وزارة التعليـم العالـي والبحـث العلمـي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

UNIVERSITE
Abdelhamid Ibn Badis
MOSTAGANEM

جامعة عبد الحميد بن باديس مستغانم

كلية الحقوق والعلوم السياسية **المرجع:** .....

قسم: القانون الخاص

مذكرة نهاية الدراسة لنيل شهادة الماستر

الأمن السيبيراني في الجزائر

ميدان الحقوق والعلوم السياسية

الشعبة: **الحقوق** التخصص: **قانون خاص**

من إعداد الطالب(ة): تحت إشراف الأستاذ(ة):

بوعلام فتيحة **حميدي فاطمة**

أعضاء لجنة المناقشة

الأستاذ(ة):..... برابح نور الهدى .....رئيسا

الأستاذ(ة):.....حميدي فاطمة..... مشرفا مقررا

الأستاذ(ة):..... مبراط حبيبة..... مناقشا

السنة الجامعية: 2025/2024

نوقشت في : 2025/06/22

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي و البحث العلمي
جامعة عبد الحميد بن باديس-مستغانم

UNIVERSITE

كلية الحقوق و العلوم السياسية
مستغانم

تصريح شرفي خاص بالالتزام بقواعد النزاهة العلمية
في إنجاز البحث

أنا الممضي أدناه،

السيد: بوحلاس فتيحة الصفة: طالب ماستر

الحامل لبطاقة التعريف الوطنية رقم: [illegible] والصادرة بتاريخ: 2022/05/26

المسجل بكلية: الحقوق والعلوم السياسية قسم: الحقوق

والمكلف بإنجاز مذكرة ماستر بعنوان:

الحق في التسريح التعسفي في التشريع الجزائري

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

التاريخ: 29-05-2025

إمضاء المعني

* ملحق القرار الوزاري رقم 933 المؤرخ في 28 جويلية 2016 الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية و مكافحتها

شكر وتقدير

الحمد لله على توفيقه وإحسانه ، والحمد لله على فضله و إنعامه ، و الحمد لله على- جوده و إكرامه ، الحمد لله حمدا يوافي نعمه ويكافئ مزيده .

أشكر الله عز وجل الذي أمدني بعونه و وهبني من فضله و مكنني من إنجاز هذا العمل ولا يسعني إلا أن أتقدم بشكري الجزيل إلى كل من ساهم في تكويني و أخص بالذكر أستاذتي الفاضلة "حميدي فاطمة "

الذي تكرم بإشرافه على هذه المذكرة ولم تبخل علي بنصائحها الموجهة لخدمتي فكانت لي نعم التوجيه و المرشدة

كما لا يفوتني أن أشكر أعضاء لجنة المناقشة المحترمين الذين تشرفت لمعرفتهم وتقييمهم لمجهوداتي

كما أشكر كل من قدم لي يد العون و المساعدة ماديا أو معنويا من قريب أو بعيد إلى كل هؤلاء أتوجه بعظيم الامتنان وجزيل الشكر المشفع بأصدق الدعوات.

الإهداء

أهدي هذا العمل إلى أعز ما يملك في هذه الدنيا إلى ثمرة نجاحي إلى من أوصى بهما الله سبحانه و تعالى:

" بالوالدين إحسانا"

إلى الشمعة التي تحترق من أجل أن تضيء أيامي إلى من ذاقت مرارة الحياة وحلوها ، إلى قرة عيني وسبب نجاحي و توفيقي في دراستي إلى

" أمي"

أطال الله في عمرها

إلى الذي أحسن تربيتي وتعليمي وكان مصدر عوني و نور قلبي و جلاء حزني و رمز عطائي و وجهني نحو الصلاح و الفلاح إلى

" أبي"

إلى أخواتي وجميع أفراد عائلتي

إلى أستاذتي "حميدي فاطمة" وجميع الاساتذة الكرام الذين أضاءوا طريقي بالعلم

وإلى كل أصدقاء الدراسة و العمل و من كانوا برفقتي أثناء إنجاز هذا البحث إلى كل هؤلاء وغيرهم ممن تجاوزهم قلمي ولن يتجاوز هم قلبي أهدي ثمرة جهدي المتواضع .

مقدمة

المقدمة

شهد العقد الاخير من القرن الماضي تطورات معتبرة على مستوى تكنولوجيا المعلومات و الاتصالات وشبكات الانترنت على اختلاف استعمالاتها،صاحب ذلك التطور ملحوظ في نشاط الجريمة السيبرانية والتهديدات الامنية التي تستهدف المجال السيبراني الدول ضمن الفضاء الالكتروني في إطار ما يسمى" الحروب الالكترونية"

ويشيرالامن السيبراني الى التقنيات و الإجراءات التي تهدف إلى حماية أجهزة الكمبيوتر والشبكات والبيانات من الدخول غير القانوني ونقاط الضعف والهجمات المنقولة عبر الانترنت من قبل المتسللين وقراصنة الانترنت وتشكل الدراسات المتعلقة بالامنالسيبراني والحريمة السيبرانية إحدى أهم المحاور و الملفات البحثية التي أولى لها الباحثين والدراسيين في الاوساط الاكاديمية،كنا يولى لها النهر وصناع القرار السياسي والامني والعسكري اهتماما بالغا وواسعا نظرا لخطورته وتأثيره على سيادة الدول وأمنها.

وفي هذا السياق يلعب الأمن السيبراني دورا حيويا في حماية الانظمة الالكترونية ،فهو بشكل الدرع الواقي الذي يسعى لتحسين قدرة الدول و المؤسسات على اكتشاف واحتواء ومكافحة الهجمات الالكترونية.وبتطبيق إستراتيجيات الأمن السيبراني الفعالة،يمكن تقليل تأثير الجرائم الالكترونية والحد من الاختراقات والاحتيالات السيبرانية.

إلى جانب ذلك،تعزيز الاتفاقيات الدولية التعاون في مكافحة الجرائم الالكترونية وتعزيز الأمن السيبراني عبر الحدود،فهي تساهم في تطوير إطار قانوني دولي يوفر أسسا قانونية قوية لمكافحة الجرائم الالكترونية على المستوى العالمي.

ويمكن تعريف الأمن السيبراني بأنه مجموع الاطر القانونية والتنظيمية التي تهدف إلى حماية الفضاء السيبراني الوطني والدولي مع التركيز على ضمان توافر أنظمة المعلومات وتمتين الخصوصية وحماية سر المعلومات الشخصية وإتخاذ جميع الإجراءات الضرورية لحماية المواطنين والمستهلكين من مخاطر الفضاء السيبراني[1].كما عرفتها وكالة الأمن القومي في الولايات المتحدة الامريكية فقد عرفته المنظمة الدولية الاتحاد الدولي الاتصالات بم جموع الادوات والسياسات والمفاهيم الامنية والضمانات الامنية والمبادئ التوجيهية و التقنيات التي يمكن استخدامها لحماية البيئة الالكترونية وتنظيم أصول المستخدم حيث تشمل توصيل أجهزة الحوسبة و الموظفين و البنية التحتية و الخدمات و نظام الاتصالات السلكية واللاسلكية ومجمل المعلومات المرسلة أو المخزنة في البيئة الالكترونية[2]

وفي ظل هذا التحدي الرقمي التكنولوجي الجديد سعت الدول إلى سن حزمة من التشريعات والاليات القانونية و المؤسساتية لتصدي لهذه الجريمة التي أضحت تسمى في الادبيات الاكاديمية بالجريمة السيبرانية.

و الجزائر هي أيضا مستهدفة كسائر الدول من التهديد السيبراني وتداركت الوضع بداية من سنة 2004 بسن القانون 04_15[3] المعدل والمتمم القانون العقوبات المتضمن الجرائم الماسة بأنظمة المعالجة الالية للمعطيات،والقانون 06-22[4]المعدل

---

[1]إدريس عطية ،مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري،مجلةمصداقية،كلية الحقوق والعلوم السياسية ،جامعة العربي التبسي،تبسة،الحزائر،المجلد01،العدد01، 2019 ، صفحة 103

[2]التقرير الصادر عن الاتحاد الدولي الاتصالات حول اتجاهات الاصلاح في الاتصالات ،عام 2010_2011.

[3]قانون رقم 04-15 المؤرخ في 10 ديسمبر 2004 ،يعدل ويتمم الأمر رقم 66-156 المتضمن قانون العقوبات ،الجريدة الرسمية،العدد:10،2004/11/74.

[4]القانون رقم 06-22 المؤرخ في 29 ذي القعدة عام 1427 الموافق 20 سبتمبر سنة 2006 ، يعدل ويتمم الأمر رقم 66_155 المؤرخ في 18صفر عام 1386 الموافق 8 يونيو سنة 1966

والمتمم القانون الإجراءات الجزائية باستخدام تدابير اجرائية لمكافحة الجريمة السيبرانية.

وتشير الاحصائيات المسجلة في الجزائر ان الجريمة السيبرانية أخذت منحا تصاعديا في الآونة الأخيرة ،وهو ماينبأ بخطورة الوضع،لاسيما في ظل تواجه الجزائر نحو تبني مقاربة الحكومة الالكترونية ،ومن هذا المنطلق فإن السلطات الجزائرية ملزمة باتخاذ الاحتياطات الامنية اللازم لتفادي أي نوع من الجرائم الالكترونية.

و فيما يخص ترتيب الجزائر على المستوى العربي فقد احتلت المرتبة العاشرة حسب التزامها بتلك التدابيرالتي وضعها الرقم القياسي العالمي الأمن السيبراني حسب تقرير سنة 2015 أيضا.

وأما عن التقرير الصادر عن الاتحاد الدولي الاتصالات السلكية واللاسكية لسنة 2017 فيما يخص الرقم القياسي العالمي الأمن السيبراني فإن الجزائر قد احتلت المرتبة 67 عالميا بتنقيط 0.432 من أصل 164دولة،والمرتبة 9 عالميا متراجعة بكثير الى الخلف في الترتيب العالمي.[1]

ومن المعلوم أن الدفاع الوطني منذ الاستقلال تولى مسؤولية الدفاع عن الوطن في جميع الميادين،وتوفير الأمن بمعناه الواسع،الامر الذي فرض عليه التعامل من المتغيرات الحديثة والتكيف معها،بغية تحقيق هدفه الاسمى،وتوجهت منظومة الأمن الوطني الى وضع استراتيجية أمنية شاملة من أجل ضمان "الأمن السيبراني"،لان

والمتضمن قانون الإجراءات الجزائية، الصادر في الجريدة الرسمية الجزائرية عدد رقم 84،المنشور بالجريدة الرسمية الجزائرية بتاريخ 24 ديسمبر سنة 2006

[1] الاتحاد الدولي للاتصالات السلكية واللاسكية ،تقرير صادر عنها ،صفحة 01

أمن المعلومات تعتبر ضمن الأمن الوطني الشامل ، فالأجهزة الامنية الجزائرية تدرك أن التغيرات المصارعة في التكنولوجيا تؤدي الى خلق تهديدات ليست بالسهلة ،إذ لابد من ضرورة العمل على ضمان أمن المعلومات وشبكات الانترنت خلال خطوات مهمة تعتمد على مجموعة كبيرة من وسائل قانونية وتقنية لمقاومة الاستخدام غير الشرعي للشبكة العنكبوتية واختراقها

وبناءا عليه كانت الحاجة ملحة لوضع هذا الموضوع موضع الدراسة والتحليل ولتعريف الأمن السيبراني أو الجريمة السيبرانية وذلك في التشريع الجزائري ،وبناءاعلى ذلك،نطرح الاشكالية الدراسة المحورية:

ماهي الطبيعة القانونية الأمن السيبراني في التشريع الجزائري ؟

ويكسب هذا الموضوع أحد أبرز مواضيع الساعة،إذ يعد الأمن السيبراني من أهم المواضيع في اختصاص الدراسات الاستراتيجية والامنية.وتمكن في إعطاء تصور واضح لعلاقة الأمن السيبراني بأمن الدولة.

من بين الاسباب التي دفعتني الى اختيار هذا الموضوع "الأمن السيبراني في التشريع الجزائري" هي الرغبة في التعرف على الأمن السيبراني والجرائم السيبرانية الذي تعاني منه الدول المتقدمة وعرفته الدولة الجزائرية في الآونة الأخيرة حيث أن هذا الأخير قد تغش في مجتمعنا هذا من ،ومن جهة أخرى هو الفضول لمعرفة الاليات و الإجراءات وكذا الهيئات التي اتخذتها الدولة الجزائرية لمجابهة هذا النوع من الجرائم .

استخدم الباحث في هذا البحث المنهج الوصفي ،لأن بحثنا هذا سيرتكز على وصف المفاهيم العامة و الخاصة و الإجراءات المتبعة والتحقيق في الجرائم السيبرانية

للاجابة عن الاشكالية الرئيسية للموضوع،قمنا بتقسيم الدراسة إلى مقدمة ،وفصلين،وخاتمة.

خصصنا الفصل الاول لدراسة كل مايتعلق بالامنالسيبراني من خلال مبحثين،بينما تناولنا في المبحث الاول ماهية الأمن السيبراني ،كما درسنا في المبحث الثاني الأمن السيبراني بين الابعاد والتهديدات السيبرانية.

أما في الفصل الثاني تطرقنا الى النظام المؤسساتي الأمن السيبراني وذلك في مبحثين،في المبحث الاول الاليات القانونية و الإجرائية لمواجهة الجريمة السيبرانية في التشريع الجزائري ،والمبحث الثاني الى الأمن السيبراني في الجزائر

الفصل الأول: النظام القانوني للأمن السيبراني في التشريع الجزائري

تمهيـــــــد:

يعتبرالأمن السيبراني أحد الركائز الأساسية لتقوية المنظومة لسائر الدول، فهو ضرورة حتمية لمواجهة المخاطر السيبرانية التي تتهدد كيان الدول واستقرار سيادتها وذلك لطبيعتها الخاصة التي لا تنفرق بالحدود الوطنية وهي مخاطر عابرة للحدود، ومعصوبة تعقب مرتكبيها وذلك لسهولة إزالة أدلة الاثبات للإدانة وقد اقتحمت هذه التهديدات السيبرانية جميع مناحي الحياة نتيجة التطور السريع والمذهل لتكنولوجيات الإعلام والاتصال، وبالتالي يسهل اختراق خصوصيات المؤسسات والشركات الخاصة بل وحتى الحياة الخاصة للأفراد.

لقد أثارت هذه الجرائم تساؤلات كثيرة باعتبارها ظاهرة جديدة ونظرا لجسامة اخطارها وسرعة انتشارها, وأصبح التعامل مع صور هذه الجرائم موضع اهتمام بالغ من الفنيين والمهتمين بأن الصدح المعلوماتي لتحديد مفهومها وخصائصها، وهذا ما سنحاول إستعراضه في هذا الفصل من خلال مايلي:

المبحث الأول: ماهية الأمن السيبراني الذييتضمن مطلبين، المطلب الأول مفهوم الأمن السيبراني ونشأته والمطلب الثاني أنواع الجرائم السيبرانية وأركانها.

المبحث الثاني: الأمن السيبراني بين الأبعاد والتهديدات السيبرانية والذي يتضمن في المطلب الاول أبعاد الأمن السيبراني وفي المطلب الثاني التهديدات السيبرانية

المبحث الاول: ماهية الأمن السيبراني.

يعتبر الامن السيبراني من المفاهيم التي اصبحت تتداول في الدراسات الأكاديمية نظرا لأهميتها في الحد من اختراقات السيبرانية ومواجهة الجرائم الإلكترونية بشتى الطرق والاساليب الموضوعية والاجرائية، وبالتالي كثر استخدام هذا المصطلح عبر العالم.

المطلب الأول: مفهوم الأمن السيبراني ونشأته

يتضح كليا ان الأمن السيبراني يعد أساسا لمواجهة التحديات الأمنية الحديثة في عالم متصل بشكل متزايد ومنه سنتناول في هذا المطلب تعريف الأمن السيبراني في الفرع الاول ونتطرق إلى نشأته في الفرع الثاني.

الفرع الاول: التعريف الفقهي والقانوني الأمن السيبراني

أولا: التعريف الفقهي:

1. بالنسبة للأكاديميين:

– عرفه ريتشارارد كمرر Richard Akemmerr على أنه عبارة ع ن دفاعية من شأنها كشف وإحباط المحاولات التي تقوم بما القراصنة.[1]

– ويعرفه كذلك إدوارد مورسو Edward Amorso على أنه: "وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشركات. وتشمل

[1] محمد مختار،cybersecurity هل يمكن تجنب الدولة مخاطر الهجمات الالكترونية ؟,مجلة مفاهيم المستقبل، العدد 06 ، بيروت,لبنان, يناير 2015 ,ص05

تلك الوسائل الادوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها وتوفير اتصالات المشفرة[1]

يعرفه كذلك الكاتبان "Matti" "pekky" في كتابهما الموسوم "Analytics, Technology and I cyber Security : Automation حيث أعتبر الأمن السيبراني عبارة عن مجموعة من اجراءات التي اتخذت فى الدفاع ضد هجمات قراضة الكمبيوتر وعواقبها، ويتضمن تنفيذ التدابير المضادة المطلوبة [2]

2. **بالنسبة للدوائر الحكومية :** ركزنا على أهم الفواعل الدولة والهيئات المختصة) بالولايات المتحدة الأمريكية المستهدف رقم 01 من طرف المجرمين، تعرف وزارة الدفاع امريكية الأمن السيبراني على أنه مجموعة الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها (الالكترونية والمادية) من مختلف الجرائم ، الهجمات، التخريب، التجسس والحوادث .
3. **وكالة الامن الرقمي الاوروبية :** الأول من صدرت تشريع هدا المجال فعرفته بأنه قدرة النظام المعلوماتي على مقاومة محاولات اختراق أو الحوادث غير المتوقعة التي تستهدف البيانات المتداولة أو المخزنة وفق إطار توافقي.[3]

[1]صالح بن على بن عبد الرحمان الربيعة, الامن الرقمي وحماية المستخدم ضدمخاطر الانترنت, ،, متاح على REPS://Www.google.com/unisi ، تاريخ التصفح: 2025/02/16

[2]فارس محمد العمارات,إبراهيمالحمامصة,الأمنالسيبراني(المفهوم و تحديات العصر),الطبعة01, دار الخليج للنشروالتوزيع,الاردن,عمان,2022,ص 15

[33]أول اتفاقية تناولت هذا الموضوع هي الاتفاقية التي صدرت في بوداباست 2001.

ثانيا: التعريف القانوني للأمن السيبراني.

1-التعريف القانوني الدولي للأمن السيبراني الدولي:

كما ندكر التعريف الدي جاء به الاتحاد الدولي للاتصالات الصادر في تقرير حول اتجاهات الاصلاح الاتصالات عام" 2010 – 2011 " والذي يعتبر بمثابة أرضية إجماع لمختلف التوجهات الفكرية والمهنية: هو مجموعة من المهمات، مثل تجميع وسائل وسياسات. وإجراءات أمنية، ومبادئ توجيهية، ومقاربا ت ادارة المخاطر وتدريبات، وممارسات فضلي، وتقنيات، يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين[1]

2 – تعريف المشرع الجزائري للأمن السيبراني:

أعطى المشرع الجزائري تعريف في الفقرة الثالثة من م العاشرة من القانون رقم 18-04 بانه مجموع ادوات والسياسات ومفاهيم الامن والأليات الامنية والمبادئ التوجيهية وطرق تسيير المخاطر والاعمال والتكوين والممارسات الجيدة والضمانات والتكنولوجيات التي يمكن استخدامها في حماية الاتصالات الكترونية ضد أي حد ت من نشانه المساس بتوفير و سلامة البيانات المخزنة أو المعالجة أو المرسلة [2]

[1]أنظر التقرير الصادر عن الاتحاد الدولي للاتصالات حول اتجاهات الاصلاح في الاتصالات عام 2015 – 2011

[2]انظر المادة 10/03 من القانون رقم 18/04 المؤرخ في 24 شعبان عام 1933 اموافق 10 يوسنة 2018 ، الذي يحدد التواعد العامة المتعلقة بالبريد و الاتصالات الالكترونية، الصادر في الجريدة الرسمية الجزائرية ، العدد 2 صفحة 3

وقد عرف المشرع الجزائري الجريمة السيبرانيةف ي نص المادة 02 الفقرة –ا– من الفصل الاول من القانون رقم 09–04[1] المؤرخ 05 اوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال و مكافحاتها تحت عنوان مصطلحات بأنها "جرائم المساس بأنظمة المعالجة الالية للعمليات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يشمل ارتكبها عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية[2]

إن طبيعة الجرائم السيبرانية وتمييزها عن الجرائم التقليدية يرجع إلى الوسط الذي ترتكب فيه الجريمة وهي الاداة أو الوسيلة اتي استخدمها الجاني في ارتكاب فعله غير المشروع وتتطلب توفر مقرفة او حد داتي من الثقافة الفعلية لدئ الجاني، وهي للتخرج عن كون ما سلوك اجرامي ينشأ بارتكاب فعل جرمه القانون او الامتناع عن فعل أمربه القانون وتتجه إرادة الجاني إليه رغم وجود نص قانوني في يجرم السلوك. يمكن استخلاص من مجموعة من الخصائص في نقاط:

1. جرائم تتم باستخدام الحاسب الآلي كأداة الارتكاب الجريمة، وتستخدم شبكة الانترنت كوسيلة لذلك.
2. جرائم لا يتم في أغلب احيانا التبليغ عنها، خاصة إذا تعلق الأمر بالمؤسسات والشركات التجارية ، تجنبا للإساءة السمعة

[1] أنظر المادة 102 من القانون 04/09 المؤرخ في 14 شعبان عام 1439 ، الموافق 5 غشت سنة2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها, المنشور بالجريدة الرسمية الجزائرية، العدد47 بتاريخ 16أوت 2009 صفحة 05

[2] بلال بن جامع , الجرائم الكترونية على شبكة الانترنت دراسة حالة جامعة عبد الحميد مهري,قسنطينة 02 / رسالة دكتوراه، مكتب علم التوثيق ، 2016 / 2017 ، صفحه 116.

3. جرائم صعبة الاستكشاف لعدم تركها أثار مادية يمكن من خلالها حل القضية ويطلق هذه الاثار ابالآثارا لمعلوماتية الرقمية.

4. جرائم غامضة لصعوبة إثباتها وذلك بسبب غياب الدليل المرئي والأن اغلب البيانات عبارة عن رموز لا يمكن قراتها.

5. جرائم تستدعى المام مرتكبيها بالمعرفة التقنية والخبرة الفائقة في مجال الحاسب الالي.

6. – جرائم لا تمتاز بالعنف، لا تستخدم مرتكبيها القوة الجسدية أو العضلية للقيام بالجريمة.[1]

الفرع الثاني: نشأة الأمن السيبراني:

نشأت المفهوم للأمن السيبراني بعد اختراع الحاسوب بعدة عقود ، كان اول ظهور لمفهوم للأمن السيبراني سنة 1972 ، ادا كان مجرد فكرة نظرية في ذلك الوقت واستمرت النقاشات والتحليلات خلال فترة التسعينات إلا أنه ظهر الأمن السيبراني كمفهوم فعلي قابل للتطبيق حينها طرح الباحث بو بنطوماس برنامج كميوت اطلق عليه CREEPER وقد تمكن هدا البرنامج من التحرك عبر الشبكةArparet

تم طرح تومليسون أول برنامج Reofore لمطاردة وحذف CREEPER من خلال تعقب مساراته وعليه كان REAPER أول برنامج ذاتي النسخ لمكافحة

[1]مهدي رضا, الجرائم السيبرانية وآليات مكتفحتها في التشريع الجزائري، مجلة إيليزا للبحوث والدراسات المجلد06 ، العدد02, 2021 صفحة 114

الفيروسات حيث اعتبارعندها أول دودة حاسوب تلاحق الفيروسات في الكمبيوتروتقضي عليها

وقد أنشى العديد من المشاريع الامن المبكر من قبل الجهات المختلفة من العهود والجهات الحكومية ففي عام 1979 رصدت أول عملية اختراق الانظمة التشغيل من قبل كفين ميتيك البالغ من العمر 16 سنة إذ قام ننسخ برنامج وتوزيعها أدى إلى سجنه لصبح بعدها مدير لشركة Security consulting Mintick وفي بداية الثمانينات كان الفيروس الذي أوجده توماس موريس سببا في بداية مجال جديد تماما في أمان الكمبيوتر وهو الامرالدي دفع الكثير البحث عن الطريقة التي يمكنهم فيها تصميم فيروسات أكثر فعالية وفتحا بأنظمة الشبكات والكمبيوتر

وفي عام 1985 حددت وزارة الدفاع معايير لتقيم نظام الكمبيوتر الموثق به إلا انه في عام 1985اخترقت بوابة انترنت في كاليفورنيا وتم هگر 400 جهاز كمبيوتر عسكري بالإضافة إلى الأجهزة المركزية في مقر البنتاغون وذلك بهدف بيع المعلومات.

و بعد عام 1987 تطلق أول برنامج تجاري لمكافحة الفيروسات، ثم توالت شركات تطوير برنامج محافظة الفيروسات في الظهور عام 1988، ومنها شركة Avast وكان عمل المكافحة محصورا بالرد على الهجمات الحالية ويذكر أن عام وجود شبكة واسعة ساعد على الحد من نشر التحديثات، وشهد هذا العقد تأسيس أول منتدى الكترونى مختص لأمن مكافحة الفيروسات اضافة إلى تأسيس مطبعة

مكافحة الفيروسات لحماية بيانات مستخدمي الفضاء السيبراني من اي قرصنة إلكترونية إجرامية وهو ما مهد لظهور للأمن السيبراني بعدها[1]

خلال سنة 1996 سجلت اول قضية في الولايات المتـــحدة امريكية تتعلق بارتكاب افعال إساءة الاستخدام الحاسوب اين تمت محاكمة مهندس يعمل في البنك من أجل قيامه بالتحايل على برنامج الاعلام الالي لاختلاس مبلغ مالي.

وفي اليابان سجلت اول قضية خلال سنة 1970تتعلق بالمساس بالأنظمة المعلوماتية عل اثر اكتشاف عملية سرقة ونشر معطيات شخصية لزبائن شركة تجارية.

وفي السويد في سنة 1973 اصدرت قانون المعطيات المعلوماتية.

فرنسا سنة 1978. اصدرت قانون يتعلق المعطيات بالمعلوماتية والحريات

وفي سنة 1988 اصدرت معطيات قانون يتعلق بالجرائم المساس بالأنظمة الالية المعالجةللمعطيات GOPFRAN1[2]

وكانت شركة أرامكو السعودية، أكبر شركة نفطية في العالم قد تعرضت إلى هجوم إلكتروني في 2012[3] يقولو مسؤولون في الاستخبارات الامريكية انه مرتبط باىران

ومن بين 54 دولة تم تقييمهم بالمستوى المرتفع في مجال لأمن السيبراني أربع دول عربية هي بالترتيب السعودية وعمان وقطر ومصر. وحصلت السعودية

[1] طمطاي سالم، الصحافة الكترونية والأمن السيبيراني, مذكرة لنيل شهادة الماستر فى الا علام والاتصال، جامعة احمده راية,ولاية أدرار كلية العلوم الانسانية والاجتماعية والعلوم الاسلامية، صفحة 18-17.

[2] مختار الاخضرى, الإطار القانوني لمواجهة الجرائم المعلوماتية في الفضاء الافتراضي , مداخلة القيت خلال أعمال الملتقى الاولى الجزائر بعنوان محاربة الجريمة المعلوماتية والقضائية طبعة 2011 ، صفحة 54.

على المركز الاول عربيا و 13 عالميا في 2018، بعدما كانت تحتل المرتبة الخامسة عربيا وال 64 عالميا في2017.[1]

و في العراق لا يقصر الارهاب السيبراني على صورة واحدة ومهنية، فهو يبدأ من الجرائم الالكترونية باستخدام انترنت كنوافذ للتخطيط والتنفيذ وصولا إلى الجرائم الاتجار بالبشر، ثم تجارة المخدرات وحتى إلى ارتكاب الجريمة المنظمة والقرصنة الالكترونية ومنصات الجيش العسكري، وجرائم الاحتيال المالي ا ضافة إلى تزوير البيانات ومي جرائم السيبرانية الاكثر انتشارا د اخل العراق وقد تعود ت مخاطر الارهاب السيبراني على الامن القومي. مما يفتح بابا لاختراقت واستخدامات غير مشروعة، مما ينتج عنها اعمال تجسسية، أو حتي المساس بأمن الدول الأخرى[2]

"عام 2008 تعرصت المغرب إلى أول هجوم الكتروني من قبل قراصنة لعدة مواقع حكومية ومؤسسات خاصة . لكن لهجوم اكثر شهرة كان في 2012 عند ما قامت مجموعة قراصنة تعرف باسم "Anonymous Monacoباختراق «مواقع حكومية، ومصارف مغربية ضمن حملة احتجاجية على السياسات الحكومية. كما استهدف القراصنة بعض الشركات الأجنبية العاملة في المغرب [3]

والجزائر هي أيضا مستهدفة كسائر الدول من التهديدات السيبرانية وخاصة في المؤسسات الوطنية والاختراق الاخير البرنامج يقاسوس الإسرائيلي خير دليل

---

[1]– ترتيب الدول العربية في الامن السيبراني|https://www.JLhan.com22 ,2025/02/ 16:25

[2]رعد خضير صليبي، تعزيز الامنالسيبراني في الع راق (التحديات والفرص)، مجلة دراسات دولية ، العدد تسعة وتسعون30/ 10/ 2024، صفحة 514.

[3]المغرب و الهجمات الالكترونيةو https.eljph.com 2025/02/22 16:40.

على هذا التهديد ، ناهيك عن جرائم احتيال والنصب على شبكات التواصل الاجتماعي اتي تطال الافراد و المؤسسات يوميا والعدد في تزايد مستمر ومضيف و تداركت الوضع سنة 2004 بسن القانون 04-15 المعدل والمتمم لقانون العقوبات ستضمن الجرائم الماسة بأنظمة المعالجة الالية للمعطيات والقانون6 0 - 22 المعدل والمتمم القانون اجراءات الجزائية باستحداث تدابير الجزائية لمكافحة الجرائم الالكترونية، وأيضا سن المشرع نصوص خاصة نذكر أهمها القانون تف 04-03 المتضمن الوقاية من الجرائم المتصلة بتكنولوجيات اعلام واتصال ومكافحتها الذي من مضامينه التشجيع على التعاون الدولي والمساعدة القضائية [1]

احتلت الجزائر المرتبة 23 عالميا من أصل 29مرتبة في مستوى التأهب في مجال الأمن السيبراني اما على المستوى العربي فقد احتلت قلت الجزائر المرتبة العاشرة حيت التزامها تلك التدابير التي يحددها الرقم القياسي العالمي للأمن السيبراني[2]

المطلب الثاني: أنواع الجرائم السيبرانية

اختلف الفقه والقانون في تصنيف الجرائم الالكترونية باختلاف الزاوية التي ينغار إزاء الاعتداء الموجه ضد أحد مكونات النظام المعلوماتي وتقوم هذه الجريمة بدورها على أركان، حيث سنتناول في الفرع الاول: أنواع الجرائم السبرانية وأركانها في الفرع الثاني

[1] قطاف سليمان,الاليات الموضوعية و الاجرائية المتبعة لتحقيق الامن السيبراني,مجلة الحكومة و القانون الاقتصادي, المجلد20,العدد 20, 2022, صفحة 80.

[2] بن مرزوق عنترة ,الأمن السيبراني كبعد في السياسة الدفاعية الجزائريةوجامعة محمد بوضياف المسيلة, كلية الحقوق و العلوم السياسية ,المركز الجامعي افلو,صفحة70.

الفرع الاول: أنواع الجرائم السيبرانية في القانون الجزائري

قسم المشرع الجزائري الجريمة الكترونية إلى جناية وهي أخطر الجرائم، وجنحة وهي متوسطة الخطورة، ثم مخالفة وهي أقل خطورة، وتصنف بحسب طبيعتها إلى جريمة عادية وجريمة سياسية، جريمة عسكرية وأخرى إرهابية [1]

وعلى خلاف هذه الجريمة فإن الجريمة الإلكترونية عرفت اختلافًا حول تقسيماتها، وذلك بسبب الاختلاف في تشميتها، حيث استند كل اتجاه على معيار معين. فالبعض يصنفها حسب الأسلوب المتبع في الجريمة، والبعض الآخر يستند إلى دوافع ارتكابها، وآخرون يؤسسون تقسيماتهم على تعدد محل الاعتداء وتعدد الحق المعتدى عليه.

أما بالنسبة للمشرع الجزائري فقد قسم الجريمة الإلكترونية إلى جرائم مرتكبة بواسطة النظام المعلوماتي نص عليها المشرع ولم يحددها، وبالتالي تشمل كل الجرائم المرتكبة بواسطة تكنولوجيا الإعلام والاتصال. أما النوع الثاني من الجرائم فيتمثل في الجرائم الواقعة على النظام المعلوماتي، وحددها المشرع بموجب قانون العقوبات، وهذا ما سيتم بيانه في الفرعين التاليين.

أولًا: الجريمة السيبرانية المرتكبة باستخدام النظام المعلوماتي.

يشمل هذا التصنيف أهم الجرائم التي تتصل بالمعلوماتية، ويعد الحاسب الآلي وسيلة لتسهيل النتيجة الإجرامية ومضاعفًا لجسامتها. وهي أنواع منها: الجريمة

[1] حسن بوسقيعة، الوجيز في القانون الجزائي العام، الطبعة 1 ،الديوان الوطني للأشغال التربوية،الجزائر،2002، ص24

الواقعة على الأشخاص، الجريمة الواقعة على النظم المعلوماتية الأخرى، الجريمة الواقعة على الأسرار[1]. وسأوضح كل نوع منها في البنود الآتية.

ثانيًا: الجريمة السيبرانية الواقعة على الأشخاص الطبيعية

تنقسم هذه الجرائم بدورها إلى جرائم واقعة على حقوق الملكية الفكرية، وجرائم واقعة على حرمة الحياة الخاصة.

1. الجريمة السيبرانية الواقعة على حقوق الملكية الفكرية:

يكون النظام المعلوماتي وسيلة للاعتداء على حقوق الملكية الفكرية، ومثاله السطو على بنك المعلومات وتخزين واستخدام هذه المعلومات دون إذن صاحبها، لأن استخدام معلومة معينة دون إذن صاحبها يعتبر اعتداءً على حق معنوي، إضافة إلى كونه اعتداءً على قيمتها المالية، كون أن للمعلومة قيمة أدبية بجانب قيمتها المادية. ويندرج ضمن الحقوق الفكرية كذلك براءات الاختراع، إذ تمثل فكرة للمخترع تحتوي على حق معنوي وآخر مالي للمخترع. وقد نص المشرع الجزائري على حقوق الملكية الفكرية من خلال نصوص قانونية وهي الامر رقم 05/03 الصادر في 2003 المتعلق بحقوق المؤلف والحقوق المجاورة، والأمر رقم 03-07 الصادر في 2003 المتعلق ببراءات الاختراع.[2]

2. الجريمة السيبرانية الواقعة على حرمة الحياة الخاصة:

[1] سفيان سوي، جرائم المعلوماتية، مذكرة ماجستير، جامعة ابو بكر بلقايد تلمسان، كلية الحقوق والعلوم السياسية،2010-2011, ص33.

[2] نفس المرجع, ص 34.

لقد كرس الدستور الجزائري حرصه على حماية الحياة الخاصة للمواطنين وعدم الاعتداء على هذه الحرمة. ولما كان الحاسب الآلي بمثابة مخزن لأهم المعلومات المتعلقة بالأفراد لقدرته على تخزين أكبر قدر ممكن من المعلومات، وهذا ما جعل للحاسب الآلي دورًا في تسهيل الحصول على هذه المعلومات عن طريق الغير بإفشائها لتحقيق مصالح مختلفة. ومثاله أن يقوم شخص يعمل بالنظام المعلوماتي بإعداد ملف يحتوي على معلومات تخص شخص آخر بدون علمه، أو أن يجمع المعلومات بعلم الشخص المعني ولكن يقوم المكلف بحفظها بإطلاع الغير عليها دون إذن صاحبها، أو أن يقوم شخص باختراق معلومات هي بمثابة أسرار مكتوبة وسير ذاتية ومذكرات شخصية لشخص آخر.

ثالثًا: الجريمة السيبرانية الواقعة على النظم المعلوماتية الأخرى

تتحقق هذه الجريمة بالولوج المادي من جانب الشخص في مركز المعالجة المعلوماتية، أو استخدام أداة إلكترونية معينة تسمح بالتقاط المعلومات والتنصت عليها لدى النظم المعلوماتية الأخرى، بالإضافة إلى إساءة استخدام البطاقة الائتمانية. بالنسبة للحالة الأولى المتمثلة في الولوج المادي في مركز المعالجة المعلوماتية، حيث يستطيع الجاني هنا الاستيلاء على المعلومات المخزنة لدى النظام المعلوماتي بعدة طرق باستخدام آلة الطباعة، أو استخدام شاشة النظام، أو الاطلاع على المعلومات بما هو مكتوب عليها، أو باستخدام مكبر الصوت. أما الحالة الثانية فتكون في حالة إساءة استخدام العميل البطاقة الائتمانية، وذلك عن طريق عدم احترام العميل المصدر إليه البطاقة الائتمانية لشروط العقد المبرم بينه وبين البنك، كاستعماله بطاقة ائتمانية انتهت مدة صلاحيتها أو تم إلغاؤها. أما

الحالة الثالثة كما في حالة قيام سارق باستعمال بطاقة ائتمانية للحصول على السلع والخدمات[1].

رابعًا: الجريمة السيبرانية الواقعة على الأسرار

تقوم هذه الجريمة باستعمال النظام المعلوماتي لإفشاء الأسرار، سواء كانت الأسرار عامة أو أسرار خاصة تتعلق بالأفراد أو المؤسسات المختلفة. ويتخذ هذا النوع من الجرائم صورتين: الأولى تتعلق بالجرائم الواقعة على أسرار الدولة [2]، حيث أتاح الإنترنت للكثير من الدول ممارسة التجسس على دول أخرى، وذلك بالاطلاع على أسرارها العسكرية والاقتصادية، خاصة فيما يتعلق بالدول التي يكون فيها نزاعات. والثانية تتعلق بجرائم الواقعة على الأسرار المهنية، والهدف من ارتكاب هذه الجريمة هو سرقة معلومات قصد التشهير بشخص أو بجماعة معينة أو بيع هذه المعلومات لتحقيق مصالح مختلفة، كالحصول على عائد مادي ممن يهمه الأمر أو استخدامها للضغط على أصحابها من أجل القيام بعمل أو الامتناع عن القيام بعمل [3].

وقد حرص المشرع الجزائري على حماية هذه الأسرار من خلال الباب الأول المتعلق بالجنح ضد الشيء العمومي من المادة 61 إلى المادة 96 مكرر من قانون العقوبات، بالإضافة إلى المادة 394 مكرر 03 التي تنص على: "تضاعف العقوبات المنصوص عليها في هذا القسم إذا استهدفت الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون إخلال بتطبيق عقوبات أشد [4]

خامسًا: الجريمة السيبرانية الواقعة على النظام المعلوماتي.

[1] سفيان سوير, مرجع سابق, ص35-37.

[2] سفيان سوير, مرجع سابق, ص38.

[3] سفيان سوير, مرجع سابق, ص38.

[4] الامر 04-15 ،القانون الصادر في 10 نوفمبر 2010، يعدلويتمم الامر رقم 156/66 ،الصادر في 08 جوان 1966 ،المتمم لقانون العقوبات، ج ر العدد 71

من أجل سدّ الفراغ الذي عرفّه التشريع الجزائري في هذا المجال، جاء القانون رقم 04/15 الصادر في 10 نوفمبر 2004، المتضمن قانون العقوبات، بتجريم كل أنواع الاعتداءات التي تستهدف أنظمة المعالجة الآلية للبيانات. وقد ورد النص على هذه الجرائم في القسم السابع مكرر من قانون العقوبات، تحت عنوان "المساس بأنظمة المعالجة الآلية للبيانات"، وذلك في المواد 394 مكرر إلى 394 مكرر 07. وتأخذ صور الاعتداء صورتين هما: الدخول والبقاء في منظومة معلوماتية، والمساس بمنظومة معلوماتية، كما تضمن صورًا أخرى للغش، وهذا ما سأتناوله فيما يلي.

أولًا: جريمتي الدخول والبقاء غير المشروعان في منظومة معلوماتية

تنص المادة 394 مكرر من قانون العقوبات السابق الذكر على معاقبة كل شخص يدخل أو يبقى بواسطة استعمال الغش في كل أو جزء من منظومة للمعالجة الآلية للبيانات أو يحاول ذلك، وإذا نتج عن هذا الدخول أو البقاء تخريب في النظام المعلوماتي فإن العقوبة تضاعف. فالصورة البسيطة للجريمة تتمثل في مجرد الدخول أو البقاء، بينما الصورة المشددة تتحقق في الحالة التي ينتج فيها عن هذا الدخول أو البقاء غير المشروع إما محو أو تغيير في البيانات الموجودة في النظام[1].

- **فعل الدخول غير المشروع:**

لا نعني هنا الدخول بالمعنى المادي، أي الدخول إلى مكان معين كمنزل أو غيره، وإنما ينظر إليه كظاهرة معنوية تشابه تلك التي نعرفها عندما نقول الدخول إلى فكرة أو إلى ملكية التفكير لدى الإنسان، أي الدخول إلى العمليات

[1] حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية تخصص 1 علم الإجرام والعقاب، جامعة باتنة، 2011–2012 ،ص 13

الذهنية التي يقوم بها نظام المعالجة الآلية للبيانات. وتقع هذه الجريمة من كل إنسان أياً كانت صفته، سواء كان شخصًا يعمل في مجال المعلوماتية أو لا يعمل، وسواء كان يستطيع أن يستفيد من الدخول أم لا، يكفي أن يكون الجاني ممن ليس له الحق في الدخول إلى النظام أو من الذين ليس لهم الحق في الدخول بالطريقة التي دخلوا بها. كما تقع الجريمة سواء تم الدخول إلى النظام كله أو إلى جزء منه فقط، أي أن الجريمة تقوم بالفعل الدخول إلى النظام مجردًا عن أي نتيجة أخرى، ولا يشترط لقيامها التقاط أو حصول الشخص على المعلومات الموجودة داخل النظام أو بعضها، بل إن الجريمة تتوافر حتى ولو لم تكن لدى الجاني القدرة الفنية على تنفيذ العمليات على النظام. ففعل الدخول يتسع ليشمل كل فنيات الدخول الاحتيالي في منظومة محمية كانت أو غير محمية، كما تشمل استعمال من لا حق له في ذلك المفتاح للدخول إلى المنظومة.

- **فعل البقاء غير المشروع:**

يقصد بفعل البقاء التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام، وقد يتحقق فعل البقاء المعاقب عليه مستقلاً عن الدخول في النظام وقد يجتمعان، ويكون البقاء معاقباً عليه استقلالا حين يكون الدخول إلى النظام مشروعاً، ومن أمثلة ذلك إذا تحقق الدخول إلى النظام بالصدفة أو عن طريق الخطأ، وهنا يجب على المتدخل أن يقتطع وجوده داخل النظام و ينسحب، فإذا بقي رغم ذلك فإنه يعاقب على جريمة البقاء غير المشروع، ويكون البقاء جريمة في الحالة التي يطبع لشخص فيها نسخة من المعلومات في الوقت الذي كان مسموحاً له فيه الاطلاع فقط، ويتحقق ذلك أيضاً بالنسبة للخدمات المفتوحة للجمهور مثل الخدمات الهاتفية،

والتي يستطيع الجاني فيها الحصول على الخدمة دون أن يدفع المقابل الواجب دفعه أو يحصل على مدة أطول من المدة التي دفع مقابلها، فعل البقاء يشمل البقاء بعد الدخول الشرعي أكثر من الوقت المحدد، وذلك بغية عدم الدفع، كما تقوم الجريمة سواء حصل الدخول مباشرة على الحاسوب أو حصل عن بعد، كما يحرم البقاء حتى لو حصل الدخول بصفة عرضية.[1]

سادساً: جريمة المساس بمنظومة معلوماتية:

نصت المادة 394 مكرر 01 من قانون العقوبات رقم 04 بمعاقبة كل شخص قام بإدخال معطيات في نظام المعالجة الآلية، أو أزال أو عدل هذه المعطيات وذلك عن طريق استعمال الغش. هذا السلوك الإجرامي يتجسد في ثلاث صور هي الإدخال، المحو، التعديل، كما أن المشرع لم يشترط اجتماع هذه الصور بل يكفي أن يصدر عن الجاني إحداهما فقط لكي يتوافر الركن المادي، وأفعال الإدخال والإزالة والتعديل تنطوي على التلاعب في المعطيات التي يحتويها نظام المعالجة الآلية للمعطيات، سواء بإضافة معطيات جديدة غير صحيحة، أو محو أو تعديل معطيات موجودة من قبل، كما أن هذا السلوك يجسد فعل التخريب وإفساد المعطيات التي يتضمنها نظام المعالجة الآلية، مثال ذلك إدخال فيروس معلوماتي في البرامج من أجل إتلافها

سابعاً: أفعال إجرامية أخرى:

جرمت المادة 394 مكرر 02 من قانون العقوبات السابق الذكر الأعمال الآتية: تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية، يمكن أن ترتكب بها إحدى

[1] حمزة بن عقون، المرجع السابق، ص 183وما بعدها .

جرائم الغش المعلوماتي السابقة الذكر [1]، ويقصد بتصميم المعطيات هنا الفيروسات المعلوماتية، البرامج القرصنة التي يمكن أن تستعمل في ارتكاب جرائم معلوماتية إما ضد

عليه نتيجة إجرامية تربطها بالسلوك الإجرامي ربطة سببية مادية، بمعنى أن الركن المادي يتكون من الأنظمة المعلوماتية، أو المعطيات المعلوماتية في حد ذاتها. كما جرم المشرع كذلك أفعال الحيازة أو الإفشاء أو نشر أو استعمال المعطيات المتحصلة من إحدى جرائم الغش المعلوماتي لأي غرض.

الفرع الثاني: أركان الجريمة السيبرانية.

لا تختلف أركان الجريمة السيبرانية عن أركان أي جريمة أخرى فلابد من توافر الركن المادي والركن المعنوي وما يميزه هو الركن المفترض وهذا ما نستعرضه في هذا الفرع وهو كالتالي :

أولا: الركن المادي

يعرف بأنه: "النشاط المادي الذي يصدر عن الجاني متخذا مظاهر خارجية يتدخل من أجله القانون بتقرير العقاب". ويتمثل الركن المادي للجريمة في سلوك إرادي يترتب ثلاث عناصر.

[1] حمزة بن عقون، المرجع السابق، ص184.

1-السلوك الإجرامي:

هو صورة متعددة كالسلوك الإجرامي الإيجابي وذلك بمخالفته نصاً ينهي ع الإتيان بهذا الفعل كسرقة بيت أو جهاز معين، سواء كان التحرك الإيجابي بحركة واحدة كالقتل بالرصاص، أو بحركات متعددة كالمشاجرة التي تنتهي بالوفاة.

وقد يكون سلبياً بمخالفة نص يأمر بإتيان فعل معين، كإمتناع ممرضة عن إعطاء جرعة الدواء لمريضها العاجز بما يؤدي لوفاته. وقد يكون السلوك الإجرامي بصورة بسيطة كما في جريمة القذف، وقد تكون بصورة معقدة كما في جريمة الإرهاب أو السطو المسلح، فالقانون الجنائي لا يعول كثيراً على الوسيلة التي ارتكبت بها الجريمة أو وقع بها السلوك الإجرامي، ولا يعتد بزمان أو مكان وقوع الجريمة إلا عند تقديره للظروف المشددة أو المخففة، فيستوي القتل أن يكون بمسدس أو بالسكين، أو حتى عن طريق الريموت كنترول أو بواسطة أجهزة الحاسوب.

فأهمية هذه الصور المجرمة والظروف المصاحبة لها تظهر مدى توافر القصد الجنائي، كما تفيد تحديد الاختصاص القضائي، والقانون واجب التطبيق، وبدء سريان مدة التقادم في الأنظمة المقارنة[1]

.كما يمكن تقسيم وتكييف الجرائم بنفس تقسيم الجرائم التقليدية، وذلك حين تتشابه معها في ذات السلوك الإجرامي

2- النتيجة الإجرامية

[1] روان بنت عطيةالله الصحفي، الجرائم السيبرانية، المجلة الالكترونية الشاملة متعددة التخصصات، العدد 24 ،شهر 5 1 سنة 2020 ،ص 21وما بعدها.

وتثير مسألة النتيجة الإجرامية في الجرائم السيبرانية جدلاً كبيراً بين أنصار المذهب المادي وأنصار المذهب القانوني حول تحديد الجريمة السيبرانية: هل هي جرائم مُرتكبة سلوكاً أو نتيجةً في العالم الافتراضي، أم أن هناك امتداداً للنتيجة لتحقيق وجودها المادي؟ وتنقسم النتيجة الإجرامية إلى قسمين :

-جرائم الضرر: هي التي يطلب القانون في ركنها المادي حصول ضرر معين، وذلك مثل حصول الضرر في الجرائم السلبية والإيجابية .

-جرائم الخطر :فهي جرائم السلوك المجرد حتى لو لم تقع النتيجة الإجرامية، وكذلك كما في جرائم الشروع، والتي تعاقب عليها الأنظمة في حالة كونها جناية، وذلك لما يمثله السلوك الإجرامي من خطر دون النظر في نتيجة ذلك الفعل، بينما يختلف الأمر في الجنح والمخالفات فلا يعاقب عليها القانون بصفة عامة نظراً لقلة خطورة الدافع الإجرامي في نفس الفاعل[1]

3-**علاقة السببية** لم يحدد القانون الجنائي معياراً لتحديد الرابطة السببية، فناقش علماء القانون واستقر رأيهم على ثلاث نظريات:

-نظرية تعادل الأسباب: وهي تساوي جميع العوامل التي تساهم في إحداث النتيجة الإجرامية، فهي متعادلة من حيث قوة أثرها في حصول النتيجة .

-نظرية السبب الأقوى أو السبب المباشر: فهي لا تساوي بين الأسباب المساهمة في حصول الجريمة، بل تنظر إلى السبب الأقوى سواء كان هو سلوك الجاني أو غيره، وهذه النظرية حصرت النتيجة في عامل واحد هو أقوى الأسباب، وهذا يؤدي بالجاني إلى الإفلات من العقاب.

[1] روان بنت عطيق الصحفي ، المرجع السابق ، ص23 وما بعدها.

-نظرية السببية الملائمة: ومضمونها أن الجاني يُسأل عن النتائج المحتملة أو المتوقعة لفعله وذلك حسب المجرى العادي للأمور، ما لم يتدخل لقطع تلك العلاقة سبب شاذ أو غير مألوف، وقد تكون هذه النظرية هي أنسب النظريات. (فلو أرسل الجاني فيروساً إلى بريد المجني عليه الإلكتروني مما تسبب في تلف الجهاز بالكامل لدى فتح المجني عليه بريده الإلكتروني، فهذا سبب مباشر يُسأل الجاني عنه، بينما لو كان المجني عليه قد أُرسلت له عدة فيروسات من عدة أشخاص وتسببت بمجموعها بتلف الجهاز، فإن القضاء حينئذٍ يعمل بإحدى النظريات السابقة.[1]

ثانياً: الركن المعنوي

إن الركن المعنوي في الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات يتخذ صورة القصد الجنائي:

1-الركن المعنوي بالنسبة للدخول والبقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات:

إن الركن المعنوي لجريمة الدخول والبقاء غير المشروعين، يتخذ صورة القصد الجنائي من علم وإرادة باعتبارها من الجرائم العمدية، وقد عبر نص المادة 394 مكرر عن القصد الجنائي العام بتطلبه أن يكون الدخول أو البقاء "عن طريق الغش"، فاستخدام هذه العبارة يعني أن الفاعل على علم بأن دخوله أو بقاءه في نظام المعالجة الآلية للمعطيات غير مشروع، وهو نفس ما عبر عنه المشرع الفرنسي في نص المادة32.

[1] روان بنت عطيق الصحفي ، المرجع السابق ، ص24 و25.

يتطلب القصد العام أن يحيط علم الجاني بكل واقعة ذات أهمية قانونية في تكوين الجريمة، وبناء أركانها، واستكمال عناصرها، وخاصة الركن المادي منها، وأول هذه العناصر هو موضوع الحق المعتدى عليه، فيتعين توافر علم الجاني بأن فعله ينصب على نظام المعالجة الآلية للمعطيات بما يتضمنه من معلومات وبرامج، باعتباره محل الحق الذي يحميه المشرع، فإذا اعتقد الفاعل بناءً على أسباب معقولة بأنه يقوم على سبيل المثال بإجراء بعض العمليات الحسابية عن طريق الحاسب الآلي، دون أن يتجه علمه إلى أنه يقوم بالدخول أو البقاء في نظام المعالجة الآلية للمعطيات، فإن قصد الدخول أو البقاء لا يتوفر فيه.[1]

كذلك يتعين أن يعلم بخطورة الفعل الذي يقوم به، فإذا كان غير ذلك ينتفي القصد الجنائي. يتطلب القصد الجنائي أيضاً أن يتوقع الجاني النتيجة الإجرامية التي ستترتب عن القيام بفعله، فتوقع النتيجة هو أساس النية التي تقوم عليها إرادتها، فحيث لا يكون التوقع لا نتصور الإرادة، والنتيجة التي يجب أن يتجه إليها توقع الفاعل هي النتيجة التي يحددها القانون، وهي الدخول والبقاء غير المشروع لنظام المعالجة الآلية للمعطيات.

ولا يشترط أن يتوقع الضرر الذي سوف يلحق بالنظام أو صاحبه من جراء هذا الدخول[2]، فإذا توقع الفاعل أنه بصدد الدخول إلى نظام معين، ثم ترتب على فعله الدخول إلى نظام آخر، فإن القصد الجنائي يظل متوافرًا لديه .

وهناك وقائع يُسأل فيها الجاني عن الجريمة دون أن يتطلب القانون علمه بها، فحين يقرر القانون لبعض الجرائم عقاباً معيناً إذا أحدث الفعل نتيجة ذات جسامة

[1] نائلة عادل محمد فريد قورة،جرائم الحاسب الآلي الاقتصادية، الطبعة الأولى، منشورات الحلبي الحقوقية، سنة 2005،بيروت, ص365.

[2] نائلة عادل, مرجع سابق, ص366.

معنوية، وإذا ازدادت جسامة هذه النتيجة فأفضت إلى نتيجة أشد جسامة، شدد القانون العقاب، ويتطلب المشرع انصراف القصد الجنائي إلى النتيجة الأقل جسامة ولكنه لا يتطلب انصرافه إلى النتيجة الأشد جسامة، بحيث يُسأل الجاني عنها بالرغم من عدم توقعه له.[1]

وهذا ما ينطبق على الفقرة الثانية والثالثة من المادة 394 مكرر من قانون العقوبات، حيث يعاقب الجاني على النتيجة الأشد بمجرد ترتبها عن الدخول أو البقاء غير المشروع الذي قصده.

ويجب أن يعلم مرتكب جريمة الدخول أو البقاء غير المشروعين داخل أنظمة المعالجة الآلية للمعطيات، أن دخوله إلى هذا النظام غير مشروع أو غير مصرح به، فلا يتوافر القصد الجنائي إذا وقع الجاني في خطأ، كأن يجهل وجود حظر للدخول أو البقاء، أو كان يعتقد خطأً أنه مسموح له بالدخول أو البقاء .

أما بالنسبة لإرادة الجاني فيجب أن تتجه إلى الدخول أو البقاء غير المشروع داخل النظام، أي أن تتجه إرادته لتحقيق هذه النتيجة، ولا عبرة بعد ذلك للباعث أو الغاية من وراء هذا الدخول أو البقاء سواء كان هذا الباعث هو الفضول، أو إثبات القدرة على المهارة والانتصار على النظام، حتى وإن كانت الغاية نبيلة كمن يدخل إلى النظام غير المصرح له بالدخول رغبةً في الكشف عن أوجه القصور التي تعتري النظام الذي تمكن من الدخول إليه, وذلك لتجنب هذا القصور مستقبلا.[2]

[1] ناطلة عادل, مرجع سابق, ص367.

[2] ناطلة عادل, مرجع سابق, ص368.

2: الركن المعنوي للاعتداءات على سير نظام المعالجة الآلية للمعطيات والاعتداءات على المعطيات خارج وداخل النظام:

إن الاعتداءات على سير نظام المعالجة الآلية للمعطيات بصورتيها التعطيل أو العرقلة، وإفساد النظام، لا تكون إلا عمدية، هذا ما يميزها عن الاعتداء غير العمدي لسير النظام الذي يشكل ظرفاً مشدداً لجريمة الدخول والبقاء غير المشروعين داخل النظام[1].

وهذه الاعتداءات تتطلب القصد الجنائي العام من علم وإرادة، شأنها شأن الاعتداءات العمدية على المعطيات، فيجب أن يعلم الفاعل بأنه يقوم بإحدى هذه الأعمال التي أوردها النص القانوني، والتي من شأنها إتلاف المعلومات، فيعلم بأنه يقوم بفعل الإدخال أو المحو أو التعديل، ويعلم بخطورة النشاط الإجرامي الذي يقوم به وما يترتب عنه من عقاب.

كما يجب أن تتجه إرادة الفاعل إلى فعل الإدخال أو المحو أو التعديل، فلا يسأل من قام بذلك خطأً أو عن غير قصد، بل يسأل طبقاً للمادة 394 مكرر 2 المشددة لجريمة الدخول أو البقاء غير المشروعين في نظام المعالجة الآلية للمعطيات، كونها تعاقب الفاعل عن الحذف والتغيير المترتب عن الدخول أو البقاء غير المشروعين حتى وإن كان خطأً، كون أن نص المادة 394 مكرر 1 من قانون العقوبات اشترط أن ترتكب هذه الأفعال "بطريق الغش"

وهي العبارة المستعملة كذلك في نص المادة 323 من قانون العقوبات الفرنسي.أي أن يعلم أنه ليس له الحق في القيام بذلك، وأنه يعتدي على صاحب الحق في السيطرة على تلك المعطيات دون موافقته. ولا يتطلب نص المادة 394

[1] امال قارة،الحماية الجزائية للمعلوماتية في التشريع الجزائري، الطبعة الأولى، دار هومة الجزائر ، ص 124 .

مكرر 1 قصداً جنائياً خاصاً، إذ لا يوجد فيه ما يشير إلى ذلك، عكس بعض التشريعات المقارنة التي اشترطت قصداً خاصاً إلى جانب القصد العام، يتمثل في اتجاه نية المتهم إلى الإضرار بالغير أو إلى تحقيق ربح غير مشروع له أو للغير، وهو ما كان عليه النص الفرنسي القديم قبل تعديله، ويبرز ذلك في عبارة "ارتكاب الفعل دون مراعاة حقوق الآخرين."

وقد انتقدت هذه المادة قبل تعديلها بشدة لتطلبها القصد الجنائي الخاص، كون أن اشتراط هذا القصد الخاص سوف يؤدي إلى الإعفاء من العقاب في الحالات التي لا تتجه فيها نية الفاعل إلى تحقيق ربح، على الرغم من أهمية المعلومات التي قد يتم إتلافها، مثل إتلاف معلومات علمية[1].

وهو ما دعا المشرع الفرنسي إلى استبعاد القصد الخاص من هذه الاعتداءات، حيث اقتبس المشرع الجزائري نص المادة 394 مكرر 1 من نص المادة 323 المعدلة من قانون العقوبات الفرنسي.

أما بالنسبة للاعتداءات العمدية الماسة بالمعطيات الموجودة خارج النظام، فيجب لقيام الركن المعنوي أن يتوافر القصد الجنائي العام، وهو ما عبرت عنه المادة 294 مكرر بعبارة "كل من يقوم عمداً وعن طريق الغش ".

بالتالي يجب توافر العلم والإرادة لدى الجاني لقيام الركن المعنوي، فيجب أن يكون عالماً أن المعطيات المخزنة أو المعالجة أو المرسلة عن طريق منظومة معلوماتية، يمكن أن ترتكب بها إحدى الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات، وذلك بتصميمه أو بحثه أو جمعه أو توفيره أو نشره أو الاتجار في

[1] ناطلة عادل, مرجع سابق, ص368.

هذه المعطيات، أي علمه بأن هذه المعطيات يمكن أن تكون وسيلة لارتكاب الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات.

ويجب أن يعلم الجاني كذلك، أن إتيانه أحد الأفعال السابقة ينصب على معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية، وكذلك أن يعلم بخطورة الفعل الذي يقوم به، وأن يتوقع النتيجة المترتبة عن القيام بأحد الأفعال السابقة.

ثالثا:الركن المفترض

يُعدّ نظام المعالجة الآلية للبيانات الركن الأساسي في الجرائم المرتكبة ضده، فوجوده شرطٌ لا بد منه للبحث عن توافر أركان الجريمة .يُؤدي توافر هذا الشرط إلى الانتقال للمرحلة التالية من التحقيق .لذا، من الضروري تعريف نظام المعالجة الآلية للبيانات ومدى خضوعه للحماية الفنية.

1-**تعريف نظام المعالجة الآلية للبيانات** :يُعرف هذا النظام بتعريف تقني متطور، يخضع لتغيرات سريعة ومتلاحقة في مجال الحاسوب. لم يُعرّفه المشرّع الجزائري تحديداً، مُوكلاً مهمة تعريفه للفقه والقضاء .قدّمت المادة الأولى من الاتفاقية الدولية لمكافحة الجريمة المعلوماتية تعريفاً "لمنظومة الكمبيوتر" على النحو التالي:[1]

"قصد بمنظومة الكومبيوترأي جهاز أو مجموعة أجهزة متصلة ببعضها البعض أو ذات صلة بذلك، ويقوم واحد أو أكثر منها، تبعاً للبرنامج، بعمل معالجة آلية للبيانات ."أما "بيانات الكمبيوتر" فهي "أي عملية عرض للوقائع أو المعلومات أو

[1] امال قارة, مرجع سابق,ص102.

المفاهيم في شكل مناسب لعملية المعالجة داخل منظومة الكمبيوتر، بما في ذلك البرنامج المناسب لجعل منظومة الكمبيوتر تؤدي وظائفها."

أما الفقه الفرنسي، فقد عرّفه من خلال الأعمال التحضيرية للمادة 323 من قانون العقوبات الفرنسي، مُتبنياً التعريف الوارد في قانون المعلومات وحماية الحريات لعام 1978، بأنه "كل مركب من وحدة أو مجموعة وحدات للمعالجة، تتكون كل منها من الذاكرة والبرمجيات والبيانات وأجهزة الإدخال والإخراج، وأجهزة الربط التي تربط بين العناصر المختلفة للنظام، كالشاشة ولوحة المفاتيح والطابعة والبطاقات المغناطيسية التي تشكل وسيلة للدخول، والتي تربط بينها مجموعة من العلاقات التي عن طريقها تتحقق نتيجة معينة، وهي معالجة البيانات، على أن يكون هذا المركب خاضعاً لنظام الحماية الفني[1]."

هذه العناصر المادية والمعنوية مذكورة على سبيل المثال لا الحصر، ويمكن إضافة عناصر جديدة أو حذف بعضها حسب التطور التقني .فإذا تم الاعتداء على أحد هذه العناصر بمعزل عن النظام، فلا تقوم الجريمة، بل لا بد من الاتصال بينها.

يُعتبر نظام المعالجة الآلية للبيانات قيد التشغيل عند إرسال إشارة كهربائية نحو وحدة المعالجة المركزية، التي تقوم بدورها بإرسال البرنامج المسؤول عن تشغيل ذاكرة القراءة، وهذه الأخيرة تبحث عن البيانات التي تسمح بتشغيل النظام المسؤول عن البحث، ثم تسجلها في ذاكرة القراءة والكتابة التي تتابع المراحل اللاحقة[2] .

[1] ناطلة عادل, مرجع سابق, ص131.

[2] ناطلة عادل, مرجع سابق, ص131.

2- الحماية الفنية لأنظمة المعالجة الآلية للبيانات :تكفل بعض القواعد الأمنية حماية أنظمة المعالجة الآلية للبيانات، كوضع عوائق تحول دون التقاط الموجات الكهربائية المنبعثة من الأجهزة المختلفة، والتي يمكن عن طريقها معرفة محتوى المعلومات التي يتم نقلها .ويتأتى ذلك عن طريق حماية الكابلات والوصلات الكهربائية لارتباطها بالأجهزة .ومن بين هذه القواعد، أسلوب يعتمد على توزيع العمليات التي يقوم بها نظام المعالجة الآلية للبيانات ونقلها إلى نظام احتياطي (مركز للمساعدة) عند الضرورة، وهو أسلوب تلجأ إليه عادة البنوك وشركات التأمين، ويظل هذا الموقع سرياً ويخضع لدرجة عالية من الحماية .ومن الأساليب المستعملة أيضاً، الاعتماد على الاختبارات الفسيولوجية للدخول إلى النظام عن طريق التحقق من شخصية القائم بعملية الدخول عن طريق بصمة الإصبع أو نبرة الصوت أو شكل الأذن أو شبكية العين.[1]

لكن يبقى نظام التشفير لحماية المعلومات هو الأسلوب الأكثر انتشاراً، خاصة البيانات المتناقلة عبر الشبكات، كشبكات الإنترنت، لما تنطوي عليه من سرية البيانات الشخصية كرسائل البريد الإلكتروني، وكذلك البيانات الخاصة بالأعمال التجارية الرقمية[2].

يقوم نظام التشفير على تحويل المعلومات والبيانات إلى شكل رمزي غير مفهوم بدون مفتاح لحل رموزه، يعرفه عادةً مرسل المعلومات والمرسل إليه .داخل جهاز الكمبيوتر توجد أجهزة مهمتها التحقق من شخصية القائم بعملية الدخول عن طريق الشفرة.

[1] نائلة عادل, مرجع سابق, ص353

[2] امال قارة, مرجع سابق,ص103.

وقد ثار تساؤل حول ضرورة وجود أو عدم وجود حماية للنظام كشرط للتمتع بالحماية الجنائية؟ .و بالرجوع إلى نص المادة 394 مكرر [1] من قانون العقوبات، لا نجد إشارة إلى ضرورة خضوع النظام للحماية الفنية ليتمتع بالحماية الجنائية، وكذلك الحال بالنسبة للمادة 323-1 من قانون العقوبات الفرنسي .يظهر من خلال الأعمال التحضيرية لقانون 1988 المتعلق بالمعلوماتية والمقتبسة منه المادة 323، أنه كان من المقترح ضرورة شمول النص بهذا الشرط، ولكن اشتراط وجود حماية أمنية في نظام المعالجة الآلية للبيانات لم يتم الاتفاق عليه في المناقشات الأخيرة في البرلمان الفرنسي، ولذلك جاء النص خالياً من هذا الشرط .وُجد أن هذا الشرط قد يؤدي إلى الحد من الحماية الجنائية للأنظمة غير المشمولة بتجهيزات أمنية داخل النظام.

لذلك اكتفى المشرع الفرنسي في النص النهائي بأن يكون التوصل قد تم "بطريقة الغش"، وهذا التعبير يترك تفسيره لقاضي الموضوع[2].

وهذا ما فتح أبواب النقاش حول هذه النقطة من خلال ظهور آراء مختلفة :

الرأي الأول: يقول بعدم جدارة الأنظمة التي لا تحميها نظم أمنية بالحماية الجنائية، كون أنه من غير المعقول حماية معلومات هامة تركها المسؤولون عنها دون أي إجراءات تتكفل لها الحماية. ويقيس أنصار هذا الرأي جريمة الدخول غير المشروع في أنظمة المعالجة الآلية، التي تنص المادة 394 مكرر من قانون العقوبات: "يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50000 دج إلى

[1] تنص المادة 394مكرر من قانون العقوبات":يعاقب بالحبس من ثلاثة أشهر الى سنة وبغرامة من 50000 دج الى 100000دج لكل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك"

[2] صلاح سالم، تكنولوجيا المعلومات والاتصالات والأمن القومي للمجتمع، الطبعة الأولى،عين للدراسات والبحوث الانسانية والاجتماعية ، القاهرة ، 2003 ،ص117.

100000 دج لكل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك ."ويشبهون جريمة الدخول غير المشروع للمعطيات على جريمة انتهاك حرمة المنزل، حيث لا تقوم الجريمة لمجرد أن الدخول إلى المسكن قد تم بدون رضا صاحبه، كترك مسكنه دون حماية بسبب عدم وجود أقفال أو أبواب أو نوافذ، فيجب أن يكون الدخول مصحوباً باستعمال وسائل تدل على عدم رضا صاحب المسكن. ويستند أنصار هذا الرأي إلى عدة أسباب تنصب جميعها في اتجاه واحد هو ضرورة أن يكون هناك نظم أمنية يتم اختراقها لامتياز الحماية الجزائية للمعلومات، وأول هذه الأسباب يتعلق بالمادة 28 من القانون 78-07 لسنة 1978 الخاص بالمعلوماتية وحماية الحريات الفرنسي، حيث تتطلب أن تكون الأنظمة مشمولة بتدابير أمنية لحمايتها، والسبب الثاني يكمن في إقامة الدليل على قيام الركن المادي للجريمة وكذا التحقق من توافر القصد الجنائي لدى مرتكبها، لأن اختراق الأنظمة الأمنية من طرف الفاعل يترك آثاراً، ويؤكد طريق الغش والاحتيال الذي سلكه.

الرأي الثاني: فهو يذهب إلى أنه ينبغي حماية أنظمة المعالجة الآلية للمعطيات جزائياً بغض النظر إن كانت تتمتع بحماية النظم الأمنية من عدمه. ويقيس أنصار هذا الاتجاه جريمة الدخول غير المشروع على جريمة السرقة، حيث أن تمتع المال المسروق بحماية صاحبه أو عدم تمتعه بهذه الحماية لا يؤثر في قيام جريمة السرقة، بغض النظر عن مقدار الصعوبة التي واجهت الجاني في تنفيذها، كما أن طلب مثل هذا الشرط يضيق من تطبيق الحماية الجزائية،

ويتجاهل الحالات التي يتم فيها الدخول إلى النظام نتيجة خطأ قام به المبرمجون، أو المسؤولون عن أمن النظام[1].

هذا الرأي هو الأقرب إلى الصواب استناداً إلى المبادئ العامة المستقرة في القانون الجنائي كحرفية النص، وعدم جواز تقييد النص المطلق أو تخصيص النص العام، إلا إذا وجد نص يجيز ذلك، ولا يوجد في حالتنا نص خاص يقيد إطلاق النص أو يخصص عمومه، وبالتالي يجب الالتزام حرفية النص في التفسير، فعدم ذكر المشرع لشرط الحماية الفنية يعني أن المشرع أراد استبعاده.[2]

وأكدت محكمة استئناف باريس في حكم صادر لها في 1994/05/04 أنه من غير الضروري لقيام جريمة الدخول غير المصرح به أن يكون فعل الدخول قد تم بمخالفة التدابير الأمنية، وأنه يكفي أن يكون هذا الدخول قد تم ضد إرادة المسؤول عن النظام.

[1] نائلة عادل, مرجع سابق, ص355.

[2] امال قارة, مرجع سابق,ص105.

المبحث الثاني: الأمن السيبراني بين الابعاد والتهديدات السيبرانية

إن للأمن السيبراني أهمية كبيرة في المحافظة والحماية من المقيدات السيبرانية التي باتت خطرا يداهم الجميع ولهذه الأهمية أبعاد شتى للأمن السيبراني سنتطرق إليها في المطلب الاول وفي المطلب الثاني التهديدات السيبرانية.

المطلب الاول: أبعاد الأمن السيبراني

سيتم في هذا المطلب التطرق الى أبرز ابعاد الأمن السيبراني ويشمل العديد من و ابعاد سيتم ذكرها كالتالي :

الفرع اول: الأبعاد القانونية والسياسية والعسكرية للأمن السيبراني

أولا : البعد القانوني :

يترتب على النشاط الفردي والمؤسساتي والدعم هي في الفضاء السيبراني نتائج قانونية وموجبات ستدعي اهتماما خاصا لحل النزاعات التي يمكن أن تنشأ عنها، وهو ما يستدعى مواكبة التحولات التي رافقت امور مجتمع المعلومات فظهرت حقوق أخرى كحق النفاذ إلى الشركة العالمية للمعلومات وتوسعت بعض المفاهيم لتشمل أساليب الممارسة الجديد نه باستخدام تقنيات المعلومات و اتصالات الحقفي انشاء المدونات الكترونية و والحق ف ي انشاء التجمعات على الانترنت والحق في حماية ملكية البرامج المعلوماتية[1]

[1]– سمير بارة, الامن السيبراني في الجزائر السياسات والمؤسسات, المجلة الجزائرية للأمن الإنساني,المجلد 2، العدد04 ، 2017 – صفحة 263 .

ثانيا: البعد السياسي :

هناك أمثلة كثيرة تدفع الاهتمام بالبعد السياسي للأمن السيبراني ، كالتسريبات المختلفة للوثائق الحساسة ، التي تؤدي إلى مشكلات عويصة جدا، على المستوى الخارجي والدولي، كما أنه لا يذكر أحد الدور ا امته لشبكات التواصل الاجتماعي على المستوى السياسي لحملات انتخابية تظاهرات افتراضية، حركات احتجاجية الكترونية ، كما يتم استغلال هذه المواقع من طرف العديد من الحكومات التقرير سياساتها وفي سياق آخر يجب أن لا نغفل عن استخدام ا هذه المواقع من طرف الحركات الارهابية لتجنيد أفرادها وجمع التمويل لعملياتها ، وآلية للاتصال بينها كأفراد وكجماعات وهو ماستوجب على الدول العمل على حماية امنها من التهديدات و المخاطر التي قد تتعرض لها من خلال شبكة الانترنت.[1]

ثالثا : البعد العسكري

تكمن الميزة النسبية للقوة السيبرانية في قدرتها على ربط الوحدات العسكرية ببعضها البعض عبر الشبكات العسكرية في الفضاء الإلكتروني، وإيصال الأوامر العسكرية والقدرة على إيصال الأهداف عن بعد وتدميرها. وقد تتحول هذه الميزة إلى نقطة ضعف لا قوة إن لم تكن الشبكة الإلكترونية المستخدمة في ذلك مؤمنة جيدًا من أي اختراق خارجي قد يتسبب في تهديد الأمن العسكري للدول وتعطيل قدرة الدولة على النشر السريع لقدراتها وقواتها أو قطع أنظمة الاتصال بين الوحدات العسكرية وتعطيل الشبكات الكمبيوترية. كما يمكن أن يتمثل الخطر في

[1] محمد مختار،مرجعسابق،ص 07.

شل وتعطيل عمل أنظمة الدفاع الجوي أو التوجيه الإلكتروني، فضلاً عن إمكانية فقدان السيطرة على وحدات القيادة[1].

الفرع الثاني: الأبعاد الاجتماعية والاقتصادية للأمن السيبراني

أولاً: الأبعاد الاجتماعية

كل ما هو مطروح على المدونات وشبكات التواصل الاجتماعي يمثل مجالًا يسمح لكل مواطن أن يعبر بكل حرية ودون سابق إنذار عن تطلعاته السياسية وطموحاته الاجتماعية. كما يفتح المجال لكل شرائح المجتمع ومكوناته للمساهمة في إثراء وتطوير المجتمع من خلال فرص الاطلاع على الأفكار والمعلومات المختلفة، ومن خلال الانفتاح والتواصل مع مجتمعات أخرى مما يدفع لتأسيس آفاق للشراكة والتعاون لتبادل الخبرات والأفكار التي قد تفيد، مع الحاجة إلى الحفاظ على استقرار الفضاء السيبراني والمجتمع الذي يرتكز عليه.

يضاف إلى ذلك أن هذه الوسيلة في أبعادها لا تقف عند حدود توفير الاطمئنان للمواطن في حياته اليومية والاستفادة من طاقات تقنيات المعلومات والاتصالات لتطوير نشاطاته المختلفة، بل تسمح كذلك بتنمية الإمكانات والقدرات في المجالات العلمية والثقافية والخدماتية، ناهيك عن الدور الذي يمكن أن تؤديه في أوقات الأزمات الإنسانية والكوارث، خاصة وأن وجود آلية لتبادل المعلومات يعدل من تنظيم عمليات تقديم المساعدات في الوقت المناسب[2].

[1] إدريس عطية ,مكانة الامن السيبراني في منظومة الامن الوطني الجزائري,مجلة مصداقية, كلية الحقوق و العلوم السياسية , المجلد 09, العدد03, 2020 و ص 105.

[2] بوازدية جمال, الأمن السيبراني, محاضرات مقدمة لطلبة السنة الثانية ماستر, جامعة الجزائر3, كلية العلوم السياسية و العلاقات الدولية,2020-2021, ص 16.

ثانيا: الأبعاد اقتصادية:

لقد أصبح الفضاء الالكتروني جاذبا بالقطاعات المجتمع كافة وباتت المعرفة محرك الانتاج والنمو الاقتصادي، كما أيقن الجميع أن مبدأ التركيز على المعلومات والتكنولوجيا يعد عاملا من العوامل الاساسية للنهوض باقتصاد وهو ما دفع بالدول في الآونة الاخيرة تزيد من استثمارها في المعرفة، وأصبحت عصرنة اقتصاد مرتبطة بالتحكم في اقتصاد الرقمي من طرف مختلف الفاعلين الاقتصاديين والاجتماعيين.[1]

كما أنا استخدام الكومبيوتر و شبكة الانترنت في تطوير الصناعات وتكريك الاقتصاد، ومعالجة كل المعاملات الاقتصادية والمالية، زاد من أهمية ضرورة توفير الأمن السيبراني لضمان حماية هذه المعلومات فعلى سبيل المثال، يشير تقدير صادر من شركة Emgheten إلى حجم التجارة الالكترونية بلغ 1 ,5 تريليون دولار عام 2015 بزيادة نسبتها 20% مقارنة بعام 2013 الذي بلغت فيه1,2 تريليون دولار، و نظرا لارتفاع معدل الجرائم السيبرانية المنظمة والخطيرة ، فإن ذللا يمثل تهديدات صريحا لنمو اقتصاد الرقمي ، مالم تقم الدول بتعظيم معاير الأمن السيبراني مالم تقم الدول بتعظيم معاير الأمن السيبراني بما يضمن الحد من هده الجرائم.[2]

[1] أمال بوجليدة, الاقتصاد الرقمي التحول من الاقتصاد الصناعي الى اقتصاد المعلومات, مجلة الخبير, العدد63, جانفي 2016,ص 45-47.

[2] محمد مختار, مرجع سابق , ص 06.

المطلب الثاني: التهديدات السيبرانية

اصبحت التهديدات السيبرانيةاحدى التحديات الرئيسية التي يتحتم على الدول مواجهتها خلال الفترة الحالية ، ومع تزايد اعتماد على انترنت خاصة في المجالات التي تتعلق بالأمن القومي مثل الشركات العسكرية والبيانات المالية والمصرفية وتزايد الحديث عن أهمية مواجهة هذه التهديدات

وفي هذا الإطار سيتم التطرق إلى ماهية التهديدات السيبرانية التي يمكن تتعرض لها الدول، وسيتم توضيح ذلك فيما يلي:

الفرع الأول: مفهوم التهدياتالسيبرانية

اولا: تعريفها

هي تلك الهجمات والمخاطر اتي تتم باستخدام آليات وشبكات انترنت وأجهزة الحاسب الالي ، وتهدف إلى إلحاق الضرر باجهزة و الشركات الكترونية ذات الاتصال بالانترنت، حيث تتباين التهديدات السيرانية وتختلف منا دولة إلى أخرى بتطور وهيمنة التطور التكنولوجي .

و يمكن تعريفها بأنها فعل يقوض من قدرات وظائف شبكة الكومبيتر لغرض قومي أو سياسي من خلال استغلال نقطة ما يمكن للمهاجم من التلاعب بالنظام، كما تعرف بانها هجوم عبر الفضاء الإلكتروني يهدف إلى السيطرة على مواقع الكترونية لتعطليها او تدميرها أو الاضرار بها [1]

[1] أحمد عيس الفتلاوي,الهدماتالسيبرانية مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولى المعاصر, مجلة العلى للعلوم القانونية والسياسية,كليةالقانون,جامعة بابل,العدد04 ، 2016 صفحة 614.

وقد عرفتها القيادة الاستراتيجية الامري[1]كية بأنها تطويع عمليات نظام الكمبيوتر بهدف منع الخصوم من الاستخدام الفعال لها ، فضلا عن التسلل إلى أنظمة المعلومات وشبكات التواصل بهدف جمع وحيازة وتحليل البيانات اتى تحتويها.

إذا التهديدات السبيرانية أو الهجمات السبيرانية هي التي تهدد أمن المجتمع وأمن الاقتصاد الوطني والجانب ا مني والعسكري للدول . كما أن للتهديدات السيبرانية أهداف مسطرة ، حيث تمس كلا من الجانب المعنوي والجانب المادي وعلى جميع الاصعدة. [2]

إن الأحداث الدولية الاخيرة ساهمت بشكل أو بآخر في رفع وعي الباحثين والدراسين وكذا صناع القرار بشان التهديدات السيبرانية التي تطورت وسائلها وممارسيها وشمل جملة من مجالات الحياة. أبرز هذه الحالات فيما يلي:

- DDOS TTACKSأستونيا أبريل 2007 : بدأت سلسلة من الهجمات التي يطلق عليها

المواقع التي تديرها الحكومة الاستونية، وتسبب الهجوم في عرقلة ولوج المواطنين الى بعض المواقع مثل موقع الحزبالسياسيالذييينتميالىهرئيسالوزراء . واستخدامالروابطالتيترعاهاالحكومةفيتضليلاالمستخدمين واعادةتوجيههمالىصورللجنودالسوفيين.

[1]بنصابر بلقاسم ، حيدرة محمد, الصدمات السيبرانية ومواجهتها في ضوء القانون الدولي المعاصر, مجلة حقوق الانسان والحريات العامة، جامعة مستغانمو المجلد 02، العدد04, جوان 2017, ص 189.

[2]– أحمدالسيدالنجار، محمد عبد الهادي علام، حروب المعلومات منيواجهها؟, مجلة الاهرام, العدد139, 13يوليو2015, ص 26.

– كوريا الجنوبية و الولاياتالمتحدةيوليو : 2009

تماستهدافمواقعالبيتالابيض،ووكالةالامنالقوميوزارةالخارجية،والخدمةالسرية Federal Aviation Administration Federal والإدارةالاتحاديةللطيرانفضلا، Trade Commission والخزانة،ولجنةالتجارةالاتحادية،Secret Service

عنجهاز المخابراتالوطنيفيكوريا الجنوبية.

– وكذلكالهجومعلىشركةسونيبيكتشرز الامريكيةفيعام 2014 ،بسببفيلممنانتاجهوليودعنزعيمكوريا الشمالية كيميونغاون . واستخدامفيروس " ستكسنت – "سابقا – لمهاجمةبرنامجايرانالنوويفينوفمبر 2007 ،ويعتقدأنهمنتطويرالولاياتالمتحدةواسرائيل،وقدتماكتشافهفيعام2010.[1]

وفييوليو 2011 أعلنتنائبوزيرالدفاعويلياملينأناكثرمن 24 الفملفمنملفاتوزارةالدفاعقدسرق،قبلذلكببضعةاشهرتماختراقاحدىالمختبراتالعلميةالرئ يسيةالتابعةلحكومةالولاياتالمتحدة،ولمتعلنالحكومةالامريكيةعنهويةمرتكبيالهجوم

– وفيعام 2012 ،تمتدمير 35 الفجهازكمبيوترفيشركةالنفطالسعودية "ارامكو "،لتخريبصادراتالنفطوالقتالمخابراتالامريكيةاللومعلىايران،وفيعام 2016 ،هاجمالقراصنةاحدىالوكالاتالحكومية السعودية،بالاضافةالىمنظماتفيقطاعاتالطاقةو الصناعةو النقل،و الهيئةالعامةللطيرانالمدنيالتيتنظمالطيرانالسعودي.

– وشهدتعام 2016

،التسللالروسيإلىخوادمالبريدالالكتروني للجنةالوطنيةالديمقراطة،كماتماختراقالبريدا لالكتروني الخاصبجونبوديستارئيسالحملةالانتخابيةالرئاسيةلهيلاري كلينتون،وقام

[1] العربية سكاي نيوز، "اسكسنت فيروس ضد إيران"، فبراير 2013 ،من الرابط :
www.Synewsarabia.com/web/article/114276/%d8%b3%d8%%d9% تاريخ التصفح 2019/3/21.

علىإثرهاقامتالولاياتالمتحدةالأمريكية Wikileaksالوسطاءبتسريبرسائلالكترونيةال ىموقعبطرد 35 دبلوماسيارو سيا[1] .

ويمكنالقولفيضوءتلكالحالاتأنهرغماختلافغرضوهدفكلحالةمنالحالاتالسابقة،إلا أنهمنالواضحانحجمالهجماتالسيبرانيةيتزايدبشكلحادوكبير،ولذايصعبتحديدحجمهاالحق يقيوبخاصةأنعديدمنهالايتمالتبليغعنه .

وتتمثلالقواسمالمشتركةبينتلكالحالاتفيصعوبةتحديدمرتكبي تلكالهجماتعلىوجهالدقة،وغيابالردالمضاد،كنتيجةلها .والاهمأن ليستحكراعلىالدولالمتقدمة

ذاتالانظمةالمعلوماتيةالهائلةوالمتطورةفحسبلقدتمسأيضاالدولالمتخلفة.

ثانيا : أنماط التهديدات السيبرانية

تتعددأشكالالتهديداتالسيبرانيةوتختلفمنحيثالطبيعةوالمصادروالأهدافكالتجسسوسرقةال معلوماتوشنالحروبوبالتالياتالعديدمنالفواعلالدوليينيلجئونالىآلياتالكترونيةلتحقيقها .و علىالرغممنتعددصوروأشكالالهجماتالإلكترونية،غيرأنهمنالممكنتقسيمهاالىالانواع الرئيسيةالتالية:

1. خطرالكوارثالطبيعية أو (العرضيةللكابلاتالبحرية SubmarineCable) :

تعد الكابلات

جزءاهامالتوفيرخدمةالاتصالاتبينودولالعالمفيمجالالانترنت،وشبكاتالكمبيوترو غيرها .

[1] العربية سكاي نيوز، "تفاصيل الهجوم ....قراصنة يدمرون كومبيوترات في وكالة الطيران السعودي.. ويستبدلون البيانات بصورة الطفل السوري الان كريد"، من الرابط 2019/03/21 :التصفح تاريخ www.Skynewsarabia.Comweb/article/114276/d.

فمنذعام 2005 ،أصبحتالكابلاتالبحريةمأهولةعلىمجال الإتساعو الإنتشار ،أماعلىنطاقالتقدمو التطورتحولتإلىتقنياتأخفوزناو أصغرحجما،كما تعرضت

تلكالكابلاتإلىعددمنالمشكلاتالتيتؤثرسباعلىأعماالبنىالتحتيةبالضرر ،حيثلاتقعفيمياه المحيطالعميق،هذاوقد تعرضت دو لالشرقالأوسطلإنقطاعمفاجئللانترنتبنسبة 80 %،وحدث إنقطاعل % 50 كابلافيالمحيطالأطلنطيفيونيو 2005 ،كذلكحدثخللفيشبكةالانترنتجراء زلازلفيجنوبشرقآسيافي % 27 ديسمبر 2006 ،أدىإلىتعطيلالاتصال[1].

2. التجسسالإلكتروني Cyber Espionage:

يعدأحدأنواعالتجسسالتقليدي،باستخداموسائلالتكنولوجياالفائقة،ومعظمالهجماتالسيبرانية

المتطورةالتيتقعضمنهذهالفئة،حيثيتمالحصولعلىمعلوماتسريةبطرقغيرمشروعةدفالحصول علىأفضليةإقتصادية،أوإستراتيجيةأوعسكرية[2].

فالتجسسالسيبرانيهوذلكالتجسسالذييعتمدعلة

إستخداماالتقنياتالإلكترونيةفيالحصولعلىمعلومات،ويختلفالتجسسالسيبرانيمنحيثالنوع، فهناك

التجسسعنطريقالأفراد،ومنخلالالشبكاتالسلكيةأوالتجسسمنخلالالأقمار الصناعية[3].

---

[1] عادلعبدالصادق،"الفضاءالالكترونيوتهديداتجديدةللأمنالقومي"،المركزالعربيللأبحاثالالكترونية,2012, ص 13

[2] نانسيالبناء،" الأمنالسيبراني بيئة تكنولوجيةأكثرأمنا "، 20 جانفي h21:142018http//boutiqueceena.eg

[3] حسنبنأحمدالشهري،"الأنظمةالالكترونيةالرقميةالمطورةلحفظوحمايةسريةالمعلوماتمنالتجسس"،مركزالنورللأبحاثالإلكترونية، (2010) ص11

3. الجريمةالسيبرانية(Cyber Crime): :

الجريمةالسيبرانيةهيكلفعلأوإمتناعيتمإعدادهأوالتخطيطله،ويتمبموجبهاستخدامأينوع منالحواسيبالآليةسواءحاسبشخصيأوشبكاتالحاسبالآليأوالانترنتأووسائلالتواصلالاجتماعيلتسهيلإرتكابجريمةأوعملمخالفللقانون،أوتلكالتيتقععلىالشبكاتنفسهاعنطريقإختراقهابقصدتخزينهاأوتعطيلهاأوتحريفومحوالبياناتأوالبرامجالتيتمتحويلها،وتتكونالجريمة السيبرانية ويستخدممصطلحالسيبرانية (cyber) والسيبرانية (crime) أوالإفتراضيةمنمقطعينهما :الجريمة لوصففكرةجزءمنالحاسبأوعصرالمعلومات،أماالجريمةفهيالسلوكياتوالأفعالالخارجية على القانون .

والجرائمالسيبرانيةهيالمخالفاتالتيترتكبضدالأفرادأومجموعاتمنالأفرادبدافعالجريمةقصد

إيذاءسمعةالضحيةبأذىماديأوعقليللضحيةمباشرأوغيرمباشرباستخدامشبكاتالاتصال مثل الانترنت) كغرفالدردشة،البريدالالكترونيوالموبايل (فالأعمالذاتالصلةبالحاسوبلأغراضشخصيةأو مكاسبماليةأوضرر،بمافيذلكأشكالالجرائمالمتصلةبالهوية،والأفعالالمتعلقةبمحتوياتالك مبيوتر جميعهاتقعضمنمعنىأوسعلمصطلح" الجريمةالسيبرانية.[1]

فالجريمةالسيبرانيةأوالمعلوماتيةهيالإمتناعالعموديأوفعلينشأعننشاطغيرمشروعلنسخأو

تغييرأوحذفأوالوصولإلىالمعلوماتالمخزنةفيالحاسب،ويهدفإلى الاعتداءعلىالأموالوا

---

[1] ذيابموسى،"الجرائمالالكترونية :المفهومو الأسباب،ملتقىعلميحول :الجرائمالمستحدثةفيظل المتغيراتو التحولاتالإقليميةو الدولية"،كليةالعلومالاستراتيجية،عمان،المملكةالأردنيةالهاشمية,2014, ص05

لممتلكات والخصوصياتالماديةوالمعنوية [1]فالجريمةالسيبرانيةلهامسمياتكثيرةهي :

الجريمةالمعلوماتية،جرائمالفضاء

الافتراضي،جرائمالكمبيوترو الانترنت،جرائممجتمعالمعلوماتوجرائممجتمعالمعرفةو

جرائممجتمعمابعد

المعلومات،وعلىاختلافالتسمياتوتعددمداخلالدراساتوالتعاريفتتفقكلهاعلىعنصروحيد

رئيسيلمفهومالجريمةالسيبرانيةوهو الحاسبالآليكأداةلكنهأيضاقديكونمعتدىعليهأوبيئةال

جريمة[2] .

فالجريمةالسيبرانيةأو الجريمةالإلكترونيةهيالاستخدام السيئلجهاز الحاسبالآليومايماثلهب

وسائل

غيرمشروعةللوصولإلىأهدافمتعددةومتنوعة،وجميعجرائمالحاسبالمعروفةو المسجلة

تتضمنأدوارا أخرىو التييكونللحاسبأثرافيهاوتتمثلفي

"الهدفو البيئةو الأداةو الرمز "،ومنهفجرائمالحاسبالآلي

هينشاطإلكترونييؤديإلىإلحاقالضرربالغيرماديأومعنوياعنطريقاستخدام الحاسبمنالجان

يضد حاسباليعليه،فلقديمكنأنيكونالحاسبالآليبيئةللجريمةكتدميرالبياناتأو التخريبلأجزاء

الحاسبالآليأوبرامجه [3]فالجريمةالمعلوماتيةهيكلاستعمالاحتياليأوغيرقانونيللشبكاتالمعل

وماتية

---

[1] سليممزيود،"الجرائمالمعلوماتيةواقعهافيالجزائرو آلياتمكافحتها"،جامعةالمدية،الجزائر2015 , ص96

[2] خديجةقصعة،جمالبنمرزوق، "

تفعيلآلياتالحمايةالقانونيةللحدمنإنتشار الجريمةالإلكترونيةفيالعالمو الجزائر"،مجلةتاريخالعلوم،العددالسادس،جانفي 2010 ,

ص2

[3] عباسحفصي،" جرائمالتزويرالالكتروني،دراسةمقارنة"،أطروحةدكتوراه،جامعة وهران 1- -

،أحمدبنبلة،كليةالعلومالإسلامية،تخصصشريعةوقانون، 2015 ,ص14

والاعتداءاتعلىأنظمةالمعلوماتأوالمعطياتالمعالجة،وكذاالاعتداءاتعلىالحياةالخاصةوا
لمعلومات
الشخصية،ونشرالفيروساتالمعلوماتيةوتبييضالأموال،والاحتيالوالنصبعلىالأشخاصو
تنظيم الشبكاتالإرهابيةوغيرها .
والجريمةالمعلوماتيةتنطويعلىصنفينمنالجرائمالمرتبطةمباشرةبتكنولوجيا
المعلوماتكأداةلارتكابهذاالنوعمنالجرائموهيتتضمنالجرائمالتيتواجهفيالعالمالماديوأماال
يومفهي تواجهفيالعالمالافتراضيللأنترنت[1] .

فالجريمةالمرتكبةعبرالانترنتهينشاطإجراميستخدمفيهاالتقنيةالإلكترونيةبطريقةمباش
رةأوغير
مباشرةكوسيلةلتنفيذالفعلالإجراميالمستهدف،وهينوعمنالجرائمالتيتتطلبالموضوعإلما
مخاص
بتقنياتالحاسبالآليونظمالمعلوماتلارتكاأوالتحققفيهاومقاضاةفاعليها .كماأنأيتصرفغير
مشروعمنأجلالعملياتالإلكترونيةتمسبأمنالأنظمةالمعلوماتيةوالمواضعالتيتعالجهافالج
ريمةالتي
يستخدمفيهاالحاسبالآليكوسيلةأوأداةلارتكاويمثلإغراءبذلك،أوجريمةيكونالحاسبنفسه
ضحيتها[2] .

4. الارهابالسيبراني (Cyber Terrorism):

[1] حنانبراهمي،" جريمة تزويرالوثيقةالرسميةالإدارية،ذاتالطبيعةالمعلوماتية "،أطروحةدكتوراه كلية العلوم السياسية والحقوق, تخصص جنائي,جامعة محمد خيضر بسكرة,015,ص 38

[2] يوسفصغير،" الجريمةالمرتكبةعبرالانترنت"،رسالةماجيستير،جامعةمولودمعمري،تيزيوزو،كليةالحقوق،تخصص : قانوندوليللأعمال، 2014 , ص52

المقصودبالإرهابالمعلوماتأوالإرهابالسيبرانيهوذلكالإستخداماللموارد المعلوماتية،المتم
ثلةفي
الإعلاموأجهزةالحاسوبوشبكةالانترنتوالفضائياتمنأجلأغراضالتخويفأوالإرغاماًلأغرا
ض
سياسية،أوالاقناعالفكريوالتثقيفالسلبيوالعدواني،ويرتبطالإرهابالمعلوماتيإلىحدكبيربال
مستوى
المتقدمللغايةوالذيباتتتكنولوجياالمعلوماتوالإعلامتؤديهفيجميعمجالاتالحياةفيالعالم،ويم
كنأن
يتسببالإرهابالمعلوماتيفيإلحاقالشللبأنظمةالقيادةوالسيطرةوالاتصالاتأوقطعشبكات الات
صالين والوحداتوالقيادةالمركزيةوتعطيلأنظمةالدفاعالجويوغيرها .
فقدركزالرئيسالأمريكيالسابق " **بيل** (Bee Klenton)**كلينتون**
علىالتصديلاحتمالاتالإرهابالمعلوماتي،حيثأنانتشارالجهاديةعلىشبكةالانترنتمشكلةب
ذلكتهديدالإلكترونياويعدهذاالتهديدهوالأكبروالأقربلكلدول
العالم،لأنهيمسبصفةمباشرةفكرالإنسانوعقله،حيثأرجعكثيرمنالباحثينالمتخصصينفيظا
هرة الإرهابيعودبصفةعامةإلىوجودانحراففكريلدىمنيقومذهالأعمال[1] .

فالإرهابالسيبرانيهوعبارةعنهجماتغيرمشروعة،أوتهديداتجماتضدالحاسباتأوالشبكاتأو
المعلوماتالمخزنةإلكترونيا،توجهمنأجلا لانتقامأوالابتزازأوالإجبارأوالتأثيرفيالحكوما
ت أوالشعوبأواتمعالدوليلتحقيقأهدافسياسيةأودينيةأواجتماعيةمعينة[2] .

[1] إدريس عطية, مرجع سابق, ص 24-25.

[2] سارةبوحادة،"أثرالإرهابالالكترونيعلىأمنواستقرارالدول"،أطروحةدكتوراه،جامعةالجزائر- 3 -
،المدرسةالوطنيةالعلياللعلومالسياسية،تخصص دراساتدولية، 2014 ،ص63

كماأنالإر هابالسيبر انيهو التخويفأو التهديدماديأومعنوياباستخدام الوسائلالإلكتر ونيةال صادر ةمنالدو لأو الجماعاتأو علىالإنسانسو اءافيدينهأونفسهأو عرضهأو عقلهأو مالهبغير حقبشتىأشكالهوصور الفسادفيالأرض[1] .

كماأنالإر هابالسيبر انيأيضاهو نشاطأو هجو ممتعمديملكدو افعسياسيةويسعى للتأثير فيالقر ار اتالحكو ميةو الر أيالعامالعالمي،ويستخدمالفضاء الالكتر ونيبو صفهعاملام ساعداو وسيطا

فيعمليةالتنفيذللعملالار هابي،ويأتيهذا العملفيصور ةرقميةعبر استخدام آلياتالأسلحةالإلكت رونية الجديدةلتصلإلىالإضر اربأهدافماديةتتعلقبالبنيةالتحتيةالحيوية[2] .

5. الحروبالسيبر انية(Cyber Warfare):

تشملالحر وبالسيبر انيةالناجحةعلىأكثرمن " مشغلي " حر وبإلكتر ونية،وتعتمدعلىفريقمنالمختصينفيالمعار كالإلكتر وني،حيثكلمنهميتميزبم سؤو لياتهو مهار اتهالخاصةلتر سيخالقدر ةعلىالقتال

و التحكماو إبر از هضمنالفضاء السيبر اني،ويقو ممشغلو "الحر وبالسيبر انية " بالتخطيطللنشاطاتالهجو مية و الدفاعيةو إدر اكو تنفيذهاعبر الفضاء السيبر اني .

تبلور تالمصالحالقو ميةللدو لفيالفضاء السيبر اني،إثر تز ايد الاعتمادعلىر بطالبنىالتحتيةل ها،فأيهجوم، (NTI)

بذلكالفضاء فيبيئةعملتشابكيةو احدة،تعر فبالبنيةالتحتيةالقو ميةللمعلو ماتأو

[1] ذياب موسى, مرجع سابق, ص06.

[2] أمجدالمنيف،"الإر هابالالكتر وني -معركةحديثة"،المجلةالعربية،العدد 07 ،يوليو 2015 ص02

تهديد محتمل على تلك المصالح قد يشكل حدوث عدم توازن إستراتيجي، وهو ما يكشف عن نمط جديد من التهديدات للأمن القومي للدول، وأبرزها[1] :

-

تزايد إرتباط العالم الفضائي السيبراني، الأمر الذي يتسع معه خطر البنية التحتية الكونية للهجمات السيبرانية.

-

تراجع دور الدولة في ظل العولمة وانسحاب من بعض القطاعات الإستراتيجية لمصلحة القطاع الخاص.

- نشوء نمط جديد من الضرر على خلفية الهجمات السيبرانية، يمكن تسببه (الدولة أو للدولة ب) دون الحاجة للدخول المادي إلى أراضيها.
- تحول الحرب السيبرانية إلى إحدى أدوات التأثير في المعلومات في مستويات مراحل الصراع المختلفة
- توظيف الفضاء الإلكتروني في تعظيم قوة الدول، من خلال إيجاد ميزة أو تفوق أو تأثير في البيئات المختلفة، وبالتالي ظهر ما يسمى بـ "الإستراتيجية السيبرانية" للدول.
- اتساع نطاق مخاطر الأنشطة العدائية التي يمارسها الفاعلون، سواء الدول أو من غير الدول.

فتفرض طبيعة الأذى الذي يتعرض له الأمن القومي للمخاطر السيبرانية، إجراءات وأساليب مناسبة يمكن الحفاظ عليه، فالأسلحة التقليدية منها المتطورة، وحتى النووية، عاجزة عن حماية "الفضاء السيبيري"[1]

[1] عادل عبد الصادق، " أنماط" الحرب السيبرانية "وتداعياتها على الأمن العالمي"، مجلة الاتجاهات النظرية، البنك العربي الافريقي، 14 ماي 2017 ص 13

الفرع الثاني: التهديدات السيبرانية وتأثيرها على الأمن القومي

سنحاول في هذا الفرع التطرق الى العلاقة الارتباطية بين التهديدات السيبرانية والامن القومي، وكيف تؤثر التهديدات السيبرانية على الامن القومي.

فقد صاحب التطور التكنولوجيا لتكنولوجيا الاعلام والاتصال تصاعد وتزايد المخاطر والتهديدات السيبرانية على الامن القومي للدول والتي من بينها الجزائر، وذلك من خلال الاشكال المتعددة للتهديدات والتي من بينها :

1. .الحرمان من الخدمة وهو ذلك الهجوم الذي يهدف الى ايقاف قدرة الهدف على تقديم الخدمات المعتادة او المفترض تقديمها، وذلك عن طريق اغراق جهاز الحاسب الالي المقدم للخدمة بكم هائل من الاوامر تؤدي الى توقفه عن العمل، وذلك عن طريق اخترق الاجهزة الالكترونية للخصم وتحميل برامج عليها ليتم استخدامها لاحقا في شن هجوم على الخصم بشكل متزامن من خلال ارسال اشارة بدء الى هذه البرامج الموجودة على كافة الاجهزة التي تم اختراقها، حيث لا يستوجب أن يكون أصحاب الحواسيب المخترقة على علم بذلك، كما يلاحظ ان الاجهزة المخترقة قد تتواجد في منطقة بالعالم ولا يشترط ان ترتبط كلها بنطاق مكاني معين، ويشار الى هاته الاجهزة التي تمت مهاجمتها بالاكواد والبرامج الخبيثة بعدد من المصطلحات ابرزها zombies او Bots.12[2]

[1]- Timothy Franz.TheCyber Warfare professionnel Realization for Devloping the NextGeneration.Summer 2011.p 04

[2]نوران شفيق، "اشكال التهديدات الإلكترونية مصادرها"المركز الاوربي لدراسات ومكافحة الإرهاب والاستخبارات، المانيا وهولندا على الموقع الالكتروني بتاريخ يناير 2020 14:56https://www.europarabct.com/%D8%A3%D8%B4% :

2. التجسس السيبراني وتعتبر هاته الجريمة من اخطر التهديدات السيبرانية فهي نتاج أسفر عنه التقدم العلمي والتكنولوجي الحديث في شأن اجهزة التنصت الحديثة ذات القدرة الفائقة، حيث تهدف الى جمع المعلومات العسكرية او السياسية أو حتى جمع المعلومات غير العسكرية كجمع تلك المتعلقة بالمجال الاقتصادي والتجاري، فالتجسس قد يهدف الى تعطيل عمل الشبكات العنكبوتية وحواسيبها وانظمتها بهدف سرقة معلومات سرية سياسية أو عسكرية أو مالية من دولة ونقلها الى اخرى،
فالتجمسالسيبرانيتعتبر من الاساليب التي تلجأ اليها التنظيمات الاجرامية والارهابية لجمع معلومات حول المؤسسات والقطاعات الحكومية ليتم استخدامها من اجل الاضرار بالمجتمع ومصالحه[1]
3. **الارهاب السيبراني** وهو استخدام شبكات المعلومات والكمبيوتر من اجل التخويف والارغام لتحقيق اهداف سياسية، حيث تقوم الجماعات الارهابية بالتهديد عبر وسائل الاتصالات من خلال الشبكة العالمية للمعلومات وتتعد أساليب التهديد وتتنوع طرقه وذلك من أجل نشر الخوف والرعب بين الاشخاص والدول والشعوب، ومحاولة الضغط عليهم للرضوخ لأهداف تلك التنظيمات الارهابية من ناحية، ومن اجل الحصول على التمويل المالي او ابراز قوة التنظيم الارهابي من ناحية أخرى، فالإرهاب السيبراني يشمل اي نشاط يتم من خلال شبكة الانترنت بهدف بث الافكار المتطرفة سواء كانت سياسية أو دينية أو عنصرية للسيطرة على وجدان

[1] أميرة عبد العظيم, محمد عبد الجواد, المخاطر السيبرانية و سبل مواجهتها في القانون الدولي العام,مجلة الشريعة و القانون,العدد 35, 2020, ص415-416

الافراد وافساد عقائدهم وإذكاء تمردهم واستغلال معاناتهم في تحقيق مآرب خاصة تتعارض مع مصالح المجتمع.[1]

4. **سرقة المعلومات والبيانات العسكرية** او التلاعب بها من خلال اختراق قواعد البيانات العسكرية وسرقتها او تزيفها او تدميرها الكترونيا، حيث تسعى الهجمات الالكترونية في هذه الحالة الى اختراق الشبكات الخاصة بالمؤسسات العسكرية بهدف سرقة خرائط نشر انظمة التسليح او التصميمات الخاصة بالمعدات العسكرية، وقد انطلقت واحدة من اخطر الهجمات ضد انظمة حواسيب الجيش الامريكي في عام 2008، من خلال وصلة "USBمتصلة بكمبيوتر محمول تابع للجيش في قاعدة عسكرية موجودة في الشرق الاوسط، عدم اكتشاف انتشار برامج التجسس في كل الانظمة السرية وغير السرية في الوقتالمناسب شكل ما يشبه جسر رقمي تم من خلاله نقل الاف الملفات من البيانات الى خوادم خارجية.[2]

كل هاته التهديدات وغيرها تؤثر بشكل او بأخر على الامن القومي، باعتبار ان الفضاء السيبراني فضاء واسع ومرن فالتهديدات الامنية الحديثة اخذت بعدا اخر ذو طابع الكتروني، مرتبط ارتباطا ويثقا بالتطور التكنولوجي الذي وصل اليه العالم في السنوات الاخيرة، ومن جانب اخر ان التكنولوجية الحديثة لوسائل الاعلام والاتصال هي من نتاج الدول الغربية التي هي مصدر التهديدات السيبرانية، ومن جانبثالث نجد ان البنية التحتية الالكترونية للجزائر هشة مقارنة بالدول الاوروبية والامريكية التي تمتلك امكانيات قوية لضمان امن معلوماتها من

[1] أميرة عبد العظيم, محمد عبد الجواد, نفس المرجع, ص 421.

[2] ايهاب خليفة,تنامي التهديدات السيبرانية للمؤسسات العسكرية ,مجلة اتجاهات الاحداث,العدد22, المستقبل للابحاث و الدراسات المتقدمة,ابوظبي,يوليو اغسطس 2017, ص 57.

مختلف التهديدات الامنية والتي لم تسلم هي الاخرى من هاته التهديدات، فاذا كانت دول العالم المتقدم والمسيطرة بشكل كامل على التطور التكنولوجي لوسائل الاعلام والاتصال فكيف بالجزائر التي تعتبر من دول العالم الثالث والمستورة بشكل كبير لهاته التكنولوجيا لذلك يتوجب على الجزائر استحداث منظومة دفاع قوية تجاه مختلف التهديدات السيبرانية التي اصبحت تهدد الامن القومي في كل دقيقة وثانية وهو ما سنحاول التطرق اليه في المحور الموالي ومن جانب آخر يعتبر الامن القومي من أهم الوظائف التي تولي لها الدول والانظمة السياسية في العالم اهمية كبيرة، باعتباره يرتبط ارتباطا وثيقا بأمن المؤسسات والافراد والهيئات الحيوية داخل الدولة وخارجها، فالتهديدات السيبرانية اصبحت اليوم من اخطر التهديدات التي تمس بأمن المعلومات للدول وهو ما يعني المساس بشكل مباشر بالأمن القومي للدولة، فالتهديدات المتعلقة بالتجسس وقرصنة المعلومات خصوصا المعلومات المتعلقة باستراتيجيات الدولة في كافة المجالات السياسية والاقتصادية والاجتماعية، وكذا الارهاب السيبراني، كلها تهديدات تعصف بكيان الدولة واستمراريتها، فالتعاملات العصرية اليوم اصبحت مرتبطة ارتباطا وثيقا بالتطور التكنولوجي لوسائل الاعلام والاتصال، وبالتالي اي تهديد بإمكانه، تعطيل المصالح الاستراتيجية للدولة.

ومن ذلك يمكن القول ان تحدي الأمن السيبراني يعد أعلى تحديات الأمن القومي في القرن الواحد والعشرين، لان المفهوم الحديث للأمن لا يقتصر فقط على الجوانب العسكرية بل يواكب كل التهديدات والتحديات التي يمكن أن تشكل عائق امام الاقتصاد الرقمي وتدفق المعرفة، فقد اسقطت تكنولوجيا المعلومات والاتصالات مفهوم الحدود الجغرافية والسياسية والاقتصادية والاجتماعية بين الدول وهو ما يضع السيادة الوطنية والامن القومي على المحك خاصة مع

الاختراق المتكرر والمتزايد للمواقع الحكومية الرسمية والتجسس المعلوماتي على الدول.[1]

[1] لامية طالمة, التهديدات و الجرائم السيبرانية وتاثيرها على الامن القومي للدول و استراتيجيات مكافحتها, مجلة معالم للدراسات القانونية و السياسية ,المجلد04,العدد02, 2020, ص 56

الفصل الثاني
النظام المؤسساتي للأمن الس
يبراني في التشريع الجزائري

تمهيـد:

لوضع حماية جزائية للجريمة السيبرانية استجابت عدة دول لها فمثلا الولايات المتحدة الأمريكية التي أصدرت قانونا فيدراليا سنة 1984 متعلقا بالاحتيال وإساءة استخدام الكمبيوتر، كما أصدرت فرنسا قانون رقم 88-19 الموافق ل 05-01-1988 بشأن الغش المعلوماتي، والذي أُدمج في قانون العقوبات الفرنسي وأصبح يشكل بابا جديدا هو الباب الثالث من قانون العقوبات الفرنسي، ثم صدر تعديل جديد لهذا القانون بتاريخ 1993/03/01

أما عن التشريعات العربية، فقد تبنى المشرّع الجزائري في القسم السابع مكرر نصوص الجريمة السيبرانية، أو ما يصطلح عليه بجرائم المساس بأنظمة المعالجة الآلية للمعطيات، وذلك بالقانون رقم 04-15 المؤرخ في 2004/11/10 المتضمن قانون العقوبات الجزائري.

وقد شهد العالم مولد أول معاهدة دولية لمواجهة جرائم الكمبيوتر وذلك في سبتمبر 2001 في مدينة بودابست، بتوقيع 26 دولة من الاتحاد الأوروبي إضافة إلى كندا وجنوب إفريقيا والولايات المتحدة الأمريكية، والحقيقة أن تلك المعاهدة وإن كانت أوروبية المنشأ فهي دولية النزعة فهي مفتوحة للدول الأخرى التي تطلب الانضمام أو الترشح للانضمام لها.

وفي هذا الصدد، سنتناول في هذا الفصل من خلال المبحث الأول الآليات القانونية لمواجهة الجريمة السيبرانية في التشريع الجزائري، وفي المطلب الأول الآليات المقاوِمة لمواجهة الجريمة السيبرانية، والمطلب الثاني الآليات الإجرائية لمواجهة الجريمة السيبرانية في التشريع الجزائري، وأما في المبحث الثاني فسنتطرق إلى الأمن السيبراني الجزائري حيث في المطلب الأول الاهتمامات الأمنية الجزائرية و في المطلب الثاني أسباب اهتمام الجزائر بالأمن السيبراني.

المبحث الأول: الآليات القانونية والإجرائية لمواجهة الجريمة السيبرانية في التشريع الجزائري

إن التطور المتسارع لتكنولوجيا الاتصال والمعلومات أدى إلى حصول نوع من الفراغ التشريعي المنظم للجرائم السيبرانية، التي تتميز بنوع من الحداثة في الفضاء الإلكتروني، بحيث لا يمكن إخضاعها بأي حال من الأحوال إلى القواعد التقليدية الواردة في النصوص التشريعية العقابية، وهو الأمر الذي يؤدي إلى سن تشريعات جديدة تطبق على هذا النوع من الجرائم. وبناءً على ذلك، استحدثت الجزائر، على غرار العديد من الدول، آليات لمكافحة الجرائم السيبرانية، وهذا ما يتم توضيحه في هذا المبحث.

المطلب الأول: الآليات القانونية لمكافحة الجرائم السيبرانية في التشريع الجزائري

من خلال هذا المطلب، سنتطرق لمختلف القوانين الشاملة في التصدي والمواجهة لمثل هذه الجرائم المستحدثة في الجزائر، وذلك من خلال الفرعين الآتيين:

الفرع الأول: مكافحة الجرائم السيبرانية بموجب القوانين العامة

أولا: الدستور الجزائري

لقد كفل دستور الجزائر لسنة 1996، وكذا التعديل الطارئ عليه بموجب القانون المعدل له سنة 2016، حماية الحقوق الأساسية والحريات الفردية، وهذا ما ضمنه تعديل دستور 2020، على أن تضمن الدولة عدم انتهاك حرمة الإنسان. وقد تم تكريس هذه المبادئ الدستورية في التطبيق بواسطة نصوص تشريعية أوردها قانون العقوبات والإجراءات الجنائية وقوانين خاصة أخرى، والتي تحظر كل مساس بهذه الحقوق. ومن أهم المبادئ الدستورية العامة ما يلي:

- المادة 37: كل المواطنين سواسية أمام القانون، ولهم الحق في حماية متساوية، ولا يمكن أن يُتذرع بأي تمييز يعود سببه إلى المولد أو العرق, الجنس, الرأي, أي شرط, ظرف آخر شخصي أو اجتماعي
- المادة 74: حرية الإبداع الفكري، بما في ذلك أبعاده العلمية والفنية، مضمونة.

لا يمكن تقييد هذه الحرية إلا عند المساس بكرامة الأشخاص أو بالمصالح العليا للأمة أو القيم والثوابت الوطنية.

- يحمي القانون الحقوق المترتبة على الإبداع الفكري، ففي حالة نقل الحقوق الناجمة عن الإبداع الفكري، يمكن للدولة ممارسة حق الشفعة لحماية المصلحة العامة.
- إذ لا يجوز انتهاك حرمة حياة المواطن الخاصة وحرمة شرفه، كما أن القانون يحمي سرية المراسلات والاتصالات الخاصة بكل أشكالها المضمونة، والقانون يحمي حقوق المؤلف، ولا يجوز حجز أي مطبوع أو تسجيل أو أي وسيلة أخرى من وسائل التبليغ والإعلام إلا بمقتضى أمر قضائي[1].

ثانيا : قانون العقوبات الجزائري

لقد تطرق المشرع الجزائري إلى تجريم الأفعال الماسة بأنظمة الحاسب الآلي، وذلك نتيجة تأثره بما أفرزته الثورة المعلوماتية من أشكال جديدة من الإجرام، مما دفع المشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون رقم 04-

[1] فضيلة عاقلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، المؤتمر الدولي الرابع عشر الجرائم الإلكترونية، طرابلس 24-25 مارس 2017، صفحة 127.

15 المؤرخ في 10 نوفمبر 2004، المتمم للأمر رقم 15-22 المتضمن قانون العقوبات، تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات"، ويتضمن هذا القسم ثماني مواد، من المادة 394 مكرر إلى المادة 394 مكرر7. [1]

وبغرض تدارك الفراغ القانوني، فقد قام المشرع الجزائري بموجب القانون رقم 04-15 [2]باستحداث جملة من النصوص، والتي جَرَّم من خلالها الأفعال المتصلة بالمعالجة الآلية للمعطيات، وحدد لكل فعل منها ما يقابله من الجزاء، إذ قام المشرع بسَنِّ جملة من القوانين القانونية الموضوعية والتي حدد من خلالها كل الأفعال الماسة بنُظم المعالجة الآلية للمعطيات وما يقابلها من جزاء أو عقوبة، [3] وإلى جانب ذلك فقد قام المشرع الجزائري بسَنِّ قواعد إجرائية جديدة تتعلق بالتحقيق تتماشى مع الطبيعة المميزة للجرائم الإلكترونية، وذلك من خلال تعديل قانون الإجراءات الجزائية بموجب القانون رقم 06-22.[4]

إذ نصت المادة 394 مكرر منها ما يلي: "يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50,000 إلى 100,000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك، وتتضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير المعطيات المنظومة، وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة

[1] فضيلة عاقلي، نفس المرجع، الصفحة 127.

[2] قانون رقم 04-15، مرجع سابق.

[3] قانون رقم 06-22 مؤرخ في 2006/12/20 يعدل ويتمم بالأمر رقم 66-155 يتضمن قانون الإجراءات الجزائية، عدد 84 الصادر في 2006/12/24.

[4] جمال براهيمي، مكافحة الجريمة الإلكترونية في التشريع الجزائري، المجلة النقدية للقانون والعلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة مولود معمري – تيزي وزو، العدد 2 الصادر في 2006/11/15، صفحة 124 وما بعدها.

الحبس من ستة أشهر إلى سنتين والغرامة من 50,000 إلى 150,000 دج، وذلك مهما كانت قاعدة المعلوماتية أو طبيعتها. لذلك يمكن أن تندرج ضمن هذه الاعتداءات تلك التي تمس ببعض صور الحياة الخاصة."

ونصت المادة 394 مكرر 2 على أنه: "يعاقب كل من يقوم عمداً وعن طريق الغش بما يأتي:

- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن تُرتكب بها الجرائم المنصوص عليها في هذا القسم.
- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كل المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم ".

وتضيف المادة 394 مكرر 6 أنه "بالإضافة إلى العقوبات الأصلية أي الحبس والغرامة، والاحتفاظ بحقوق الغير حسن النية، يُحكم بالعقوبات التكميلية التالية: يُحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلًّا لجريمة من الجرائم المعاقب عليها وفقًا لهذا القسم، علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتُكبت بعلم مالكها. [1]

[1] نوارة حسين، آليات تنظيم المشرع الجزائري لجريمة الاعتداء على الحق في الحياة الخاصة إلكترونياً، الملتقى الوطني: آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، كلية الحقوق والعلوم السياسية، جامعة مولود معمري – تيزي وزو، الجزائر 2017، صفحة 118 وما بعدها.

ثالثا : قانون الإجراءات الجزائية الجزائرية

بالنسبة لمتابعة الجريمة الإلكترونية، تتم بنفس الإجراءات التي تُتبع بها الجريمة التقليدية كالتفتيش والمعاينة واستجواب المتهم والضبط والتسرب والشهادة والخبرة.[1]

نجد أن المشرع الجزائري نص على تمديد الاختصاص المحلي لوكيل الجمهورية في الجرائم الإلكترونية في المادة 37 من قانون الإجراءات الجزائية يتحدد الاختصاص المحلي لوكيل الجمهورية بمكان وقوع الجريمة، وبمحل إقامة أحد الأشخاص المشتبه في مساهمتهم فيها أو بالمكان الذي تم في دائرته القبض على هؤلاء الأشخاص حتى ولو حصل هذا القبض لسبب أخر، ونص على التفتيش في المادة 45 الفقرة 7 [2]من نفس القانون المعدلة إذا جرى التفتيش في مسكن شخص أخر يشتبه بأنه يجوز أوراقا أو أشياء لها علاقة بالأفعال الإجرامية فإنه يتعين حضوره وقت إجراء التفتيش وإذا تعذر ذلك اتبع الإجراء المنصوص عليه في الفترة السابقة، حيث اعتبر أن التفتيش المنصب على المنظومة المعلوماتية يختلف عن التفتيش المتعارف عليه في القواعد الإجرائية العامة من حيث الشروط الشكلية والموضوعية، فالتفتيش وإن كان إجراءً من إجراءات التحقيق، قد أحاطه المشرع بقواعد صارمة، وبالتالي لا تُطبّق الأحكام الواردة في المادة 44 من قانون الإجراءات الجزائية إذا تعلق الأمر بالجرائم الإلكترونية.

[1] فضيلة عاقلي، مرجع سابق، صفحة 130.

[2] مولود ديدان، قانون الإجراءات الجزائية، المادة 37 والمادة 45، الأمر 11-02، دار بلقيس – الجزائر، صفحة 33.

ونص على توقيف النظر في جريمة المساس بالأنظمة المعالجة في المادة 51 الفقرة 6، وكذا على اعتراض المراسلات وتسجيل الأصوات والتقاط الصور في المادة 65 مكرر 5[1].

لقد أدرك المشرع الجزائري جيدًا بأن المواجهة الفعالة للإجرام الإلكتروني لا تكون فقط بإرساء قواعد قانونية موضوعية ذات طبيعة ردعية، إنما لابد من مصاحبة هذه القواعد بقواعد أخرى إجرائية وقائية وتحفظية والتي من شأنها أن تتفادى وقوع الجريمة أو على الأقل الكشف عنها في وقت مبكر يسمح بتدارك مخاطرها، وهو ما استدركه المشرع بتضمين القانون رقم 06-22 المعدل لقانون الإجراءات الجزائية تدابير إجرائية مستحدثة تتعلق بالتحقيق في الجرائم الإلكترونية تتمثل في مراقبة الاتصالات الإلكترونية، تسجيلها.

يقصد باعتراض المراسلات اعتراض أو تسجيل أو نسخ المراسلات التي تكون في شكل بيانات قابلة للإنتاج والتوزيع، التخزين، الاستقبال، والعرض، التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية في إطار البحث والتحري عن الجريمة وجمع الأدلة

ولقد أشار المشرع الجزائري إلى ظروف وكيفية اللجوء لهذا الإجراء في المادة 65 مكرر خمسة من قانون الإجراءات الجزائية على النحو: إذا اقتضت الضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، يجوز لوكيل الجمهورية المختص أن يأذن بـــ:

[1] فضيلة عاقلي، مرجع سابق، صفحة 130.

- اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية.
- وضع الترتيبات التقنية دون موافقة المعنيين من أجل الالتقاط والتثبيت وبث وتسجيل الكلام المدفوع به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن مخصصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص .

فبموجب هذه المادة، المشرع الجزائري يسمح لسلطات التحقيق والاستدلال – إذا استدعت الضرورة في الجريمة المتلبس بها والتحقيق في الجريمة الإلكترونية – باللجوء إلى إجراء اعتراض المراسلات السلكية واللاسلكية وتسجيل المحادثات والأصوات والتقاط الصور والاستعانة بكل الترتيبات التقنية اللازمة لذلك من أجل الوصول إلى الكشف عن ملابسات الجريمة وإثباتها دون أن يتقيدوا بقواعد التفتيش والضبط المألوفة.

ومع هذا، فإن المشرع الجزائري لم يُطلق حق اللجوء إلى هذا الإجراء، بل أحاطه بمجموعة من الضمانات القانونية التي تحد من تعسف سلطات الاستدلال والتحري وتصون الحقوق والحريات العامة والحياة الخاصة للأفراد[1].

الفرع الثاني: مكافحة الجرائم السيبرانية بموجب القوانين الخاصة

أولا: القانون الخاص بحماية حق المؤلف والحقوق المجاورة

[1] براهيمي جمال، مرجع سابق، صفحة 138-140.

يرى معظم الفقه أن الموقع الإلكتروني مصنف متعدد الأغراض، يتم استخدامه من الشركات التجارية كعلامة تجارية لتمييز منتجاتها المعروضة للتسويق أو الدعاية عن غيرها على شبكة الإنترنت، أو كاسم تجاري أو شعار لجذب الجمهور. كما يمكن أن يُستغل كمصنف أدبي أو فني من المؤلفين عند عرض أفلامهم السينمائية أو لوحاتهم الزيتية وغيرها.

وفي كل الحالات، يختار صاحب الموقع العنوان الذي يريده في شكل علامة أو اسم تجاري أو مصنف بهدف تحديد هويته عبر الشبكة لكي يعرض ما يريد من سلعة أو خدمة عند إبرام العقد مع إحدى الشركات التي تقدم الخدمات على الشبكة. وبمجرد تسجيل اسم الموقع، يحظى بالحماية القانونية المقررة لحقٍ من مثيله الفكري الذي يتضمنه، أي بتحديد القانون الواجب التطبيق حسب الوضعية القانونية للمواقع.

فعند تسجيل الموقع كمصنف أدبي أو فني، لا يجوز أن يُعتدى على أي جانب من جوانب الحياة الخاصة للأفراد، كاستعمال اسم كامل لشخص معين معروف دون الحصول على الموافقة من صاحبها، أو استغلال صورة أي شخص في الموقع دون الموافقة عليها. وبهذه الصورة، فإن حماية مواقع الإنترنت التي تستغل مصنفاً أدبيًا أو فنيًا على شبكة الإنترنت بقانون حق المؤلف والحقوق المجاورة، ينتج عنها حماية الحق الأدبي والمالي للموقع المسجل كمصنف، وحماية قانونية لأي حق آخر يتم الاعتداء عليه مثل الحياة الخاصة للأفراد، كالحق في الاسم والصورة والمعلومات الخاصة.

وفي كل الأحوال، لا يمكن الفصل بين حماية المصنف المستعمل في الموقع وحماية الموقع في حد ذاته، لأنهما يخضعان لقانون حق المؤلف والحقوق

المجاورة في الوقت نفسه، لأن حماية الموقع تؤدي بالضرورة إلى حماية محتوياته بما في ذلك المصنف[1].

ثانيا: القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها:

صدر القانون رقم 09-04 بتاريخ 5 أوت 2009 ويتضمن 19 مادة موزعة على ستة فصول، وهو ثمرة عامين من التحضير والدراسة والتحليل والمقارنة مع أحدث القوانين، وقامت بإعداده نخبة من رجال القانون بمشاركة خبراء ومهنيين مختصين في مجال الإعلام الإلكتروني من كافة القطاعات المهنية. كما يتضمن هذا القانون أحكامًا خاصة بالمراقبة الإلكترونية التي لا يجوز إجراؤها إلا بإذن من السلطة القضائية المختصة وفي حالات تم تحديدها، وهي الأفعال الموصوفة بجرائم الإرهاب والتخريب والجرائم الماسة بأمن الدولة أو حالة توفر معلومات عن اعتداء محتمل يهدد منظومة من المنظومات المعلوماتية لمؤسسات الدولة أو الدفاع الوطني أو النظام العام.

نص القانون على إنشاء هيئة وطنية للوقاية من الإجرام المتصل بتكنولوجيات الإعلام والاتصال ومكافحته، تتولى تنشيط وتنسيق عملية الوقاية من الجرائم الإلكترونية ومساعدة مصالح الشرطة القضائية في التحريات التي تجريها بشأن هذه الجرائم، كما تتكفل اللجنة أيضا بتبادل المعلومات مع نظيراتها في الخارج، علمًا أن القانون أكد على مبدأ التعاون الدولي من منطلق المعاملة بالمثل .

[1] نوارَة حسين، مرجع سابق، صفحة 120 وما بعدها .

ويعتبر القانون رقم 09-04 ذو نطاق شامل في مجال مكافحة الجريمة الإلكترونية، حيث جاء بتجريمه للأفعال المخالفة للقانون والتي ترتكب عبر وسائل الاتصال عامة، وبالتالي فهو يطبق على كل التكنولوجيات الجديدة والقديمة، بما في ذلك شبكة الإنترنت وعلى كل تقنية تظهر مستقبلا[1].

ثالثا: القانون الخاص المتعلق بالقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية:

حيث استحدث هذا القانون ووضع مجموعة آليات للتصدي للجرائم المتعلقة بالعالم الافتراضي، منها استحداث سلطة الضبط، ومن بين مهامها السهر على احترام متعاملي البريد والاتصالات الإلكترونية للأحكام القانونية والتنظيمية المتعلقة بالبريد والاتصالات الإلكترونية والأمن السيبراني[2].

تجريم انتهاك سرية المراسلات المرسلة عن طريق البريد أو الاتصالات الإلكترونية أو إنشاء مضمونها أو نشرها أو استعمالها دون ترخيص من المرسل أو المرسل إليه أو الإخبار بوجودها، وتجريم محاولة فتح أو تخريب أو تحويل البريد أو المساعدة في ارتكاب هذه الجريمة، وسنّ مجموعة من العقوبات ضمن المواد من 164 إلى 188 من هذا القانون.

رابعا: القانون المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي

[1] عائشة، نايري عائشة، الجريمة الإلكترونية في التشريع الجزائري، رسالة ماستر حقوق تخصص قانون إداري، جامعة أدرار 2016-2017، صفحة 39 وما بعدها.

[2] المادة 13 من القانون 18-04 المؤرخ في 10 ماي 2018 الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، الجريدة الرسمية عدد 27 الصادرة بتاريخ 13 ماي 2018.

وضع المشرع الجزائري مجموعة من الآليات المتعلقة بالعالم الافتراضي والتي جاء إيجازها في عدة نقاط:

- استحداث السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي
- وضع مجموعة التزامات مُلقاة على عاتق المسؤول عن المعالجة الآلية للمعطيات ذات الطابع الشخصي
- اتخاذ السلطة الوطنية لمجموعة إجراءات إدارية في حالة خرق أحكام القانون من المسؤول عن المعالجة
- يمكن للسلطة الوطنية القيام بتحريات ومعاينة المحلات والأماكن التي تتم فيها المعالجة باستثناء محلات السكن، كما يمكنها الولوج إلى المعطيات المعالجة وجميع المعلومات والوثائق أيا كانت دعامتها.
- تأهيل أعوان رقابة للقيام ببحث ومعاينة الجرائم المتعلقة بالمعطيات ذات طابع شخصي تحت إشراف وكيل الجمهورية.
- يمكن للمدعي بالمساس بحق من الحقوق المنصوص عليها في هذا القانون أن يطلب من الجهة القضائية اتخاذ أي إجراءات تحفظية للحد من التعدي أو الحصول على تعويض.
- تختص الجهة القضائية الجزائرية بمتابعة الجرائم التي تُرتكب خارج إقليم الجمهورية من طرف جزائري أو شخص أجنبي مقيم في الجزائر أو شخص معنوي خاضع للقانون الجزائري، كما تختص بمتابعة الجرائم المنصوص عليها في هذا القانون وفقًا لقواعد الاختصاص المنصوص عليها في المادة 588 من قانون الإجراءات الجزائية[1].

[1] المادة 53 من القانون 18-07 مؤرخ في 10 يونيو 2018، متعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية عدد 34 الصادر بتاريخ 10 يونيو 2018، صفحة 22.

- تجريم الاعتداء على المعطيات ذات الطابع الشخصي بإفراد عقوبات مالية وأخرى سالبة للحرية وفقًا للمواد من 54 إلى 74 من هذا القانون[1].

المطلب الثاني: الآليات الإجرائية في مكافحة الجرائم السيبرانية في التشريع الجزائري

سنتناول في هذا المطلب أهم الهيئات المتخصصة والفعالة في مواجهة الجرائم السيبرانية في الجزائر، وقد خصصنا لها أربعة فروع، وهي كالتالي:

الفرع الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

نصت على إنشاء هذه الهيئة المادة 13 من القانون 09-04 المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها. تُنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، وتُحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم، أما مهامها فقد أوردتها المادة 14 من نفس القانون.

أولا: تنظيم الهيئة

بالرغم من الأهمية المرجوة من هذه الهيئة، إلا أنه لم يتم إلى حد الساعة إنشاؤها. وباستقراء نصوص القانون 09-04، فإن تشكيلتها تحتوي مجموعة من

[1] مهدي رضا، الجرائم السيبرانية وآلية مكافحتها في التشريع الجزائري، مجلة اليزا للبحوث والدراسات، جامعة المسيلة، المجلد 06، العدد 02، 2021، صفحة 121 وما بعدها.

ضباط الشرطة القضائية، والتي ستسمح لهم هذه الصفة بتنفيذ المهام التي أوكلها المشرع لهذه الهيئة. وهو نفس الأمر في فرنسا، إذ أُنشئت الوكالة المركزية لمكافحة الإجرام المتعلق بتكنولوجيا الإعلام والاتصال.

ثانيا: مهام الهيئة

- الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

-إن إجراءات الوقاية تكون بتوعية مستعملي تكنولوجيا الإعلام والاتصال بخطورة الجرائم التي يمكن أن يكونوا ضحايا لها وهم يتصفحون أو يستعملون هذه التكنولوجيات. ومن أهم هذه الجرائم: التجسس على الاتصالات والرسائل الإلكترونية، التلاعب بحسابات العملاء أو بطاقات ائتمانهم، اختراق أجهزة الشركات والمؤسسات الرئيسية والجهات الحكومية.

- مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

وبحسب نص المادة 14 من القانون 09-04، فهناك نوعان من المكافحة تقوم بهما هذه الهيئة:

- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية (المادة 14 فقرة "ب" من القانون 09-04).

بالنسبة للوكالة المركزية لمكافحة الإجرام المتعلق بتكنولوجيا الإعلام والاتصال في فرنسا، فإن لها مهام أدرجها المرسوم رقم 2405 المؤرخ في 15 ماي 2000 المتضمن إنشاء هذه الهيئة، وتتمثل في :

- تنشيط وتنسيق، على المستوى الوطني، عمليات المكافحة ضد الفاعلين والمشتركين في ارتكاب الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.
- القيام بإذن من السلطات القضائية، بجميع إجراءات التحري والأعمال التقنية الخاصة بالتحقيقات كمساعدة لمصالح الشرطة القضائية المختصة، بتحقيقات الجرائم الخاصة التي ارتُكبت أو سهل ارتكابها استعمال تكنولوجيات الإعلام والاتصال، ولكن دون المساس باختصاص باقي الهيئات الوطنية المختصة بمكافحة جرائم معينة ونص عليها القانون.
- تقديم المساعدة لمصالح الأمن والدرك الوطنيين، ولجميع إدارات ومصالح الدولة المركزية، فيما يخص الجرائم التي تدخل في اختصاص هذه الهيئة، إذا طلبت منها هذه المصالح ذلك، ودون أن يؤدي ذلك إلى رفع يد هذه المصالح.
- التدخل من تلقاء نفسها، بعد موافقة السلطات القضائية المسبقة (المادة 4 فقرة 2 من القانون 09-04)، في كل مرة تفرضها الظروف من أجل البحث الميداني في وقائع مرتبطة بتحقيق تقوم به.
- من أجل القيام بمهامها، فلها تركيز وتحليل واستقراء كل المعلومات المتعلقة بأفعال وجرائم متصلة بتكنولوجيات الإعلام والاتصال، والاتصال بكل من مصالح الأمن والدرك الوطنيين، وإدارات ومصالح الدولة، وكذا كل الإدارات والمصالح العامة للدولة المعنية للقيام بمهامها.
- يجب على كل مصالح الأمن والدرك الوطنيين، إدارة ومصالح الدولة، في أقرب الآجال، إخطار الهيئة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، فيما تسمح به القوانين، وخاصة منها ما يتعلق بالسر المهني، بما كشفته أو وصل إلى علمها من جرائم متصلة بتكنولوجيا الإعلام والاتصال .

–تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وتحديد مكان تواجدهم. وفي هذا الشأن، تقوم الهيئة على المستوى الوطني بتنشيط وتنسيق الأعمال التحضيرية الضرورية، ومن ثم تُشاركها المنظمات أو الهيئات المماثلة لها على مستوى الدول، بدون المساس بتطبيق الاتفاقيات الدولية ومبدأ المعاملة بالمثل. كما أنها تدرس الروابط العملياتية مع الهيئات والمصالح المختصة مع الدول الأخرى، من أجل البحث عن جميع المعلومات المتعلقة بالجرائم المعلوماتية، وكذلك التعرف على الفاعلين وأماكن تواجدهم[1].

الفرع الثاني: المعهد الوطني للأدلة الجنائية وعلم الإجرام

يتكون المعهد الوطني للأدلة الجنائية وعلم الإجرام من 11 دائرة متخصصة في مجالات مختلفة، جميعها تضمن إنجاز الخبرة، التكوين والتعليم، وتقديم مساعدات تقنية، البحوث والدراسات والتحاليل في علم الجريمة.

أولا: دائرة الإعلام الآلي والإلكتروني

1. هي مكلفة بمعالجة، تحليل، وتقديم كل دليل رقمي وتماثلي للعدالة، كما تقدم مساعدة تقنية للمحققين في التحقيقات المعقدة. أفراد الدائرة يسهرون على تأمين اليقظة التكنولوجية من أجل تحسين المعارف أو التقنيات والطرق المستعملة في مختلف الخبرات العلمية لإنجاز المهام المنوطة بها. تنقسم الدائرة إلى ثلاثة مخابر، وذلك حسب نوع المعلومات: سمعية،

[1] عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، 2007، صفحة 232 وما بعدها

بصرية، والإعلام الآلي. كل مخبر مزود بقضية مهمتها إنشاء المعطيات من حوامل المعلومات وضمان نزاهة وشرعية الدليل. وهذه المخابر هي :[1]

1. **مخبر الإعلام الآليمن مهامه :**تحليل ومعالجة حوامل المعطيات الرقمية (الهاتف، الشريحة، القرص الصلب، ذاكرة الفلاش

–تحديد التزوير الرقمي للبطاقات البنكية

2. **ومن تجهيزاته** :محط ة ترميم وتصليح الأجهزة والحوامل المعطلة، والشبكات الإعلامية كخبرات الإعلام الآلي والتجهيزات البيانيةمحطة ثابتة ومحمولة لإجراء خبرات الإعلام الآليجهاز اقتناء معلومات الهواتف والحواسب

والقاعات التي يحتوي عليها تتمثل في سبع قاعات هي :

مكتب التوجيه, فصيلة الأنظمة المشحونة, فصيلة اقتناء المعطيات, قاعة موزع, قاعة تخزين[2]

3. **مخبر الفيديو**يختص مخبر الفيديو بـــ:

- مقارنة الأوجه وشرعية الصورة والفيديو
- اعادة بناء مسرح الجريمة بالتشكيل الثلاثي الأبعاد
- تحسين نوعية الصورة (فيديو أو صورة) بمختلف التقنيات

و من تجهيزاته :جهاز فيديو بوكس, حوامل فيديو رقمية وممغنطة, حبكات إعلامية, كونيتيك, استوديو وماكس ثلاث أبعاد, موزع لحفظ الشرائح الفيديو.

---

[1] هواري عياش، مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية، المعهد الوطني للأدلة الجنائية وعلم الإجرام، كلية الحقوق، جامعة بسكرة، 2016، صفحة 03

[2]: سالم عبد الرزاق، ملتقى حول المنظومة التشريعية الجزائرية في مجال الجريمة المعلوماتية، محكمة سيدي محمد، الجزائر، صفحات 4–6

أما بالنسبة للقاعات، يحتوي مخبر الفيديو على أربع قاعات : قاعات للتحليل, قاعة التخزين, قاعة موزع[1]

4. **مخبر الصوت**ومن المهام التي يؤديها:

- تحسين نوعية إشارة الصوت بنزع التشويش وتعديل السرعة
- معرفة وتحديد المتكلم
- تحديد شرعية التسجيلات الصوتية

من أجهزته :الأجهزة الازدواجية والسماع, حبكات إعلامية, معالجة وتحسين التسجيلات الصوتيةنسخ الأقراص المضغوطة, أجهزة التصليح والتعبير

أما بالنسبة للقاعات، فإنه يحتوي مخبر الصوت على خمس قاعات : ثلاث قاعات للتحليل, قاعة تخزين, قاعة موزع[2]

الفرع الثالث: المعهد الوطني للبحث في علم التحقيق الجنائي

بالإضافة إلى المعهد الوطني للأدلة الجنائية وعلم الإجرام، تم استحداث أيضاً المعهد الوطني للبحث في علم التحقيق الجنائي، تحت وصاية المديرية العامة للأمن الوطني، بموجب المرسوم الرئاسي رقم 04-432 المؤرخ في 2004/12/29، والذي نصّ أيضاً في المادة 05 منه على مجموعة من المهام من بينها: إعداد تقارير الخبرة، وأيضاً القيام بالتكوين وتجديد المعارف في ميدان علم التحقيق الجنائي والإجرام.

[1] سالم عبد الرزاق، مرجع سابق، صفحة 7

[2]: سالم عبد الرزاق، مرجع سابق، صفحة 8

ويحتوي هذا المعهد على مصلحة الخبرات الخاصة بالأدلة التكنولوجية، بحيث تُكلف بتحليل الأدلة المادية التي جُمعت إثر معاينة المخالفات والتحريات في ميدان الجريمة المعلوماتية، وإعداد تقارير الخبرة.

الفرع الرابع: الهيئات القضائية الجزائية المتخصصة

يقصد بها الأقطاب الجزائية المتخصصة المنشأة بموجب القانون رقم 14-04 المؤرخ في 1 نوفمبر 2004،[1] وتختص هذه الجهات القضائية بموجب المواد 37، 40، 329 من قانون الإجراءات الجزائية بالنظر في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، بالإضافة إلى الصلاحيات الأخرى الممنوحة للجهات القضائية أو للضبطية القضائية في إطار معالجة مثل هذه الجرائم.[2]

ولقد أثمر مسار إصلاح العدالة التي شرعت فيه الجزائر سنة 2000، والذي انصب على دراسة ثلاث نقاط أساسية، وهي دعم حقوق الإنسان، وتسهيل حقل اللجوء إلى القضاء، وإعادة الاعتبار للنظام التكوين والتأهيل بإحداث تغييرات جذرية في قطاع العدالة، خاصة تعديل واستحداث قوانين تنسجم والالتزامات الدولية للجزائر، وكذلك تحسين خدمات قطاع العدالة، ولعلّ أهم ما جاءت به توصيات لجنة إصلاح العدالة تعديل القانون الجزائري بشقيه الموضوعي والإجرائي في مواجهة الظواهر الإجرامية الخطيرة وتزايد المنظمات الإجرامية، وتزايد مخاطر التقنية المعلوماتية على حياة الأشخاص وخصوصياتهم.

إضافة إلى أن هذا النوع من الجرائم تمتد آثاره خارج حدود الدولة الواحدة مهدداً بذلك اقتصاديات الدول وأمنها، حيث شهدت السنوات الأخيرة تزايداً في العمليات

---

[1] القانون 04-14، مرجع سابق

[2] سعيدة بعرة، الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر، دراسة مقارنة 2015-2016، صفحة 52

الإرهابية وتزايداً في أعمال المنظمات الإجرامية واستعمالها الفضاء الافتراضي للاستفادة من خصائص الجريمة المعلوماتية.

ومن أجل كل هذا، عكف المشرع الجزائري، وقبله التشريعات المقارنة خاصة المشرع الفرنسي، إلى استحداث الأقطاب الجزائية المتخصصة، وهي محاكم ذات اختصاص إقليمي موسع بموجب القانون 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري، الذي أجاز توسيع اختصاص بعض المحاكم ووكلاء الجمهورية وقضاة التحقيق في جرائم محددة على سبيل المثال لا الحصر، وتوصف بأنها خطيرة وعلى درجة عالية من التعقيد والتنظيم، وهي: جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، تبييض الأموال، الجرائم الإرهابية والتخريبية، وجريمة مخالفة التشريع الخاص بالصرف[1].

ولقد تم بالفعل صدور النص التنظيمي الخاص الذي مدّد الاختصاص لأربع جهات قضائية، وهو المرسوم رقم 06-348 المؤرخ في 2006/10/05، المعدل والمتمم بالمرسوم التنفيذي رقم 16-267 المؤرخ في 17 أكتوبر 2016، والذي تم بموجبه تحديد هذه المحاكم مع تعديل طفيف في المرسوم بحيث شمل التقسيم إضافة إلى بعض المجالس القضائية، بمقتضى المواد 3 و4 و5 المعدلة للمواد 3 و4 و5 من المرسوم السابق، وجاء التقسيم كالتالي[2]:

[1] كريمة علة، الجهات القضائية الجزائية ذات الاختصاص الموسع، المجلة الأكاديمية للبحث القانوني، المجلد 11، العدد 01، 2015، صفحة 117

[2] سعيدة بوزنون، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة العلوم الإنسانية، المجلد "ب"، العدد 52، ديسمبر 2019، صفحة 54.

- محكمة سيدي محمد (الجزائر العاصمة): ويمتد اختصاصها الإقليمي إلى المجالس القضائية التالية: الجزائر، الشلف، الأغواط، البليدة، تيزي وزو، الجلفة، المدية، المسيلة، بومرداس، البويرة، عين الدفلى .

–محكمة قسنطينة: ويمتد اختصاصها إلى المجالس القضائية: قسنطينة، أم البواقي، باتنة، بجاية، تبسة، جيجل، سطيف، سكيكدة، عنابة، قالمة.

- محكمة ورقلة: ويمتد اختصاصها إلى المجالس القضائية: ورقلة، أدرار، تمنراست، إليزي، بسكرة، الوادي، غرداية.
- محكمة وهران: ويمتد الاختصاص بها إلى المجالس القضائية التالية: وهران، بشار، تلمسان، تيارت، تندوف، سعيدة، سيدي بلعباس، مستغانم، البيض، تيسمسيلت، النعامة، عين تموشنت، غليزان.

بحيث يشمل الاختصاص كل جهة قضائية مجموعة من المجالس القضائية تقع في منطقة جهوية من الجزائر (شمالاً، جنوباً، شرقاً، وغرباً)، وذلك لدى أربع محاكم تسمى أقطاباً جزائية، كما تم تدعيم هذه الأخيرة باستحداث وسائل التحري الخاصة لمواجهة الإجرام المنظم بما فيه الجريمة الإلكترونية[1].

المبحث الثاني: الأمن السيبراني الجزائري

في ظل التوجه الدولي نحو الحكومة الإلكترونية أصبحت قضية الأمن المعلوماتي السيبراني من التحديات الكبرى على الصعيدين الإقليمي والعالمي، لا سيما مع تزايد التهديدات الأمنية والإلكترونية، والجزائر كغيرها من الدول سعت منذ

[1] سعيدة بوزنون، مرجع سابق، صفحة 55.

انتهاجها للإدارة الإلكترونية حماية منظوماتها المعلوماتية من خلال العديد من الأجهزة والخلايا الأمنية، ولقد أصبح الأمن المعلوماتي السيبراني ركنا أساسيا ضمن المنظومة الأمنية المعاصرة، والتي يجب على الدفاع الوطني من خلال أجهزته تحقيق الأمن الداخلي في ظل تنامي الجريمة الرقمية، وكذا نظرا للاستغلال المتنامي للشبكات الإلكترونية لأهداف إجرامية والتي تؤثر سلباً على سلامة البنية التحتية للمعلومات الوطنية العامة لا سيما على المعلومات الشخصية.

المطلب الأول: الاهتمامات الأمنية الجزائرية

لقد وضعت الجزائر الأمن السيبراني أحد أولوياتها على غرار باقي دول العالم التي سارعت إلى مراجعة سياستها الأمنية.

الفرع الأول: مكانة الأمن السيبراني في السياسة الأمنية الجزائرية

وضعت الجزائر خطوة جديدة نحو مجابهة الجرائم السيبرانية التي شهدت أرقامها قياسية في السنة الماضية، وأخذت أشكالا جديدة جعلت مسؤوليها يعلنون حالة استنفار لمجابهة الجريمة الإلكترونية.

وبهدف محاربة الجرائم الإلكترونية، كشفت الجزائر على أنها جهزت أكثر من 24,000 مهندس وتقني مختص في الأمن السيبراني، وشرعت في تكوين أعداد أخرى ذات كفاءة عالية، ففي سنة 2002 قامت بإبرام اتفاقيات مع عمالقة في

هذا المجال على غرار Microsoft وHuaweiو Ciscoفي إطار الاستراتيجية الوطنية لتطوير الاقتصاد الرقمي والأمن السيبراني المرافق له[1].

وفي هذا الإطار، فإن الجزائر وضعت أجهزتها الأمنية لحماية منظومتها السيبرانية اعتمادا على مؤسسة الدفاع الوطني كأحد أولوياتها على غرار باقي دول العالم التي سارعت إلى مراجعة سياستها الأمنية وإدراجها للآليات وميكانيزمات جديدة لهذه المسائل، بالموازاة مع تطوير البنيات الأساسية المتعلقة بتكنولوجيات العالم الرقمي. ويفرض مطلب الأمن مضاعفة أنظمة المراقبة التي قد تشكل تهديدا للحريات الفردية ولهذا وجب مرافقة كل المقاربات الأمنية في مجال الأمن الرقمي بالإجراءات القانونية والتكنولوجية الملائمة وتُؤخذ بعين الاعتبار دقة الهجمات الإلكترونية وتعقيداتها والتي يزداد خطرها مع التطور التكنولوجي واستخداماتها اليومية.

وتجسيدا لذلك، باشرت الدولة الجزائرية وفي مقدمتها مؤسسة الدفاع الوطني إلى إعداد برامج خاصة لمجابهة الجريمة الإلكترونية والحد من انتشارها وإنشاء أجهزة جديدة تنسجم أدوارها وتجهيزاتها مع المتغيرات الحاصلة في هذا المجال، أصبحت الحماية السيبرانية جزءاً مهماً في أي منظومة أو وزارة من خلال حماية النطاق المعلوماتي[2].

---

[1] يونس بوزيان، الجزائر: 24,000 مختص في الأمن السيبراني لمواجهة الجرائم الإلكترونية، على الرابط التالي، تصفح في 2025/04/21:
www.searchnewworld.com

[2] بكوش روميساء، انعكاسات التهديدات السيبرانية على الأمن الوطني الجزائري، مذكرة ماستر، جامعة العربي التبسي – كلية الحقوق والعلوم السياسية، صفحة 48.

أولا: وزارة الدفاع الوطني

السيد رئيس الجمهورية القائد الأعلى للقوات المسلحة وزير الدفاع الوطني يترأس مراسم افتتاح الملتقى الوطني حول الاستراتيجية الوطنية للأمن السيبراني "من أجل جزائر صامدة سيبرانياً."

ترأس السيد عبد المجيد تبون رئيس الجمهورية القائد الأعلى للقوات المسلحة وزير الدفاع الوطني يوم الأربعاء 7 جوان 2023 مراسم افتتاح الملتقى الوطني حول الأمن السيبراني، المرسوم بالاستراتيجية الوطنية للأمن السيبراني "من أجل جزائر صامدة سيبرانياً" الذي نظمته وزارة الدفاع الوطني بالنادي الوطني للجيش ببني مسوس – الجزائر العاصمة.

وكان في استقبال السيد رئيس الجمهورية السيد الفريق الأول السيد شنقريحة، رئيس أركان الجيش الوطني الشعبي، حيث أدّت التحيّة الشرفيّة للسيد الرئيس . عرفت أشغال الملتقى حضور كل من السيد الوزير الأول، ومدير الديوان، والأمين العام لرئاسة الجمهورية، والمستشار لدى رئيس الجمهورية المكلّف بالشؤون المتصلة بالدفاع والأمن، وأعضاء من الحكومة، وسعادة السفيرة فوزية بومزوزة مباركي، والمندوب الدائم للجزائر لدى الأمم المتحدة بجنيف، وكذا ضباط وعمّال بوزارة الدفاع الوطني وأركان الجيش الشعبي الوطني، فضلاً عن إطارات سامية في الدولة وشخصيات وطنية وخبراء ومختصين.

وبهذه المناسبة، ألقى السيد رئيس الجمهورية الكلمة الافتتاحية للملتقى، حيث أكّد أن مقتضيات الأمن الوطني تستدعي العمل على تطوير استراتيجية وطنية متكاملة في المجال الرقمي.

إن تحديد التهديدات السيبرانية ووضع آليات الرقابة والرصد الناجحة وجاهزية الاستراتيجية في حالات الخطر يشكّل اليوم أحد أهم الشروط الاستباقية لتوفر الحماية اللازمة والكاملة للمنشآت بشكل آمن ومستمر، وذلك ضمن منظومة التكفل بالأمن الوطني بأبعاده السياسية والعسكرية والاقتصادية والمجتمعية، بل وحتى التكنولوجية، وهو الأمر الذي يستوجب تطوير استراتيجيات وطنية متكاملة في المجال الرقمي والجمع بين الاستباقية والوقاية من التهديدات في الفضاء السيبراني وحماية المنظومات، والسهر على ترقية ثقافة رقمية مواطِنية ووطنية عمادها التحسيس المستمر واليقظة الاستراتيجية لكل المؤسسات.

وأضاف السيد رئيس الجمهورية أن كسب رهان الأمن السيبراني يعتمد أساساً على تثمين العنصر البشري الذي تنبثق منه الكفاءات المتمرسة :إن كسب رهان الأمن السيبراني يعتمد أساساً على تثمين العنصر البشري الذي ينبثق منه الكفاءات المتمرسة المدركة لصعوبة المهام المسندة إليها، وهو ما توليه الأهمية القصوى في توجه الدولة لإحداث نقلة نوعية على مستوى تسيير الشأن العام من خلال وضع الأسس الاستراتيجية والوطنية المدروسة للرقمنة، وهو خيارنا السيادي المبني على إدراكنا الجماعي لارتباط التنمية المنشودة بترشيد الحكامة والرفع من جودة أداء المؤسسات وتثمين القدرات وتعبئة الموارد .أشدّد على ضرورة تجسيد ما ليس عملية تقنية بل معبّرة عن قناعة راشدة وفي صلب أولويات بناء الجزائر الجديدة[1].

ثانيا: صدور المرسوم الرئاسي المتعلق بإنشاء المدرسة الوطنية العليا في الأمن السيبراني

[1] الاستراتيجية الوطنية للأمن السيبراني "من أجل جزائر صامدة سيبرانياً" بتاريخ 2025/04/27، الموقع الرسمي لوزارة الدفاع الوطنيwww.ndn.dz

صدر في العدد الأخير من الجريدة الرسمية المرسوم الرئاسي المتضمن إنشاء مدرسة وطنية عليا في الأمن السيبراني، والتي تساهم في المجهود الوطني للبحث العلمي والتطور التكنولوجي في مجال أمن الأنظمة المعلوماتية، وتقديم حلول مبتكرة ذات تقنيات عالية.

ويشير المرسوم الرئاسي رقم 24-181 إلى أن هذه المدرسة تتولى مهمة ضمان التكوين العالي والبحث العلمي والتطوير التكنولوجي للمهندسين وحاملي الدكتوراه في الكفاءات العلمية والتقنية ذات المستوى العالي، وتمكنهم من ممارسة وظائف التطوير أو التقييم في ميادين الأمن السيبراني .كما تُكلف هذه المدرسة بالتعاون مع وكالة أمن الأنظمة المعلوماتية بتعزيز تطوير القدرات التقنية الوطنية في ذات المجال.

وللتذكير، كان رئيس الجمهورية السيد عبد المجيد تبون قد أسدى تعليمات خلال مجلس الوزراء المنعقد بتاريخ 12 سبتمبر 2023 باستحداث مدرسة وطنية في الأمن السيبراني

بالتنسيق مع وزارة الدفاع الوطني، لضمان توحيد الجهود ومضاعفة الفعالية في هذا المجال الحساس، من أجل تحصين الأمن الوطني القومي[1].

ثالثا:وزارة الداخلية

[1] المرسوم الرئاسي رقم 24-181 المؤرخ في 12 سبتمبر 2023 المتضمن إنشاء المدرسة الوطنية العليا في الأمن السيبراني، الجريدة الرسمية للجمهورية الجزائرية، العدد 39 الصادرة يوم السبت 22 ذو الحجة 1445، الموافق لـــ 8 يونيو 2024 م

أكد السيد محمود شرف الدين بوضياف المدير العام بوزارة الداخلية والجماعات المحلية أن المواطن يعد محور اهتمامات الدولة الجزائرية والسيد عبد المجيد تبون، حيث يعتبر المورد البشري الركيزة الأساسية للتنمية المستدامة، وأوضح أن تأهيل هذا المورد البشري هو عنصر حاسم في تحقيق التحولات الاقتصادية والاجتماعية التي تشهدها الجزائر في ظل المتغيرات العالمية.

وأشار السيد محمد شرف الدين بوضياف، الذي نزل ضيفًا على برنامج ضيف الصباح في القناة الإذاعية الأولى، إلى أن قطاع الداخلية والجماعات المحلية يعتمد على استراتيجيات شاملة ترتكز على التكوين المستمر والتأهيل بالإضافة إلى التحول الرقمي الذي يعد أولوية وطنية كبرى، كما التفت إلى أهمية التعاون بين مختلف القطاعات مثل قطاع البناء والأشغال العمومية لتقديم خدمات تتماشى مع متطلبات الحياة اليومية للمواطن. وأضاف أن الوزارة بصدد تطوير برامج خاصة بالأمن السيبراني وتحديث البرامج التي من شأنها أن تسهل حياة المواطنين[1].

رابعا: مجلة الشرطة

سلط العدد الأخير من مجلة الشرطة الصادرة عن المديرية العامة للأمن الوطني الضوء على موضوع الأمن السيبراني المندرج ضمن مسعى تعزيز الشفافية الرقمية لدى المواطن وحماية أسس السيادة الرقمية في الجزائر .

وتناول العدد 158 من مجلة الشرطة تحت عنوان "لأجل مجتمع واع في الفضاء السيبراني" ملف الأمن والفضاء الرقمي من عديد الجوانب التي تندرج في

[1] وزارة الداخلية ترتكز على التحول الرقمي و التكوين المستمر لتحسين الخدمات العمومية, 2025/04/27, news.nddioalgenie .dz

مجملها ضمن رقابة رئيس الجمهورية السيد عبد المجيد تبون الرامية إلى ترقية شفافية رقمية مواطِنية عمادها التحسيس واليقظة الاستراتيجية.

وبهذا الخصوص نصت افتتاحية المجلة على أنه في ظل النقلة النوعية لطبيعة التهديدات التي يمكن أن تمس بالأمن القومي، لاسيما منها حروب الجيل الجديد، كان لا بد من رفع مستوى التأهب واليقظة ووضع آليات رصد جديدة لكسب رهان الأمن السيبراني، وهو ما يندرج ضمن توصيات السلطات العليا للبلاد وعلى رأسها السيد رئيس الجمهورية.

وفي هذا المنحنى توقفت المجلة عند ماهية الجريمة السيبرانية، مبرزة الارتفاع المسجل في نسق هذا النوع من الجرائم ذو تعدد أشكاله، لتبرز بالمقابل مجهودات المديرية العامة للأمن الوطني من خلال مصالح مختصة للتوعية بمخاطر هذه الجرائم وسبل تفاديها.

وأشارت مجلة الشرطة إلى التنسيق الحاصل بين المصلحة والشرطة الدولية "الأنتربول" حول تورط الأشخاص في القضايا المتعلقة بالجرائم المعلوماتية، على غرار استغلال القُصّر وسرقة المعلومات الخاصة بالبطاقات البنكية وغيرها من جرائم تُرتكب في الفضاء الرقمي.

وفي ذات السياق، تم أيضًا التطرق إلى الشق القانوني المتعلق بالجريمة السيبرانية وفقًا لما ينص عليه التشريع الجزائري، حيث تم تسليط الضوء على جملة من المفاهيم والمصطلحات القانونية الخاصة بهذا النوع من الجرائم[1].

خامسا: الجزائر تتخذ خطوات جديدة لتعزيز التحول الرقمي

[1] السيد لشطر محمد صالح، لأجل مجتمع واعٍ في الفضاء السيبراني، مجلة الشرطة، العدد 158، 5 جوان 2024، ص 17-19، صفحة 22.

أكد وزير البريد والمواصلات السلكية واللاسلكية سيدي علي زروقي أن الجزائر ستتخذ خطوات جديدة نحو التحول الرقمي مشددًا على ضرورة تعزيز التغطية بشبكات النقال وتحسين تجربة المستخدم.

وترأس وزير البريد والمواصلات السلكية واللاسلكية سيدي علي زروقي، حسب بيان للوزارة، في إطار مركبة الاستراتيجية الوطنية للتحول الرقمي وتطور التكنولوجيات الحديثة، لقاء هامًا مع مسؤولي متعاملي الهاتف النقال، بحضور محمد الهادي رئيس مجلس سلطة ضبط البريد والاتصالات الإلكترونية .

وشكل هذا اللقاء فرصة للتأكيد على أهمية اتخاذ التدابير اللازمة لتحقيق أهداف استراتيجية واضحة أبرزها تحسين أداء الشبكة وتوسيع التغطية لتشمل كافة المناطق السكانية وتدارك النقائص المسجلة وتوفير التغطية الكاملة لمحاور الطرق الرئيسية لضمان اتصال مستمر وفعال.

وأبرز الوزير أهمية تحسين سعة التدفق للارتقاء بتجربة المستخدم لتواكب أعلى المعايير الدولية وتسريع إنجاز برنامج الخدمة الشاملة للاتصالات الإلكترونية لتغطية 1400 منطقة ذات كثافة سكانية منخفضة بالهاتف والإنترنت من الجيل الرابع.

وجدد الوزير التزام الوزارة بمرافقة ودعم متعاملي الهاتف النقال لضمان تنفيذ هذه المشاريع الحيوية ضمن الآجال المحددة بما يعكس الرؤية المسطرة لتعزيز البنية التحتية الرقمية وتحقيق تحول رقمي شامل يخدم المواطن ويدفع عجلة الابتكار في الجزائر.

وتبنت الجزائر الاستراتيجية الوطنية للتحول الرقمي 2023/2025 التي تعتبر المرجعية الوطنية والإطار المحدد لتجسيد مسار التحول الرقمي للبلاد، حيث

ترتكز هذه الاستراتيجية على خمسة محاور وهي: البنية التحتية الأساسية لتكنولوجيا المعلومات والاتصالات، والموارد البشرية، والتدريب، والبحث والتطوير، والحوكمةوالرقمنة، والمجتمع الرقمي[1].

سادسا:وزارة العدل

في إطار التعاون مع البرنامج الأوروبي لمكافحة الجريمة السيبرانية :CyberSud

شارك 03 إطارات وقاضيان في الاجتماع السادس للجنة المديرة للبرنامج الأوروبي لمكافحة الجريمة السيبرانية عبر الإنترنت يوم 08 جويلية 2021 من الساعة 9:30 إلى غاية 12 صباحاً بتوقيت الجزائر من تنظيم المجلس الأوروبي، وتم خلال الاجتماع مناقشة التقدم المنجز ضمن هذا البرنامج خلال الأشهر الماضية في الجزائر مقارنة بالنتائج المنتظرة منه وتقديم مقترحات وخطة عمل خلال الفترة المتبقية من هذه السنة واعتمادها، بما في ذلك الجانب المتعلق بتقديم الدعم في برنامج التكوين القاعدي والمستمر في مجال الجريمة السيبرانية.

وشاركت قاضية في دروس عبر الإنترنت باللغة الإنجليزية حول دور النظام البيئي السيبراني للاتحاد الأوروبي في استقرار الأمن السيبراني العالمي من 6 إلى 8 جويلية 2021 من تنظيم هيئة الأمن الرقمي القبرصي وأكاديمية الدفاع والأمن القبرصية تحت رعاية كلية الدفاع والأمن الأوروبية. يهدف هذا التكوين إلى تقديم الركائز الأساسية للنظام البيئي السيبراني للاتحاد الأوروبي ودراسة

[1] نحو تعزيز التغطية بشبكات النقال وتحسين تجربة المستخدم على الرابطhttps://www.elikhbjhij.dz:وتم التصفح فيه2025/04/22.

كيف يمكن لهذه الركائز أن تعزز استقرار الأمن العالمي من خلال تعزيز المرونة السيبرانية وبناء الثقة وزيادة التعاون بين الجهات الفاعلة المعنية وتبادل الآراء وأفضل الممارسات مع خبراء من مؤسسات الاتحاد الأوروبي والدول الأعضاء.

وفي إطار التعاون مع المنتدى العالمي لمكافحة الإرهاب GCTF ، شارك أربعة قضاة منهم قاضيان من مديرية الشؤون الجزائية وإجراءات العفو في ورشة افتراضية حول مكافحة تمويل الإرهاب في منطقة إفريقيا الغربية يومي 6 و7 جويلية 2021 من تنظيم فوج العمل للمنتدى العالمي لمكافحة الإرهاب المكلّف بتعزيز القدرات حول مكافحة الإرهاب في منطقة غرب إفريقيا، والذي تترأسه كل من الجزائر وألمانيا في إطار برنامج عمله السنوي. تشكل هذه الورشة فرصة جيدة لبلدنا لمعرفة القضية الحساسة لتمويل الإرهاب في منطقة غرب إفريقيا والجهود والمبادرات المقدمة بصفة انفرادية أو جماعية من أجل تجفيف مصادر التمويل، واغتنام هذه المناسبة للتذكير مجدداً بتجريم دفع الفدية للجماعات الإرهابية ونتائجه الوخيمة على بلدان وشعوب المنطقة. للعلم، شارك في هذه الورشة الدولية أعضاء المنتدى العالمي لمكافحة الإرهاب، 29 دولة، ودول الاتحاد الأوروبي، و22 دولة إفريقية، و21 منظمة جهوية ودولية. وقد تم تنظيم هذه الورشة بالنظر لتصاعد التهديدات الإرهابية في منطقة غرب إفريقيا والعلاقة الوطيدة للتعاون بين الإرهاب والجريمة العابرة للحدود في هذه المنطقة المجاورة لبلادنا[1].

[1] العمليات التكوينية المبرمجة بالجزائر لفائدة القضاة والموظفين من 4 إلى 8 جويلية 2021 على الرابط www.justice.dzتم التصفح في 6 ماي 2025

وفي إطار التعاون مع المركز العربي للبحوث القانونية والقضائية شارك قاضٍ في الندوة العلمية عبر تقنية التحاضر المرئي عن بعد حول قانونية وعدالة توقيف أي حدث عن الحرية بعد تنفيذ حكم المحكمة والقضاء وإنهاء مدة التوقيف المذكورة في حكم المحكمة، من 6 إلى 8 جويلية 2021 من تنظيم المركزوتم التطرق خلال هذه الندوة إلى إجراءات التوقيف على ذمة التحقيق وكيفية تمديدها، أي الأسباب والمسوغات والسلطة العائد لها هذا الأمر، وإجراءات الحجز الإداري كالأسباب والظروف والسلطات المنوط بها وقانونية وعدالة التوقيف(حجز الحرية الإداري) بعد تنفيذ حكم المحكمة والقضاء وإنهاء مدة التوقيف (عرض تجارب).

سابعا: سوناطراك تقدم لقاء توعوي حول تعزيز ثقافة الأمن السيبراني

شكلت المخاطر والتهديدات السيبرانية محور لقاءٍ توعوي نظمته المديرية المركزية للرقمنة والأنظمة المعلوماتية بمجمع سوناطراكيوم الاثنينبالجزائر العاصمة بغية تعزيز ثقافة الأمن السيبراني ونشر الوعي بين الموظفين حول أهمية الالتزام بالسياسات الأمنية ذات الصلة.

أشرف على افتتاح هذا اللقاء الرئيس المدير العام لسوناطراك رشيد حشيشي، بمقر المديرية العامة للمؤسسةبحضور المدير العام لوكالة أمن الأنظمة المعلوماتية لدى وزارة الدفاع الوطني العميد عبد السلام بلغول إلى جانب مشاركة الإطارات المسيرة ومدراء نشاطات المؤسسة وهياكلها الوظيفية ك وذلك بغية تعزيز ثقافة الأمن السيبراني ونشر الوعي بين الموظفين بأهمية الالتزام بالسياسات الأمنية ذات الصلة.

بالمناسبة، أكد السيد حشيشي أن الجرائم الإلكترونية تعد مسألة حساسة وتشكل تهديدا حقيقيا يمكن أن يؤثر على أمن وديمومة العمليات الصناعية لسوناطرا ك كما يضع الإطارات المسيرة في صدارة المعركة للوقاية من هذه المخاطر والتهديدات .

كما شدد على ضرورة إدراك رهانات الأمن السيبراني والمخاطر السيبرانية لحماية البيانات والأنظمة والشبكات، وألحّ على ضرورة الحرص على التطبيق الصارم للتوجيهات المتعلقة بالأمن السيبراني في المنشآت الصناعية، سيما منها تلك الصادرة عن المصالح الداخلية المتخصصة، وتلك التي ترد من السلطات العليا للبلاد عبر وكالة أمن الأنظمة المعلوماتية.

ومن جانبه، أكد المدير العام لوكالة أمن الأنظمة المعلوماتية لدى وزارة الدفاع الوطني أن الأمن السيبراني مهمة معقدة وحساسة ومشتركة تتطلب من جميع الفاعلين الوطنيين في مختلف الميادين مضاعفة اليقظة والجهود من أجل المحافظة على السيادة الوطنية الرقمية، لا سيما في السياق الحالي، مشيراً إلى أن مشروع إعداد الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية قد بلغ مرحلته النهائية .[1]

وفي وثيقة تم توزيعها على الصحافة بالمناسبة، أشارت سوناطراك إلى أنها تعتمد استراتيجية شاملة بخصوص إدارة مخاطر الأمن السيبراني، تستند على تنفيذ سياسات وقائية تعتمد على أحدث التكنولوجيات، واتخاذ إجراءات صارمة لحماية البيانات والأنظمة الحيوية. كما تركز على نشر وتعزيز الوعي الأمني

[1] تنظيم لقاء توعوي حول ثقافة الأمن السيبراني على الرابط www.jps.dz تم التصفح في 6 ماي 2025.

بين الموظفين، حيث يتم تدريب المستخدمين على أساسيات الأمن السيبراني لتجنب الأخطاء الشائعة مثل النقر على روابط غير معروفة أو الولوج إلى حسابات الشركة عبر شبكة غير آمنة.

وعرف اللقاء عدة تدخلات تناولت التهديدات والهجمات الإلكترونية التي قد تعطل الأنظمة التكنولوجية للمؤسسات وتعرقل خدماتها المعلوماتية. وتشمل هذه التهديدات، التي تؤثر بشكل كبير على استقرار وأمن المؤسسات في عصر التحول الرقمي، اختراقات البيانات، والاحتيال الإلكتروني، والتجسس الإلكتروني، وكذا تخريب المنشآت الحيوية عن طريق البرمجيات الخبيثة، حسب الشروحات المقدّمة. كما ناقش المتدخلون عدة محاور لمواجهة المخاطر السيبرانية، وأكدوا على الحاجة إلى إرساء تعاون بين جميع الأطراف المعنية، مع التشديد على أهمية تعزيز التنسيق مع الهيئات الحكومية المعنية من أجل تبادل المعلومات والخبرات.

الفرع الثاني: العلاقة بين الأمن السيبراني والأمن القومي

في عصر الثورة التقنية والمعلوماتية وجب الوقوف على حدود التفاعل الرقمي القائم بين أمن المعلومات الإلكترونية والأمن القومي للدول، فمع انصهار الحدود الجغرافية وتقلص المسافات بين أركان المعمورة بفعل الثورة الإلكترونية، أحدثت هذه التغييرات العديد من التأثيرات على الأمن القومي نتيجة البيئة التكنولوجية التي أتاحت للدول إمكانية الولوج في فضاء إلكتروني يحوي العديد من عناصرها

ومعلومات القومية والأمنية والاقتصادية والسياسية والاجتماعية وغيرها من المقومات[1].

لقد أصبحت العلاقة بين الأمن والتكنولوجيا علاقة متزايدة، مع إمكانية تعرض المصالح الإستراتيجية ذات الطبيعة الإلكترونية إلى أخطار إلكترونية و دد بتحول الفضاء الإلكتروني الى وسط ومصدر الأدوات الجديدة للصراع المتعدد الأطراف ودورها في تغذية التوترات الدولية.[2]

ومن جهة أخرى فرضت تلك التطورات إعادة التفكير في مفهوم الأمن القومي الذي يعنى بحماية قيم المجتمع الأساسية وإبعاد مصادر التهديد عنها وغياب الخوف من خطر تعرض تلك القيم للهجوم، وبذلك يتوافر أمن الفضاء الإلكتروني حال تحقيق إجراءات الحماية ضد التعرض للأعمال العدائية وللإستخدام السيئ للتكنولوجيا الإتصال والمعلومات.[3]

فالأمن بمفهومه العام يشير نظريا وعمليا إلى "السلام والطمأنينة وديمومة مظاهر الحياة واستمرار مقاوماتها وشروطها بعيدا عن عوامل التهديد ومصادر الخطر[4]."

---

[1] عادل عبد الصادق، "الحروب السيبرانية: تصاعد القدرات والتحديات للأمن العالمي"، (المركز العربي لأبحاث الفضاء الإلكتروني، د.ش، 2017.)، ص02.

[2] عادل عبد الصادق، "ال الأعلى للأمن السيبراني خطوة في دعم استراتيجية الأمن القومي"، الرابط 2019/03/01. : التصفح تاريخwww.aceronline.com/article-detal.Aspxd=20284

[3] دل عبد الصادق، "الحروب السيبرانية: تصاعد القدرات والتحديات للأمن العالمي"، مرجع سابق، ص04

[4] لي عباس مراد، "الأمن والأمن القومي، مقاربات نظرية"، (الجزائر: ابن النديم للنشر والتوزيع، 2017 ،ص 12.

لقد أصبح الأمن السيبراني والإلكتروني جزء لا يتجزأ من الأمن القومي خاصة مع تنامي حجم التهديدات وعلاقة البعد الإلكتروني بعمل المنشآت الحيوية سواء كانت مدنية أو عسكرية[1].

ويمكن الإشارة هنا إلى أن الأمن القومي لأي دولة له محاوره الرئيسية والمتمثلة في المحاور العسكرية السياسية، الجغرافية، الاجتماعية، الاقتصادية والأمنية وأخيرا التقنية، وهو المحور الذي يهم الدول اليوم نظرا لاستنادها على منظومة تقنية وإلكترونية عالية الدقة

وغزيرة التكنولوجيا تعتمد على صناعة المعلومات والبحث العلمي والمعلوماتي في جميع الجوانب، ولذا يمكن الإشارة إلى أن الأمن القومي المعلوماتي هو عبارة عن "مدى جاهزية الدول من الناحية التقنية والمعلوماتية لحماية مخزونها الإلكتروني من المعلومات وعدم الوصول إليها بأية طريقة تقنية أو تقليدية[2]."

لقد أدخلت ثورة المعلومات دول العالم في هاجس أمني قوي خاصة وأن هذه الدول قد قامت بوضع مدخرا القومية على شكل معلومات رقمية عبر فضاء مذاب الخصوصية وضعيف الأمن لبعض دول العالم وفائق السرعة ومتغيرة بشكل كبير، مما زاد من الفجوة المعلوماتية القومية بين الدول. شكل هذا التعاونالمعلوماتي القومي بين دول العالم هاجس الخوف من الطرف الآخر ومدى امتلاكه للأسلحة التكنولوجية والمعلوماتية المدمرة والتي لم تعد حكرا على القطاعات العسكرية للدول فحسب، بل أصبحت سلاحا تتقن استخدامه غالبية مستخدمي الحواسيب ووسائل الاتصال الحديثة، وفي صورة زادت من تفاعل

[1] ادل عبد الصادق، موقع سابق.

[2] وليد غسان سعيد جلعود، "دور الحرب الإلكترونية في الصراع العربي الإسرائيلي"، أطروحة ماجستير في التخطيط والتنمية السياسية (بكلية الدراسات العليا، جامعة نابلس، فلسطين، 2013 ،(ص53

المعلومات الإلكترونية والأمن القومي بحيث رفعت من وتيرة الخوف الذي تعاني منه شعوب العالم المعاصر.

ومن هنا نستنتج أن الأمن السيبراني والأمن القومي يتشابكان من ناحية الهدف، حيث يسعى كل منهما إلى حماية البنى التحتية والحدود من كل الاختراقات التكنولوجية والتخوف من زعزعة أمن الدول.[1]

المطلب الثاني: اهتمام الجزائر بالأمن السيبراني

الفرع الأول: أسباب اهتمام الجزائر بالأمن السيبراني

من بين أسباب اهتمام الجزائر بالأمن السيبراني نجد فيما يلي:

أولا : أسباب سياسية

هناك أمثلة كثيرة تدفع نحو الاهتمامبهذا الجانب كالتسريبات المختلفة للوثائق الحساسة التي تؤدي إلى مشكلات عويصة جدا على المستوى الخارجي والدولي كما أنه لا ينكر أحد الدور المتعاظم لشبكات التواصل الاجتماعي على المستوى السياسي (حملات انتخابية، تظاهرات الكترونية ،حركات احتجاجية الكترونية . كما يتم استغلال هذه المواقع من طرف العديد من الحكومات لتمرير سياستها وفي سياق اخر يجب أن لا نغفل عن استخدام هذه المواقع من طرف الحركات الإرهابية لتجنيد أفرادها وجمع التمويل لعملياتها ،واليه للاتصال بينها كأفراد وكجماعات، وهو ما استوجب على الدول العمل على حماية أمنها من التهديدات والمخاطر التي تتعرض لها من خلال شبكات الانترنت.

ثانيا : أسباب عسكرية وأمنية

[1] وليد غسان سعيد جلعود، مرجع سابق، ص54

شكل التطور الاهتمام التقني بالشبكات وبرامج المعلوماتية أهم عناصر لفك ألغز الجرائم السيبرانية محور اهتمام مؤسسة الدفاع الوطني في تطوير إمكاناته وقدراته على جميع الأصعدة ،ويكمن أن يلاحظ بشكل جلي في درجة الاحترافية التي يتمتعبها أفراد الدرك

الوطني فقد استطاعت لحماية البنى التحتية المعلوماتية ضد كل المخاطر الرقمية ،وتكوين أفرادها على المستويات ويتضح ذلك في الأدوار التي تؤديها انجازاتها، إذا يعتكف إفراجها وضع التدابير اللازمة لمنع تسرب امتحانات البكالوريا 2017.[1]

واستطاعت قيادة الدرك الوطني من خلال التكوين المستمر والمتميز لأفرادها والملتقيات الدولية والوطنية وتبادل الخبرات مع دول أخرى أن توفر القوى المؤهلة وذات الكفاءة من مهندسي الإعلام الآلي، رجال القانون، وهذا من أجل التصدي لها في ذات السياق استطاع مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني رصد أزيد من 100جريمة الكترونية سنة2014 وما يفوق 500 قضية رقمية خلال سنة 2015 ،منها 300 جريمة تتعلق بمواقع التواصل الاجتماعي "فيسبوك"و 20 جريمة رقمية تعلقت بإختراق مواقع رسمية لمؤسسات خاصة وعامة ،استهدف مجرموها أنظمة المعالجة الآلية للمعطيات ويتحقق

الدفاع الوقائي الالكتروني وفق ثلاث أساليب رئيسية:

[1] بن مرزوق عنترة، حرشاوي محي الدين،" الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية "، الملتقى الدولي حول سياسات الدفاع الوطني، (جامعة قاصدي مرباح ورقلة، كلية الحقوق والعلوم السياسية،31/01/2017 ص 12

1. **الكشف المبكر عن الهجمات في وقتها الحقيقي:** وذلك باستخدام sensorsعلى شبكات والبرامج والتطبيقات مع توظيف المعلومات الاستخبارتية .
2. **الهجوم الالكتروني ألاستباقي** : وذلك بنشر الديدان البيضاء worms whiteباعتبارها برامج قادرة على اكتشاف التطبيقات الضارة وتدميرها قبل التوظيف، وإطلاق هجمات الكترونية مضادةBack Hack
3. **التضليل والإخفاء والتضليل والخداع:** وذلك بإخفاء هويات الأهداف الإستراتجية للدولة للأنترنيت عن طريق تضليل الخصوم بأدوات التمويه والخداع وتغيير ملامح الأهداف واستجابة لمطلب الأمن المعلوماتي ومحاربة التهديدات الأمنية الناجمة عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وأضيف هيكل تنظيمي لمديرية الشرطة القضائية.الالكترونية قامت مصالح الأمن بإنشاء المصلحة المركزية للجريمة الالكترونية التي عملت على تكييف التشكيل الأمني لمديرية الشرطة القضائية لمحاربة الجريمة الالكترونية على مستوى المديرية العامة للأمن الوطني والتي أنشئت سنة 2011 ،ليتم بعدها انشاء المصلحة المركزية لمحاربة الجرائم

ثالثا: أسباب قانونية

يترتب على النشاط الفردي والمؤسساتي والحكومي، في الفضاء السيبراني، نتائج قانونية وموجبات تستدعي اهتماما خاص ،لحل ال نزاعات التي يمكن أن تنشأ عنها وتستدعي مواكبة التحولات التي رافقت ظهور مجتمع المعلومات ،فظهرت حقوق أخرى،كحق النفاذ إلى الشبكة العالمية للمعلومات توسعت بعض المفاهيم، لتشمل أساليب الممارسة الجديدة باستخدام تقنيات المعلومات

والاتصالات كالحق في إنشاء المدونات الالكترونية، والحق في إنشاء التجمعات على الانترنت، والحق في ملكية البرامج المعلوماتية كما ظهرت موجبات جديدة ذات انعكاسات 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 على المستوى الحقوق أو على مستوى البيئات والعمليات[1].

الفرع الثاني: الاتفاقيات الجزائرية في مجال الأمن السيبراني

أولا: على المستوى العربي والإفريقي

من خلال الدراسات الأكاديمية وتحليل المعطيات الملقاة من المؤسسات المتخصصة في الأمن السيبراني، والمتضمنة النقائص والثغرات في حماية الأنظمة المعلوماتية للدول العربية، المعلن عنها خلال اللقاءات، يتضح أن المقومات البشرية والمادية المتوفرة والقادرة على تفادي المخاطر لم تجدِ نفعاً، والدليل أن السلبيات التي أصبحت تشكل نسبة كبيرة من المخاطر لا تزال تطرح نفسها بشدة[2].

ورغم تعدد اللقاءات والاجتماعات والندوات التي توالت في السنوات الأخيرة حول الجرائم الإلكترونية ومختلف التهديدات التي تتربص بالأمن القومي العربي عموماً، فإنه من غير المعقول أن تتصف كل تلك الأعمال والمنشآت بالهامشية وعدم الجدية في التجاوب معها من طرف صانع القرار العربي، فكل أو جل

[1] سمير بارة،" الأمن السيبراني في الجزائر السياسات والمؤسسات "، المجلة الجزائرية للأمن الإنساني، العدد الرابع، (جويلية 2017 ,ص 14.

[2] جمال بوزديه، "الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية: التحديات والآفاق المستقبلية"، مجلة العلوم القانونية والسياسية، المجلد 04، العدد رقم 01، الجزائر، أفريل 2019، ص. 284

الآليات المطبقة في الدول العربية ميدانياً غير فعالة مقارنة مع المعايير الدولية، وكذلك ضعف الأداء الداخلي للقوانين والتنظيمات والهيئات الموكلة إليها هذه المهام .

وفي نفس الإطار وبغية تحقيق التكامل بين المؤسسات الأمنية والقضائية العربية، سعت الدولة الجزائرية من دائرة التقارب لتشمل تبادل الزيارات الميدانية، الدورات التكوينية، واللقاءات التشاورية في المجالات التي شملتها السياسة الجنائية لمكافحة الإجرام عامة، والاستفادة من خبرات بعض الدول العربية والتعرف على البيئة التشريعية، وكذا الآليات المستعملة في مواجهة الفضاء السيبراني والقدرات البشرية المسخرة لهذه المهمة[1].

وفيما يخص التعاون مع الدول الإفريقية، وكذا الاتحاد الإفريقي في حد ذاته، يمثل خطوات هامة بالنسبة للجزائر التي تحاول الدفع جاهدة في مجال الأمن السيبراني نحو الأمام، على الرغم من التفاوت والاختلافات المسجلة في هذا الصدد من دولة لأخرى.

وبتاريخ 27 جوان 2014، قطع الاتحاد الإفريقي شوطاً مهماً في طريقه لتجسيد مسار رقمنة إفريقيا، بحيث تبنى خلال قمته 23 التي انعقدت بمالابو بجمهورية غينيا الاستوائية اتفاقية حول الأمن السيبراني وحماية البيانات الشخصية، [2] والتي كانت الجزائر إحدى أهم الدول الأعضاء المشاركين بفعالية في بلورة نتائج واقعية وملموسة على أرض الواقع.

[1] نفس المرجع, 285.

[2] جمال بوازدية, مرجع سابق, ص 294.

وتحكي معاهدة مالابو درجة وعي الدول الإفريقية بالخطر الذي يهددها، بحيث يندرج تبنيها ضمن حرص دول الاتحاد الإفريقي على تحيين قوانينها وتشريعاتها الإقليمية في مجال الأمن السيبراني، ومن أهمها القرار بشأن تكنولوجيا الإعلام والاتصال في إفريقيا، وإعلان أوليفر تامبو 25 بتاريخ 9 نوفمبر 2009، وإعلان أبيجان بتاريخ 22 فيفري 2012، وكذا إعلان أديس أبابا الصادر في 22 جوان 2012[1].

واكتشف مهندسون جزائريون وإثيوبيون متخصصون بأنظمة المعلومات أجهزة تجسس مزروعة في كافة أرجاء مقر الاتحاد الإفريقي الذي بناه الصينيون عام 2012 في العاصمة الإثيوبية أديس أبابا، وقالت صحيفة لوموند الفرنسية إنه وفقاً لمسؤولي أنظمة المعلومات في المقر، وضع الصينيون أجهزة تنصت في كل المصاعد وجذوع النخيل البلاستيكية، بما في ذلك البرج الزجاجي الحديث الذي أنشأته الصين عام 2012 والذي تُعقد فيه القمة الإفريقية، ووفقاً لعدة مصادر داخل مقر الاتحاد الإفريقي، تجسست الصين على محتويات ومعلومات حساسة وقامت بتسريبات مذهلة[2].

ثانيا: على المستوى الأوروبي

لتشييد مبدأ الشراكة الأورو–متوسطية الذي وقعت عليه الجزائر مع الدول الأعضاء في الوحدة الأوروبية بتاريخ 22 أفريل 2002، المتضمنة التعاون في المجال الأمني والقضاء لمحاربة مختلف الجرائم، وذا الاتفاق المبرم مع فرنسا

[1]: إسماعيل جنادي، "الأمن السيبراني: التحدي القادم للاتحاد الإفريقي"، مجلة الجيش، العدد 63، أكتوبر 2018، ص. 44

[2]موقع الجزيرة، حسب لوموند الفرنسية: "الصين زرعت أجهزة تجسس بمقر الاتحاد الإفريقي"، بتاريخ 2018/01/18، www.aljazeera.net، تم الاطلاع عليه يوم 07 ماي 2025

بتاريخ 25 أكتوبر 2003 المتضمن التعاون في المجال الأمني ومكافحة الإجرام المنظم، وانطلقت الجزائر في خطوة بعنوان التعامل لمواجهة الجرائم السيبرانية في الضفة الجنوبية للاستفادة من التجربة الأوروبية، وعقدت في هذا الشأن عدة لقاءات في الجزائر جمعت فريقاً من الخبراء من مختلف المؤسسات الفاعلة في هذا المجال وخبراء أجانب[1].

ثالثا: على المستوى الدولي

تمت مطابقة التشريع الداخلي مع ما جاء في التشريعات الدولية، وخاصة الاتفاقية الدولية المبرمة في عاصمة المجر بودابست بتاريخ 23 نوفمبر 2001، المتضمنة الجرائم السيبرانية. وتُعتبر هذه الاتفاقية بمثابة المرجعية القانونية لكل التشريعات الدولية الصادرة في هذا المجال، ويُعتبر التعاون الإقليمي والدولي في مكافحة التهديدات السيبرانية بالنسبة للدولة الجزائرية شكلاً من أشكال المؤشرات الخمسة التي أقرها الاتحاد الدولي للاتصالات السلكية واللاسلكية سابقا[2].

[1] جمال بوازدية، مرجع سابق، ص. 286

[2] نفس المرجع, ص 286.

الخاتمة

الخاتمة

إن مايتم استخلاصه من هذه الدراسة المتعلقة بموضوع الأمن السيبراني والذي هو يندرج ضمن المفهوم الاوسع للأمنالسيبراني بصفة عامة ،وكل القضايا المتعلقة به والتي تشكل جوهر وأساس وجود البشر لما يمثله هذا العنصر الحيوي من أهمية قصوى في حياتهم مهما حدث له من تحول وتغير في مفهومه ومكوناته وكذا عناصره.

ففي ظل التسارعات والتجاذبات الرهيبة لعناصر الاعلام الآلي و تكنولوجيا الاتصالات و المعلومات ،التي جعلت من العالم كله ومن يسكنه بمثابة قرية واحدة موحدة، تبرز لنا في هذا الشأن أهمية مجال الأمن السيبراني كتحد يفرض نفسه بقوة في الحياة لا غنى لنا عنه بما أن أغلب خيوط العلاقات التي تربط بين الدول و الديانات مجموعات وأفراد هي خيوط تكنولوجيا بحثة تستلزم منا جميعا الحيطة والحذر في التعامل مع بعضنا البعض.

وفي الجزائر وكغيرها من الدول كان لزاما عليها التوجه نحو تبني مقاربة معينة في مجال الدفاع السيبراني على غرار مقاربتها الامنية التي اعتمدت في سبيل مكافحة الارهاب سابقا ،وهذا إدراكا من صانع القرار بأهمية ايلاء أهمية قصوى لهذا المجال الحيوي الذي تتشابك فيه عناصر التكنولوجيا ودفعا نحو التصدي الحازم لمختلف التهديدات الموجودة والمحتملة في هذا الشأن وبالتالي شكل الأمن السيبراني الجزائري قطعة أساسية من أساليب الاستراتيجية الدفاعية ككل.

وللوقوف على مدى نجاعة هذه السياسات و الاستراتيجية المعتمدة في الجزائر ،كان من المهم إسقاطها على مؤشرات وتقارير إحدى أهم المؤسسات و الهيئات الدولية التابعة للأمم المتحدة والمتخصصة في هذا الشأن ألا وهي الاتحاد الدولي للاتصالات السلكية واللاسكية ،وذلك من خلال المؤشرات الخمسة التي تم وضعها في هذا الخصوص والتي من خلالها يمكن قياس مدى التزام الدول وحالة تأهيلها لمعايير وسمات السلامة السيبرانية وهو ما أظهرت الدراسة التي أسقطت على الجزائر مدى تقدمها أو تراجعها أو حتى أخرها مقارنة مع هذه المعايير والمؤشرات الموضوعية.

والجزائر كغيرها من الدول اتجهت نحو تبني مقاربة الحكومة الالكترونية ،وعلى الرغم من حداثة التوجه إلا أن عدد الجرائم المرتكبة يوحي بحجم الاخطار التي تتربصها ،وهو مايجعل مؤسسة الدفاع الوطني أمام تحدي جديد ،وهو تحقيق الأمن السيبراني.

وختاما،نورد بعض التوصيات ،التي يتبناها المرصد العربي السلامة والامن في الفضاء السيبراني ،وأهمها:

- التزام القرارات الصادرة عن الامم المتحدة وعن القمة العالمية لمجتمع المعلومات بشقيها ،والداعية إلى نشر ثقافة الأمن السيبراني.
- اتخاذ تدابير تعتمد الأمن كعنصر ضروري في الإنتاج ،لاسيما ما يخص البرامج والاجهزة المستخدمة في تقنيات الاتصال.
- وضع إطار تعاون ،يضمن تبادل المعلومات ،ونقل الممارسات الفضلى،في المجال الامنية.
- تأميم انسجام الانظمة القانونية ،المكافحة للجرائم السيبرانية ،بما يمنع نشوء جنات رقمية .
- وضع استراتيجية لنشر الوعي ،وبنائه ،لدى مختلف شرائح المجتمع ،سواء منهم المستخدمين العاديين ،او المهنيين ،أو متخذي القرار،والمسؤولين عن سياسات الأمن و السلامة .
- اعتماد مبادئ خلقية للسلوك السيبراني ،على مثال اخلاقيات وأصول التعامل القائمة في المجتمع التقليدي ،وتكون بمثابة عقد اجتماعي ،يؤسس لسلوك يضمن سلامة الجماعة وسلامة مواردها.
- وضع إستراتيجية ،وسياسة أمنية واضحة وملزمة،لكل المغنيين بصناعة المعلومات ،وبادراه وسائل الاتصالات ،والبني التحتية ،كما لأولئك المغنيين بصناعة أدوات وبرامج الاتصال ،وخزن المعلومات ومعالجتها.
- أخذ جميع أبعاد الأمن السيبراني ،بعين الاعتبار لدى وضع أي إستراتيجية أو سياسة ،بما في ذلك ،حاجات المواطنين و المؤسسات ،كما حقوقهم وواجباتهم ،بحيث تأتي الخطة متكاملة ،ومنسجمة مع مايمكن توقع الالتزام به ،من قبل المعنيين ،بأمن مجتمع المعلومات.

- الاقرار بامسؤولية عن تحقيق الأمن السيبراني ،كجزء لايتحزأ من الأمن القومي و الوطني.
- إنشاء مراكز للسلامة المعلوماتية ،ولطوارئ الاتصالات ،تتعاون فيما بينها، وفق الية واضحة وشفافة وفاعلة
- تدريب وتأهيل وحدات عسكرية وأمنية خاصة،يمكنها مراقبة البنى التحتية للاتصالات ،بحيث تقوم بتحديد المخاطر المحتملة ،وإزالتها.
- تأهيل الاجهزة القضائية المختصة ،والشرطة القضائية ،بحيث تتمكن من القيام بواجبها ،في مجال ملاحقة ومحاكمة المجرمين السيبرانيين .
- تحويل الأمن السيبراني ،إلى جزء من خطط التنمية والتطوير كافة .
- توجيه دعوة من خلال جامعة الدول العربية ،الى دول العالم ،لمناقشة إقرار معاهدة دولية ،تنطلق ديباجتها من مقررات القمة العالمية لمجتمع المعلومات ،مضافا إليها ،الاقرار بضرورة عدم تحويل الفضاء السيبراني الى مجال يهدد السلم الدولي ،مع الالتزام بعدد من المبادئ ،وفي مقدمها : مبدأ سيادة الدول ،والمساواة فيما بينهم، وحق كل دولة في الافادة من قدرات تقنيات المعلومات و الاتصالات ،بما يضمن قدرتها على المنافسة في هذا المجال ،وتحقيق رفاه شعوبها.
- إنشاء هيئات تحكيم وطنية ،متخصصة في القضايا السيبرانية ،وخدمات استشارات ،مسبقة ولاحقة لأي نشاط الكتروني ،يمكن أن يرغب اللجوء إليها.

المصادر والمراجع

قائمة المصادر والمراجع

المراجع باللغة العربية:

أولا :الكتب

1 -أمال قارة ،الحماية الحزائية للمعلوماتية في التشريع الجزائري ، الطبعة الاولى ، دار هومة ، الجزائر.

2 -حسن بن أحمد الشهري ، الانظمة الالكترونية الرقمية المطورة لحفظ وحماية سرية المعلومات من التجسس ، مركز الدور للأبحاث الالكترونية، 2010 .

3 -حسن بوسعتيعة ، الوجيز في القانون العام ، الطبعة الاولى ، الديوان الوطني للأشغال التربوية ، الجزائر ، 2002 .

4 -صلاح سالم ، تكنولوجيا المعلومات والاتصالات والامن القومي للمجتمع ، الطبعة الاولى ، عين الدراسات والبحوث الانسانية والاجتماعية ، الطبعة الاولى ، منشورات الحلبي الحقوقية ، سنة 2005 ، بيروت .

5 -عبد الفتاح بيومي حجازي ، الاثبات الجنائي في جرائم الكمبيوتر و الانترنت ، دار الكتب القانونية ، مصر ، 2015 .

6 -فارس محمد العمارات ، إبراهيم الحمامصة ، الأمن السيبراني (المفهوم وتحديات العصر) ، الطبعة الاولى ، دار الخليج للنشر والتوزيع ، الأردن ، عمان ، 2022 .

7 -نائلة عادل محمد فريد ، جرائم الحاسب الآلي الاقتصادية ، الطبعة الاولى ، منشورات الحلبي الحقوقية ، سنة 2005 ، بيروت .

ثانيا : المذكرات و الرسائل

1 – بكوش رميساء ، انعكاسات التهديدات السيبرانية على الأمن الوطني الجزائري ، مذكرة ماستر ، جامعة العربي التبسي ، كلية الحقوق والعلوم السياسية

2 – بلال بن جامع ، الجرائم الالكترونية على شبكة الانترنت دراسة حالة ، جامعة عبد الحميد مهري ، قسنطينة 02 ، رسالة دكتوراه ، مكتب علم التوثيق ، 2017/2016 .

3 – بن مرزوق عنترة ، الأمن السيبراني كبعد في السياسة الدفاعية الجزائرية ، جامعة محمد بوضياف ، المسيلة ، كلية الحقوق والعلوم السياسية ، المركز الجامعي أفلو.

4 – بوزادية جمال ، الأمن السيبراني ، محاضرات مقدمة للطلبة السنة الثانية ماستر ، جامعة الجزائر 03 ، كلية العلوم الانسانية و العلاقات الدولية ، 2021_2020 .

5 – حمزة بن عقون ، السلوك الاجرامي للمجرم المعلوماتي ، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية ، تخصص 01 علوم الإجراء والعقاب ، جامعة باتنة ، 2011 _2012 .

6 – حنان براهمي ، جريمة تزوير الوثيقة الرسمية الادارية ذات الطبيعة المعلوماتية ، أطروحة دكتوراه ، كلية الحقوق والعلوم السياسية ، تخصص جنائي ، جامعة محمد خيضر ، بسكرة .

7 – سارة بوحادة ، أثر الارهاب الالكتروني على أمن و استقرار الدول ، أطروحة دكتوراه ، جامعة الجزائر 3_3 ، المدرسة الوطنية العليا للعلوم السياسية ، تخصص دراسات دولية ،2014 .

8 – سعيدة بدرة ، الجريمة الالكترونية في التشريع الجزائري ، مذكرة لنيل شهادة الماستر ، دراسة مقارنة ، 2015، 2016 .

9 – طمطامي سالم ، الصفاحة الالكترونية والامن السيبراني ، مذكرة لنيل شهادة الماستر في الاعلام والاتصال ، جامعة أحمد راية ، ولاية أدرار ، كلية العلوم الانسانية والاجتماعية.

10 – عائشة نايري ، الجريمة الالكترونية في التشريع الجزائري ، مذكرة لنيل شهادة الماستر ، حقوق تخصص قانون إداري ، جامعة أدرار ، 2016/2015.

11 – عباس حفصي ، جرائم التزوير الالكتروني ، دراسة مقارنة ، أطروحة دكتوراه ، جامعة وهران 01 ، أحمد بن بلة ، كلية العلوم الانسانية ، تخصص شريعة و قانون ،2015 .

12 – وليد غسان بلعود ، دور الحرب الالكترونية في الصراع العربي الاسرائيلي ، أطروحة ماجستير في التخطيط والتنمية السياسية ، جامعة نابلس ، فلسطين ، 2013 .

13 – يوسف صغير ،الجريمة المرتكبة عبر الانترنت ، رسالة ماجستير ، جامعة مولود معمري ، تيزي وزو ، كلية الحقوق ، تخصص قانون دولي للأعمال ، 2014 .

ثالثا : المجلات و الملتقيات

1 -أحمد السيد النجار ، محمد عبد الهادي علام ، حروب المعلومات من يواجهها ؟ مجلة الاهرام ، العدد 139 ، 13 يوليو 2015 .

2 -أحمد عبيس الفتلاوي الهجمات السيبرانية مفهومها و المسؤولية الدولة الناشئة عنها في ضوء التنظيم الدولي المعاصر ، مجلة العلى للعلوم القانونية والسياسية ، كلية القانون ، جامعة بابل ، العدد 04 ، 2016 .

3 -اسماعيل جنادي ، الأمن السيبراني: التحدي القائم للاتحاد الأفريقي ،مجلة الجيش ، العدد 63 ، أكتوبر 2018 .

4 -السيد لشطر محمد صالح ، لأجل مجتمع واع في الفضاء السيبراني ، مجلة الشرطة ، العدد 158 ، 5 جوان 2024 .

5 -إدريس عطية ، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري ، مجلة مصداقية ، كلية الحقوق والعلوم السياسية ، جامعة العربي التبسي ، تبسة ، الجزائر ، المجلد 01 العدد 01 ، 2019

6 -أمال بوجليدة ، الاقتصاد الرقمي التحول من الاقتصاد الصناعي إلى اقتصاد المعلومات ، مجلة الخبير ، العدد 63 ، جانفي2016.

7 -أمجد المنيف ، الارهاب الالكتروني " المعركة حديثة " ، المجلة العربية ، العدد 07 ، يوليو 2015 .

8 -بن صابر بلقاسم ، حيدرة محمد ، الصدمات السيبرانية ومواجهتها في ضوء القانون الدولي المعاصر ، مجلة حقوق الانسان والحريات العامة ، جامعة مستغانم ، المجلد 02 ، العدد 04 ، جوان 2017 .

9 -رعد خضر صليبي ، تعزيز الأمن السيبراني في العراق (التحديات والفرص) ، مجلة دراسات دولية ، العدد 99 ، 2024/10/30 .

10 -روان بن عطية الله الهحفي ، الجرائم السيبرانية ،المجلة الالكترونية الشاملة متعددة التخصصات ، العدد 24 ،شهر 15 سنة 2020 .

11 -سالم عبد الرزاق ، ملتقى حول المنظومة التشريعية الجزائرية في مجال الجريمة المعلوماتية ، محكمة سيدي محمد ، الحزائر .

12 -سمير بارة ، الأمن السيبراني في الجزائر السياسات و المؤسسات ، المجلة الجزائرية للأمن السيبراني ، المجلد 02 ، العدد 04 ،2017 .

13 -قطاف سليمان ، الاليات الموضوعية و الإجرائية المتبعة لتحقيق الأمن السيبراني ، مجلة الحكومة و القانون الاقتصادي ، المجلد 20 ، 2022 .

14 -كريمة علة ، الجهات القضائية الجزائية ذات الاختصاص الموسع ، المجلة الاكاديمية للبحث القانوني ، المجلد 11 ، العدد 01 .

15 -لامية طالمة ، التهديدات والجرائم السيبرانية وتأثيرها على الأمن القومي للدول واستراتيجيات مكافحتها ، مجلة معالم للدراسات القانونية والسياسية ، المجلد 04 ، العدد 02 ، 2020 .

16 -محمد مختار ، , cyber security هل يمكن أن تتجنب الدولة مخاطر الهجمات الالكترونية ؟ ، مجلة مفاهيم المستقبل ، العدد 06 ، بيروت ، لبنان ، يناير 2015 .

17 -مختار الاخضري ، الإطار القانوني لمواجهة الجرائم المعلوماتية في الفضاء الافتراضي ، مداخلة ألقيت خلال أعمال الملتقى الأول ، الجزائر بعنوان محاربة الجريمة المعلوماتية و القضائية ، طبعة 2011 .

18 -مهدي رضا ، الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري ، مجلة إيليزا للبحوث والدراسات ، المجلد 06 ، العدد 02 ،2021 .

19 -نوارة حسين ، آليات تنظيم المشرع الجزائري لجريمة الاعتداء على الحق في الحياة الخاصة الكترونيا ، الملتقى الوطني: آليات مكافحة الجرائم الالكترونية في التشريع الجزائري ، كلية الحقوق والعلوم السياسية ، جامعة مولود معمري ، تيزي وزو ، الجزائر ، 2017 .

رابعا : الاتفاقيات و القوانين

1 -الاتفاقية التي صدرت في بوداباست سنة 2001 ،الصادرة عن وكالة الأمن الرقمي الاوروبية .

1 - القوانين:

2 - المادة 53 من القانون 07_ 18 مؤرخ في 10 يونيو 2018 ، متعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي ، الجريدة الرسمية ، العدد 34 ، الصادر بتاريخ 10 يونيو 2018 .

3 – المادة 13 من القانون 04_18 المؤرخ في 10 ماي 2018 ، الذي يحدد القواعد العامة المتعلقة بالبريد و الاتصالات الالكترونية ، الجريدة الرسمية ، العدد 27 ، الصادرة بتاريخ 13 ماي 2018 .

4 – قانون رقم 06_ 22 ، مؤرخ في 2006/12/20 يعدل ويتمم بالامر رقم 66 _ 155 يتضمن قانون الإجراءات الجزائية ، عدد 84 الصادر في 2006/12/24 .

5 – المادة 10/03 من القانون رقم 18/04 المؤرخ في 24 شعبان عام 1933 الموافق 10 يونيو سنة 2018 ، الذي يحدد القواعد العامة المتعلقة بالبريد و الاتصالات الالكترونية ، الصادر في الجريدة الرسمية الجزائرية ، العدد 02 .

6 – المادة 102 من القانون 04/09 المؤرخ في 14 شعبان عام 1439 ، الموافق 5 غشت سنة 2009 ، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال ومكافحتها ، المنشور بالجريدة الرسمية الجزائرية ، العدد 47 بتاريخ 16 أوت 2009 .

7 – القانون رقم 04 _15 المؤرخ في 10 ديسمبر 2004 ، يعدل ويتمم الأمر رقم 66 _156 المتضمن قانون العقوبات ، الجريدة الرسمية الجزائرية ، العدد 10 ، 2004/11/7 .

8 – القانون رقم 06_22 المؤرخ في 29 ذي القعدة عام 1427 الموافق عام 1427 الموافق 20 سبتمبر سنة 2006 ، يعدل ويتمم الأمر رقم 66 _155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية ، الصادر في الجريدة الرسمية الجزائرية ، عدد رقم 84 ، المنشور بالجريدة الرسمية الجزائرية بتاريخ 24 ديسمبر سنة 2006 .

2 –المراسيم:

1 - المرسوم الرئاسي رقم 24 _181 المؤرخ في 12 سبتمبر 2023 المتضمن إنشاء المدرسة العليا في الأمن السيبراني ، الجريدة الرسمية للجمهورية الجزائرية ، العدد 39 الصادرة يوم السبت 22 ذو الحجة 1445 ، الموافق ل 8 يونيو 2024 .

3_الأوامر :

1_ الامر 04_ 15 القانون الصادر في 10 نوفمبر 2010 ، يعدل ويتمم الأمر رقم 156/66 ، الصادر في 08 جوان 1966 ، المتمم لقانون العقوبات ، الجريدة الرسمية الجزائرية ، العدد 71 .

خامسا: المواقع الالكترونية

1-RFPS://www.google.com/unlsl.

2-Www.aljazera .net.

3-Www.jps.dz.

4-Www.justice.dz

5-Www.elikhbjhiji.dz.

6-news.radio Algérie.dz

7-Www.ndn.dz

8-Www.search New sould .com.

9-https://Www.europanabct .com.

10- https://boutique ceema.eg.

11- Www.sky news Arabia .com web .

الفهرس

الفهرس

الفهرس

الفهرس

الفهرس

الملخص

الملخص:

يعتبر الأمن السيبراني أحد الركائز الاساسية لتقوية المنظومة الامنية لسائر الدول ، بل أضحى ضرورة حتمية لمواجهة المخاطر السيبرانية التي تهدد كيان الدول وإستقرار سيادتها وذلك لطبيعتها الخاصة التي لاتعترف بالحدود الوطنية وهي مخاطر عابرة للحدود، وصعوبة تعقب مرتكبيها وذلك لسهولة إزالة أدلة الاثبات للإدانة ، وقد اقتحمت هذه التهديدات السيبرانية جميع مناحي الحياة نتيجة للتطور السريع والمذهل لتكنولوجيات الاعلام والاتصال ،وبالتالي يسهل اختراق خصوصيات المؤسسات والشركات الخاصة، بل وحتى الحياة الخاصة للأفراد.

والجزائر هي أيضا مستهدفة كسائر الدول من التهديد السيبراني ،وتداركت الوضع بداية من سنة 2004 بسن القانون 04-15 المعدل والمتمم لقانون العقوبات المتضمن الجرائم الماسة بأنظمة المعالجة الالية للمعطيات، و القانون 06-22 المعدل والمتمم لقانون الإجراءات الجزائية باستحداث تدابير الإجرائية لمكافحة الجريمة الالكترونية.وأيضا سن المشرع الجزائري نصوص خاصة نذكر أهمها القانون 09-04 المتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها الذي من مضامينه التشجيع على التعاون الدولي و المساعدة القضائية.

الكلمات المفتاحية :

الأمن السيبراني ، الجريمة السيبرانية ، الفضاء السيبراني ، الجريمة المعلوماتية ، الجريمة الالكترونية ،المجرم السيبراني.

Abstract:

Cyber security is considered one of the basic pillars for strengthening the security system of all countries .Rather , is has become an inévitable necessity to confront cyber theats that does not recognize national borders and are cross-border threats , ans the difficulty of tracking their prepetrators due to the ease of removing evidence of conviction.these cyber theats have invaded all aspects of life as a result of the rapid and amazing développement of information and communication technologies .The following makes it easy to penetrate the privacy of private institutions and even the private lives of individuals.

Algeria is also reassured, like other countries, of the cyber theats and has shared the situation since 2004 betwwen Law 15_04 amending and supplementing the criminal procedure code by introducing procedural meassures to combat cybercrime .The Algerian legislator also has special texts, the most important of which is Law 04_o9, which includes the prevention and combating of crimes related to informations and communication technologies, the contents of which encourage international cooperation and space assistance.

Keywords:

Cyber security, cyber crime, cyber Space, Information crime,cybercrime,cybercriminal.