وفقا للمواد 164إلى 166، و قرر عقوبات ردعية لتلك الجرائم المرتكبة مع إعطاء السلطة التقديرية لقاضي الموضوع لتسليط عقوبة أو أكثر من العقوبات التكميلية المنصوص عليها في المادة 09 من قانون العقوبات.[36] (قانون 18 -04، 2018 ،ص 30)

في حين شملت المادة 166فقرة 2 من نفس القانون المستخدمين لدى متعامل الاتصالات الإلكترونية في حالة تحويلهم بأية طريقة كانت المراسلات أثناء تأدية مهامهم و قرر لهم المشرع العقوبات المناسبة .
و في نفس المجرى نصتت المادة 165 فقرة 2 على تسليط عقوبة الحبس من سنة إلى 03 سنوات و الغرامة من 1.000.000دج إلى 5.000.000دج أو إحدى هاتين العقوبتين ،كل متعامل للاتصالات الإلكترونية الذي يحول بأية طريقة كانت المراسلات الصادرة، أو المرسلة أو المستقبلة عن طريق الاتصالات الإلكترونية أو أمر أو ساعد في ارتكاب الأفعال، كما يجوز للسلطة القضائية تسليط إحدى العقوبات تكميلية المنصوص عليها بالمادة 09من قانون العقوبات .

وفي أواخر سنة 2018 أصدر المشرع قانون 18- 07 المؤرخ في 10 جويلية2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي ، و قرر العقوبات المناسبة عن الأفعال المكونة للجريمة.[37](قانون 18-07، 2018،ص11)

و في مطلع سنة 2020 واصل المشرع سن القوانين الخاصة المكملة للقوانين العامة حيث أصدر قانون رقم20-05 المؤرخ في 28 أفريل سنة 2020 ، المتعلق بالوقاية من التمييز و خطاب الكراهية و مكافحتهما الذي و وضع من خلاله قواعد موضوعية و أخرى إجرائية بالنسبة للجرائم المرتكبة بواسطة وسائل تكنلوجية فضلا عن تلك الواردة في قانون الإجراءات الجزائية ، و ذلك بدء بالمادة 22 إلى 28 و قرر عقوبات ردعية لمرتكبيها ،كما تضمن إنشاء المرصد الوطني للوقاية من التمييز و خطاب الكراهية.[38] (قانون 20 -2020،05،ص 07و08)

2.3. القواعد الإجرائية الهادفة لتحقيق الأمن السيبراني

لم ينص المشرع الجزائري على قواعد إجرائية لمكافحة الجرائم الإلكترونية عموما إلا بحلول سنة 2006 إثر تعديله لقانون الإجراءات الجزائية بموجب القانون رقم 06-22 ، حيث أقر هذا الأخير العديد من الإجراءات التي من شأنها مكافحة الجريمة السيبرانية بكل أشكالها وذلك من أجل تحقيق الأمن السيبراني وتتمثل في التالي :

أولا : بالنسبة للإختصاص

قام المشرع على مستوى قواعد الإختصاص بتعديلات هامة فتم تمديد الإختصاص المحلي لكل من ضباط الشرطة القضائية ، وكلاء الجمهورية و قضاة التحقيق في هذه الجرائم و هذا يبرز تصميم المشرع على تحقيق الأمن السيبراني.

ثانيا: بالنسبة للتحقيقات

أولى المشرع للتحقيقات في مختلف الجرائم عناية خاصة من حيث الدقة في الإجراءات مع حرصه على إحاطتها بعدة ضمانات شكلية وأخرى موضوعية لما لها من مساس بالحياة الخاصة للأشخاص ، و مع ذلك فقد قلص من تلك الضمانات في الجرائم الخطيرة من بينها الجرائم السيبرانية ، لا سيما ما تعلق منها بالتفتيش و التوقيف للنظر.

فبالرجوع لأحكام المادة 47فقرة 3من نفس القانون نجد أن المشرع جرد من خلالها التفتيش المتعلق بتلك الجرائم من بعض الضمانات، إذ أتاح التفتيش و المعاينة والحجز في كل محل سكني، أو غير سكني ، و في كل الأوقات ليلا او نهارا و حتى دون الحصول على إذن مسبق من وكيل الجمهورية.

بالإضافة إلى ذلك خول المشرع لضباط الشرطة القضائية اتخاذ كل التدابير التحفظية وفقا للفقرة الأخيرة من المادة 47من نفس القانون، و ذلك للحصول على الأدلة الثبوتية و القبض على الجناة و الحد من الإجرام السيبراني .

عطفا على ما تقدم جعل المشرع التوقيف للنظر وفقا للمادة 51فقرة 5 من قانون الإجراءات الجزائية في الجرائم السيبرانية مختلفا عنه في الجرائم التقليدية المقرر فيها التوقيف للنظر ب 48 ساعة، وذلك لما لهذه الجرائم من دقة في التحري و جمع الأدلة، إذ تمدد المدة مرة واحدة بإذن من وكيل الجمهورية المختص ، كل ذلك شريطة أن تقوم دلائل قوية ضد المشتبه به .

فضلا عن ذلك لجأ المشرع للترصد الالكتروني كآلية للتحقيق حيث نص عليها في الفصل الرابع من الباب الثاني تحت عنوان " في اعتراض المراسلات و تسجيل الأصوات و التقاط الصور، بدء بالمادة 65مكرر 5 إلى 65 مكرر 10. من القانون المذكور أعلاه ، إذ نصت المادة 65 مكرر5 : " إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبيض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد ، يجوز لوكيل الجمهورية المختص أن يأذن بما يلي :

- اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية و اللاسلكية .
- وضع الترتيبات التقنية دون موافقة المعنيين، من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة وسرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص...."

و قد نص المشرع أيضا على آلية التسرب للحد من العديد من الجرائم منها المعلوماتية وفقا للمادة 65 مكرر11 من نفس القانون.[39] (قانون06-22، 2006 ،ص 07 و 08 و09)

و في ما يتعلق بالقواعد الإجرائية التي تضمنها قانون 09 -04 فتتمثل في :المراقبة الالكترونية وفقا للمادة 04 منه ، القيام بإجراءات التفتيش و الحجز طبقا للمادة 03 منه حيث تتم هذه الإجراءات داخل منظومة معلوماتية ،و أخيرا إنشاء هيئات وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحته و التي استحدثت بموجب الأمر 21-22 المعدل والمتمم لقانون الإجراءات الجزائية . و تكملة لمسرى الإصلاحات قام المشرع بتعديل قانون الإجراءات الجزائية سنة 2021

بموجب الأمر رقم 21-11، حيث أضاف باب سادس للكتاب الأول أستحدث بموجبه القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال.

إن هذا الأمر يتضمن ثمانية مواد بدء بالمادة211مكرر 22 إلى211مكرر29 فبالعودة للمادة 211مكرر22 نجدها تقضي بإنشاء على مستوى محكمة مقر مجلس قضاء الجزائر، قطب جزائي وطني متخصص في المتابعة و التحقيق في جرائم ذات الصلة بتكنولوجيات الإعلام و الاتصال و الجرائم المرتبطة بها، كما يختص بالجرائم المنصوص عليها في نفس الباب إن كانت ذات طبيعة جنحيه، و قد مدد المشرع بموجب المادة 211 مكرر23 من نفس الأمر، الإختصاص المحلي لكل من وكيل الجمهورية لدى القطب، قاضي التحقيق و رئيس ذات القطب ليصبح وطنيا.[40] (الأمر رقم 21 -11، 2011،ص 08و 09)

2. المؤسسات المنوط بها تحقيق الأمن السيبراني

يعد التشريع إحدى الأليات القانونية لتحقيق الأمن السيبراني على اعتبار أن النص القانوني يتوخى من خلاله المشرع الوقاية والردع، لذا أسند لبعض المؤسسات والهيئات صلاحية الوقاية ومكافحة الجرائم السيبرانية بكل أشكالها علما أن هذه الأخيرة تتمتع بالخصوصية، لا سيما من حيث صعوبة الكشف عن مرتكبيها و الوسائل التقنية المتطورة المستخدمة لارتكابها.
من أجل ذلك رصد المشرع بعض المؤسسات تسهر على تحقيق الأمن السيبراني و هذا ما سنتطرق له بنوع من التفصيل .

1.4. الأجهزة التابعة للدفاع الوطني

إيمانا بالمهام الملقاة على عاتقها تكفلت مؤسسة الدفاع الوطني بالحماية السيبرانية للجزائر، و مرجعتيها في ذلك نصوص القانون و المهارات البشرية والأجهزة التقنية المتطورة، و رصد لهذه المهمة جهاز عملياتي متخصص .

إن هيئة الدفاع الوطني تعمل باحترافية عالية و في إطار القوانين العامة والخاصة للبلاد و في طليعتهم قانون العقوبات و قانون الإجراءات الجزائية من أجل الوقاية من الجرائم السيبرانية ومكافحتها، وبفضل اعتماده على المهارات البشرية، الوسائل التقنية، المعدات التكنلوجية في مجال الإعلام الآلي و الاتصالات اللاسلكية و التمتع بقاعدة بيانات واسعة تتسم بالتحديث المستمرة والقدرة على تصميم البرامج المعلوماتية و تطويرها، يعد من المسائل التقنية الداعمة للأمن السيبراني.[41](بارة ، 2017، ص 269)

و قد عملت الجزائر على التكوين المستمر لأفراد هذا الجهاز و بالفعل لقد أثبت جدارته سواء من حيث الكشف عن التهديدات أو الجرائم السيبرانية و التصدي لها و تعد الإحصائيات السالفة الذكر الصادرة عن الدرك الوطني كجهاز تابع للدفاع الوطني خير دليل على ذلك .
و قد أنشأت مراكز و معاهد و هيئات وطنية ، تضطلع بتحقيق الأمن السيبراني سنتعرض لها تبعا.

أولا: المراكز المتخصصة في الأمن السيبراني

ينبثق عن جهاز العملياتي التابع للدرك الوطني مراكز وقائية وردعية متخصصة في الوقاية و مكافحة الاجرام السيبراني و تتمثل في التالي:

- مركز الوقاية من جرائم الإعلام الألي و الجرائم المعلوماتية للدرك الوطني

يهدف المركز المتخصص لتأمين منظومة المعلومات لخدمة الأمن العمومي.[42](شويرب ،مراد، 2023، ص168) ويعزز المركز أيضا عمليات البحث و التحقيق في الجرائم الماسة الأنظمة المعلوماتية

عبر الوطن باعتباره مركز تقنيي، كما توجد مصالح أخرى تابعة للدرك الوطني نذكر منها: مصلحة مكافحة الإجرام السيبراني، مديرية الأمن العمومي و الاستغلال.، المصلحة المركزية للتحريات الجنائية.

ثانيا : المعاهد المتخصصة و المصالح التابعة للدرك الوطني

لتحقيق الأمن السيبراني أنشأ المشرع معاهد و مصالح منوط بها تحقيقه لما لها من قدرة وكفاءة وتتمثل في التالي :

- **المعهد الوطني للأدلة الجنائية و علم الإجرام للدرك الوطني**: أنشأ سنة 2004 بموجب المرسوم الرئاسي رقم 04-183 .[43](مرسوم رئاسي رقم 04-183، 2004 ، ص 18)

يعتبر المعهد الوطني للأدلة الجنائية و علم الإجرام للدرك الوطني مكسبا مؤسساتي حيث رصد المعهد لتدعيم قدرات الدرك الوطني ، عن طريق إدراج العلوم في الكشف عن الحقيقة و تحقيق العدالة ، كما أن التحكم في التقنيات الحديثة يدعم قدرات المؤسسة لمكافحة الإجرام المتطور الذي أضحى يعتمد على التكنولوجيات الحديثة.

و يناط بالمعهد عدة مهام من بينها : إنجاز الخبرات و التحاليل بناء على طلبات القضاة، المحققين و السلطات المؤهلة ،الدعم التقني للوحدات أثناء التحقيقات المعقدة ، تصميم بنوك معطيات و إنجازها وفقا للقانون، المشاركة في الدراسات والبحوث المعمقة، الاسهام في تحديد سياسة جنائية مثلى لمكافحة الإجرام، العمل على ترقية البحث التطبيقي وأساليب التحري التي تثبت فعاليتها في ميادين علمي الإجرام و الأدلة الجنائية على الصعيدين الوطني والدولي، المشاركة في تنظيم تحسين المستوى و التكوين ما بعد التدرج في تخصصات العلوم الجنائية.[44] (الدرك الوطني وزارة الدفاع الوطني)

ثالثا: المنظومة الوطنية لأمن الأنظمة المعلوماتية

هي مصلحة موضوعة لدى وزارة الدفاع الوطني أنشأت سنة 2020 بموجب المرسوم الرئاسي رقم 20- 05 المؤرخ في 20-01- 2020 المتعلق بوضع منظومة و طنيه لأمن الأنظمة المعلوماتية، و قد بينت المادة 2 من المرسوم مهامها حيث نصت على: "المنظومة أداة الدولة في مجال أمن الأنظمة المعلوماتية ، و تشكل الإطار التنظيمي لإعداد الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية و تنسيق تنفيذها."

و تتشكل المنظومة الوطنية لأمن الأنظمة المعلوماتية وفقا لنص المادة 03 من نفس المرسوم من: مجلس وطني لأمن الأنظمة المعلوماتية، يكلف بإعداد الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية، و الموافقة عليها وتوجيهها، و قد فصلت المادة 4 من نفس المرسوم المهام المنوطة بالمجلس.

فضلا عن المجلس تتكون المنظومة الوطنية لأمن الأنظمة المعلوماتية من "و كالة"، تكلف بتنسيق تنفيذ الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية. بالإضافة للوكالة تتوفر لدى المنظومة الو طنيه لأمن الأنظمة المعلوماتية، هياكل مختصة لوزارة الدفاع الوطني في هذا المجال. [45](مرسوم رئاسي رقم 20- 05، ص 6)

2.4. الهيئات الوطنية الهادفة لتحقيق الأمن السيبراني

في إطار عملية الإصلاحات استحدث المشرع هيئات وطنية منوط بها الوقاية من الاجرام السيبراني و مكافحته منها ما هو ذو طبيعة إدارية و منه ما هو ذو طبيعة قضائية، و تتمثل هذه الهيئات التي تصبو لتحقيق الأمن السيبراني في: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، و القطب الجزائي المتخصص في الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال.

أولا : الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها

تضمن قانون 09-04 في مادته 13 ضرورة إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، و بالفعل تم تحديد تشكيلتها و تنظيمها وكيفية سيرها المرسوم الرئاسي رقم 15-261 المؤرخ 08 أكتوبر 2015 .

إن هذه الهيئة قد اعتبرتها المادة 2 من ذات المرسوم ذات طبيعة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي ، توضع لدى الوزير المكلف بالعدل، و تمارس مهامها المذكورة في المادة 14 من قانون 09-04، بالإضافة للمهام المذكورة في المادة 04 من ذات المرسوم الرئاسي.[46](مرسوم رئاسي رقم 15-261، 2015،ص16)

و قد تم إعادة تشكيل و تنظيم و كيفية تسيير هاته الهيئة بموجب المرسوم الرئاسي رقم 19-172 المؤرخ في 9-06- 2019، وأصبحت تحت سلطة و زارة الدفاع الوطني و فقا للمادة الثانية منه. [47] (المرسوم الرئاسي رقم 19- 172، 2019 ، ص 05)

غير أن المرسوم المذكور أعلاه تم تعديله في أواخر سنة 2020 و أصبحت الهيئة تحت سلطة رئيس الجمهورية و ذلك و فقا للمادة الثانية من المرسوم الرئاسي رقم 20-183 المؤرخ في 13- يوليو 2020. [48](مرسوم رئاسي رقم 20-183، 2020 ،ص05)

و في نهاية سنة2021 عدل أيضا المرسوم المذكور أعلاه لكنه أبقى الهيئة تحت سلطة رئيس الجمهورية وفقا للمادة 02 من المرسوم الرئاسي رقم 21-439 المؤرخ في 07-11-2021 ومقرها الجزائر العاصمة، ويمكن تغيير هذا المقر بمرسوم رئاسي وفقا للمادة 03 منه و تمارس مهامها وفقا للمادة 04 من هذا المرسوم تحت رقابة السلطة القضائية ،و طبقا لقانون الإجراءات الجزائية ، و قانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها. [49](مرسوم رئاسي رقم 21 -439، 2021، ص05)

و تتشكل الهيئة من الأجهزة تتولى مهامها و هي: مجلس التوجيه و مديرية عامة، يقدمان لرئيس الجمهورية عرضا عن نشاطهما، و يتولى الأمين العام لرئاسة الجمهورية رئاسة المجلس الذي يتكون 10أعضاء و فقا للمادة 6 من نفس المرسوم الرئاسي ، و يدير المديرية العامة مدير عام يعين بموجب مرسوم رئاسي و تنهي مهامه حسب نفس الأشكال القانونية وفقا للمادة 9 و يتولى المهام المذكورة في المادة 10 من ذات المرسوم الرئاسي، و تضم المديرية العامة و فقا للمادة 11 عدة أجهزة تتمثل في: مديرية المراقبة الوقائية و اليقظة الإلكترونية، مديرية الإدارة والوسائل، مصلحة للدراسات و التخصيص، مصلحة لليقظة التكنلوجية و ملحقات جهوية .

ثانيا : القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال

واصل المشرع مسيرة الاصلاحات لتحقيق الأمن السيبراني المستدام فأنشأ على مستوى محكمة مقر مجلس قضاء الجزائر القطب الجزائي الوطني المتخصص في المتابعة و التحقيق في الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و الجرائم المرتبطة بها، و ذلك سنة 2021 بموجب الأمر رقم 11/21 المؤرخ في 25 غشت 2021 المعدل و المتمم لقانون الإجراءات الجزائية ، و يتضمن 08 مواد.

لقد جعلت المادة 211 مكرر 24 الإختصاص وطنيا حيث نصت على :"مع مراعاة نص المادة 2 من المادة 211 مكرر22 أعلاه ، يختص كل من وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و قاضي التحقيق و الحكم في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المذكورة أدناه و كذا الجرائم المرتبطة بها:

-الجرائم التي تمس بأمن الدولة أو الدفاع الوطني.

-جرائم نشر وترويج أخبار كاذبة بين الجمهور من شأنها المساس بالأمن أو السكينة العامة أو استقرار المجتمع .
- جرائم المساس بأنظمة المعالجة الآلية للمعطيات المتعلقة بالإدارات و المؤسسات العمومية.
- جرائم الإتجار بالأشخاص أو الأعضاء البشرية أو تهريب المواطنين .
- جرائم التمييز و خطاب الكراهية ." [50] (الأمر 21-11، 2021 ، ص 08) .

وقد منحت المادة 211مكرر 25 من ذات القانون لكل من : وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال ، و كذا قاضي التحقيق و رئيس ذات القطب ، حصريا بالمتابعة و التحقيق و الحكم في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال الأكثر تعقيدا و الجرائم المرتبطة بها.

الخاتمة :

نخلص بالقول إلى أن التطور التكنلوجي أنجب إجراما مستحدثا ولد من رحم تكنلوجيا ت الإعلام الاتصالات و الرقمنة ، فبرز الإجرام السيبراني بكل أشكاله و سبيله في ذلك أجهزة الحاسوب وما في حكمه و كل ما تعلق بالأنظمة المعلوماتية فأصبح يهدد اقتصاد الدولة وأمنها.

إن هذا الإجرام المستحدث فرض على الدول تحديات جديدة ألا وهي السعي لتحقيق الأمن السيبراني و من بينها الجزائر التي جعلت من التشريع آلية قانونية لتحقيقه، و تعد التعديلات التي قام بها المشرع سواء على مستوى القوانين العامة أو الخاصة مع اسناد ه مهمة تحقيق الأمن السيبراني لهيئات مؤسساتية متخصصة برهان قاطع ، على عزم المشرع على تحقيق الأهداف المبتغاة من كل تلك الإصلاحات التشريعية، و قد توصلنا في الختام للنتائج التالية:

1-إن المشرع الجزائري جعل من التشريع إحدى الآليات القانونية لتحقيق الأمن السيبراني أو كما أطلق عليه الجرائم المتصلة بالإعلام و الاتصال ، و هذا ما جعله يلجأ للقيام بالعديد من التعديلات المتواترة و المتواصلة الدالة على عزمه على الوقاية من تلك الجرائم و مكافحتها، و في ذلك تحقيق للأهداف و الأبعاد التي توخاها ألا وهي تحقيق أمن سيبراني مستدام .

3- إن إنشاء المشرع لهيئات مؤسساتية تضطلع بتحقيق الأمن السيبراني يعكس الخطر الذي تشكله الجرائم السيبرانية بكل صورها.

4- لقد نجح المشرع لحد كبير في تحقيق الأمن السيبراني عن طريق الترسانة القانونية التي رصدت للوقاية ومكافحة الجريمة السيبرانية ، و مع ذلك تبقى خصوصية الجرائم السيبرانية لا سيما من حيث اثباتها و اتساع نطاقها يشكل ثغرة تؤرق كل القائمين على تحقيق الأمن السيبراني لا سيما في ظل التطور التكنلوجي المتسارع .

5- بالرغم من حرص المشرع على تعزيز الترسانة القانونية بقوانين تعمل على تحقيق الأمن السيبراني إلا أن معدل الجريمة السيبرانية في تزايد مستمر ، و هذا يستدعي القيام بالتعديلات المستمرة لمواكبة التطور التكنلوجي المتسارع ، كما أن القانون الوضعي لا يرتقي للكمال لأن لكل عمل نقصان لذلك نقترح التوصيات التالية:

1- التركيز على التأهيل الدوري لكل القائمين على تحقيق الأمن السيبراني ليمتلكوا من المهارات العالية و التقنيات المستحدثة في هذا المجال من أجل رصد الجريمة السيبرانية و التحكم من تقنيات إثباتها .

2- تفعيل دور المجتمع المدني في الجانب التوعوي بأهمية الإبلاغ عن الجرائم السيبرانية وذلك الأمن لتعزيز الأمن السيبراني .

3- نقترح على المشرع استبدال تسمية الجرائم المتصلة بالإعلام و الاتصال بالجريمة السيبرانية كما هو معمول به في معظم دول العالم و لتتناسق مع مصطلح الأمن السيبراني .

الهوامش و المصادر

1- بارة سمير 2017 ،" الأمن السيبراني في الجزائر السياسات والمؤسسات"، *المجلة الجزائرية للأمن الإنساني"* المجلد 2 0 ،(العدد 04) صادر في 01-07 [online] ص ص255 ،الرابط الإلكتروني https://www.asjp.cerist.dz/en/article66092 ،تاريخ الاطلاع: 15 -11-2023 على الساعة 16.

2- شويرب جيلاني ; مراد فايزة 2023،"مفهوم الحروب السيبرانية و الأمن السيبراني "، *مجلة الحقوق و الحريات*، مجلد 11،(العدد01)صادر في 20-04 [online].ص157-178،الرابط الإلكتروني https://www.asjp.cerist.dz/en / article/219023 تاريخ الإطلاع: 15-11 -2023 على الساعة 15

3- السمحان منى عبد الله بن صالح 2010 " متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود"،*مجلة كلية التربية بالمنصورة*، مجلد 111، (العدد01) ، صادر في يوليو [online].ص ص 03-31، ص 10 ، الرابط الإلكتروني https://maed.journal.ekb.eg/article140786 تاريخ الإطلاع: 21-10-2023 على الساعة 11

4- زروقة إسماعيل 2019 ، "الفضاء السيبراني و التحول في مفاهيم القوة و الصراع "، *مجلة العلوم القانونية والسياسية* ، المجلد 10، (العدد01) online]الصادر في 28-04 ص ص 1016-1031،الرابط الالكتروني، https://wwwasjp.cerist.dz/en/article/91423 تاريخ الإطلاع: 21-10-2023 على الساعة 21 و15د.

5- بوضياف سهام 2018،"الجريمة الالكترونية والإجراءات التشريعية لمواجهتها في الجزائر"، *مجلة الأستاذ الباحث للدراسات القانونية و السياسية*، المجلد 03 ،(العدد 03) [online.] الصادر في 01-09، ص375-348،الرابط الإلكتروني https://www. asjp.cerist.dz/en/article/81720 تاريخ الإطلاع: 22-10-2023 على الساعة 21 و20د.

6 – بوازدية جمال 2019 "الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية – التحديات و الأفاق المستقبلية "، *مجلة العلوم القانونية و السياسية*، المجلد1،(العدد01)[online]صادرفي28-04،ص ص 1262-1293،الرابط الإلكتروني https://wwwasjp.cerist..dz .تاريخ الإطلاع: 30 -09-2023 على الساعة 21 و15د.

7- الصحفي روان بنت عطية الله 2020،"الجرائم السيبرانية"، *المجلة الإلكترونية المتعددة التخصصات*،(العدد24).شهر 5[online] ص ص 01-53 الرابط الالكتروني https://www eimj.org. تاريخ الاطلاع15-10-2023 على الساعة 14

9- لعلوم الشرطة أكاديمية السلطان قابوس ،(2016)، " *الجريمة الإلكترونية في المجتمع الخليجي و كيفية مواجهتها* "، *الأمانة العامة لمجمع البحوث و الدراسات الأكاديمية*، [online]، ص ص 7-208، الموقع الالكتروني www.gcc-sg.org تاريخ التصفح 27-12-2023على الساعة 14

10- مريزق عدمان; بوقلاشي عماد2010،"الأمن المعلوماتي في ظل التجارة الإلكترونية –إشارة إلى حالتي تونس والجزائر." *مجلة الاقتصاد الجديد*، المجلد 01 (العدد02) صادر في 01-12[online] ،ص ص 7-25، الرابط الإلكتروني https://wwwasjp.cerist..dz/en/article/56345 ، تاريخ الإطلاع: 28-12-2023 على الساعة 17

11-الحديدي أيمن أحمد 2022 ، *الأمن السيبراني في ظل الانفجار المعرفي*.، *دار اليازوري العلمية للنشر و التوزيع*.

12- روبدين ، أمن الشبكات –أنواعه و دوره في الحماية من التهديدات السيبرانية 2023، [online]، الرابط الإلكتروني: https://robodin.com ، تاريخ الاطلاع 08-01-2024على الساعة 19 و10د

13-*للتعلم بكة* ، أواع الأمن السيبراني ومجالاته وعناصر تكوينه2023، [online] ،الرابط الالكتروني
https://bakkah.com. : تاريخ الاطلاع : 07-01-2024 على الساعة 16
14 - بزنس اعمل، أكاديمية كل ما ترغب معرفته عن الأمن السيبراني، كل ما ترغب معرفته عن الأمن السيبراني - مفهومه و خصائصه و أشهر أنواع التهديدات فيه-،2023 ، [online] ،الرابط الالكتروني
https://www.e3melbusinesse.تاريخ الإطلاع 7-01-2024 على الساعة 16و40د.

15- للتعلم بكة ، 2023 .

16- خدماتك، ماهي أنواع الأمن السيبراني و مجالاته و أهميته 2022 ، [online]،الرابط الالكتروني
https://khadamatk.com . تاريخ الإطلاع 30-12-2023على الساعة 14و15د

17- بزنس اعمل، أكاديمية ، 2023.

18- للتعلم بكة ، 2023.

19-السمحان ، 2020 .

20- علي مفيد عوض حسن ،(2023) مقدمة في الأمن السيبراني، ط ،*مكتبة نور* [online]،ص 12، الرابط الإلكتروني: https://www. nour-book.com. ،تاريخ الاطلاع 27-12-2023 على الساعة 17
.
- 21 الحديدي أيمن أحمد ، 2022 . .

22- قرة فارس ، 2019 "الأمن السيبراني"، *الموسوعة السياسية* ،صادر في 28-08[online]. الرابط الإلكتروني https://political-encylopedia.org تاريخ الإطلاع على الساعة 18و30د

23. – السمحان منى عبد الله بن صالح ،2020.
24. – بارة سمير ، 2017.

25- عطية إدريس 2019، "مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري "، *مجلة مصداقية* ، المجلد 01 (العدد01). الصادر في 01-012[online]، ص106، الرابط الإلكتروني.
https://wwwasjp.cerist..dz/en/article/125955 .تاريخ الإطلاع01-02-2024 على الساعة 17

26. -توميات أحمد رمزي، "2023 مصالح الدرك الوطني تعالج 500جريمة سيبرانية مند بدء 2023"، *صحيفة شرشال نيوز*[online]15 فيفري، الرابط الإلكتروني https://national.cherchellnews.dz تاريخ الإطلاع:25-11-2023 على الساعة 15و15د

27- ب عبد الرزاق 2023.، "هذا هو عدد *مستخدمي الإنترنيت و شبكات التواصل بالجزائر عام 2023* "[أونلاين] 14 فيفري ،الرابط الإلكترونيhttps ;//www. echroukonline.com ،تاريخ التصفح 28-12-2023على الساعة 19.
.
32-جمال براهيمي 2016 ،"مكافحة الجرائم الإلكترونية في التشريع الجزائري "، *المجلة النقدية للقانون و العلوم السياسية*، المجلد 11 (العدد02) صادر في 15-11.[online]، ص ص 124-155، الرابط الإلكتروني
https://wwwasjp.cerist..dz/en/article/22167 .تاريخ الإطلاع :25-12 -2023 على الساعة 21و30د
33 -براهيمي، 2016.

41- بارة سمير ، 2017.
42- شويرب ،مراد، 2023.

44 – الدرك الوطني، وزارة الدفاع الوطني " المعهد الوطني للأدلة الجنائية و علم الإجرام للدرك الوطني [online]، الرابط الإلكتروني http://www.mdn.dz تاريخ الإطلاع : 30-12-2023 على الساعة 20.

30- أمر رقم 03-05 المؤرخ في 19 يوليو، "متعلق بحقوق المؤلف والحقوق المجاورة" *الجريدة الرسمية*، عدد 44 المؤرخة في 23 يوليو.2019.

40-أمر رقم 21 -11، 2011،المؤرخ في 25-08- المعدل و المتمم للأمر رقم66-155 "المتضمن قانون الإجراءات الجزائية الجزائري "، *الجريدة الرسمية* العدد65،المؤرخة في 26غشت.2011

50 –أمر رقم 21-11، 2021.

28- دستور2020، المرسوم الرئاسي رقم 20/ 442 المؤرخ في 30-12 "متعلق بالتعديل الدستوري *"الجريدة الرسمية"*، (العدد 82) المؤرخة في 30ديسمبر، 2020.

31- قانون 04-15 ،2004، مؤرخ في 10-نوفمبر، "معدل ومتمم للأمر رقم 66-156 المتضمن قانون العقوبات" ، *الجريدة الرسمية* (عدد71)،المؤرخة في 10-نوفمبر، 2004.

29 - قانون 05 -10، مؤرخ في 20 يونيو، يعدل و يتمم للأمر رقم 75-58 المؤرخ في 26 سبتمبر 1975 "المتضمن القانون المدني"، الجريدة الرسمية، (عدد44) المؤرخة في 26 يونيو، 2005 .

39- قانون06-22، 2006 ،مؤرخ في 20-12، المعدل والمتمم للأمر رقم66-155 1966 "المتضمن قانون الاجراءات الجزائية الجزائري" ، *الجريدة الرسمية* (العدد84)،المؤرخة في 24ديسمبر، 2006.

8 –قانون 09-04 ،2009 المؤرخ 05 غشت، " المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنلوجيا الإعلام و الاتصال و مكافحتها، *" الجريدة الرسمية* "، (العدد 47)، المؤرخة في 16غشت 2020 .

35 قانون09-04، 2009.

36 - قانون 18 -04، 2018 ، مؤرخ في 10 ماي " يحدد العلاقات العامة المتعلقة بالبريد و الاتصالات الإلكترونية*"*، *الجريدة الرسمية* (العدد 27)المؤرخة في 13 ماي، 2018.

37- قانون 18-07، 2018 ، مؤرخ في10 يونيو ، "المتضمن حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي"، *الجريدة الرسمية* ،(عدد 34) ،المؤرخة في 10يونيو، 2018.

38- قانون 20 -05، 2020 ، المؤرخ في 28أفريل ،"متعلق بالوقاية من التمييز و خطاب الكراهية ومكافحتهما" ، *الجريدة الرسمية* (العدد 25) المؤرخة في 29 أفريل،2020. .

43- مرسوم رئاسي رقم 04-183، 2004، مؤرخ في 06يونيو " يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي." *الجريدة الرسمية*، رقم 41 مؤرخة في 27يونيو، 2004.

46-مرسوم رئاسي رقم 15-261، 2015 ، مؤرخ في 08 أكتوبر" يحدد تشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ."*الجريدة الرسمية*"(العدد53) مؤرخة في 8أكتوبر.، 2015.

47- مرسوم رئاسي رقم 19- 172، 2019 "يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها و تنظيمها و كيفيات سيرها"، *الجريدة الرسمية* ،(العدد 37) المؤرخة في 09- يونيو، 2019.

48- مرسوم رئاسي رقم 20-183، 2020، مؤرخ في 13 يوليو " يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها "، *الجريدة الرسمية، العدد (40) مؤرخة في 18 يوليو 2020.*

45- مرسوم رئاسي رقم 20- 05، 2020 .

49- مرسوم رئاسي رقم 21 -439، 2021، مؤرخ في 07 نوفمبر " يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها"، *الجريدة الرسمية*، (العدد 86) مؤرخة في11 نوفمبر.2021.