جامعة سعيدة، الدكتور مولاي الطاهر

كلية الحقوق والعلوم السياسية

قسم القانون الخاص

الإطار القانوني للأمن المعلوماتي في التشريع الجزائري

مذكرة لاستكمال متطلبات الحصول على درجة ماستر في الحقوق

تخصص:الإدارة الالكترونية

من إعداد الطالب:

- شريفي بومدين
- حميدي قادة

تحت إشراف الأستاذة:

د . دلال مولاي ملياني

أعضاء لجنة المناقشة

الدكتور بن زايد أمحمد	أستاذ محاضر	جامعة سعيدة	رئيسا
الدكتورة دلال مولاي ملياني	أستاذة محاضرة	جامعة سعيدة	مشرفا ومقررا
الدكتورة عمارة فتيحة	أستاذة محاضرة	جامعة سعيدة	عضوا

السنة الجامعية: 2026/2025

﴿ بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ ﴾

﴿ يَا أَيُّهَا الَّذِينَ آمَنُوا كُلُوا مِنْ طَيِّبَاتِ مَا رَزَقْنَاكُمْ وَاشْكُرُوا لِلَّهِ إِنْ كُنْتُمْ إِيَّاهُ تَعْبُدُونَ ﴾

البقرة: الأية 172

الشكر و التقدير

الحمد لله الذي أكمل لنا دينه ، وأنزل لنا نعمه ، وهدانا الى العلم والحكمة وما كنا لنهتدي لو لا أن هدانا الله.

بداية .. نحمد الله ونشكره شكر من يطمع بالمزيد مصدقا لقوله تعالى"وَإِذْ تَأَذَّنَ رَبُّكُمْ لَئِن شَكَرْتُمْ لَأَزِيدَنَّكُمْ ۖ وَلَئِن كَفَرْتُمْ إِنَّ عَذَابِي لَشَدِيدٌ "

و لأنه من لا يشكر الناس لا يشكر الله ، نتقدم بالشكر الجزيل للأستاذة الفاضلة المشرفة دلال مولاي ملياني عرفانا بفيض رعايتها للباحين ، إنطلاقا من رعاية لا تسأم وجهد لا يكل ، تهيئة لمناخ علمي للدارسين ، يعينهم على مواصلة مسيرتهم العلمية .وكذلك الشكر الجزيل للأستاذة الفاضلة سويلم فضيلة من خلال إرشادتها وتوجيهاتها لنا لإتمام هذا العمل ، لها كل الإحترام والتقدير

والشكر الجزيل للأساتذة الأجلاء أعضاء لجنة المناقشة على تفضلهم بقبول مناقشة هذه المذكرة فكل الشكر والتقدير لهم .

الإهداء

أهدي ثمرة جهدي هذا الى

الى روح والدي رحمه الله ..والى والدتي أطال الله في عمرها وإخوتي رحمهم الله قادة شريفي الذي راح ضحية في سبيل الوطن وأخي نورالدين رحمه الله ، والى جميع إخوتي وأخواتي والى زوجتي ورفيقة دربي والى أبنائي وبناتي ، والى جميع أصدقائي وزملائي والى الطاقم التربوي والإداري لمدرسة الشهيد خلدون خالد قرية أم الدود بلدية مولاي العربي .

كما أهدي ثمرة هذا الجهد المتواضع الى كل باحث علم والى كل من أضاء بعلمه عقل غيره أو هدى بالجواب الصحيح حيرة سائليه ؛ فأظهر بسماحته تواضع العلماء وبرحابته سماحة العارفين.

بومدين شريفي

أهدي ثمرة جهدي هذا الى

إلى روح من غاب عن العين و لم يغب عن الوجدان، إلى من تمنيت أن يشهد لحظة نجاحي هذه إلى والدي العزيز (رحمه الله وأسكنه فسيح جناته)، و إلى منبع الحنان والصبر، إلى من لا توفيها الكلمات حقها، والدتي الغالية، حفظها الله وأطال في عمرها.

إلى شريكة الدرب، ورفيقة الكفاح، التي ساندتني بصبرها ودعمها، زوجتي العزيزة، و إلى قرة عيني وبسمة غدي، ومن أجلهم أبذل الجهد... أبنائي الأعزاء.

إلى سندي وعضدي، من تقاسمت معهم عبق الطفولة وطموح الشباب، إخوتي وأخواتي.

إلى من جمعتنا بهم مهنة الشرطة، وتبادلنا معهم التحديات والنجاحات، زملائي الكرام في جميع مصالح الشرطة التي عملت بها.

حميدي قادة

قائمة المختصرات

ج ر ج ج .....الجريدة الرسمية الجمهورية الجزائرية

د ب ن .....دون بلد النشر

د ر ط ..... دون رقم الطبعة

د س ن ..... دون سنة النشر

ص ..... الصفحة

ط .....الطبعة

م .... المجلد

مقدمة

يشهد العالم حالات من النفور و الإضطراب، عالم غير مستقر به غشاوة وتشوبه الشوائب، دائم في التغير والتحول بصفة جذرية من جديد الى جديد فالأحدث كأنه يوحي الى ثورة تستهدف الى كل ما هو تقليدي ضاربة عرض الحائط فجوة الزمان والمكان حتى أنها طالت ما هو ورقي غايتها الأساسية إعدامه وإنكاره وجعله في الرفوف ، فمن اتصالات ومراسلات تخط باليد بحبر و رقع من ورق الى تواصل إلكتروني عبر فضاء معنوي وافتراضي منه تستقبل وترسل المراسلات وتبرم العقود وتنجز الأعمال وتتم المعاملات منها التجارية والمدنية ، إلا انه قد تصادف جملة من الإعتراضات بأساليب متطورة فتسلب خصوصيتها وتنتهك موثوقية معاملاتها الإلكترونية فهي أمام تحديات جوهرية تمس سلامتها وسريتها . فهذا الفضاء الرقمي يزخر بشوائب و مخاطر تشكل خرقا لمبادئ الآمان الرقمي.

مما أدى للفكر البشري لإبتكار و إستعمال أساليب وتقنيات بها تستطيع مجابهة هذه الإعتداءات وصدها ، جاءت هذه التقنيات على سبيل المثال لا الحصر لأنها تحتاج لتحيين وتحديث، فهي مرتبطة بالتكنولوجيا خاصيتها التطور والغاية منها السرية ، السلامة فالإتاحة و التوافر و بهذا نكون أمام أمن معلوماتي، إلا أنه لا يتم التكامل بين هذه العناصر فيظل ناقصا إن إكتفى بالحماية التقنية بمفردها ؛ إذ تظل هذه التدابير محدودة الفعالية ما لم تعزز بآليات حماية جزائية رادعة تقر على تجريم هذه الأفعال و تفرض عليها عقوبات ؛ و أخرى بنية مؤسساتية كدرع تنفيذي هادف لحماية أمن المعلومات لها عدة مهام .

يعد تكامل آليات الحماية معيارا عاما ومبدأ تسعى جميع الدول الى بلوغه ؛ فإن إعمال هذا المبدأ يبقى مرهونا بخصوصية كل منظومة ومدى إستيعابها لمتطلبات الأمن المعلوماتي ، فنجد المشرع الجزائر قد أدرك هذا الإشكال لا نقول مبكرا وإنما ساير التطور في قوانينه ، أين جاء بجملة من التشريعات وترسانة قانونية كآلية جزائية رادعة أين شدد العقاب لكل الأفعال التى لها علاقة بالأمن المعلوماتي ؛ وأيضا إنشاء هيكل مسؤول عن أمن الأنظمة المعلوماتية وحماية المعطيات في المؤسسات والإدارات والهيئات العمومية وتحديد مهامه وتنظيمه و تسييره.[1]

[1] مرسوم رقم 07/26 المتضمن إنشاء هيكل مسؤول عن أمن أنظمة المعلوماتية ، ج ج،ج،ر،العدد الرابع، 7جانفي 2026.

تكمن أهمية موضوع بحثنا هذا في كونه أهم المواضيع المعاصرة التى تعي خطورة إختراق أنظمة معلوماتية ؛ وكذلك الإهتمام الكبير الذي أولته الجزائر للأمن المعلوماتي من خلال تحيين تشريعاتها من حين الى آخر مسايرة للتطور و إرساء أطر مؤسساتية ، كما يعد انتقالا من النظرية القانونية الى التطبيق العملي حيث أنه لم يعد مكافحة الإجرام على مستوى الفضاء المعلوماتي مجرد نصوص عقابية، بل أصبحت تتطلب منظومة متكاملة من الهيئات و اليقظة الإستباقية و تعاونا محليا ودوليا لحماية الأفراد والمجتمع ، وكذلك من أهميتها أنها تحتاج إلى التركيز على البحث و التطوير كون العالم يتجه نحو المزيد من الإعتماد على التكنولوجيا مما يعني أن التحديات المتعلقة بالأمن المعلوماتي تزداد سوءا وتعقيدا وبالتالي فهذه الدراسة تمثل خطوة إيجابية نحو فهم معمق لهذه القضايا.

حيث تهدف الدراسة الى ماهية الأمن المعلوماتي من خلال إعطاء مفهوم دقيق للأمن المعلوماتي وما يفرقه عن المفاهيم الأخرى (الأمن السيبراني، أمن الشبكات) وعناصره ومدى تكاملها ، و مصادره القانونية الداخلية والخارجية، وتحديد آليات الحماية التقنية للامن المعلوماتي من خلال عرض الأساليب التقنية وذكر لبعض الجرائم للأمن المعلوماتي وعقوباتها المتفاوتة بصفتها أساليب جزائية ؛ مع تحديد آليات الحماية المؤسساتية وإبراز دورها للأمن المعلوماتي ثم إظهار العلاقة التكاملية بين الآليات الحماية والوقوف على واقع البيئة التشريعية للأمن المعلوماتي .

كما يعود إختيارنا لهذا الموضوع لعدة أسباب منها ميولنا الشخصي له و رغبتنا بالبحث فيه كما أنه يعتبر مجال تخصصنا وشعورنا بالمسؤولية الإجتماعية والشغف بالتكنولوجيا وخباياها ؛فأمن المعلومات أرض خصبة للإكتشاف والتعلم المستمر والتحسيس بضرورة الإهتمام بالحماية التقنية للمعلومات بالنسبة للفرد والمجتمع وبضرورة تطبيق السياسة الأمنية لمختلف وسائل المعلومات ؛ مع التطلع لتبيان أهمية الأمن المعلوماتي لفرض السيادة الرقمية و بناء مجتمع مستقر و تبيان أهمية تكامل آليات الحماية للأمن المعلوماتي.

وبعدما أضحت الجزائر واعيةبالترصدات التى تحيط بها و المؤامرات التى تحاك من وراءها مما يتطلب منها الحيطة والحذر بأسلوب واعي وإدراك تام بالمخاطر التى تفرضها إستعمال تكنولوجيا المعلومات كالإتصالات في الفضاء الرقمي، مما يستدعي إهتماما أكبر بحماية المعلومات وإرساء إستراتيجية وطنية شاملة بإعتبارها الأساس لضمان أمن المعلومات.

و عليه من خلال كل ما سبق ذكره يمكن طرح الإشكالية التالية:

ما مدى فاعلية المنظومة القانونية والمؤسساتية في إرساء دعائم الحماية للأمن المعلوماتي ؟ .

إعتمدنا في هذه المذكرة على العديد من الدراسات السابقة التى تم إعدادها من طرف أساتذة ودكاترة في شكل مقالات علمية وقانونية وكذلك طلبة من خلال مذكرات تخرج لنيل شهادة الماستر تناولوا في مجملهم الإطار المفاهيمي للامن المعلومات و آليات الحماية على المستويين الدولي و الوطني وقد تم إدراج هذه الدراسات كمصادر في قائمة المراجع يمكن أن نذكر منها على سبيل المثال لا الحصر .

– عنوان الدراسة نظام أمن المعلومات في الجزائر دراسة حالة بلدية سوق الاثنين من طرف الطالبة حمودي كاهنة مذكرة مقدمة لنيل شهادة الماستر في العلوم السياسية والعلاقات الدولية ، تطرقت فيها الباحثة الى كافة المصطلحات المتعلقة بنظم أمن المعلومات ، كما بينت المشاكل والمخاطر التى تتعرض لها الأنظمة من إختراق وتزوير للمعطيات والبيانات الإلكترونية ، إضافة الى السياسات الأمنية المتبعة من قبل المنظمات وتناولت دراسة ميدانية واقع نظام أمن المعلومات في الإدارة المحلية وإظهار المعوقات التى تواجهها عند القيام بالمهام الإدارية .

– الأمن السيبراني في الجزائر السياسات والمؤسسات دراسة للدكتور بارة سمير منشورة في المجلة الجزائرية للأمن الإنساني جامعة باتنة المجلد :02 العدد الرابع سنة 2017 قدم فيها الباحث أساسيات عن الأمن السيبراني وأبعاده وكذا ماهية الجريمة السيبرانية وأنماط التهديدات بالإضافة الى الأجهزة الأمنية الجزائرية المختصة بمكافحة الجرائم السيبرانية كما أشار في الأخير الى عوائق الأمن السيبراني في ظل التحديات الآنية والمستقبلية .

محاولة للإجابة عن الإشكالية إعتمدنا على المنهج الوصفي وذلك لإعطاء إطار مفاهيمي للأمن المعلوماتي وكذلك إبراز التعاريف الأخرى المقاربة له مع تحديد عناصره وأهدافه ومصادره ، كما أنه لا يخلو من المنهج التحليلي من خلال تحليل المواد القانونية و التى تناولناها في آليات الحماية للأمن المعلوماتي .

من الصعوبات التى واجهتنا أن مجال أمن المعلومات يتميز بظهور مفاهيم و تقنيات جديدة بشكل شبه يومي، مما يخلق صعوبة في تحيين معلومات التي نحن بصدد دراستها؛ والتى جاءت محددة من خلال تناول الأمن المعلوماتي في التشريع الجزائري بصفة خاصة.

وللإجابة على الإشكالية المطروحة فخطة الدراسة جاءت في قالب ثنائي نوردها كالأتي:

الفصل الأول خصصناه للإطار المفاهيمي للأمن المعلوماتي في التشريع الجزائري حيث تناولنا المدخل المفاهيمي للأمن المعلوماتي في المبحث الأول بينما إستعرضنا في المبحث الثاني الإطار التشريعي للأمن المعلوماتي.

أما الفصل الثاني تطرقنا فيه آليات الحماية للأمن المعلوماتي في التشريع الجزائري قسمناه الى مبحثين تناولنا آليات الحماية التقنية والجزائية في المبحث الأول و خصصنا المبحث الثاني للإطار المؤسساتي للأمن المعلوماتي.

الفصل الأول

الإطار المفاهيمي للأمن المعلوماتي

في التشريع الجزائري

في عصر التحول الرقمي المتسارع ، ارتقى أمن المعلومات ليحتل مكانة إستراتيجية محورية تستوجب إهتماما عاليا من الدول والمؤسسات والأفراد على حد السواء ، ومع تسارع وتيرة التطور التقني و إنتشار المخاطر التكنولوجية التى باتت تهدد كيان المجتمعات ، نجد أن التكنولوجيا رغم ما قدمته من خدمات جليلة للإنسانية تحمل في طياتها وجهين متناقضين ، وجه مضيْ ينير معالم الإستمرارية و آخر مظلم تنبعث منه تحديات جسيمة إن أهملت أو تركت بلا حصانة.

إن المجتمع المعلوماتي في هذا العصر يهتم كثيرا بأمنية المعلومات حيث أصبحت المعلومات مصدرا مهم يجب حمايته مثلما تتم عملية حفظ وحماية الأموال أو المقتنيات الثمينة الأخرى.([1])

هذا التحول الرقمي الجذري ، رغم ما وفره من فرص هائلة للإبداع و الإتصال والكفاءة ، فقد إستتبع معه ظهور مخاطر من نوع جديد ، مخاطر لا ترى بالعين المجردة لكن عواقبها ملموسة و كارثية .

سوف نواجهه في المستقبل القريب أزمات في مجال المعلوماتية يمكن أن تهدد أمننا الوطني وأمننا الشخصي إضافة الى بنيتنا الإقتصادية، هذا النمو السريع في التكنولوجيا المعلومات أصبح عامل مؤثر في هذا التهديد .([2])

وعليه سيتم التطرق من خلال هذا الفصل الإطار المفاهيمي للأمن المعلوماتي في التشريع الجزائري أين تناولنا المدخل المفاهيمي للأمن المعلوماتي في المبحث الأول و الإطار التشريعي للأمن المعلوماتي في المبحث الثاني .

[1]– خضر مصباح إسماعيل الطيطي ، أساسيات أمن المعلومات والحاسوب ط الأولى، دار الحامد، عمان الاردن2009، ص 20.

[2]– خضر مصباح إسماعيل الطيطي ،المرجع نفسه، ص 20

المبحث الأول

المدخل المفاهيمي للأمن المعلوماتي

يعد الأمن المعلوماتي من المفاهيم الحديثة التى برزت بقوة مع تطور تكنولوجي المعلومات و الإتصال ، و إتساع نطاق إستخدام النظم المعلوماتية في مختلف مجالات الحياة الاجتماعية، الإقتصادية والإدارية.

وقد أدى هذا التطور الى بروز مخاطر متعددة تهدد المعلومات ، سواء من حيث سريتها أو سلامتها أو إمكانية الوصول إليها ، الأمر الذي فرض ضرورة وضع إطار مفاهيمي وتشريع يضمن حمايتها .

وأهم ما أدرجناه من خلال دراستنا لمدخل المفاهيمي للأمن المعلوماتي في هذا المبحث هو الإطار المفاهيمي أي كل ما يتعلق بموضوع الأمن المعلوماتي سواء من حيث التعريف و الأنواع كمطلب أول ثم العناصر و أهداف الأمن المعلوماتي في مطلب ثاني.

المطلب الأول

مفهوم الأمن المعلوماتي

في عصر التحول الرقمي الذي أصبحت فيه البيانات و المعلومات هي العصب الأساسي للحياة الشخصية والمؤسسية والدولية، يبرز مفهوم أمن المعلومات كحجر الزاوية لضمان استمرارية الأنشطة وحماية الحقوق ودرء المخاطر ، وحتى يكتمل لدينا تعريف الأمن المعلومات ، وحتى لا يبقى في ذهن القارئ أي تساؤل أو لبس حول مفهوم الأمن المعلوماتي من الناحية اللغوية و الإصطلاحية أو القانونية وكذا أنواعه فقد تم تقسيم هذا المطلب الى فرعين.

تم التطرق في الفرع الأول الى تعريف الأمن المعلوماتي، أما الفرع الثاني تناولنا أنواع الأمن المعلوماتي.

الفرع الأول

تعريف الأمن المعلوماتي

حتى نتمكن من تبيان ما المقصود بالأمن المعلوماتي، سيتم التطرق إلى تعريفه من الجانب اللغوي والاصطلاحي و الفقهي و القانوني ، وهذا كالأتي:

أولا : تعريف الأمن المعلوماتي لغة

أ–الأمن لغة:

أمن: الأمان و الأمانة بمعنى وقد أمنت فأمن ، وأمنت غيري من الأمن والأمان ، والأمن ضد الخوف ، و الأمانة ضد الخيانة ، و الإيمان ضد الكفر ، الإيمان : بمعنى التصديق ، ضد التكذيب يقال : أمن به قوم ، وكذب به قوم، فأما أمنته المتعدي فهو ضد أخفته ([1])

يقول الله تعالى في محكم تنزيله ﴿الَّذِي أَطْعَمَهُم مِّن جُوعٍ وَآمَنَهُم مِّنْ خَوْفٍ﴾ ([2])

يقول أبو الحسن على بن إسماعيل المعروف بابن سيده: الأمن نقيض الخوف ،أمن فلان يأمن أمنا وأمنا. ([3]) معنى كلمة الأمن في اللغة العربية تعني الطمأنينة وزوال الخوف([4]) كما تحمل عدة معاني إذا يقصد به : سكون القلب ورقة النفس والشعور بالرضا و الإستقرار وعدم الخوف.([5])

ب– المعلومة لغة:

المعلومة في اللغة العربية هي إسم مفعول مؤنث، مشتقة من الفعل أعلم يعلم إعلاما ، بمعنى أبلغ وأفاد، فهي تعني حرفيا: الشيء الذي تم إبلاغه أو الإخبار به أو جعله معلوما، وهي ما أدرك بعد جهل مشتقة من الفعل علم بمعنى أدرك وحقق.

---

[1] ابن منظور جمال الدين محمد بن مكرم الأنصاري ، لسان العرب ،م 1 ط .6 ،بيروت : دار صادر،2011 ، ص 66.

[2] الآية رقم 04 ، سورة قريش .

[3] ابن منظور جمال الدين محمد بن مكرم الأنصاري ، المرجع نفسه، ص 66.

[4] على بن فايز الجحني، الإعلام الأمني والوقاية من الجريمة ، د ر ط ، دار جامعة نايف للنشر ، الرياض ، 2000/04/10ص66.

[5] محمد الأمين البشيري ،الأمن الغربي: المقومات والمعوقات، ط الاولى ،أكاديمية نايف للعلوم الامنية ،الرياض2000 ، ص 18.

هي إسم مفعول تدل علم موصل إليه بالعلم الإدراك، هي العلم نقيض الجهل فالمعلومة هي محصلة العلم أي ما تحقق إدراكه بعد أن كان خافيا([1])

ثانيا : تعريف الأمن المعلوماتي اصطلاحا

أ – الأمن اصطلاحا :

بعد أن رسمنا في أيدينا الخيط اللغوي المتين ، أصبحنا جاهزين الآن لنسير في أروقة التعريف الإصطلاحي ، لنرى كيف صاغ الباحثين والفقهاء هذا المفهوم الحيوي ، وكيف اختلفت تأويلاته بإختلاف توجهاتهم يرى الفقيه (برث ويلز) انه لا يمكن للأفراد والمجموعات تحقيق الأمن المستقر إلا إذا إمتنعوا على حرمان الآخرين منه و يتحقق ذلك إذا نظر الى الأمن انه عملية تحرر، الأمن سلسلة من الإجراءات الردعية التى تتخذها الدول لحفاظ أمنها دون المساس بأي من الحقوق الفعلية كانت أو المكتسبة منها على المستوى الداخلي الوطني أو الخارجي الإقليمي العالمي،([2]) الأمن هو مسألة إحساس وشعور و إدراك.

ب – المعلومات إصطلاحا:

تعرف المعلومات على أنها بيانات تم تصنيفها بشكل يسمح بإستخدامها و الإستفادة منها، وبالتالي فالمعلومات لها معنى، وتؤثر في ردود أفعال وسلوك من يستقبلها. ([3])

فهي تلك البيانات والعناصر التى يتم معالجتها وتحليلها لتصبح ذات دلالة ومنفعة لمستخدميها، بعد أن نزيل الغموض عنها ونعطي لها صورة واضحة،([4]) و منه تعرف البيانات هي المواد الخام التي تعتمد عليها المعلومات والتي تأخذ شكل أرقام أو رموز أو عبارات أو جمل لا معنى لها إلا إذا تمت معالجتها وارتبطت ببعضها بشكل منطقي مفهوم لتتحول إلى معلومة أو معلومات.

---

[1] – دويب العيد، "مفهوم الأمن في الفكر الديني دراسة لابعاد الأمن الإنساني في الإسلام"، **مجلة الدراسات القانونية والسياسية** ، م: 01 العدد الخامس، جانفي2017 ، ص 250.

[2] –دويب العيد ، المرجع السابق ، ص 251.

[3] –فريدة حمودي ، "الأمن المعلوماتي في الجزائر بين التطورات التكنولوجية وضعف البيئة الرقمية –المجال المصرفي نموذجا – " **دراسة قانونية** مجلة الأبحاث القانونية المعمقة ، العدد الواحد و الأربعين، الصادرة في 2020/08/17، ص91.

[4] –حمودي كاهنة ، نظام أمن المعلومات في الجزائر ، مذكرة شهادة الماستر في العلوم السياسية العلاقات الدولية، كلية الحقوق والعلوم السياسية جامعة مولود معمري تيزي وزو، 2016 ، ص 16.

ويكون ذلك عن طريق البرمجيات والأساليب التقنية ، ([1]) فالمعلومة إذا هي تعبير يستهدف جعل رسالة قابلة للتوصيل الى الغير كما تتطلب بطبيعتها وجود وسط تخزن فيه، ([2])كما أنها تقترب في معناها من مصطلح المعطيات، حيث إعتبر المشرع الجزائري هذه الأخيرة في نص المادة 03 من القانون 07/18 المتعلقة بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي على أنها معلومات بغض النظر عن دعامتها متعلقة بشخص معرف قابل للتعرف عليه.

ثالثا : تعريف الأمن المعلوماتي.

يوم بعد يوم يتسع مفهوم الأمن المعلوماتي ليشمل العديد من الآراء والمفاهيم إلا انه لم يحظى بتعريف موحد بل تعددت تعريفاته بتعدد الزوايا التى تناولته ، فهناك من عرفه من منظور أكاديمي ومنهم من ركز على البعد التقني والقانوني.

أ – التعريف الأكاديمي: الأمن المعلوماتي هو العلم الذي يبحث في نظريات وإستراتيجيات توفير الحماية للمعلومات من المخاطر التى تهددها ، و من أنشطة الإعتداء عليها. ([3])

ب – التعريف التقني: جملة من الأساليب الوقائية التى تهدف إلى توفير حماية أمنية لمجموع المعلومات المتعامل بها في البيئة الرقمية من خلال ضمان سريتها و صحتها وعدم قدرة أجنبي الوصول إليها وتغييرها أو إستبدالها بما يؤدي الى تغير مضمونها وأهدافها، ([4]) حيث تستعمل هذه الإجراءات والتدابير سواء في المجال الفني أو الوقائي لصيانة المعلومات الخاصة بالإدارة الإلكترونية والإجراءات القانونية التى تتخذ للحماية من حدوث أي تدخلات غير مشروعة صدفة أو بشكل متعمد.([5])

---

[1] حسيبة قيدوم، محاضرات في الأنظمة المعلوماتية ، مطبوعة موجهة لطلبة السنة الثانية ماستر، تخصص اتصال تنظيمي، كلية علوم الإعلام و الاتصال ، جامعة الجزائر 3، 2020-2021، ص 20.

[2] ليتيم فتيحة ، ليتيم نادية ، "الأمن المعلوماتي للحكومة الإلكترونية وإرهاب القرصنة" ، **مجلة الفكر**، كلية الحقوق و العلوم السياسية جامعة محمد خيضر بسكرة، العدد الثاني عشر ، 2015/03/25، ص 239.

[3] هاني مطر ابو سعود ، عباسة طاهر ،" إرتباطات الامن المعلوماتي بالأمن القومي" ، **مجلة الدراسات الحقوقية** م7 ، العدد الثاني جوان 2020 ، ص 21

[4] -أوبراهم صونية ، ملاك فانزة ،" الأمن المعلومات في ظل الإقتصاد الرقمي" ، **مجلة البحوث القانونية الإقتصادية** ، المجلد 8 العدد العدد الثاني جوان 2025، ص 977.

5-أوبراهم صونية ، ملاك فانزة ، المرجع السابق ، ص 977

ويتم ذلك من خلال حماية المعلومات الموجودة على الأجهزة وشبكات الحاسب الآلي في مواجهة أي تدخل غير مصرح به، قد يستهدف إحداث تغيير في المعلومات و إتلافها أو الحرمان من الوصول اليها. ([1])

ج – التعريف القانوني:

إن أمن المعلومات هو محل دراسات وتدابير لحماية سرية وسلامة المحتوى وتوفر المعلومات ومكافحة أنشطة الإعتداء عليها ، أو إستغلال نظمها في إرتكاب الجريمة ، الهدف والغرض من التشريعات حماية المعلومات من الأنشطة غير القانونية التى تستهدف المعلومات ونظمها([2]) ، فهو الإطار القانوني والتنظيمي الذي يهدف الى حماية البيانات والمعلومات من أي إعتداء أو إستغلال غير المشروع وضمان الحقوق المرتبطة بها ، مع تحديد المسؤوليات والجزاءات المترتبة عن الإخلال بها .

الفرع الثاني

أنواع الأمن المعلوماتي

لا يقتصر الأمن المعلوماتي على كونه حاجزا تقنيا واحد ، بل هو نسيج متكامل من الاستراتجيات التدابير التى تتشابك لتشكل دفاعا متعدد المستويات ، ولهذا تفرع الأمن المعلوماتي الى عدة تخصصات دقيقة كل منها يركز على جانب معين من المنظومة ، بهدف سد الثغرات وتأمين إستمرارية الأعمال وحماية الخصوصية ، و بما أن الأمن المعلوماتي درع تقني وإجرائي الذي يحمي الفضاء الرقمي فإن الأمن القانوني بدوره يحمي الحقوق في العالم المادي و الإفتراضي على المستوى التشريعي فهو الثقة والبيئة الحاضنة التى تسمح لأي نشاط سواء اقتصادي أو اجتماعي أو تقني بالإزدهار دون خوف من الفوضى أو التعسف ، وفي هذا السياق قبل أن نستعرض أبرز أنواع الأمن المعلوماتي نعرج على إحدى المبادئ الدستورية ألا هو الأمن القانوني.

[1] – أوبراهم صونية ، ملاك فانزة ، المرجع السابق ، ص 977

[2] - هاني مطر أبو سعود ، عباسة طاهر ، المرجع السابق، ص 211

أولا : الأمن القانوني

الأمن القانوني هو إحدى الأنظمة القانونية التى تكفل للمواطنين الثقة والطمأنينة في القانون الوضعي؛ وكذا المحافظة على ماهية الأمن من خلال إنعدام الخوف منه وضمان إستقرار القاعدة القانونية ووضوحها وديمومتها وثباتها، وهو من أهم المهام التي ينبغي على الدولة تجسيدها و من أولى وظائفها حيث يتحتم على جميع مؤسساتها وهياكلها تحقيق قدر معين منه وفي شتى المجالات . ([1])

بعض الفقهاء أعطوا تعريفا له من خلال إبراز أهدافه كما جاء في تعريف (برنارد) الإستقرار الضمان ،الحماية واليقين ، الثقة المرجوة في القانون ، فالأمن في نفس الوقت حماية ضد الأثر الرجعي ، الوضوح ، الدقة، الإنسجام و المعرفة .

يمتاز مبدأ الأمن القانوني بمجموعة من الخصائص الأساسية التى تجعله ركيزة مهمة في الأنظمة القانونية؛ فهو يتسم بالعمومية والتجريد والإلزام مما يمنحه طابعا عاما و أمرا، كما أن هذا المبدأ يتحلى بالمرونة و القدرة على التكيف مع مختلف الظروف من خلال حماية أمن العلاقات القانونية في الماضي و كذا المستقبل ؛ بمعنى قابليته للتطور والحداثة ،([2]) أما بالنسبة لميزة العالمية من خلال إتجاه جل الدول الى إعتباره المنطلق الأساسي في تحقيق الإستقرار وضمانه عن طريق إدراجه في نصوص تشريعاتها فيما يخص خاصية الثبات والديمومة تظل نسبية و هذا حتى لا تتعارض مع خاصية المرونة ، إذ يسعى المبدأ لمواكبة التطورات المستجدة في المجتمع.([3])

يعد الأمن القانوني من أهم المبادئ الدستورية؛ وعبر الدساتير السابقة لدولة الجزائرية كان تكريس مبدأ الأمن القانوني ضمني إلا أن تعديل الدستور 2020 كان تكريسا صريحا للأمن القانوني حيث جاءت في المادة 34 منه (تحقيقا للأمن القانوني ، تسهر الدولة، عند وضع التشريع المتعلق بالحقوق والحريات ، على ضمان الوصول إليه و وضوحه و إستقراره).([4])

---

[1] - إفتيسان وريدة، بن ناصر وهيبة ،" دسترة مبدأ الأمن القانوني التجربة الجزائرية نموذجا" ، **مجلة الدراسات القانونية صنف ج** ، جامعة يحي فارس بالمدية الجزائر، م 08، العدد الثاني ، جوان 2022 ، ص 972

[2] – إفتيسان وريدة ، بن ناصر وهيبة ، المرجع السابق ، ص 976

[3] – إفتيسان وريدة ، بن ناصر وهيبة ، المرجع نفسه ، ص 977

[4] - المادة 34 الفقرة 4 ، دستور الجزائر 2020 معدل متمم المؤرخ في 30 ديسمبر 2020، ج ج ج ر العدد اثنان و ثمانون ، الصادر بتاريخ 2020/12/30 ص 11

ثانيا : أمن الشبكات

لقد إستعرضنا في ما سبق لمفهوم الأمن لذا سوف نتركه جانبا لنخطو نحو مفهوم الشبكات التي يقصد بها نظام معين لربط جهازين حاسوب أو أكثر بإستخدام إحدى تقنيات الإتصال ؛ وذلك بهدف تبادل المعلومات والبيانات المتاحة بين أكثر من طرف ، يتم أيضا من خلالها تشارك الموارد المتاحة مثل الطابعات ، والبرامج التطبيقية ؛ كما تسمح بالتواصل المباشر بين أفراد مجتمع الشبكة ، فهي نوع من تقنية الاتصالات التى تستخدم في عمليات الربط بين مجموعة من مراكز المعلومات.([1])

تنقسم الشبكات الى نوعين رئيسين، شبكة سلكية و أخرى شبكة لا سلكية، وفقا للمعايير التالية:

أ – حسب نوع الوسيط الناقل للبيانات:

نجد الشبكات السلكية التي تعتمد على كابلات مادية مثل النحاس والألياف الضوئية لنقل البيانات و هناك الشبكات اللاسلكية تستخدم الموجات الكهرومغناطيسية مثل موجات الراديو أو الإتصال عبر الأقمار الصناعية .

ب –حسب النطاق الجغرافي و الإمتداد المكاني:

تتكون من ثلاثة أنواع منها الشبكات الداخلية LAN مثل شبكات المستشفيات وشبكات المدارس والشركات الصغيرة و الشبكات الواسعة WAN مثل الشبكة الدولية التى تربط بين أجزاء بين الدول و أيضا الشبكة الخاصة INTRANET.

أمن الشبكات هو مجموعة من الإجراءات التى يمكن خلالها توفير الحماية القصوى للمعلومات والبيانات في الشبكات من كافة المخاطر التى تهددها ، وذلك من خلال توفير الأدوات و الوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية .([2])

[1] – رجب عبد الحميد حسنين،" أمن شبكات المعلومات الإلكترونية : المخاطر والحلول" ، ج ، جامعة الحصن أبو ظبي الإمارات العربية المتحدة ، العدد ثلاثون ، ديسمبر 2012 ، ص .75

[2] – جلال جناجرة ، أمن الشبكات وحمايتها ، قسم تكنولوجيا المعلومات ، د ن جامعة فلسطين التقنية 2022، ص 3.

هو عبارة عن مجموعة من المعايير التى تحول دون وصول المعلومات المخزنة في الشبكات الى الأشخاص غير المخول لهم الحصول عليها،([1]) وهذا ما يتبين لنا انه مصطلح واسع يغطي العديد من التقنيات والأجهزة والعمليات ومجموعة من القواعد والتكوينات المصممة لحماية سلامة الشبكات والبيانات وسريتها وإمكانية الوصول إليها بإستخدام البرامج والأجهزة.

ثالثا : الأمن السيبراني

قبل أن نعطي مفهوم الأمن السيبراني نعرج على كلمة السيبرانية كمصطلح إذ أنها علم يعني بضبط الأنظمة وتنظيمها و توجيهها بطريقة ذاتية وفعالة ، السيبرانية هذه الكلمة مأخوذة من سيبر (cyber) وهي صفة تطلق على كل ما هو مرتبط بثقافة الحواسيب أو تقنيات المعلومات أو الواقع الإفتراضي .([2])

وردت عدة تعاريف للأمن السيبراني منها ما جاء به أستاذ جامعة كاليفورنيا (ريتشارد كمرر) حيث اعتبره وسائل دفاعية من شأنها كشف وإحباط المحاولات التي يقوم بها القراصنة .([3])

(إدوارد أموروزو) يقول عنه أنه وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة و كشف الفيروسات ووقفها وتوفير الإتصالات المشفرة . ([4])

الإتحاد الدولي للإتصالات بدوره أعطى تعريفا للأمن السيبراني جاء ذلك في التقرير حول إتجاهات الإصلاح في الإتصالات للعام 2011/2010 على أنه مجموعة من الوسائل التقنية والتنظيمية والإدارية التى يتم إستخدامها لمنع الإستخدام غير المصرح به ، وسوء الإستغلال و إستعادة المعلومات الإلكترونية ، ونظم الاتصالات والمعلومات التى تحتويها.

---

[1] – جلال جناجرة ، المرجع السابق ، ص 3

[2] – بوطمين وائل خليل الرحمان ، البعد السيبراني للأمن القومي الجزائري ، دراسة مقاربة لنماذج دولية، مذكرة شهادة الماستر في ميدان الحقوق والعلوم السياسية ، المدرسة الوطنية العليا للعلوم السياسية الجزائر ، السنة الجامعية 2025/2024 ، ص 27

[3] – إدريس عطية ، "مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري" ، **دراسة قانونية**، كلية الحقوق والعلوم السياسية جامعة العربي التبسي ، تبسة ، الجزائر ، 2019/12/01، ص 104

[4] – إدريس عطية ، المرجع نفسه ، ص 104

وذلك بهدف ضمان توافر و إستمرارية عمل نظم المعلومات ؛ وتعزيز حماية وسرية وخصوصية البيانات و إتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني.[1]

إن مصطلح الأمن السيبراني أو الإلكتروني ظهر حديثا وهو يعني مجمل القوانين السياسية الأدوات ، النصوص ، المفاهيم و ميكانيزمات الأمن وطرق تسيير الأخطار والممارسات التكنولوجية المتعلقة بتكنولوجيا المعلومات و الإتصالات المستخدمة لحماية الدول والمنظمات والأشخاص. [2]

لم يقتصر تعريف الأمن السيبراني على هذا الحد فقط بل نال الكثير و بالرجوع الى أهدافه يمكننا تعريفه على أنه النشاط الذي يؤمن حماية الموارد البشرية والمالية التى لها علاقة بتقنيات الإتصالات المعلومات من خلال الحد من الخسائر والأضرار الناجمة عن المخاطر والتهديدات السيبرانية بدوره يعيد الوضع الى ما كان عليه سابقا بسرعة آنية ؛ فتستمر عملية الإنتاج . [3]

أما بالنسبة للتعريفات التى جاءت بها الدوائر الحكومية نجد وزارة الدفاع الأمريكية عرفت الأمن السيبراني على أنه مجموعة الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها الإلكترونية والمادية من مختلف الجرائم ، الهجمات ، التخريب ، التجسس ، الحوادث . [4]

وكالة الأمن الرقمي الأوربية أول من أصدرت تشريع في هذا المجال فعرفته بأنه قدرة النظام المعلوماتي على مقاومة محاولات الإختراق أو الحوادث غير المتوقعة التى تستهدف البيانات المتداولة أو المخزنة وفق إطار توافقي.([5])

---

[1] – فارس محمد العمارات ، إبراهيم الحمامصة، الأمن السيبراني المفهوم وتحديات العصر ، ط 1 دار الخليج للنشر والتوزيع الاردن ، عمان ، 2022 ، ص 18

[2] – مسكية محمد ، "الفضاء السيبراني وتحديات الأمن القومي للدول" ، **مجلة العلوم القانونية والإجتماعية**، جامعة زيان عاشور بالجلفة الجزائر ،م:7، العدد الرابع، ديسمبر 2022 ، ص 457.

[3] – بارة سمير ، "الأمن السيبراني في الجزائر السياسيات والمؤسسات" ، **المجلة الجزائرية للأمن الإنساني**، العدد الرابع، جامعة قاصدي مرباح ورقلة، جويلية 2017، ص 257 .

[4] – فارس العمارات ، ابراهيم محمد الحمامصة ، المرجع السابق ، ص 18 .

[5] – فارس العمارات ، إبراهيم محمد الحمامصة ، المرجع نفسه ، ص 18 .

رابعا: أمن التطبيقات

تتعاقب الأزمنة وتستمر التكنولوجيا دون إستقرار لتنتج الجديد فالأحدث ؛ لنجد أمامنا مصطلح حديث النشأة التطبيقات ، يذكر في مصطلحات الانترنيت على شبكة الواب أن التطبيقات الإلكترونية عبارة عن برامج مستقلة مصممة لتعمل على الأجهزة المحمولة مثل الهواتف الذكية أو لوحة لمس وهي متنوعة بتنوع الأغراض التى تستخدم لأجلها .([1])

فهي عبارة عن برمجيات بسيطة يتم تصميمها وفقا لسمات برنامج التشغيل ، ويكون كل تطبيق مصمم لأداء وظيفته، ([2]) و لكن ما الفائدة من التطبيقات إذا كانت عرضة للإختراقات، هذا يقودنا الى تعريف أمن التطبيقات الذي هو مجموعة من الإجراءات والتقنيات التى تطبق خلال مراحل تطوير التطبيق، من التصميم حتى النشر بهدف حماية التطبيق وبيانات المستخدمين من الإختراق و هو فرع أساسي من فروع الأمن السيبراني يهتم بحماية البرمجيات والتطبيقات من التهديدات والهجمات الإلكترونية ، وظيفته حماية بيانات المستخدمين من التسريب ، تقليل المخاطر القانونية والمالية والتوافق مع أنظمة الحماية العالمية مثل إيزو 27001 ، فهو الذي يحافظ على سمعة الشركة المنتجة كما يقوم بوضع تدابير لحماية البرامج من الفيروسات الضارة وعدم سرقة المعلومات السرية، وذلك بالسعي إلى إفشال أي نوع من الهجمات على الأمن السيبراني بواسطة إستخدام العديد من الأجهزة والبرامج خلال مرحلة تطوير المشروع الإلكتروني،([3]) تتمثل مهمة أمن التطبيقات في حماية جهاز الكمبيوتر و واجهات برمجة التطبيقات من التهديدات ونقاط الضعف ، إذ يتأكد أن المعلومات التى تستخدمها تلك البرامج تتيح إرشادات السرية والنزاهة والتوافر وتشمل ممارسات الترميز الآمنة و الإختبارات الأمنية، مراقبة الدخول ، التشفير ، التوثيق و الإذن.([4])

---

[1] – بن علية سميرة ، سالمي عبد المجيد ، "التطبيقات الإلكترونية السياحية في الجزائر" ، **دراسة لغوية سيميائية**، العدد الأول جامعة الجزائر 2 ، 2019 ، ص 233.

[2] - بديع بوخبزة ، عبير عيد، تطبيقات الهواتف الذكية وأثرها على الأداء البحثي للطالب الجامعي ، مذكرة شهادة ماستر بقسم علوم الإعلام والإتصال وعلم المكتبات ، جامعة قالمة ، 2020-2021 ، ص20.

[3] – الرجوع لموقع العطاء الرقمي وزارة الإتصالات وتقنية المعلومات، **أمن التطبيقات** ، تاريخ النشر 2025/05/06 ، تاريخ التصفح2026/05/07 على الساعة 00.01، على الوصلة: https://attaa.mcit.gov.sa/library/view/2178

[4] الرجوع لموقع بكه للتعليم ، **أمن المعلومات وأهميته والأنواع والعناصر والإستراتجيات والبرامج والأهداف** ، تاريخ النشر جوان 2025 تاريخ التصفح2026/05/07 على الساعة 00:18، على الوصلة: أمن المعلومات/bakkah.com /ar/knowldge.center

خامسا : أمن الحوسبة السحابية

مع تصاعد وتيرة الإنفجار المعلوماتي، الذي بات يغذي الوسط الرقمي ، وعدم قدرة الوسائط التقليدية كالأقراص الصلبة على استيعاب هذا الكم الهائل من البيانات حتى أننا نقول عجزت عن مواكبتها ، إذ أصبحت مهددة بفقدان قيمتها الوظيفية ، إلا أن هذه الأزمة التقنية كانت بمثابة البوتقة التي إنبثقت منها الحوسبة السحابية ، فهذه الأخيرة هي تكنولوجيا تعتمد على نقل المعالجة ومساحة التخزين الخاصة بالحاسوب الى ما يسمى السحابة ، وهي أجهزة خوادم يتم الوصول إليها عن طريق الأنترنت لتتحول البرامج من منتجات إلى خدمات ويتاح للمستخدمين الوصول إليها عبر الأنترنت دون الحاجة الى إمتلاك المعرفة والخبرة والتحكم بالعتاد. ([1])

وهي مصطلح يشير الى المصادر والأنظمة الحاسوبية المتوفرة تحت الطلب عبر الشبكة و التى تستطيع توفير عدد من الخدمات الحاسوبية المتكاملة دون التقيد بالموارد المحلية بهدف التيسير على المستخدم ، وتشمل تلك الموارد مساحة لتخزين البيانات والنسخ الإحتياطية . (2)

أما بالنسبة للأمن السحابي فهو يعد تقنية سيبرانية تعتمد على ضغط المعلومات وهو جزء لا يتجزأ من الأمن السيبراني ويعرف أيضا بأنه سياسات وتقنيات وضوابط تعمل جميعها لحماية المنتشرة والتطبيقات المرتبطة بها والمكونة للحوسبة السحابية واجبها حماية البيانات والفصل بين الواجبات أمن التطبيقات ،الأنظمة السرية وغيرها من الواجبات .([3])

إن أهمية حماية البيانات يتطلب معرفة أمن الحوسبة السحابية لتعلم كيفية حمايتها بعد تخزينها ومعرفة كيفية تحديد المشكلات الأمنية في التقنيات والإجراءات المعيارية المتعلقة بالحوسبة السحابية لمنع المخاطر .([4])

---

[1] يانبي شن ، فيرن باكسون ، راندي كاتس ، بترجمة طه زروقي ، "ما الجديد في أمن الحوسبة السحابية" ، **مجلة معالم**، العدد الرابع ، 2011 ص103

[2] - العياشي زرزار، حمزة بن وريدة ، "الحوسبة السحابية ، المفهوم والخصائص"، **مجلة الأرصاد للدراسات الإقتصادية والإدارية** م 2 العدد الثاني ، ديسمبر 2019، ص 187.

[3] – شريف جيجان ، "الأمن السيبراني الصيني دراسة في دوافع والتحديات" ، **مجلة قضايا سياسية** ، جامعة النهرين ، العدد الخامس و ستون، 2022، ص 38 .

[4] – شريف جيجان ، المرجع نفسه ، ص 38.

المطلب الثاني

عناصر الأمن المعلوماتي وأهدافه

تمحورت دراسة هذا المطلب من خلال تخصيص فرع أول لعناصر الأمن المعلوماتي أما فرع ثاني لأهداف الأمن المعلوماتي .

الفرع الأول

عناصر الأمن المعلوماتي

في العصر الرقمي الذي نعيشه اليوم اصبحت المعلومات أحد أهم الأصول الإستراتجية لأي مؤسسة أو فرد ، بل و أضحت المحرك الرئيسي لصناعة القرار المصيري وتقدم المجتمعات، ومع هذا الإعتماد المتزايد على تدفق البيانات وتبادلها إلكترونيا ، برزت تحديات كبيرة تتعلق بكيفية حماية هذه المعلومات من المخاطر المحدقة بها سواء كانت داخلية ناجمة عن خطأ بشري أو خارجي مصدرها هجمات إلكترونية ، ولمواجهة هذه التحديات تبلور مفهوم أمن المعلومات كإطار متكامل يهدف توفير الحماية اللازمة للمعلومات ويقوم هذا الأخير على ثلاثة ركائز رئيسية تتمثل في تحقيق السرية ، السلامة والتوافر و هو ما يسمى بالثالوث و بالإنجليزية Confidentiality - Integrity - Availability .([1])

أولا: السرية .

ليست مجرد سيمة تلازم عناصر الأمن المعلوماتي، بل هي حق أصيل للمالك، وهي ضمان عدم إتاحة المعلومات أو الكشف عنها للأشخاص أو الأنظمة غير مصرح لها بالإطلاع ويقصد بها حماية المعلومات من أن يطلع عليها أشخاص غير مرخص لهم الوصول إليها وكشفها وربما إستخدامها إستخداما سلبيا يضر صاحبها.([2])

[1] – مالك محمد ،إستراتيجية إدارة أمن المعلومات نظمية على استشراف تطبيقات المعيار الدولي نموذجا، رسالة دكتوراه، تخصص علوم الإعلام والإتصال، كلية علوم الإعلام والإتصال ، جامعة الجزائر 3، 2015-2016 ، ص 141.

2 بن طيب إبراهيم ، "أهمية أمن نظم المعلومات لدى المؤسسات الاقتصادية الحديثة" ، **مجلة التنمية و الإقتصاد التطبيقي** ، جامعة المسيلة، العدد الثالث، مارس 2018، ص 4 .

كما يقتصر حق الوصول لأصول البيانات و المعلومات على الأشخاص المصرح لهم بذلك مع التأكيد على عدم الكشف عنها للآخرين. ([1])

فالسرية أول وأهم عناصر الأمن المعلوماتي التى ينبغي توخي الحذر حين تطبيقها في تعاملاتنا الإلكترونية على سبيل المثال إعتماد كلمة السر للبريد الإلكتروني قوية و صعبة الإختراق والحرص على عدم كشفها للآخرين وتغييرها من فترة الى أخرى لضمان السرية. ([2])

ثانيا : سلامة المحتوى و التكامل.

السلامة تعني الحفاظ على إكتمال المعلومات ودقتها وعدم تعرضها لأي تغيير أو تعديل أو إتلاف غير مصرح به ، سواء كان عمدا أو إهمالا، فهي الحفاظ على البيانات سليمة و كاملة و دقيقة أثناء تشغيل أنظمة تكنولوجيا المعلومات .([3])

فعنصر سلامة المعلومة يتكون من شقين الأول سلامة المعلومة و يعني عدم تغيير هذه الأخيرة بشكل غير ملائم سواء عن عمد أو بغير قصد ، والثاني سلامة المصدر وتعني الحصول على المعلومة من مصدرها الأصلي، ([4]) كما يقصد بها سلامة المعلومة من التغيير أو التعديل عليها أو حذفها من قبل أشخاص غير مرخص لهم بالقيام بذلك .([5])

التكامل يقصد به حماية البيانات من عمليات الحذف والتخريب ، ويتم ذلك من خلال مجموعة الأساليب توفرها نظم قواعد البيانات كقوائم الولوج والصلاحيات بالإضافة الى علاقة الترابط ما بين البيانات المخزنة فيها . ([6])

1 –شريف كامل شاهين، " أمن المعلومات"، **المجلة العربية للمعلوماتية وأمن المعلومات**، م: 01، العدد الاول، أكتوبر 2020 ص 3

2 – بن طيب إبراهيم ، المرجع السابق ، ص 05

3 – شريف كامل شاهين ، المرجع نفسه ، ص 03

4 -مالك محمد ،المرجع السابق، ص 143.

5 - بن طيب إبراهيم ، المرجع نفسه ، ص 5

6 –مالك محمد ، المرجع نفسه ، ص 143

ثالثا :التوافر والإتاحة

يشار لها بالتواجد و الإستمرارية فهي بمثابة جهاز الدموي في الجسد الذي يضخ المعلومات الى مستحقيها في اللحظة المناسبة والوقت المطلوب ، فهي نقيض الإحتكار والتعطيل .

ويقصد بها توفر المعلومات متى ما تم الحاجة إليها ، ومن ثم إمكانية الإستفادة منها من خلال قنوات أمنية سليمة ، ([1]) و التأكد من إستمرار عمل النظام المعلوماتي و إستمرار القدرة على التفاعل مع المعلومات ، وتقديم الخدمة لمواقع المعلوماتية و أن مستخدم المعلومات لن يتعرض الى منع إستخدامه لها أو دخوله إليها ، ([2]) تمتاز هذه الخاصية بسمات متمثلة في:

أ — مقاومة النظام وقدرته على الحفاظ على نفسه من العمليات التى تجعله غير متاح للمستخدمين المخولين بإستخدامه .

ب – القدرة على التوسع لسد الحاجة المستقبلية و المرونة المتمثلة في توفر الإمكانيات و الأدوات التى تمكن من إدارة النظام دون يستدعي ذلك توقفه مع سهولة الإستخدام. ([3])

الفرع الثاني

أهداف الأمن المعلوماتي

لم يعد أمن المعلومات ترفا تقنيا ، بل أصبح درعا إستراتجيا يحمي كيان المؤسسات وسمعتها، وفي ضوء الأهمية المتزايدة له كركيزة أساسية لإستدامة الأعمال وبناء الثقة ، تتحدد الغايات المنشودة في عدة أهداف إستراتجية يمكن إجمالها فيما يلي:

[1] –بن طيب إبراهيم ، المرجع نفسه ، ص 5

[2] –ليتيم فتيحة ، ليتيم نادية ، المرجع السابق ، ص 240

[3] – بوازدية جمال ، الأمن السيبراني، محاضرات مقدمة لطلبة السنة الثانية ماستر ، تخصص دراسات واستراتيجية وأمنية ،كلية العلوم السياسية و العلاقات الدولية ، جامعة الجزائر 3 ، 2020-2021 ، ص 29.

أولا : حماية البيانات من الوصول اليها.

يتم ذلك عبر تشفيرها بأعلى معايير التشفير بحيث لا يمكن فك طلاسمها أو الوصول إليها إلا من قبل المخولين اللذين يمتلكون المفاتيح السرية ، كما يتم حمايتها من القرصنة التى تعمل على كشف نقاط ضعف نظم الحماية وغالبا يتم ذلك من خلال إستغلال مختلف وظائف الأنترنت التى تحوله الى نظام مفتوح سهل الإختراق . ([1])

ثانيا : تأمين قنوات الإتصال.

تمنع التنصت أو الإعتراض و تضمن أن تظل الرسائل المتبادلة بين الأطرف عصية الإختراق وهذا التنصت يكمن في التموقع شبكة معلوماتية أو شبكة التواصل عن بعد، ومن ثم تحليل وتخزين المعلومات العابرة و ترجمة التأمرات وكل ما يدور داخل الشبكة المعلوماتية،([2]) ومن الأدوات المستخدمة لتنفيذ التنصت برامج تحليل الشبكات و بروتوكولاتها كبرنامج (سنيفر) الذي يعرف على أنه برنامج التنصت الإلكتروني الذي يراقب المعلومة المنقولة داخل الشبكة .([3])

ثالثا : الإستجابة للحوادث الأمنية.

يتم ذلك بفعالية وكفاءة عبر آليات إستباقية ، وخطط إستجابة متقنة تحد من الخسائر وتسارع الى إستعادة الوضع الطبيعي، إن نجاح المنظمة يعتمد على قدرة فريق الإستجابة للحوادث من خلال تحديد المخاطر والتهديدات و نقاط الضعف التى يجب إصلاحها لضمان سير العمليات بشكل أمن وفعال ، هناك ست خطوات رئيسية لتعامل مع الحوادث وهي الإعداد ، الإكتشاف ، الإحتواء الاستئصال و الإستعادة ثم الدروس المستفادة، يتم الإعداد من خلال جعل الفريق جاهز لتعامل مع الحادث و تنسيق مع مزودي الخدمة ، مع إعداد نظام التتبع ، بعد ذلك يتم تحديد نوع الحادث الأمني من خلال الاكتشاف على جميع المستويات مثل أجهزة المستخدمين والأنظمة والشبكة.

---

[1] – فيلالي أسماء ، وشليل عبد اللطيف ، "تهديدات أمن المعلومات وسبل التصدي لها" ، **مجلة البشائر الاقتصادية**، جامعة ابو بكر بلقايد تلمسان ، الجزائر ، م 4 ، العدد الثالث ،د س ن ، ص 168

[2] – فيلالي أسماء ، وشليل عبد اللطيف ، المرجع السابق ، ص 168

[3] - فيلالي أسماء ، وشليل عبد اللطيف ، المرجع نفسه ، ص 168

ثم يأتي دور الإحتواء و الإستئصال بعد تحديد مقدار المشكلة و وقف نموها و إغلاق المنافذ مع إزالة البرامج الضارة و منه تعود الحالة إلى طبيعتها الأولى بطريقة أمنة ليكون في الأخير درسا مع تطوير القدرات لمراجعة نقاط الضعف.([1])

رابعا : صد الهجمات الإلكترونية.

يتم ذلك دون تعطيل خدمات النظام ، ويحافظ على إستمرارية الأعمال حتى في وجه التهديدات المتصاعدة من خلال تصحيح الثغرات الأمنية التي إستعملها المخترقون لدخول الأنظمة وإصلاحها يشمل ذلك تحديث البرامج ، تطبيق التصحيحات الأمنية ، وإعادة تكوين الأنظمة لضمان عدم تكرار الإختراق، والتأكد من أن جميع الأنظمة و التطبيقات محدثة أمنيا ، ويجب فحص شامل للأمن. ([2])

خامسا : سرية البيانات.

مما يكسب المؤسسة سمعة طيبة ويعزز الثقة المتبادلة و يجعلها شريكا موثوقا في البيئة الرقمية، ويدعم التحول الرقمي والإدارة الإلكترونية في إطار قانوني أمن ، حيث تعد سرية بيانات العملاء و خصوصيتهم حجر الزاوية في أي نظام معلوماتي يحترم كرامة الإنسان وحقوقه الأساسية وقد أدرك المجتمع الدولي هذه الحقيقة الجوهرية فعمل على تجسيدها في مواد قانونية ملزمة ففي إتفاقية بودابست للجريمة الإلكترونية نجد المشرع لم يغفل هذا البعد بل ألزم الدول الأطراف بدمج ضمانات صارمة في تشريعاتها الداخلية عند تطبيق السلطات و الإجراءات المنصوص عليها فنصت المادة 15 بوضوح على أنه تسعى كل دولة طرف الى ضمان خضوع وضع وتنفيذ وتطبيق السلطات والإجراءات المنصوص عليها في هذا القسم للضمانات والشروط المنصوص عليها في قانونها الوطني ، الذي ينبغي أن يوفر الحماية الملائمة لحقوق الإنسان والحريات ....."([3])

---

[1] – الرجوع لموقع جمعية أمن المعلومات ، الإستجابة للحوادث الأمنية ، تاريخ النشر 2018/10/23 ، تاريخ التصفح 2026/05/07 على الساعة 01:25 على الوصلة: Hemaya.org.sa/?p=**8095**

[2] – موقع الدرع الرقمي للمؤسسات السعودية في مواجهة التهديدات المتقدمة، أساسيات تحليل الهجمات السيبرانية، تم الإطلاع عليها بتاريخ2026/03/13 ، على الساعة 18.15، على الوصلة :**https://www.rmg-sa.com**

[3] – المادة 15 من إتفاقية المتعلقة بالجريمة الإلكترونية بودابست ، مجلس أوروبا مجموعة المعاهدات،2001 ،ص 10.

المبحث الثاني

الإطار التشريعي للأمن المعلوماتي

في خضم التحول الرقمي المتسارع الذي يعيد تشكيل ملامح الحياة المعاصرة وفي عصر المعلوماتية الذي تهاوت فيه الحدود الجغرافية أمام زخم البيانات وتدفقها ، باتت المعلومات هي الثروة الحقيقية للأمم ، وأصبح الفضاء الرقمي ساحة مفتوحة على مصرعيها للتفاعلات الاقتصادية و الإجتماعية والثقافية ، كل هذا أدى الى بروز الأمن المعلوماتي كحارس أمين لهذه المجتمعات ، ودرع واقي يصد التهديدات التى تطول سرية البيانات وسلامتها ومدى إتاحتها ، لم يعد مجرد خيار تقني تتبناه المؤسسات الكبرى ، بل أضحى ضرورة إستراتجية تمس الأفراد والجماعات والدول على حد السواء ، فهو علم أو بالأحرى مجال معرفي قائم على مجموعة من المراجع والقواعد التي يستمد منها أحكامه وتوجهاته والأمن المعلوماتي ليس إستثناء ، فالقواعد والمعايير التى نتبعها لتأمين بياناتنا وأنظمتنا لا تأتي من فراغ بل هي مستمدة من مصادر متعددة بعضها دولي يتجاوز حدود الدول ليشمل المجتمع الرقمي بأكمله وبعضها محلي يخص كل دولة على حدى.

وبعد أن إستعرضنا في المبحث الأول المفاهيم الأساسية للأمن المعلوماتي وعناصره وأهدافه ننتقل في هذا المبحث الثاني الى إستكشاف الإطار التشريعي للأمن المعلوماتي و ذلك من خلال تقسيمه الى مطلبين رئيسين المطلب الأول يتناول المصادر الدولية التى تستمد منها قواعد الأمن المعلوماتي ، والمطلب الثاني يخصص لدراسة المصادر الوطنية للأمن المعلوماتي.

المطلب الأول

المصادر الدولية للأمن المعلوماتي

تعد الإتفاقيات الدولية أهم مصدر قانوني ملزم للأمن المعلوماتي على المستوى الدولي ، حيث تضع أطرا مشتركة لمكافحة الجرائم الإلكترونية و تعزيز التعاون بين الدول وابرز هذه الإتفاقيات.

الفرع الأول

الإتفاقية الأوروبية لمكافحة الجريمة المعلوماتية (إتفاقية بودابست)

تعتبر إتفاقية بودابست المتعلقة بالجرائم الإلكترونية هي مراجعة جماعية إستجابة للجرائم السيبرانية من قبل الدول الأعضاء في البلدان من أوروبا وبعض الدول غير الأعضاء وهي أول معاهدة ملزمة متعددة الجنسيات لفهم معالجة الجريمة السيبرانية بحذافيرها .([1])

الإتفاقية الأوروبية لمكافحة الجريمة المعلوماتية هي الاسم الرسمي لها ، مجلس أوروبا هو الجهة المنظمة لها وتم ذلك في عاصمة المجر بودابست بتاريخ 23 نوفمبر 2001 ودخلت حيز التنفيذ عام 2004 تعتبر أول معاهدة إقليمية دولية ملزمة لمكافحة الجرائم المرتكبة عبر الأنترنت و الأنظمة الرقمية ، على الرغم أن مجلس أوروبا أعدها إلا أنها تكتسي الطابع العالمي لأن العضوية فيها مفتوحة لأي دولة في العالم ، و هذا يلاحظ من خلال انضمام دول من خارج المجلس مثل اليابان والولايات المتحدة الأمريكية ، و تعتبر الإتفاقية المرجعية القانونية لكل التشريعات الدولية الصادرة في هذا المجال. ([2])

سعى مجلس أوروبا من وراء إعتماد الإتفاقية الى حماية المجتمع الدولي من خلال إصدار ترسانة من النصوص الملزمة ، حيت تتكون الإتفاقية من ديباجة وثماني وأربعون مادة موزعة على أربعة أبواب، أولهم يعالج إستخدام المصطلحات، أما الثاني يعالج التجريم والصلاحيات الإجرائية، و الباب الثالث يركز على الإختصاص والتعاون الدولي وفي الباب الأخير جاء بأحكام ختامية .

---

[1] – قطاف سليمان ، بوقرين عبد الحليم ، "الآليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل إتفاقية بودابست والتشريع الجزائري"، **المجلة الأكاديمية للبحوث القانونية والسياسية** ، جامعة عمار ثليجي ، الأغواط، الجزائر م:06 ، العدد الأول ،2022، ص337.

[2] – بوازدية جمال ، المرجع السابق ، ص 79.

أولا:إستخدام المصطلحات

المصطلحات الأساسية التى جاءت بها الإتفاقية وهي:

أ – منظومة الكمبيوتر :أي جهاز أو مجموعة أجهزة المتصلة أو ذات الصلة ، و التى يقوم واحد منها أو أكثر وفقا لبرنامج المعالجة الآلية للبيانات.

ب – بيانات الكمبيوتر : أي تمثيل للحقائق أو المعلومات بشكل مناسب للمعالجة في نظام حاسوبي.

ج – مقدم الخدمة: الكيان العام أو الخاص الذي يتيح للمستخدمين الإتصال عبر نظام حاسوبي أو يقوم بمعالجة أو تخزين البيانات نيابة عنهم .

د – بيانات حركة الإتصال: البيانات المتعلقة بالإتصال و التى تشير الى مصدره ووجهته ومساره وتوقيته ، وهذا ما جاء في نص المادة الأولى (01) من الإتفاقية.

ثانيا: التجريم والصلاحيات الإجرائية

يشكل هذا الباب الإلتزامات الوطنية وينقسم الى قسمين رئيسين القانون الجنائي الموضوعي والقانون الإجرائي بالنسبة للقسم الأول يحدد الأفعال التى يجب على الدول تجريمها في تشريعاتها الوطنية منها الجرائم التي تمس خصوصية وسلامة وتوافر بيانات ونظم الكمبيوتر، جرائم السرية السلامة تجرم الدخول غير المشروع ، ([1]) الإعتراض غير المشروع بإستخدام وسائل فنية للإرسال غير العمومي للبيانات الكمبيوتر، ([2]) التدخل في البيانات من خلال إتلاف بيانات حاسوبية، حذفها و إفسادها، التدخل في النظام و إساءة استخدام الأجهزة وهذا ما نصت عليه المادة الرابعة من نفس الإتفاقية.

الجرائم المرتبطة بالحاسوب تجرم التزوير المرتبط بالكمبيوتر إذا ما ارتكبت عمدا وبغير حق تغيير أو حذف أو إتلاف بيانات كمبيوتر بشكل يجعل البيانات غير أصلية تبدو أصلية.([3])

[1] –المادة 02 من الإتفاقية المتعلقة بمكافحة الجريمة الإلكترونية ، بودابست 2001/11/23.

[2] –تنص المادة 03 من الإتفاقية المتعلقة بمكافحة الجريمة الإلكترونية على أنه" إذا ما أرتكب عمدا وبغير حق الإعتراض بوسائل..."

[3] – تنص المادة05 من الإتفاقية المتعلقة بمكافحة الجريمة الإلكترونية أنه" إذا ما أرتكب عمدا وبغير حق الإعاقة الخطيرة ....."

كما تتحدث المادة 06 من الإتفاقية عن الإحتيال المرتبط بالكمبيوتر إذا ما إرتكبت عمدا وبغير حق وتسببت في إلحاق خسارة بملكية شخص آخر عن طريق إدخال تغيير، حذف أو إتلاف بيانات كمبيوتر أو تدخل في وظيفة نظام كمبيوتر.

القانون الإجرائي يمنح سلطات إنفاذ القانون صلاحيات اللازمة للتحقيق الفعال منها التعجيل في حفظ البيانات المخزنة خاصة عندما تكون هناك أسباب للإعتقاد بأنها معرضة لفقدان أو تعديل، هذه المادة ذات أهمية قصوى للحفاظ على الأدلة الرقمية سريعة التلاشي.([1])

أما المادة 18 من الإتفاقية تركز على التعجيل في حفظ البيانات الكمبيوتر والكشف الجزئي عن بيانات الحركة وهو الإفصاح عن البيانات تتيح للسلطات إصدار أوامر لمزودي الخدمة بالإفصاح عن بيانات المشتركين.

ومن اجل البحث والمصادرة تنظم إجراءات تفتيش أنظمة الحاسوب وضبط البيانات وكذلك جمع بيانات الكمبيوتر في الوقت الحقيقي و إعتراض بيانات المحتوى هو الجمع الفوري يتعلقان بصلاحية جمع بيانات حركة المرور في الوقت الحقيقي و التنصت على الإتصالات الرقمية .([2])

ثالثا:التعاون الدولي ونطاق الاختصاص

أ –الإختصاص القضائي: تحدد قواعد إختصاص الدول بالنظر في الجرائم المذكورة في المواد من 02 الى 11 من الإتفاقية عندما تقع على إقليمها أو على متن سفنها أو بواسطة رعاياها .([3])

ب – التعاون الدولي: تشكل الجهاز العصبي للإتفاقية ، حيث تضع إطار للمساعدة المتبادلة وتسليم المجرمين .([4])

ج – شبكة 24/7 تلزم الدول بإنشاء نقطة إتصال تعمل على مدار الساعة وطول أيام الأسبوع لتقديم المساعدة الفورية في التحقيقات العابرة للحدود هذه الآلية تضمن سرعة الإستجابة للطلبات العاجلة، وهذا ما أفرزته المادة 35 من الإتفاقية.

[1] المادة 16من الإتفاقية المتعلقة بمكافحة الجريمة الإلكترونية ، بودابست 2001/11/23

[2] تنص المادة 19 من الإتفاقية المتعلقة بمكافحة الجريمة الإلكترونية أنه" تمكين سلطاتها المختصة من النفاذ أي نظام كمبيوتر..."

[3] تنص المادة 22 من الإتفاقية المتعلقة بمكافحة الجريمة الإلكترونية أنه" لإقرار الولاية القضائية على أي جريمة تنص عليها ...."

[4] تنص المادة 23 من الإتفاقية المتعلقة بمكافحة الجريمة الإلكترونية أنه" تطبق هذه المادة على تسليم المجرمين بين الدول الأطراف.."

رابعا:الأحكام الختامية

تضمنت المواد من 36 الى 48 التنظيم القانوني لعمل الإتفاقية ذاتها مثل كيفية التوقيع و الدخول حيز النفاذ المادة 36 للإنضمام الى الإتفاقية بحيث يجوز للجنة وزراء مجلس أوروبا بعد التشاور مع الدول المتعاقدة في الإتفاقية والحصول على موافقتها بالإجماع، توجيه دعوة لأي دولة غير عضو للإنضمام، ([1]) كما انه يجوز لأي دولة بموجب إشعار خطي موجه للأمين العام للمجلس تعلن أنها تستفيد من التحفظ كما يجوز اضافة تعديلات لهذه الإتفاقية.

من دراستنا لإتفاقية بودابست لمكافحة الجريمة المعلوماتية يظهر أن المجتمع الدولي قد أحرز تقدما ملحوظا في تطوير الإطار القانوني والإجرائي للأمن المعلوماتي لمواجهة الجرائم الإلكترونية وعملت على توحيد التشريعات الوطنية وتوحيد المصطلحات وتوفير أدوات قانونية مثل الحفظ السريع للبيانات والتفتيش المعلوماتي و التنصت الرقمي ، كما أوضحت أن هذه الجرائم عابرة للحدود تستلزم التنسيق والتعاون الدولي وتبادل المعلومات، بالنسبة للتشريع الجزائري بمثابة مرجعية قانونية. [2]

الفرع الثاني

اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية

لم تكن هذه الإتفاقية وليدة فراغ ، بل كانت حاصل صراع فكري جيو سياسي حول من يمتلك تقنين الفضاء الإلكتروني ، منذ إقرار اتفاقية بودابست ظلت دول عديدة وعلى رأسها الصين وروسيا تنتقدها لكونها إتفاقية أوروبية لم يشارك في صياغتها معظم دول العالم ، في الطرف المعاكس رأت الدول الغربية في إتفاقية بودابست المعيار الأنسب ينبغي تعميمه ، و في عام 2017 كانت المبادرة روسية أين قدمت مشروع إتفاقية خاص بها ، ثم تبنت مجموعة من الدول بقيادة الصين وروسيا مبادرة من الجمعية العامة للأمم عام 2019 لبدء مفاوضات رسمية ، شارك فيها 64 دولة وهيئة إقليمية وتعد هذه الإتفاقية أول صك يعني بمكافحة الجريمة الإلكترونية على المستوى الدولي.

[1] تنص المادة 36 من الإتفاقية المتعلقة بمكافحة الجريمة الإلكترونية ، انه" تفتتح هذه الإتفاقية للتوقيع من قبل الدول الأعضاء.."

[2] سعيد مسعود الكثيري، "الجريمة الالكترونية في ضوء اتفاقية بودابست الإطار المفاهيمي و التطبيقي"، **مجلة البحوث القانونية و الاقتصادية**، م 09 العدد الأول ، جانفي 2026، ص 960 .

كان للجزائر دورا محوريا في صياغة هذه الاتفاقية من خلال رئاسة اللجنة المتخصصة بإعدادها و قيادة المسار منذ ماي 2021 والذي توج بإعتمادها خلال الدورة 79 من الجمعية العامة للأمم المتحدة في ديسمبر 2024 بهانوي عاصمة الفيتنام، ([1]) وتأتي بعد أكثر من عقدين من هيمنة إتفاقية بودابست 2001 التي كانت ذات طابع إقليمي أوروبي في الأساس ، ينظر الى هذا الإنجاز على أنه فوز لدول الجنوب العالمي في قدرتها على صياغة قواعد قانونية دولية تعكس مصالحها .

تعد إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية صرحا قانونيا دوليا طموحا يهدف الى وضع إطار عالمي شامل للمواجهة، أين حفلت نصوصها بترسانة قانونية متكاملة تجسدت في ثمانية وستين مادة موزعة بين ديباجة وتسعة فصول رئيسية.

اولا:المبادئ الجوهرية

يشمل نطاق تطبيق الإتفاقية و تعريف المصطلحات، وتتمثل في تعزيز التدابير الوقائية من خلال التشجيع وتأصيل إجراءات منع الجريمة الإلكترونية ومكافحتها بفعالية عن طريق التعاون الدولي لتيسير ودعم التبادل الأدلة الإلكترونية.([2])

والمساعدة التقنية لاسيما الدول النامية ، كما تؤكد الإتفاقية على ضرورة تنفيذ الإلتزامات بما يتسق مع مبدأ المساواة في السيادة وعدم التدخل في الشؤون الداخلية مع كفالة حقوق الإنسان، و الحريات الأساسية بما في ذلك الحقوق المتعلقة بحرية التعبير أو حرية الضمير أو الرأي أو الدين،([3]) المادة الثانية من الإتفاقية أعطت حصة وافرة من تعريف المصطلحات حيث شملت زيادة عن ما عرفته إتفاقية بودابست اضافة مصطلح معلومات المشترك ، البيانات الشخصية ، الجريمة الخطيرة والممتلكات، العائدات الإجرامية ، التجميد ، الجريمة الأصلية ، المصادرة ، و منظمة التكامل الإقتصادي . ([4])

[1] – وقعت الجزائر معاهدة الأمم المتحدة لمكافحة الجريمة السيبرانية بتاريخ 2025/10/25، موقع وزارة الشؤون الخارجية والجالية الوطنية بالخارج ، تم الإطلاع عليها بتاريخ 2026/03/13 على الساعة العاشرة و خمسة وأربعون دقيقة 10.45 ، على الوصلة:
https://www.mfa.gov.dz/ar/press-and-information/news-and-press-releases/mrmagramane-signed-the-united-nations-convention-on-c

[2] – المادة 40 من اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية ، 2024 ، ص 23 .

[3] – تنص المادة 06 من إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية2024على أنه" يسمح بقمع حقوق الإنسان ....."

[4] – تنص المادة 07 من اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية2024على أنه" الوصول دون وجه حق لنظام المعلومات.."

ثانيا :الجرائم المعلوماتية

أقامت الإتفاقية تصنيف دقيقا للأفعال المجرمة يميز الجرائم التى تستهدف الأنظمة وهي الجرائم التقنية البحتة والجرائم التى تستخدم الأنظمة كوسيلة لإرتكاب أفعال إجرامية.

من خلال المواد (05 الى 11) الجرائم التقنية البحتة تشمل الوصول غير المشروع للأنظمة التدخل في البيانات الإلكترونية عن طريق إتلافها أو حذفها أو تغييرها أو تحويرها أو طمسها عندما ترتكب هذه الأفعال عمدا ودون وجه حق، [1] التدخل في النظام ذاته بعرقلة عمله بشدة عن طريق إدخال بيانات إلكترونية أو إرسالها أو إتلافها أو حذفها أو إفسادها أو تحويرها أو طمسها عندما يرتكب الفعل عمدا ودون وجه حق ، وتكتمل هذه المنظومة بتجريم إساءة إستخدام الأدوات والأجهزة التى تصمم أو تعدل أساسا لإرتكاب هذه الجرائم . [2]

جرائم المحتوى وحماية الفئة الهشة التي أولت الإتفاقية عناية خاصة لحماية الفئات الخاصة، ولا سيما الأطفال من الإستغلال في الفضاء الرقمي ، وذلك من خلال ما أفرزته المادتين 14-15 المتعلقتين بجرائم بمواد الأنترنت المتمثلة في جريمة الإعتداء الجنسي على الأطفال و إستغلالهم جنسيا عن طريق إنتاج أو إلتماس أو حيازة مواد الإعتداء الجنسي على الأطفال أو تمويل هذه الأفعال، و جريمة الإستدراج و الإستمالة لغرض إرتكاب جريمة جنسية ضد الطفل، [3] أما جريمة غسل العائدات الإجرامية لم يكن تحديد مفاهيم الممتلكات والعائدات الإجرامية في المادة الثانية مجرد عملية إصلاحية عابرة ، بل جاء بمثابة تمهيد موضوعي دقيق ومقصود هيأ للحكم الوارد في المادة 17 فقد ألزمت هذه المادة الدول الأطراف بتجريم جميع أشكال التصرف في العائدات الإجرامية ولا سيما تحويلها أو نقلها أو تمويه مصدرها غير المشروع .

ثالثا :الإختصاص القضائي

تحدد الإتفاقية في مادتها 22 إطار قانونيا دقيقا للولاية القضائية حيث تلزم كل دولة طرف بإتخاذ التدابير اللازمة لبسط ولايتها على الأفعال المجرمة عندما ترتكب داخل إقليمها أو على متن سفينة ترفع علمها أو طائرة مسجلة بمقتضى قوانينها وقت إرتكاب الجريمة.

[1] تنص المادة 09 من إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية2024 على أنه" إتلاف بيانات الكترونية أو حذفها ....."

[2] تنص المادة 11 من اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية2024 على أنه" عندما ترتكب هذه الأفعال عمدا ....."

[3] تنص المادة 15 من إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية على أنه" فعلا متعمدا من الإتصال أو الإستدراج....."

كما تمنح الإتفاقية للدول خيارات إضافية لبسط ولايتها في حالات معينة منها وقوع الجريمة ضد أحد مواطنيها أو إرتكبت من طرفه أو شخص عديم الجنسية مقيم بصفة معتادة في إقليمها أو إذا كانت الجريمة موجهة ضد الدول الطرف نفسها، [1] من البنود الجوهرية إلتزام الدولة بحماية ولايتها القضائية عندما يكون الجاني المزعوم موجودا في إقليمها، و تقرر عدم تسليمه لمجرد كونه أحد مواطنيها، في حال وجود تحقيقات أو ملاحقات قضائية من دول أطراف متعددة بسبب نفس السلوك الإجرامي تفرض الإتفاقية على هذه الدول التشاور و التنسيق فيما بينها لتنظيم الإجراءات المتخذة .

رابعا: التدابير الإجرائية وإنفاذ القانون.

على صعيد التدابير الإجرائية و إنفاذ القانون نصت إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية على حزمة متكاملة من التدابير الإجرائية التى تشكل العمود الفقري لسلطات إنفاذ القانون في العصر الرقمي، فقد أوجبت تمكين سلطات الأطراف المختصة من إصدار أوامر بالحفظ العاجل للبيانات الإلكترونية المخزنة لفترة محددة تصل 90 يوما قابلة للتجديد لحماية الأدلة الرقمية من الضياع أو التعديل ريثما يتم إستكمال الإجراءات القانونية اللازمة ، [2] كما أعطت هذه الأخيرة صلاحيات التفتيش والحجز ، حيث تقوم بتفتيش الأنظمة والوسائط وتأمين البيانات الموجودة فيها ، و جمع البيانات الحركة في الوقت الحقيقي أقرت الإتفاقية في المادة29 آلية لجمع بيانات الإرسال والتحويل لحظيا وهي البيانات اللازمة لتتبع مصدر الإتصال ومساره. [3]

خامسا: التعاون الدولي و الآليات الوقائية.

التعاون الدولي و الآليات الوقائية أرسى الإتفاق إطارا متطورا للتعاون الدولي، متجاوزا الحدود التقليدية من خلال إلزام الدول بتقديم المساعدة المتبادلة في مراحل التحقيق والملاحقة الجنائية وتيسير إجراءات تسليم المجرمين المتهمين بإرتكاب الجرائم السيبرانية، و تتجسد آلية التعاون الفوري في إنشاء شبكة تعمل على مدار الساعة طوال أيام الأسبوع 24/7 لضمان الإستجابة السريعة للطلبات العابرة للحدود.[4]

[1] تنص المادة22 من إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية على أنه" عندما يرتكب الفعل الإجرامي في إقليم تلك دولة ...."

[2] تنص المادة 25 الفقرة 2 من إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية 2024 على انه" للإلزام ذلك الشخص بالإحتفاظ.."

[3] تنص المادة 29 من إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية 2024 على انه" صلاحية بجمع وتسجيل ....."

[4] تنص المادة 41 الفقرة1من إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية 2024 على أنه" تعين كل دولة طرف جهة إتصال..."

وإيمانا منها بأهمية بناء القدرات البشرية أولت الإتفاقية عناية خاصة لتدريب الموظفين وتأهيلهم لضمان فعالية التعاون ومواكبة التطور التقني المتسارع ، وهذا ما جاءت به المادة54 الفقرة 2 من إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية 2024.

سادسا :آليات التنفيذ والأحكام الختامية

ينص على إنشاء مؤتمر الدول الأطراف بوصفه منبرا حيويا لتعزيز الحوار وتبادل الخبرات وتقييم التقدم المحرز في تنفيذ الإلتزامات الدولية و هو مؤتمر دوري لتحسين قدرات الدول ومراجعة تنفيذ الإتفاقية، ([1]) و تعد بمثابة ميثاق عالمي يوفق بين الإحتياجات الأمنية للدول و الضرورات التقنية للعصر الرقمي على التوازن الدقيق مع الحقوق والحريات الفردية وحتى تكون ملزمة ونافذة تخضع للتوقيع حتى نهاية ديسمبر 2026 و يبدأ نفاذها بعد إيداع الصك الأربعين من صكوك التصديق .([2])

توفر هاته الاتفاقية ترسانة قانونية تحدد الجرائم الالكترونية و كيفية التعامل معها ، من أجل تعزيز الثقة في الأنظمة الرقمية ، كما تسهل أدوات التعاون عبر تبادل الأدلة الرقمية ، و تتبع المجرمين عبر الحدود و ملاحقتهم قضائيا مما يسهم في تعزيز الأمن المعلوماتي على المستوى الدولي، مع إقرار تبني تدابير قانونية مثل حفظ الأدلة الرقمية ، التفتيش الإلكتروني و الحجز الإلكتروني ، دون إغفال دور هاته الإتفاقية في حماية الفئات الهشة خاصة الأطفال من الإستغلال و الإعتداءات الجنسية عبر الفضاء الرقمي، كما انها تشجع على تدريب الموارد البشرية المتخصصة في مجال مواجهة التهديدات السيبرانية.

الفرع الثالث

إتفاقية الدول العربية لمكافحة جرائم تقنية المعلومات

بعد تخلف دام لأكثر من عقد من الزمن عن الركب في مكافحة الجرائم المعلوماتية الذي إنطلق بإتفاقية بودابست 2001، إستدركت الدول العربية هذا التأخر بوعي قانوني متقدم فكانت الإتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010 نقطة التحول الحاسمة في مسيرة التشريع العربي في مجال جرائم المعلومة.

[1] تنص المادة 57 من إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية 2024 على أنه" ينشأ بموجب هذا الصك مؤتمر للدول....."

[2] تنص المادة 64 من إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية 2024 على أنه" يفتح باب التوقيع على هذه الإتفاقية....."

لم تكتفي هذه الإتفاقية بمجرد اللحاق بالركب الدولي ، بل أتت بترسانة قانونية متكاملة تختص بها الدول العربية وحدها تستمد أحكامها من المبادئ الدينية و الأخلاقية السامية ولاسيما أحكام الشريعة الإسلامية وكذلك بالتراث الإنساني للأمة العربية،([1]) والقيم المجتمعية الأصلية لتشكل بذلك إطار تشريعيا جامعا يوازن بين متطلبات الأمن المعلوماتي و ضرورة حماية الحقوق والحريات مبنيا لخمسة فصول رئيسية تغطي الجوانب الموضوعية ، الإجرائية ، التعاونية والختامية على النحو التالي.

أولا : أحكام عامة

يحتكم هذا الفصل على الهدف من الإتفاقية في مادته الأولى ، حيث انها ترمي الى تعزيز التعاون بين الدول فيما بينها لمكافحة جرائم تقنية المعلومات التى تهدد أمنها ومصالحها وسلامة مجتمعاتها وأفرادها ، ([2]) كما أعطت هذه الأخيرة تعاريف لمصطلحات أساسية كتقنية المعلومات، مزود الخدمة والبيانات ، النظام المعلوماتي والشبكة المعلوماتية ، كما حرصت الإتفاقية على تحديد المجال التطبيقي للجرائم العابرة للحدود، دون أن يغفل ذلك على صون السيادة الرقمية ، و التأكيد على مبدأ المساواة بين الدول.

ثانيا: التجريم.

يعد هذا الفصل الركيزة الموضوعية للإتفاقية حيث يلزم الدول الأطراف بتجريم الأفعال غير المشروعة المرتكبة عبر تقنية المعلومات ، ومن ابرز الجرائم المنصوص عليها الإختراق، الإعتراض و الإعتداء على سلامة البيانات، الملكية الفكرية، إساءة إستخدام وسائل تقنية المعلومات والتزوير، الإحتيال والإباحية ، ([3]) وكذلك جرائم الإعتداء على حرمة الحياة الخاصة ، كما وسعت نطاق التجريم ليشمل الجرائم المرتكبة بواسطة التقنية و المتعلقة بالإرهاب والجريمة المنظمة و غسيل الأموال و الإستخدام غير المشروع لأدوات الدفع الإلكتروني أو الحسابات و شركات التحويل.([4])

---

[1] –تنص ديباجة الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، 2010،على أنه " و أخذا بالمبادئ الدينية والأخلاقية ...."

[2] – عماد حسين محمد الفريحات ، "الجهود العربية والإفريقية لمواجهة الجرائم الإلكترونية في الفترة 2010-2023 "، **مجلة إبن خلدون للدراسات والأبحاث**، م:03 ، العدد الخامس ، ماي 2023 ، ص 196.

[3] - عماد حسين محمد الفريحات ، المرجع السابق ، ص 196.

[4] –عماد حسين محمد الفريحات ، المرجع نفسه ، ص 198.

تناولت أيضا الشروع و المساهمة في الجرائم ، و المسؤولية الجنائية للأشخاص الطبيعية والمعنوية وتشديد العقوبات حين إرتكاب الجرائم التقليدية بواسطة تقنية المعلومات.

ثالثا : الأحكام الإجرائية.

لقد حدد هذا الفصل الصلاحيات والإجراءات في ثماني مواد مكنت السلطات المختصة من التحقيق وجمع الأدلة في جرائم تقنية المعلومات على نحو ما أوردته المادة 22 الفقرة 2 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010.

وتشمل هذه الإجراءات التحفظ العاجل على البيانات المخزنة في تقنية المعلومات لا سيما إذا كانت المعلومات عرضة للفقدان أو التعديل مع إلزام المسؤول المحافظة على السرية والكتمان على النحو المنصوص عليه في المادة 23، ([1])كما تتضمن الكشف الجزئي لمعلومات تتبع المستخدمين بما يتيح تحديد مزودي الخدمة ومسار بث الإتصالات وفقا لما ورد في المادة 24 . ([2])

وجاء كإجراء منه منحت الإتفاقية جهات إنفاذ القانون سلطة إصدار أوامر ملزمة لتسليم المعلومات المخزنة أو بيانات المشتركين ، وهو ما يمثل جسرا قانونيا للوصول الى الحقيقة التقنية ،([3]) وتوسعت الصلاحيات لتشمل تفتيش الأنظمة المعلوماتية والبيئات التقنية المرتبطة بها مع إمكانية الوصول للنظم المتصلة برمجيا لضمان عدم إفلات المجرمين من العقاب ، أما بالنسبة لضمان صون الأدلة شرعت الإتفاقية ضبط المعلومات وتأمينها عبر وسائل تقنية متعددة تشمل نسخ البيانات أو حجب الوصول اليها لمنع أي تلاعب أو المحو، ([4]) وفي خطوة متقدمة ألزمت الدول بتبني آليات الجمع الفوري لمعلومات تتبع المستخدمين بالتعاون الفني الوثيق مع مزودي الخدمة لتقفي أثر الجريمة آنيا ؛وهو ما نصت عليه المادة 28 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات ،ولم تتوقف الإجراءات عند هذا الحد بل أجازت إعتراض معلومات المحتوى وتسجيلها عبر الوسائل الفنية لضبط الأنشطة الإجرامية في لحظة وقوعها .

[1] تنص المادة 23 الفقرة 3 من إتفاقية العربية لمكافحة جرائم تقنية المعلومات على أنه تلتزم كل دولة طرف بتبني الإجراءات ....."

[2] تنص المادة 24 الفقرة 1 من إتفاقية العربية لمكافحة جرائم تقنية المعلومات ، على أنه ضمان توفر الحفظ العاجل لمعلومات....."

[3] تنص المادة 25 من إتفاقية العربية لمكافحة جرائم تقنية المعلومات ، على أنه أي شخص في إقليمها لتسليم معلومات ....."

[4] تنص المادة 27 من إتفاقية العربية لمكافحة جرائم تقنية المعلومات ، تلتزم كل دولة من عمل نسخة من معلومات التقنية ....."

رابعا : التعاون القانوني والقضائي

يشكل الفصل الرابع من الإتفاقية الموسوم بالتعاون القانوني والقضائي الركيزة الأساسية لتوحيد الجهود العربية في مواجهة التحديات الرقمية العابرة للحدود ، يعكس رؤية إستراتجية متكاملة تهدف الى تعزيز التعاون القضائي بين الدول العربية بما يضمن فاعلية العدالة الجنائية في الفضاء المعلوماتي المشترك مع مراعاة مقتضيات السيادة الوطنية .

وفي هذا الإطار يضمن هذا الأخير مجموعة من المواد التى نظمت بشكل دقيق آليات التعاون القضائي والقانوني حيث تميزت بالوضوح والتدرج المنهجي في معالجة الموضوعات ذات الأولوية أولها قواعد الإختصاص القضائي حيث نصت المادة 30 من الإتفاقية على قواعد محددة للإختصاص القضائي بهدف ضمان إمكانية ملاحقة مرتكبي الجرائم الإلكترونية وتلافي النزاعات الإيجابية أو السلبية بين السلطات القضائية في الدول الأطراف، كما جاءت المادة 31 لتنظيم إجراءات تسليم المجرمين المشتبه في إرتكابهم جرائم معلوماتية وفق ضوابط قانونية محكمة تراعي مبادئ حقوق الإنسان [1] وأرست المادة 32 دعائم التعاون في مجال المساعدة المتبادلة بين السلطات القضائية المختصة في خطوة تعكس أسمى صور التآزر القانوني العربي ، لا سيما جمع الأدلة الرقمية وإجراءات التحقيقات العابرة للحدود،[2] وعمدت على إلزام الدول الأطراف بإنشاء جهاز وطني متخصص يعمل على مدار الساعة ليكون جسرا تنفيذيا يضمن الإستجابة السريعة للطلبات القضائية المتعلقة بالجرائم المعلوماتية،[3] وعليه فإن هذا الفصل يمثل صيغة قانونية متقدمة تجمع بين الدقة الإجرائية والمرونة التنفيذية .

تعتبر اتفاقية الدول العربية لمكافحة جرائم تقنية المعلومات من أهم الآليات القانونية الإقليمية الهادفة إلى تعزيز الأمن المعلوماتي في الدول العربية ، حيث يتجلى ذلك في كونها تسعى إلى حماية الأنظمة والشبكات وقواعد البيانات من مختلف أشكال الاعتداء الإلكتروني، حيث جرّمت الأفعال التي تستهدف سلامة المعطيات والأنظمة المعلوماتية، كالدخول غير المشروع إلى الأنظمة، واعتراض البيانات، والإتلاف أو التعديل غير القانوني للمعلومات، إضافة إلى جرائم التزوير والاحتيال الإلكتروني ، من اجل

1 تنص المادة 31من إتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010 على أنه "هذه المادة تنطبق على تبادل المجرمين بين دول."

2 تنص المادة 32 من إتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010 على أنه" على جميع الدول الأطراف تبادل المساعدة.."

3 تنص المادة 43 من إتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010 على أنه" تكفل كل دولة طرف وفقا للمبادئ ....."

تحقيق هذا الهدف منحت للجهات المختصة صلاحيات الجمع و الحفظ الأدلة الرقمية و التحقيق السريع وسرعة التعامل مع الجرائم المعلوماتية.

المطلب الثاني

المصادر الوطنية للأمن المعلوماتي

بعد أن تناولنا المصادر الدولية للأمن المعلوماتي و التى كانت بمثابة الإطار المرجعي العام والمرشد الأساسي للسياسات والتشريعات على المستوى العالمي، حيث استعرضنا كل من اتفاقية بودابست كمعاهدة إقليمية ذات طابع عالمي واتفاقية العربية الإقليمية واتفاقية الأمم المتحدة الدولية ينتقل بنا المسار البحثي الى تناول المصادر الوطنية ، فإذا كانت المصادر الدولية تمثل الدفة المغيرة للإتجاهات وتصنع المبادئ العامة ، فإن المصادر الوطنية هي التجسيد والتنفيذ للنصوص القانونية الملزمة على أرض الواقع ، فهي المراجع الأساسية و التشريعات المكتوبة التى تستمد منها الدولة قواعدها القانونية وتتمثل بشكل رئيسي في الدستور والتشريعات العادية .

الفرع الأول

الدستور الجزائري

يحتل أعلى الهرم القانوني في الدولة و يعتبر المصدر الأساسي المحدد للحقوق والحريات و واجبات المواطنين داخل إقليم دولة معينة ، [1] وبالرجوع الى تعديل الدستور لسنة 2020 جاء بإضافات منها المادة 34 و التى تنص على ضمان حماية الحقوق والحريات وتعزز من أهمية توفير اطار قانوني مستقر لا يتأثر بالتغيرات .

أولا :حماية الحقوق والحريات

[1] بوكورو منال ، "محاضرات في مقياس الحريات العامة "،مطبوعة بيداغوجية في مقياس الحريات العامة ، موجهة لطلبة السنة الثالثة حقوق قانون عام ، جامعة قسنطينة 1 الاخوة منتوري ، 2020/2019 ، ص 22

وذلك من تمكين الفرد من التصرف باطمئنان لهدي القواعد والأنظمة القانونية أثناء قيامه بمعاملاته منها الرقمية بثقة دون خوف من التعرض لتصرفات مفاجئة الصادرة من السلطة العامة شأنها زعزعة هذه الطمأنينة .[1] وهذا ما يسمى بالأمن القانوني الذي سبق وأن أعطينا له حقه من التعريف.

كما جاءت المادة 34 من تعديل الدستور 2020 لتوازن بين الأمن المعلوماتي مع الحقوق والحريات فهي تضع ضوابط لتقيد الحقوق في الفضاء الرقمي يكون هذا التقييد بمقتضى قانون صادر من السلطة التشريعية ويكون مشروعا أي يكون مرتبط بالنظام العام أو حماية الثوابت التى تمس جوهر الحق.

ثانيا :عدم إنتهاك حرمة الإنسان

المادة 39 هذا النص يشكل حماية للمواطن من أي إنتهاك رقمي يمس كرامته مثلا لإبتزاز الرقمي فهو سندا دستوريا لتجريم الأفعال كذلك نأخذ على سبيل المثال التنمر الإلكتروني الذي يعرفه (بتريك سميث) على أنه سلوك سمته العنف ، التكرار و الإصرار ، أي أن التنمر الإلكتروني يمارس بقصد وعمدا وبصفة متكررة بغية إلحاق الأذى بالضحية عن طريق إستخدام أحدث التقنية وتطبيقات الأنترنت .[2]

ثالثا :حماية المال العام

يرى (أتو مايير) أنه يترتب على خضوع ملكية الأموال العامة لقواعد القانون العام بشمولها على الكثير من أوجه الحماية خصوصا سلطة البوليس (الضبط) التى تستعين بها الدولة في حماية هذه الأموال ، [3] وبما أن البنية التحتية للإتصالات المعلومات ملكية عامة وتعتبر من المال العام فوجب حمايتها من أي إعتداء أو تخريب أو إستغلال وهذا ما نصت عليه المادة 20 من الدستور2020 المعدل والمتمم.

رابعا : الحق في البيئة السليمة

---

[1] – فاطمة الزهراء رمضاني ، "التعليق على نص المادة 34 من التعديل الدستوري الجزائري "، **مجلة العلوم القانونية والسياسية** جامعةتلمسان ،العدد الاول أفريل 2021 ص 859

[2] – فرشان دليلة ، "التنمر الإلكتروني بين حرية التعبير والتشكيل القيمي "، **دفاتر البحوث العلمية** ، كلية علوم الإعلام والإتصال جامعة الجزائر ،م : 10 العدد الاول ، 2022 ، ص 281

[3] – غيتاوي عبد القادر ، دليمي رشيد ، "الطبيعة القانونية للمال العام" ، **مجلة القانون والمجتمع**،كلية الحقوق والعلوم السياسية ، جامعة أدرار ،2017/06/01 ،ص 74

البيئة هي المجموعة الشاملة لكل ما يحيط بنا وهي ليست مجرد فضاء نعيش فيه بل هو جزء لا يتجزأ من حياتنا اليومية فهي تؤثر في الإنسان تأثيرا مباشر وغير مباشر مما يفرض علينا واجب الحفاظ عليها كضرورة وجودية ولا تحتمل التجاهل أو التأخير. [1]

و إدراك لهذه الأهمية سن المشرع الجزائري هذا الحق في المادة 64 من تعديل دستور 2020 التى تمنح المواطن الحق في بيئة سليمة،كما يمكن تفسير النص بشكل موسع ليشمل البيئة الرقمية مما يلزم الدولة حماية فضاءها من الجرائم الإلكترونية و بما يعرف بالتلوث المعلوماتي الذي يهدد سلامة البيئة الرقمية وهو ليس مشكلة تواجه فقط من يبحث عن المعلومة بل قد يتعرض لها كل مستخدم إنترنت.[2]

خامسا: حماية الحياة الخاصة

يعرف الأستاذ الدكتور (حسام الأهواني) على أن الحق في الحياة الخاصة هو حق الإنسان أن يكون بعيدا عن تجسس الغير ولا يجوز نشر ما يتم العلم به دون إذن صاحب الشأن وحمايتها من تلوثها الألسن عن طريق النشر .[3] كما عزز الدستور هذه الحماية، حيث نصت المادة 47 من التعديل الدستور 2020 على أن لكل شخص الحق في حماية حياته الخاصة وشرفه ، ولكل شخص الحق في سرية مراسلاته و إتصالاته الخاصة بأي شكل كانت ،[4] وهذه الحماية تشمل جميع أشكال المراسلات و الإتصالات سوء بمفهومها العادي أو الإلكتروني .

الفرع الثاني

قانون العقوبات وقانون الإجراءات الجزائية

[1] – بويديوة يمينة ، رمطين رابح ، الحق الدستوري في البيئة ، مذكرة شهادة الماستر تخصص دولة ومؤسسات ، كلية الحقوق والعلوم السياسية ، جامعة 20أوت 1955 سكيكدة ، دورة جوان 2023 ، ص 01

[2] الحمزة منير ، لعجال حمزة ، "التلوث المعلوماتي في الفضاء الرقمي" ، **المجلة الجزائرية للأمن الإنساني** ، م: 05،العدد الاول، جانفي 2020 ،ص 103

[3] –عثماني رجاء ، بوحفص شيماء ، الحماية القانونية للحق في حرمة الحياة الخاصة ، مذكرة شهادة الماستر في الحقوق تخصص قانون عام ، كلية الحقوق والعلوم السياسية ، جامعة عبن تموشنت بلحاج بوشعيب ،2023/2022 ، ص4

[4] –المادة 47 من الدستور 2020 المعدل والمتمم، ج،ر،ج،ج العدد إثناني وثمانون ، بتاريخ 30ديسمبر2020، ص13

إن إجتماع قانون العقوبات مع الإجراءات الجزائية يشكل القوة الرادعة مع الآلية التنفيذية لهذه المنظومة القانونية ، حيث لا يقتصر دور هذين القانونين على تجريم الأفعال غير مشروعة فحسب بل يمتد لوضع قواعد رادعة وتحديد المسؤوليات وتوفير الآليات الإجرائية لمباشرة التحقيقات والمحاكمات ، مما يضمن حماية فعالة لمواجهة المخاطر الرقمية و التهديدات الإلكترونية.

أولا : قانون العقوبات

يعد قانون العقوبات كما عرفه الدكتور (نجيب حسن)مجموعة من القواعد القانونية التي تحدد الأفعال التى تعد جرائم ، فهو الواجهة الحصينة لصد المخاطر ومع التعديلات الأخيرة بموجب القانون 06/24 المؤرخ 28 أبريل 2024 شهد هذا القانون تطورا نوعيا في تجريم الأفعال التى تمس الأمن المعلومات البنية التحتية الحيوية، من بينها جريمة الخيانة التى نصت المادة 63 مكرر على أنه يعد مرتكبا لجريمة الخيانة ويعاقب بالسجن المؤبد كل جزائري يقوم بتسريب معلومات أو وثائق سرية تتعلق بالأمن الوطني أو الدفاع الوطني أو الإقتصاد الوطني عبر وسائل التواصل الاجتماعي لفائدة دولة أجنبية أو أحد عملائها .([1])

نستنتج من فحوى نص المادة أن الركن المادي لجريمة الخيانة يتوافر على مجموع من العناصر الموضوعية، السلوك الإجرامي و هو تسريب المعلومات والوثائق ، ومحل الجريمة المتمثل في المعلومات والوثائق السرية والأهم في الموضوع هي الوسيلة التى تعد ظرف مشدد المتمثلة في وسائل التواصل الإجتماعي، حيث ينفرد النص بإدراج وسيلة رقمية كآلية لإرتكاب الجريمة مما يعكس وعي المشرع بتطور تقنيات الحديثة وخطورتها كوسيلة سريعة للنشر وتسريب المعلومات والوثائق السرية.([2])

نجد أيضا أن المشرع نص في المادة 175 مكرر 2 على تجريم المساس بالبنية التحتية والتجهيزات الحساسة من خلال إستخدام هذه الأخيرة لأفعال غير مشروعة أو تسهيل جريمة أخرى كما

---

[1]- المادة 63 مكرر من قانون رقم 06/24 مؤرخ 28أبريل 2024، المعدل والمتمم للأمر 66 / 156 المؤرخ 08يونيو 1966المتضمن قانون العقوبات ،ج،ر، العددثلاثون بتاريخ 30 أبريل 2024 ص:07

[2] – عليلي عماد الدين ، بن قسيس زين الدين ، جرائم الخيانة الوطنية وتسريب المعلومات والوثائق السرية على ضوء القانون06/24 المعدل والمتمم لقانون العقوبات ، مذكرة شهادة الماستر في القانون،كلية الحقوق والعلوم السياسية ،جامعة 8ماي 1945 قالمة ، 2025/2024 ، ص 33

فرض عقوبات حين استيرادها أو إقتناءها فهي أجهزة تخضع لترخيص مسبق ، هذا النص يهدف الى إحكام الرقابة على التكنولوجيا ذات الإستخدام المزدوج يمكن توظيفها في تجسس أو التخريب ،([1]) لم يقف المشرع عند هذا الحد بل جرم كل من الجرائم المعلوماتية المستحدثة مثل التهديد الإبتزاز الإلكتروني بنص المادة 333 مكرر 4،5،6 و أعطى حماية للمنظومات المعلوماتية حيث قام بتجريم الدخول والولوج بالمادة 394 مكرر3.

ثانيا : قانون الإجراءات الجزائية

ما فائدة النصوص التجريمية دون آليات إجرائية فعالة تضمن تطبيقها و هنا يأتي دور قانون الإجراءات الجزائية الذي يزود السلطات القضائية و الضبطية القضائية بالأدوات القانونية للتحقيق وجمع الأدلة في البيئة الرقمية .

عدد المشرع الجزائري في القانون 14/25 الذي يتضمن قانون الإجراءات الجزائية مجموعة من الجرائم على سبيل الحصر منها الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال وما تفرضه من إستجابة إجرائية مرنة أين خصها بخصوصية و إستثناءات ، تجسدت في إعفاءها من القيود العامة التى تتم في عمليات التفتيش والمعاينات ، فبموجب المادة 76 من ذات القانون لا تسري الأحكام العامة للتفتيش على هذه الجرائم إلا المتعلق بالحفاظ على السر المهني وجرد الأشياء و حجز المستندات، ([2]) كما حررتها المادة 78 من قيد الميعاد، أين أجاز لسلطة التحقيق والتحري مباشرة التفتيش والمعاينة في أي وقت ليلا كان أو نهارا مخافة من إتلاف الأدلة وطبيعتها الرقمية. ([3])

و أعطى حق اعتراض المراسلات التى تتم عن طريق وسائل الإتصال السلكية ولا سلكية في نفس الجرائم التى ذكرت على سبيل الحصر مع وضع الترتيبات التقنية وتسخير أصحاب الخبرة إذا تطلب الأمر ذلك .([4])

الفرع الثالث

المرسوم الرئاسي رقم 07/26

[1] – المادة 175 مكرر 2 من القانون 06/24 المعدل والمتمم القانون السابق.

[2] تنص المادة 76 من قانون رقم 14/25 المتضمن قانون الإجراءات الجزائية المعدل والمتمم ، على أنه تتم عمليات التفتيش ....."

[3] تنص المادة 78 من قانون 14/25 المتضمن قانون الإجراءات الجزائية المعدل والمتمم ، على أنه لا يجوز البدء في تفتيش ...."

[4] تنص المادة 114 من قانون 14/25 المتضمن قانون الإجراءات الجزائية المعدل والمتمم ، على أنه إذا أقتضت ضرورات التحري..."

إذا كانت القوانين الوطنية تشكل الإطار العام الذي يحكم مسار الأمن المعلومات فإن المراسيم الرئاسية التى تصدر عن سلطة تمثل الآلية التنفيذية التى تعمل على تفعيل هذه القوانين وتجسيدها على ارض الواقع، وفي هذا السياق يأتي المرسوم الرئاسي رقم 26-07 المؤرخ قي 7جانفي 2026 يقضي بإنشاء هيكل مسؤول عن أمن الأنظمة المعلوماتية و حماية المعطيات في كل مؤسسة وإدارة وهيئة عمومية فهو وليد الظرف ونابع لعدة دوافع . [1]

أولا :الحماية

إن التزايد الملحوظ في التهديدات الإلكترونية على الصعيد العالمي الظاهر من إرتفاع هجمات الإختراق و الإبتزاز الرقمي الموجهة ضد الحكومات بنسبة تقارب 125 %منذ 2020 ، وقد أدى هذا الوضع الى تبني توجه حمائي واضح ، و يهدف هذا الأخير بالدرجة الأولى الى تعزيز البنية التحتية الرقمية خاصة في مراحل تأسيسها وتطورها .

أين يتولى الهيكل مسؤولية أمن الأنظمة المعلوماتية إضافة الى تأمين قواعد بيانات المواطنين التى تعد رصيد استراتجيا من المعلومات الوطنية وكذا اليقظة المستمرة و المراقبة الدائمة للحصول على فضاء رقمي أمن ومستقر. [2]

ثانيا :الوقائي

من خلال حماية المرحلة الحساسة من مسار التحول الرقمي بإعتبارها تكملة إستراتجية تتطلب إنشاء بنية أمنية قوية، ويقتضى هذا بوضع أسس متينة لحماية قواعد البيانات والمنصات الرقمية الكبرى قبل إكتمال عملية الرقمنة، فالتأسيس المبكر يعد ضمانا فعليا لسلامة البنية الرقمية بينما تأجيل إجراءات الحماية الى ما بعد التنفيذ لن تكون سوى معالجة ترقيعية تفتقر الى القوة المرجوة وتحسين وتكوين المستخدمين في مجال يؤمن الأنظمة المعلوماتية وحماية المعطيات ذات الطابع الشخصي . [3]

ثالثا : التنظيمي

---

[1] المادة 1 من مرسوم رئاسي رقم 07/26 المتضمن إنشاء هيكل مسؤول عن أمن أنظمة المعلوماتية ،ج،ر، العدد الرابع 18جانفي2026، ص 21

[2] المادة 4 من المصدر السابق، ص 21

[3] المادة4 الفقرة الأخيرة من المصدر نفسه ، ص 22

تسعى كل وزارة أو جهة على حلول أمنية مستقلة بذاتها و بمعزل عن غيرها لا يفضي فقط الى التفاوت ملحوظ في مستويات الحماية ، بل يسهم في إستنزاف غير ضروري للمال العام ولسد هذه الثغرة يصبح من الضروري إنشاء هيكل تنظيمي شامل يضع إطار موحد للرؤية يعمل على تنسيق الجهود بما يضمن الإستثمار الأمثل و يعزز متانة المنظومة في كل مؤسسة أو هيئة يقتضي سير الهيكل التعاون والتنسيق معها .([1])

رابعا : التوافق التشريعي

تستدعي الضرورة اليوم مواءمة التشريعات الوطنية مع المعايير الدولية للتجارة الإلكترونية حيث لم تعد ترفا قانونيا بل التزاما تفرضه المعاهدات و الإتفاقيات الدولية فهذا التماثل في التشريعات يعد الضمان الأساسي لتبادل المعلومات عبر الحدود والتعاون الدولي و السبيل الوحيد لتجنب العقوبات التي تلاحق التشريعات غير المتوافقة مع متطلبات العصر الرقمي، مع السهر على الإمتثال للأحكام التشريعية والتنظيمية في مجال معالجة المعطيات ذات طابع الشخصي .([2])

خامسا :التنمية الإقتصادية

إنه أهم دافع يتمثل في حماية الإستثمارات الرقمية وجلب أخرى جديدة ، أي حماية الأصول الرقمية كما أن استثمارات الحكومية تقدر بالمليارات الدولارات تحتاج الى حماية كافية بالإضافة الى جلب المستثمرين ، فالشركات العالمية ترفض الإستثمار في دولة دون إطار أمني معلومات مما يفرض تطوير صناعة وطنية من خلال فتح مجال لشركات أمن سيبراني جزائرية وذلك بإعطاء فرصة عمل في هذا المجال ، أما بالنسبة للهيكل التنصيب الفوري ويتم تعين وتوظيف المستخدمين المؤهلين بالأولوية و الذي يثبتون الملمح المناسب من حيث الكفاءات و الإشهادات. ([3])

[1] المادة 5 الفقرة الأخيرة من المصدر نفسه ص 22

[2] المادة 4 الفقرة الثامنة من مرسوم 07/26 المتضمن إنشاء هيكل مسؤول عن أمن أنظمة المعلوماتية ، ج ج،ج،ر،العدد الرابع، 7جانفي 2026، ص 22

[3] المادة 10 من المصدر نفسه ،ص 23

خلاصة الفصل الأول

أعطينا في هذا الفصل رؤية شاملة للأمن المعلوماتي ، مبنية على بعدين متكاملين الأول مفاهيمي والثاني تشريعي، إنطلاقا من المبحث الأول الذي تناولنا فيه مفهوم الأمن المعلوماتي عبر مطلب مكون من فرعين الفرع الأول جاءت فيه تعاريف شتى بتعدد الزوايا التي ينظر الى الأمن المعلوماتي منها سواء من الجانب الأكاديمي مع التركيز على البعد التقني والقانوني، فعرفناه على أنه جملة من الأساليب الوقائية التي تهدف الى توفير حماية أمنية للمعلومات في بيئة رقمية ،أما في الفرع الثاني عددنا أنواع الأمن المعلوماتي و كان الحظ الأوفر للأمن القانوني فهو ليس من أساليب الحماية بل مبدأ يضمن الحماية و الإستقرار و اليقين والثقة في القانون أما الأنواع الأخرى مثل الأمن السيبراني وأمن الشبكات، أمن التطبيقات و الأمن السحابي فهي الجزء من الكل فكلها هدفها حماية المعلومات وفي المطلب الثاني تطرقنا الى عناصر الأمن المعلوماتي وأهدافه فحللنا عناصر الأمن المعلوماتي في الفرع الأول منها السرية التي تضمن وصول المعلومة لمن له صلاحيات الإطلاع عليها وعنصر التكامل وسلامة المحتوى الذي يحافظ على دقتها ويمنع التلاعب فيها إضافة الى ذلك التوافر والإتاحة كعنصر ثالث ليتم ما يسمى بالثالوث و يتم ربط هذه العناصر بالأهداف الكبرى للأمن المعلوماتي في الفرع الثاني أولها حماية البيانات من الإنكشاف يليها تأمين قنوات الإتصال و الإستجابة السريعة للحوادث الأمنية من خلال إحتواء الهجمات وصدها والحد من إنتشارها .

عرجنا في المبحث الثاني لمعرفة الإطار التشريعي للأمن المعلوماتي فتم تقسيم هذا الأخير الى مطلبين ؛الأول تناولنا فيه المصادر الدولية للأمن المعلوماتي التي كانت عبارة عن إتفاقيات كأهم مصدر قانوني ملزم للأمن المعلوماتي على المستوى الدولي، والتي تناولنا في الفرع الأول والتي كانت مرجعية قانونية

لجميع التشريعات الدولية الصادرة في مجال الأمن المعلوماتي منها الإتفاقية الأوربية لمكافحة الجريمة المعلوماتية بودابيست تعد معاهدةٌ إقليمية إلا أنها إكتست الطابع العالمي نظرا لأن العضوية فيها مفتوحة لأي دولة في العالم ،حيث بادرت بترسانة قانونية حماية للمجتمع الدولي لتليها إتفاقية الأمم المتحدة في الفرع الثاني التي كانت عبارة عن صرح قانوني دولي يقنن الفضاء الإلكتروني تجسدت في 68 مادة مع الإلتزام بمبدأ المساواة في السيادة وعدم التدخل في الشؤون الداخلية مع كفالة حقوق الإنسان.

فهي بمثابة ميثاق عالمي يوفق بين الإحتياجات الأمنية للدول والضرورات التقنية للعصر الرقمي، تم التوقيع عليها من قبل الجزائر 25أكتوبر2025 كما انه كان لها دور محوري في صياغتها ، أما عن الفرع الثالث تطرقنا للإتفاقية الدول العربية لمكافحة جرائم تقنية المعلومات التي إستدركت التأخر بوعي قانوني فوضعت ترسانة قانونية متكاملة خصت الدول العربية وحدها دون سواها مستمدة أحكامها من الشريعة الإسلامية والتراث الإنساني للأمة العربية ؛ حيث ترمي الى التعاون بين الدول فيما بينها لمكافحة جرائم تقنية المعلومات التي تهدد أمنها ومصالحها وسلامة مجتمعاتها وأفرادها.

بعدما إستعرضنا في المطلب الأول للإتفاقيات الدولية إنتقلنا لمصادر الوطنية للأمن المعلوماتي حيث تطرقنا في الفرع الأول للدستور كأعلى هرم في السلطة من خلال ما جاء به التعديل الدستوري 2020 حيث أعطى الضمانة للفرد لحقوقه وحرياته مع الحق في بيئة سليمة والحق في الحماية للحياة الخاصة ، ليأتي بعد ذلك قانون العقوبات والإجراءات الجزائية كأداة رادعة للأمن المعلومات في الفرع الثاني ، حيث عرجنا على قانون 06/24 المؤرخ 28أبريل 2024 والقانون 14/25 المتضمن قانون الإجراءات الجزائية والذي شهدا تطور نوعي في تجريم الأفعال التي تمس الأمن المعلوماتي و إستثناء في بعض الإجراءات منها التفتيش مخافة من إتلاف الأدلة وطبيعتها الرقمية ،وفي الأخير ختمنا هذا الفصل بالحديث عن المرسوم رقم 07/26 المؤرخ 07جانفي 2026 الذي يقضي بإنشاء هيكل مسؤول عن أمن الأنظمة المعلوماتية في كل مؤسسة أو هيئة عمومية فهو ناتج عن ظرف ودوافع، بعد أن عالجنا الموضوع من جانبه المفاهيمي سوف ينتقل الى الفصل الثاني لنتعمق في تحديد آليات الحماية للأمن المعلوماتي في التشريع الجزائري.

الفصل الثاني

آليات الحماية للأمن المعلوماتي

في التشريع الجزائري

العالم يتغير ويتحول والتطور مستمر على مستوى تكنولوجيا المعلومات و الإتصال فهذا عصر السرعة وعصر الرقمنة ، ليس هذا فقط فالتسميات عديدة كل تسمية تشير له من زاوية خاصة فكل من هذه الأخيرة مرتبطة بالتقنية المستعملة والمعلومات المتحصل عليها ، فحيازة المعلومات مثل الحديث على قارعة الطريق إذا لم تكن محفوفة بسياج مانع يحصنها .

إن المعلومات الصحيحة والدقيقة هي الثروة الحقيقية التى تتطلب الحماية والصيانة فمع الإعتماد الكلي على التقنيات المعلومات و الإتصال تزداد المخاطر والتهديدات الغرض منها التغير في المعلومات أو الحذف أو الإتلاف ، فهي تستهدف الأنظمة المعلوماتية مما يستدعي تدخل المشرع لوضع إطار قانوني ومؤسساتي وتقني مترابط يضمن تحقيق الأمن المعلوماتي المرجو ، فهو أحد الركائز الأساسية التى يقوم عليها الأمن الوطني و السيادة الوطنية ومنه يضمن الإستقرار.

الآليات تتعدد وتتنوع لتحقيق المراد المنشود وتأكيده ، ليشمل الأمن المعلومات ثلاثة مستويات متكاملة لا تستغني عن بعضها البعض، في المقدمة نجد الآليات التقنية التي هي الدرع الأمامي لصد الإختراقات والهجمات الإلكترونية معتمدة على التشفير الذي يهتم بالسرية والحجب وجدار ناري يوفر سياسات أمنية بين الأنترنت والشبكة بكل بساطة هو عبارة عن سياج موجود حول الشبكة يهدف الى حمايتها من المتطفلين ، ([1]) وأنظمة كشف التطفل و الإختراق من خلال تمييز السلوك المشكوك به من العديد من الأنشطة غير الطبيعية لإستخدام النظام ،([2]) بالإضافة للتوقيع الإلكتروني الذي يأتي على شكل بيانات إلكترونية مرفقة أو مرتبطة منطقيا ببيانات أخرى في شكل إلكتروني وظيفته التوثيق يهدف الى ضمان المصداقية والآمان في المعاملات الإلكترونية وتعزيز الثقة ،إلا أن هذه الوسائل وحدها لا ترقى لتصل للحماية الشاملة وتحصين دائم للفضاء المعلوماتي فمهما تطورت أدوات والوسائل التقنية حين تبقى بمعزل لا تصبوا لتحقيق الحماية. لهذا يأتي الردع كآلية جزائية ويعطيها المشرع الضمانة القانونية لردع المعتديين والمنتهكين الذين يطول إعتدائهم على الأنظمة المعلوماتية ،وذلك من خلال تجريم الأفعال غير المشروعة التى تستهدف المعلومات والأنظمة المعالجة لها ، و وضع جزاءا يتناسب وحجم الجرم المرتكب من الجرائم المستحدثة وتأثيرها السلبي على المجتمع .

[1] خضر مصباح إسماعيل الطيطي، المرجع السابق ،ص 133

[2] – خضر مصباح إسماعيل الطيطي ، المرجع نفسه ، ص 134

إن الجزائر كغيرها من الدول إتجهت نحو تبني مقاربة الحكومة الإلكترونية، ([1]) فهي عازمة كل العزم على رقمنة كل القطاعات الحكومية دون إستثناء مما يجعلها تعطي الأهمية والأولوية للإطار المؤسساتي بإعتباره الهيكل التنظيمي الذي يتولى خريطة الطريق للسياسات العامة للأمن المعلوماتي، لإعداد ووضع إستراتجية قوية الغرض منها حماية البنية التحتية الحساسة والتصدي للتهديدات، ([2]) مع تظافر جهود جميع القطاعات الحكومية بكل أنواعها والخاصة، ومن هذا المنطلق يأتي المرسوم الرئاسي رقم 05/20 المؤرخ في 20 جانفي 2020 كإطار تنظيمي رائد في الجزائر حيث أنشأ بموجبه منظومة وطنية لأمن الأنظمة المعلومات متكونة من هيئتين رئيستين متمثلتين في المجلس الوطني للأمن الأنظمة المعلوماتية تحت إسم المجلس و وكالة الأمن الأنظمة المعلوماتية تحت إسم الوكالةن([3])كما تم من خلال المرسوم الرئاسي 21/439 المؤرخ في 07 نوفمبر 2021 إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال مدعما للإطار المؤسساتي .

فنحن أمام بناء تكاملي لآلية تقنية قانونية مؤسساتية وعليه سوف نتطرق في هذا الفصل لآليات الحماية التقنية والجزائية في المبحث الأول ثم نتناول الإطار المؤسساتي للأمن المعلوماتي في المبحث الثاني.

[1] بارة سمير ، المرجع السابق ، ص 277

[2] قدايفة أمينة ، "إستراتجية الأمن المعلومات "، **مجلة الأبعاد الإقتصادية**، جامعة أمحمد بوقرة ، بومرداس الجزائر، م:06 العدد الأول 2016 ، ص 175

[3] لمادة 03 من المرسوم رقم 05/20 المؤرخ 20جانفي 2020 يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية ،ج،ر الصادرة في 26جانفي 2020 ، العدد الرابع ، ص 6.

المبحث الأول

آليات الحماية التقنية والجزائية للأمن المعلوماتي

يهدأ مجتمعنا و يستقر حين تكون له سيادة وطنية رقمية تتماشى مع متطلبات العصر، من خلال إمتلاكه أمن معلوماتي متكامل ليس كحاجز دفاعي أمام التهديدات التي تستهدفه من وراء الشاشات، بل كضرورة تحمي المقدرات الوطنية المتمثلة في الموارد المادية البشرية، الإقتصادية ، والمعنوية وبالأخص الأمنية والخصوصيات الفردية والتدفقات الحرة للبيانات بأدوات ووسائل تقنية كأسلوب وقائي سابق للهجمات وحاجز مانع يحصن الأنظمة المرتبطة مع أدوات قانونية تضرب بيد من فولاذ كل من اعتدى أو تجسس على معلوماتها ودمر أنظمتها ، فالعدو في هذه الحالة لا يحتاج للسفر ألاف الأميال حتى يهاجمنا أو يحمل أطنان القنابل ويغامر حتى يصل إلينا،([1]) وفي هذا السياق سوف نتطرق للحديث عن آليات الحماية التقنية في هذا المطلب الأول، وعن الآليات الجزائية في المطلب الثاني.

المطلب الأول

آليات الحماية التقنية للأمن المعلوماتي

تتعدد الآليات التقنية وتتماشى مع التطور التكنولوجي غايتها حماية المعلومات والبيانات التي هي عبارة عن نبضات تمر عبر شبكات الحاسب وهي عرضة للإعتداء عليها في كل الأوقات .([2])

ومن أبرز طرق حمايتها من مخاطر العدوان عليها لا سيما الإطلاع غير المشروع عليها هو التشفير حتى لا يمكن قراءتها، و وضع الحاجز الذي يعرف بجدار الناري الذي يعمل كحارس للشبكة فيسمح بحركة المرور المشروعة ويمنع الدخول غير المصرح به، كذلك أنظمة الكشف للإختراقات و تراقب الأنشطة المشبوهة و إعطاء التنبيهات ، و عليه سيتناول في هذا المطلب جملة من الوسائل التقنية المعتمدة لحماية أمن المعلومات من خلال ما تم ذكره في هذه المقدمة القصيرة في اربعة فروع .

---

[1] منير الجنبيهي ، ممدوح الجنبيهي ،"أمن المعلومات الإلكترونية" ،**دار الفكر الجامعي** الإسكندرية ، مصر،د ر ط ،2005، ص 32.

[2] محمد خليفة ، الحماية الجنائية لمعطيات الحاسب الألي في القانون الجزائري والمقارن ، دار الجامعة الجديدة ، الإسكندرية ، مصر ، د رط ،2007 ، ص 93.ث

الفرع الأول

التشفير

يعود تاريخ التشفير لأكثر من 4000 سنة حيث كان الإنسان يفضل أن يبقي كتابته مخفية وبطريقة سرية ، ([1]) ويتم اللجوء للتشفير لمنع المعلومات من التداول العام ، فالمعلومات المشفرة أصعب من المعلومات غير مشفرة ،.للتشفير عدة تعريفات منه ما هو فقهي و ما هو قانوني تشريعي.

أولاً: التعريف الفقهي.

يعرفه الأستاذ (ليونال بوشرياغ) على أنه مجموعة من التقنيات التي تهدف الى حماية المعلومات عن طريق إستعمال بروتوكولات سرية تجعل البيانات مشفرة غير مفهومة لدى الغير بواسطة البرامج المخصصة ،([2]) فهو مناهج لخط البيانات من خلال لوغاريتمات أو خوارزميات بحيث لا يمكن قراءتها من طرف ثالث متطفل ، معتمدا على برمجية تضع شفرة تحمي المعلومات في الظاهر بمنعها للغير ممن ليس لهم الحق في الإطلاع عليها .([3])

هذه الخوارزميات هي عبارة عن دوال رياضية تستخدم في عملية التشفير أو فك النص المشفر للحصول على النص للرسائل الأصلية وتعمل خوارزمية التشفير بالإشتراك مع مفتاح خاص سري يستخدم لتشفير النص الأصلي المقروء لرسالة ، يعتمد أمن البيانات المشفرة بصورة كاملة على عاملين إثنين قوة خوارزمية التشفير و أمن وسرية المفتاح .([4])

[1] خضر مصباح إسماعيل الطيطي، المرجع السابق ، ص 171

[2] بنوار نية ، بن سعيد زهرة ، خصوصية العقد الإلكتروني وفقا للقانون 05/18 المتعلق بالتجارة الإلكترونية ، مذكرة شهادة الماستر في الحقوق بجامعة بلحاج بوشعيب ، 2024/2023 ، ص58

[3] – محمد خليفة ، المرجع السابق ص93

[4] خضر مصباح إسماعيل الطيطي ، المرجع نفسه ، ص172

ثانيا : التعريف القانوني

المشرع الجزائري لم يعرف التشفير و إكتفى بالتطرق الى المقصود بمفتاحي التشفير العام والخاص من خلال النص عليه في المادة 2 الفقرة الثامنة تنص على التشفير الخاص بانه عبارة عن سلسلة من الأعداد يحوزها حصريا الموقع فقط وتستخدم لإنشاء التوقيع الإلكتروني و يرتبط هذا المفتاح بمفتاح تشفير عمومي([1]) أما الفقرة التاسعة من نفس المادة تنص على التشفير العام على أنه عبارة سلسلة من الأعداد تكون موضوعة في متناول الجمهور بهدف تمكينهم من التحقق....([2])

ونظرا لأن المشرع الجزائري لم يعطي تعريفا إرتأينا أن نستعين بما جاء به المشرع الفرنسي حيث تم تعريف التشفير من خلال القانون 1170/90 بتاريخ1990/12/29 أين تضمنت المادة 27 على أنه كل الأعمال تهدف الى تحويل المعلومات أو إشارات واضحة بإستخدام وسائل مادية أو معالجة آلية الى معلومات أو إشارات غامضة للغير أو إجراء العملية العكسية عبر وسائل مادية أو معلوماتية مخصصة لهذا الغرض .([3]) أما قانون المبادرات والتجارة الإلكترونية عرفه على أنه إستعمال رموز أو إشارات غير متداولة تصبح بمقتضاها المعلومات المرغوبة تحريرها أو إرسالها غير قابلة للفهم من قبل الغير أو إستعمال الرموز أو الإشارات ولا يمكن وصول لمعلومات بدونها. (4)

من خلال التعاريف السابقة نستنتج أن التشفير هو عملية ترميز أو تشفير الرسالة حتى يكون معناها غامض وغير مفهوم ، فهو تحويل البيانات من شكلها القابل للقراءة الى شكل غير مفهوم الغرض منه إخفاء المعلومة في أساس بياناتها بحيث إذا ظهرت تلك البيانات فإنها لن تعبر عن فحواها الحقيقي .([5])

---

[1] بنوار نية ، بن سعيد زهرة ، المرجع السابق،ص59

[2] المادة 2 الفقرة 9 ، قانون 04/15 الموافق 1فبراير سنة 2015 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين ج،ر ج ج العدد السادس بتاريخ 10فبراير 2015 ،ص 7

[3] بورغداد وصال ، كواشي عبير ، حماية خصوصية المستهلك الإلكتروني في القانون الجزائري ، مذكرة شهادة الماستر في الحقوق، تخصص قاون أعمال،جامعة محمد البشير الإبراهيمي برج بوعريريج،2025/2024 ، ص10.

[4] بورغداد وصال ، كواشي عبير ، المرجع نفسه ،ص09 .

[5] محمد خليفة ، المرجع السابق، ص94

لكن الغاية من التشفير ليس الإخفاء فحسب بل يتعدى ذلك ليكون مانع لجهة غير مخولة للإطلاع أو التعديل أو إنتحال شخصية أي بمعنى المحافظة على السرية ، التكامل والمصادقة ، وله عدة أنواع نذكر منها التشفير المتماثل أو التناظري يستخدم مفتاح واحد يقوم بوظيفتين التشفير وفك الشفرة والنوع الثاني هو التشفير غير المتماثل أو غير المتناظر عكس التشفير الأول يستخدم مفتاحان أحدهما للتشفير يسمى المفتاح العام والأخر لفتح الشفرة يسمى المفتاح الخاص .([1])

الفرع الثاني

الجدران النارية

فكرة الجدار النارية مستوحاة من الطريقة الأمنية المعروفة قديما حيث يقوم الجند بحفر خندق حول القلعة لمنع أي شخص من الدخول أو الخروج مما يسمح للحراس بتفتيشه،([2]) كان أول ظهور له عام1980 على شكل موجهات الغرض منها تقسيم الشبكة الواسعة الى شبكات صغيرة محلية حتى تستطيع إحتوائها للمشاكل التي يواجهها جزء من الشبكة ومن ثم منعها والحد من إنتشارها .

مع أوائل التسعينات تم إستخدام جدار ناري لتحقيق الأمن أضيفت إليه قوانين فلترة بسيطة لتحديد الجهات المسموح لها بالنفاذ وكانت هذه الجدار النارية فعالة ولكنها محدودة،([3]) مع مرور الزمن ظهر جيل جديد أكثر مرونة ما يعرف بالمستضيفات الحصنية يستخدم البرمجيات الوسيطة للتحكم في التطبيقات، وبما أن الجدار الناري هي منتجات أمنية تتكون من برمجيات لها قابلية للتطور المستمر والتحديث مما يجعلها أرض خصبة لتنافس بين المزودين هذه المنافسات أدت الى إضافات جوهرية وتوسع لمهام الجدار الناري منها التحقق من هوية المستخدمين أين تستخدم أساليب التشفير مثل الشهادة الرقمية وكذلك اضافة التشفير البيني للجدران النارية المعروفة اليوم بإسم الشبكات الإفتراضية الخاصة كما أصبحت أداة لمراقبة المحتوى كالبحث عن الفيروسات ومراقبة عناوين الأنترنت .([4])

---

[1] خضر مصباح إسماعيل الطيطي ، المرجع السابق ، ص 239

[2] حزام فتيحة ، "حماية الأنظمة الرقمية بين الآليات التقنية وأجهزة الحماية" ، **مجلة الحقوق والعلوم الإنسانية** ، م:13 العدد الثالث ،أكتوبر2020، ص 175

[3] منير الجنبيهي ، ممدوح الجنبيهي ،المرجع السابق ، ص 25

[4] منير الجنبيهي ، ممدوح الجنبيهي ، ،نفس المرجع، ص 28

البعض يعتقد أن الجدار الناري فقط برنامج يثبت على الحاسوب لكن الأمر ليس كذلك فحسب بل هو جهاز يحجب كل معابر الدخول للشبكة الداخلية ومن ثم يعمل على فتح هذه المنافذ فقط للمستخدمين الشرعيين اللذين لهم صلاحية الدخول ، السبب في حاجتنا الى جدار الناري وجود الفجوات الأمنية التى تركت مفتوحة إهمالا أو سهوا فهذا الأخير يوقف جميع الإتصالات غير مصرح بها .([1]) ومن هنا يتضح لنا أن الجدار الناري لحماية ينقسم بشكل أساسي الى أجهزة جدران الحماية وهي أدوات مادية خارجية يتم توصيلها بالشبكة لحمايتها وبرامج جدران لحماية هي برمجيات منفصلة يتم تنصيبها على الأجهزة لحماية الشبكة .

الجدارن النارية هي سياج موجود حول الشبكة يهدف الى حمايتها ، قوته تكمن في كونه حاجزا تتحكم في النقاط الدخول لكن لديها ضعف في رصد التهديدات الداخلية حيث انه لا تعرف ما يحدث عندما يمر الشخص من خلالها وأيضا من الهجمات التى تكون من قبل الموظفين ذوي الضمير الميت.([2])

فإن البنية الأمنية المتكاملة تحقق حماية شاملة تتطلب تلاحم الجدران النارية مع أنظمة كشف التطفل هذه الأخيرة سوف نتطرق اليها في الفرع الموالي.

الفرع الثالث

أنظمة كشف التطفل

نطرح السؤال لماذا نحتاج الى كشف التطفل ؟ هل لأن جدران النارية أخفقت و لم تنجح في صد هجمات المتطفل ؟ من هذا المتطفل حتى نحتاج الى كاشف له ؟ إنه أحدى أكبر التهديدات الكبيرة للأمنية بعد الفيروسات وبصورة عامة له عدة تسميات منها الهاكر ،كاسر الأمنية ، وله ثلاثة أصناف منها المتنكر الذي هو شخص غير مصرح له بإستخدام الحاسوب يقوم بالخرق و الوصول إلى النظام من أجل الإطلاع على الإمتيازات المستفيدين الشرعيين أو القانونيين، ويكون فضولي قد يملك صلاحيات الوصول الى البيانات لكنه يسئ استخدامها من أجل المصلحة الشخصية إنه صاحب الضمير الميت ؛ ويأتي متخفيا باسم المستخدم الخفي أو السري الذي يقوم بالسيطرة والإشراف على النظام ليتمكن من تغير الإعدادات.([3]) همه الوحيد التطفل غايته الأذية أو هواية من أجل المتعة .

[1] خضر مصباح إسماعيل الطيطي ، المرجع السابق ، ص133

[2] خضر مصباح إسماعيل الطيطي ، المرجع نفسه ، ص132

[3] خضر مصباح إسماعيل الطيطي ، المرجع نفسه ، ص126

هذا الأخير عبارة عن محاولة أحدهم للولوج الى نظام الحاسوب بدون ترخيص فهي عملية إساءة إستخدام نظام الحاسوب قد يكون مؤذي مثل سرقة البيانات السرية ، أما نظام كشف التطفل عبارة عن نظام لكشف مثل هذه العمليات غير شرعية ويوجد له نوعين من الأنظمة.([1])

أولا: أنظمة كشف التطفل على الشبكة

تسعى جاهدة لإكتشاف المتطفل من خلال قاعدة بيانات المخزن فيها نماذج الهجوم المعروفة ومقارنتها مع نموذج المتطفل على هذا الأساس يتم إكتشافه كما تقوم بمراقبة حزم البيانات على كل عمليات الربط على الشبكة مراقبة طلبات الإتصال والمنافذ المختلفة على الحاسوب التى يستطيع المتطفل خرقها والدخول الى النظام والقيام بعمليات التخريب وبالتالي يتم أيضا إكتشافه فإذا أراد أحد فحص المنفذ يقوم نظام كشف تطفل الشبكة بكل العمليات من أجل منع هذا المتطفل من المرور الى الشبكة .([2])

ثانيا: نظام كشف التطفل المعتمد على المضيف

يكمن الإختلاف بين النظامين في الحيز المكاني المخصص لمراقبة والمتابعة فالنظام السابق وظيفته المراقبة على مستوى مرور الشبكة أما نظام كشف التطفل المعتمد على المضيف مهمته مراقبة كل ما يحدث في الحواسيب فهو يعمل على قراءة سجلات الأمان بشكل مستمر على سبيل المثال لا الحصر محاولات تسجيل الدخول تغير الصلاحيات إنشاء حسابات جديدة فهي عملية توثيق كل الأحداث المتعلقة بالأمان فيقوم هذا الأخير بتحليلها بحثا عن نماذج تدل على انه تطفل أو محاولة الإختراق، ينقسم هذا النظام الى نوعين أحدهما يسمى مدقق سلامة النظام يقوم بمراقبة ملفات النظام وتسجيلات للتغيرات قد تمت من قبل المتطفل هنالك العديد من البرامج التى تقوم بهذا العمل، النوع الثاني يسمى مراقبة ملف التسجيل التى يتم توليدها من قبل أنظمة الحاسوب من خلال إسترجاع و تحليلها يستطيع الموظفين بالكشف عن المتطفلين.([3])

[1] خضر مصباح إسماعيل الطيطي ، المرجع السابق ، ص127

[2] خضر مصباح إسماعيل الطيطي ، المرجع نفسه ، ص127

[3] خضر مصباح إسماعيل الطيطي ، المرجع نفسه ، ص128

ثالثا: دور أنظمة كشف التطفل

إذا تم كشف التطفل بسرعة يمكن تحديد المتطفل وإخراجه قبل أن يحصل أي تدمير أو سرقة فكلما تم الكشف مبكرا كانت الأضرار أقل ويمكن إستعادة النظام لما كان عليه سابقا وبعض أنظمة كشف التطفل الفعالة تعمل على منع التطفل لذا فهي تقوم بدور دفاعي ، وكذلك تساعد من خلال جمع معلومات عن تقنيات التطفل المستخدمة من خلال دراستها إستحداث تقنيات منع التطفل مستقبلا.([1])

الفرع الرابع

التوقيع الإلكتروني

تستدعي الظروف و المتغيرات لإتباع الوجهات من عالم ورقي تقليدي إلى عالم إلكتروني رقمي لتظهر معه واقعة مستجدة في الفكر القانوني تسمى التوقيع الإلكتروني نال عدة تعاريف حسب الزاوية التى تنظر إلى هذا المصطلح من خلالها ، فالبعض يركز على الوسائل التى يتم بها و البعض الآخر يعطي التعريف من خلال الوظيفة أو الدور الذي يقوم به؛ حيث عرفته مجموعة من المنظمات الدولية و التشريعات الكل له وجهة نظر.

أولا : تعريف التوقيع الإلكتروني في منظمة الأمم المتحدة للتجارة الدولية الأونسيترال

على الصعيد الدولي أصدرت لجنة الأمم المتحدة للتجارة الدولية قانونا نموذجيا بشأن التوقيع الإلكتروني الصادر في 05جويلية 2001 في المادة الثانية (أ) فعرف التوقيع على أنه بيانات في شكل إلكتروني مدرجة في رسالة بيانات أو مضافة اليها أو مرتبطة بها منطقيا ويجوز أن تستخدم لتعين هوية الموقع بالنسبة إلى رسالة البيانات ، و لبيان موافقة الموقع على المعلومات الواردة في رسالة البيانات .([2])

[1] خضر مصباح إسماعيل الطيطي ، المرجع السابق ، ص ص 126 الى 127

[2] حواس فتيحة ، "التوقيع الإلكتروني (الخصوصيات والتطبيقات) "، **مجلة الدراسات القانونية المقارنة** ، م:07،العدد الأول 2021، ص2989

من خلال هذا التعريف الذي جاءت به منظمة الأمم المتحدة للتجارة الإلكترونية يتضح انها اعتمدت في تعريف على الشكل الذي جاءت فيه البيانات والدعامة الإلكترونية وتعين هوية الموقع وإبراز الموافقة على المحرر و المعلومات .

ثانيا : تعريف التوقيع الإلكتروني في منظمة الإتحاد الأوربي

الإتحاد الأوربي اصدر توجيه إرشادي بشأن التوقيع الإلكتروني في قرار رقم 99/93 الصادر بتاريخ 13 ديسمبر 1999 المتعلق بالتوقيعات الإلكترونية حيث نص على أنه بيانات في شكل إلكتروني متصلة أو ملحقة منطقيا بيانات أخرى ويدل على هوية صاحبه،([1]) يلاحظ ويفهم من هذا التعريف أن التوقيع الإلكتروني أداة تكنولوجية للأمان و السرية التى يجب أن تخص بها الرسالة الإلكترونية بحيث لا يتمكن أي شخص غير المرسل اليه أن يقوم بقراءتها.

إضافة الى هذه التعريفات عرفته منظمة إيزو على أنه ذو طابع تقني معطيات مضافة الى وحدة معطيات و التى تحول تلك الوحدة الى شفرة تسمح للمرسل بالبرهنة على مصدر وسلامة وحدة المعطيات وحمايتها من التزوير، في نفس السياق عرف على أنه مجموعة من الإجراءات التقنية التي تسمح بتحديد شخصية تصدر عنه هذه الإجراءات وقبوله بمضمون التصرف الذي يصدر التوقيع من أجله ، ([2]) وهناك من عرف التوقيع الإلكتروني بأنه الرمز المصدري أو الرقم السري الذي يتم إدخاله في جهاز الحاسب الآلي عن طريق وسائل الإدخال ليتم من خلاله إنجاز بعض المعاملات بإتباع إجراءات محددة متفق عليها بين أطراف الإلتزام وضمن الحدود التى تم الإتفاق عليها بين طرفي العلاقة .([3])

من وجهتنا نرى أنه أحسن تعريف هو أن نجمع بين الجانب التقني والوظيفي فينتج عنه أنه مجموعة من الأرقام والرموز والإشارات التى توضع على المحرر الإلكتروني و تستعمل لتحديد هوية الموقع وتضمن موافقته على ما جاء في المحرر فهو أداة حماية .

[1] حواس فتيحة ، المرجع السابق ، ص 2989 .

[2] حواس فتيحة ، المرجع نفسه ، ص 2990 .

[3] حواس فتيحة ،المرجع نفسه ، ص 2990 .

ثالثا : تعريف التوقيع الإلكتروني في التشريع الجزائري

المشرع الجزائري في القانون رقم 02/26 المؤرخ قي 17فبراير2026 الذي يحدد القواعد العامة المتعلقة بخدمات الثقة للمعاملات الإلكترونية و بالتعريف الإلكتروني هذا الأخير عرف التوقيع الإلكتروني على أنه بيانات في شكل إلكتروني مرفقة أو مرتبطة منطقيا ببيانات أخرى في شكل إلكتروني يستخدمها الموقع للتوقيع تستعمل كطريقة لتوثيق ، ([1]) يركز التعريف بشكل واضح على وظيفة التوثيق كجوهر للتوقيع مما يعكس رؤية المشرع التي تهدف إلى ضمان المصداقية و الآمان في المعاملات الإلكترونية ، وتعزيز الثقة في التوقيع والختم الإلكترونيين فمنح مصادقة للشهادات الإلكترونية للشخص الحقيقي المستحق لها فحين الإخلال بذلك يعرض جهة المصادقة للعقوبات الجزائية تتمثل في الحبس من ستة أشهر الى ثلاثة سنوات وغرامة مالية من مائتي ألف 200000دج إلى 1000000 مليون دج ([2])

رابعا :أهمية التوقيع الإلكتروني:

تتجاوز أهمية التوقيع الإلكتروني كونه بديلا رقميا للتوقيع الخطي فهو يؤدي إستراتجية تبنتها جميع التشريعات فهو يحدد هوية الموقع و ذلك بربط التوقيع بشخص معين بشكل فريد لا لبس فيه، الذي يعطي القبول بالتعبير عن الإرادة والرضا من خلاله يبدي الموافقة على ما جاء في المحتوى والميزة المضافة للتوقيع الإلكتروني هي ضمانة سلامة المحتوى حيث يرتبط به المحرر بشكل يجعله قادرا على كشف أي تعديل أو تحريف يطرأ على البيانات بعد لحظة التوقيع فيمنح المحتوى درجة عالية من الموثوقية والآمان([3])

[1] المادة 02 الفقرة 02 من القانون 02/26 المؤرخ 17/فبراير 2026، يحدد القواعد العامة المتعلقة بخدمات الثقة للمعاملات الإلكترونية ج،ر،ج ج العدد الرابع عشر ، 18 فبراير 2026 ، ص 07

[2] المادة 99 المصدر نفسه ، ص 17

[3] فصيح عبد القادر ، بن عمر محمد ، "التوقيع الإلكتروني ودوره في الإثبات "، **مجلة العلوم القانونية و الإجتماعية** ،جامعة زيان عاشور بالجلفة ، العدد الثالث ، د س ن، ص 101 .

المطلب الثاني

آليات الحماية الجزائية للأمن المعلوماتي

الجزائر كسائر الدول في مسايرة التطور والتكنولوجيا تسير معهما قدم بقدم وتتوخى الحذر فالفضاء جديد وفيه تعثرات مما يفرض الحيطة والفطنة ، حيث انها في هذه الألفية باشرت الجزائر بإطلاق عدة مشاريع هادفة في مختلف القطاعات منها البنى التحتية وكانت أولويتها المشروع المسمى الجزائر الإلكترونية 2013 ، وما لا نستطيع أن ننكره أو نتحاشه أن كل تطور إيجابي لا يخلو من سلبيات فهذا الفضاء أساسه التكنولوجيا و الإتصالات و الإعتماد على الأجهزة الإلكترونية وشبكات الأنترنت مما يولد مستنقعات و يفرز جرائم ومجرمين ، هذا الأخير لم يعد فضاءا إفتراضيا منفصلا عن الواقع بل هو الواقع بذاته تعقد فيه العقود وتباشر و تدار المرافق و المؤسسات عن بعد و تحفظ الذاكرة و تصان الخصوصيات، و من هنا أي إنتهاك أو إختراق لهذا الكيان يعد جريمة قائمة يعاقب عليها قانون العقوبات، الذي هو مظلة للحماية من الأضرار الناتجة عن عمل أو الإمتناع عن عمل يقوم به الشخص بمكونات الحاسب المادية و المعنوية وشبكات الإتصال الخاصة به بإعتبارها المصالح والقيم المتطورة ، ([1]) من هذا السياق ارتأينا الحديث في هذا المطلب عن جرائم التى شدد المشرع الجزائري العقوبات فيها من خلال القانون 06/24 المؤرخ28 أبريل 2024 المعدل والمتمم للأمر رقم 156/66 المتضمن قانون العقوبات وهذا على سبيل المثال لا الحصر من خلال فروع متتالية.

الفرع الأول

جريمة الدخول غير المشروع في المنظومة المعلوماتية

جرم المشرع الجزائري كلا الفعلين سواء الدخول أو البقاء ؛ ومعنى الدخول ليس ذلك الشيء الذي نعتقده النفاذ و الإختراق إلى الأماكن المادية مثل الدخول إلى قاعة المحاضرات ، فهو ليس له طبيعة مادية و إنما ذو طبيعة معنوية يشبه الدخول في ذاكرة الإنسان أو في قدرته على التفكير.([2])

[1] زيبحة زيدان ، الجريمة المعلوماتية في التشريع الجزائري والدولي ، دار الهدى ، عين مليلة ، الجزائر ، ط 2011 ، ص 43

[2] محمد خليفة ، المرجع السابق ص 142

يعد الدخول سلوك إجرامي وفعل إيجابي الغرض منه الوصول بطريقة غير شرعية الى المنظومة فإذا تخلف السلوك إنتفى الركن المادي ولا قيام للجريمة حين ذاك ، وعليه فالدخول غير المصرح به هو الولوج الى المعلومات والمعطيات المخزنة داخل نظام الحاسب الآلي بدون موافقة المسؤول عن هذا النظام، و يعد إساءة إستخدام الحاسب الآلي و نظامه عن طريق شخص ليس من صلاحياته الدخول اليه و إستخدامه والإطلاع على المعلومات والمعطيات التى يحوزها سواء كان ذلك لمجرد التسلية أو الشعور بالتفوق .([1])

و حسب مفهوم نص المادة 394 مكرر من القانون 06/24 المعدل والمتمم للأمر 156/66 المتضمن قانون العقوبات أن الجريمة تتحقق بالصورة التالية:

– بمجرد الوصول الى نظام معلوماتي لكن بطريق الغش أي أن الجريمة عمدية هنا تقوم بتوافر القصد الجنائي العام .([2])

– أن يكون الجاني عالما بدخوله الى منظومة معلومات لا تخصه وأن جريمة الدخول غير المشروع تصبح قائمة حتى و لو لم يترتب عن ذلك أي ضرر بالمعلومات،([3]) وهي جريمة وقتية عكس جريمة البقاء التى تعد جريمة مستمرة ، التى سوف نتطرق للحديث عنها في الفرع الموالي.

الفرع الثاني

جريمة البقاء غير المشروع في المنظومة المعلوماتية

لقد ذكرنا سلفا أن جريمة البقاء عكس جريمة الدخول فهي جريمة مستمرة تتكون من فعل يقبل الإستمرار فترة من الزمن ويتطلب تدخلا متجددا من إرادة الجاني للإبقاء من خلال عدم وضع حد للتشعب داخل النظام مع الإعتقاد بأن ذلك يشكل خطأ .([4])

[1] محمد خليفة ، المرجع السابق ، ص 139

[2] – زيبحة زيدان ، المرجع السابق ، ص 49

[3] – زيبحة زيدان ، المرجع نفسه ، ص 49

[4] محمد خليفة ، المرجع نفسه ، ص 154

البقاء هو التواجد داخل نظام المعالجة الآلية للمعطيات ضد من له السلطة في السيطرة على هذا النظام، مما يؤدي الى عدم قطع الفاعل للإتصال بالنظام رغم معرفة الجاني أن تواجده فيه غير مشروع كما أن البقاء له عدة صور منها البقاء حين يكون الدخول بتصريح والجاني يتجاوز المدة المصرح له بها فهذا الأخير تحصل على إذن التواجد داخل النظام لوقت معين فيبقى بعد إنقضاء المدة المسموح له بها حين ذاك يصبح الفعل غير مشروع ([1])، أما الصورة الثانية البقاء بعد الدخول صدفة أو عن طريق الخطأ حين يعلم الشخص أنه داخل النظام أي أنه في مكان غير مصرح له بالتواجد فيه و رغم ذلك إستمر في المكوث به فالفعل غير مشروع ، المشرع الجزائري نص حتى على المحاولة والشروع ولم يتغافل عن ما ينجم عن هاتين الجريمتين من نتائج حيث يترتب عليهم أثر قانوني ، وهي حذف أو تغير معطيات نظام المعالجة الآلية للمعطيات أو تخريب النظام ([2]) ومنه القانون رقم 06/24 المعدل و المتمم للأمر 156/66 المتضمن قانون العقوبات نص في المادة 394 مكرر يعاقب بالحبس من 6أشهر الى سنتين وبغرامة من 60000دج الى 200000دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك ([3]).

المشرع ضاعف العقوبة في حالة إذا نتج عن هذا الدخول والبقاء حذف أو تغير في الفقرة الأولى من نفس المادة ([4]) أما الفقرة الثانية في حالة إذا ترتب عن الأفعال المذكور تخريب نظام إشتغال المنظومة تكون العقوبة من سنة(1) الى ثلاث سنوات (3) والغرامة من 10000 دج الى 30000 دج ([5])

[1] محمد خليفة ، المرجع السابق ، ص 154

[2] محمد خليفة ، المرجع نفسه ، ص 160

[3] لمادة 394 مكرر من قانون 06/24 المعدل والمتمم للأمر 156/66المتضمن قانون العقوبات،ج،ر،العدد ثلاثون،30ابريل 2024،ص20

[4] المادة 394مكررالفقرة 1 المصدر نفسه، ص 20

[5] المادة 394مكرر الفقرة 2 المصدر نفسه ، ص20

الفرع الثالث

جريمة إدخال معطيات في نظام المعالجة الآلية للمعطيات أو إزالتها بطرق تدليسية

يسميها البعض جرائم التلاعب بمعطيات الحاسب الآلي مثلها مثل أي جريمة لها أركانها إلا أن ركناها المادي، يأتي على شكل ثلاثة أنواع من سلوك الإدخال التعديل و المحو ولا يشترط أن تقع هذه الأفعال مجتمعة فسلوك واحد كافي لقيام الجريمة.([1])

أولا:الإدخال

نقصد به إضافة معطيات أو برامج جديدة أو معلومات وهمية أو مزيفة وظيفتها إعطاء تعليمات توجه الى كيان الحاسوب و هو ما يعرف بالتدخل في نطاق البيانات الغرض منها التمويه والتضليل لإرتكاب الجريمة و تغير الحقيقة و هي النتيجة التى يريد الجاني الوصول اليها ، وهي من أهم المراحل في الجريمة الإلكترونية ([2])،كما أنها من أهم الأساليب المستعملة في إرتكاب الإحتيال المعلوماتي.

ثانيا : التعديل

تغير حالة المعطيات الموجودة بدون تغير الطبيعة الممغنطة لها، فهي كل تغيير غير مشروع للمعلومات و البرامج عن طريق إستخدام إحدى وظائف الحاسب الآلي مما يؤدي الى عدم قابلية المعطيات للإستعمال على النحو المعدة له سوء كان التعديل مؤقتا أو دائما.([3])

ثالثـــا: الإزالـــــة.

الإزالة أو المحو هي الشكل الثالث لركن المادي فهي إقتطاع خصائص مسجلة على دعامة ممغنطة عن طريق محوها أو طمسها أي ضغط خصائص أخرى فوقها وكذلك عن طريق تحويل و رص خصائص مزالة في منطقة محفوظة في ذاكرة .

[1] محمد خليفة ، المرجع السابق ، ص 179

[2] زيبحة زيدان ، المرجع السابق ، ص 54

[3] محمد خليفة ، المرجع نفسه ، ص 183

وعملية إزالة المعطيات هي مرحلة تأتي بعد عملية إدخال المعطيات، فالإزالة تفترض الوجود السابق لعملية الإدخال ([1])، لا يكفي أن تهدد سلامة المعطيات بخطر الإزالة أو التعديل أو الإدخال وإنما لا بد أن يقع الضرر.

أما عن الركن المعنوي فيحتاج الجاني فقط القصد الجنائي العام من خلال توافر عنصر العلم والإرادة و بدورهما ينصرفان إلى كافة العناصر التي يتألف منها الركن المادي للجريمة، فالجاني يجب أن يكون عالما بأن ما يقوم به من إدخال أو إزالة أو تعديل غير مصرح به على معطيات للحاسب الآلي و أن أفعاله هذه تؤدي الى تغير حالة المعطيات ولابد من إرادة الجاني لهذه النتيجة.([2])

المشرع الجزائري في المادة 394مكرر1 من القانون 06/24 المعدل والمتمم شدد العقوبة على هذه الجريمة حيث نص على أنه يعاقب بالحبس من سنة (1) الى ثلاث سنوات (3) و بغرامة من 500000 دج الى 2000000دج كل من أدخل بطريق الغش معطيات في نظام المعالجة آلية أو أزال أو عدل بطريق الغش المعطيات التى يتضمنها ، ([3])كما أن هذه الجرائم حين تستهدف الدفاع الوطني والهيئات والمؤسسات الخاضعة للقانون العام تكون العقوبة أشد و هذا ما نصت عليه المادة 394 مكرر3 على أنه يعاقب بالحبس من سنتين (2) الى عشر (10) سنوات و بغرامة من 700000دج الى 2000000 دج و هذا دون الإخلال بعقوبات أشد. ([4])

إرتأينا ذكر هذه الجرائم للإهتمام الذي أولاه المشرع الجزائري لها حتى أنه قام بالتعديل الأمر 156/66 بالقانون 06/24 المتضمن قانون العقوبات حيث أنه لم يغير في نصوص الجرائم المذكورة أعلاه و إنما شدد في العقوبات، كما سعى جاهدا لحماية المعلومات والبيانات الخاصة في مختلف القطاعات التى تشهدها عملية الرقمنة رغبة في تأمينها تأمينا فعالا من خلال إصداره للمرسوم الرئاسي20/05المتعلق بأمن الأنظمة المعلوماتية وما جاء به من تبيان مهام وصلاحيات الهيئات المستحدثة وماجاء به القانون 04/09 والذي ترتب عنه إنشأ الهيئة الوطنية للوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام والإتصال ومكافحتها و ما لحقها من تعديلات إعادة تنظيمها من خلال مراسيم رئاسية أخرى و هذا ما سوف نتحدث عنه في المبحث الثاني كإطار مؤسساتي للأمن المعلوماتي.

---

[1] زيبحة زيدان ، المرجع السابق ، ص 54

[2] محمد خليفة ، ا المرجع السابق ، ص 186

[3] لمادة 394 مكرر1 المصدر السابق،ص20

[4] المادة 394 مكرر3 المصدر نفسه ،ص20

المبحث الثاني

الإطار المؤسساتي للأمن المعلوماتي في التشريع الجزائري

يستمر التحول الرقمي في الجزائر، فتسارع مع الزمن لرقمنة جميع قطاعاتها سواء الاقتصادية منها أو الإدارات الحكومية المركزية و المحلية إلى جانب قطاعات الطاقة و الإتصالات والبنوك فضلا عن قطاعات الصحة والعدالة والتعليم التربوي والتعليم العالي ، وهي تسعى جاهدة على تطبيق نظام من خلاله تقوم بحماية فضاء معلوماتها، وهو بمثابة درع يحمي منظومة رقمنة متكاملة، حيث أن هذه القطاعات منها من أحرزت مستويات متقدمة في الرقمنة و مع ذلك فإن هذا التطور مدفوع مع تزايد ترابط الشبكات، والذي ينذر بتدفق هائل للبيانات الحساسة مما يعرض القطاعات والمؤسسات للمخاطر متزايدة فالهجمات الإلكترونية ومحاولة الإختراق وعملية التخريب أو حتى الأعطال التقنية البسيطة كلها معوقات من شأنها تعطيل وشل الخدمات العامة وبالتالي خلق فجوة بين الجمهور و الدولة تؤدي الى نقص الثقة ، ولمواجهة هذه التحديات والظرف المفروض .

فإنه من حين لآخر يلجأ رئيس الدولة و حامي البلاد لإصدار مراسيم رئاسية كأداة قانونية سريعة فعالة لممارسة سلطته التنظيمية و تسيير المرافق العامة، أين أصدر المرسوم الرئاسي 20-05 المؤرخ في 20جانفي سنة 2020 ([1])، الذي يعد قاعدة تأسيسية في مسار بناء المنظومة الوطنية للأمن المعلوماتي ، حيث جاء كتفكير تطلعي مبني على إدراك تام أنه لم يعد الفضاء الرقمي مجرد خيار تقني مساعد بل واقع حقيقي معاش تتداخل فيه المصالح العامة بالحقوق الفردية وتتقاطع فيه متطلبات السيادة الرقمية مع ضرورة حماية المعطيات الشخصية في عصر ينتابه الإختراقات والهجمات السيبرانية التى تشكل تهديدا للمؤسسات والدول والأفراد.

يأتي هذا المرسوم الرئاسي ناصا لإنشاء هيكل مؤسسي يضم كل من مجلس وطني مكلف بإعداد الإستراتجية الوطنية للأمن الأنظمة المعلوماتية والموافقة عليها وتوجيهها و وكالة للأمن الأنظمة المعلوماتية مكلفة بتنسيق تنفيذ الإستراتيجية الوطنية للأمن الأنظمة المعلوماتية ([2])، مع إشراك مختلف القطاعات والهيئات الرسمية.

---

[1] المرسوم الرئاسي 05/20 المؤرخ بتاريخ 20جانفي 2020 ، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية ، ج ج،ج ر ،العدد الرابع، . 26جانفي 2020

[2] المادة 03 الفقرة 2 -3 من المصدر السابق ص 06 .

غير أن قيمة المراسيم والتشريعات لا تقاس بما جاء به نظريا و إنما يحسب بما تعكسه أهداف على أرض الواقع من خلال وضع إطار مؤسساتي متين مستقل عماده الشفافية والحياد، يقوم بإختصاصات محددة دون تداخل مع منحه صلاحيات قائمة على ضوابط مراقبة صارمة، حتى تكون المؤسسة المعنية بالأمن المعلوماتي أداة حماية وأمن و إستقرار ، فالعيش في بيئة مجهولة يخيم عليها ظلام الإجرام مما جعل المشرع الجزائري يدرك إلى ما سوف يؤول اليه الوضع من تفاقم حيث أصدر فيما سبق القانون رقم04/09 المؤرخ 05 غشت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ومكافحتها ، حيث أنشأ بموجب هذا القانون الهيئة الوطنية وظيفتها الوقاية ، الرصد و المكافحة،([1]) ولتكون درعا وطنيا في وجه الإختراقات والجريمة المنظمة لم يقف المشرع عند هذا الحد بل ساير الأوضاع والتطورات، لضرورة مواكبتها وبروز الحاجة تتابعت النصوص التنظيمية أين تمت إعادة تنظيم هذه الهيئة بإستمرار كأن المشرع يواكب التغير من خلال مرسوم 183/20 ومرسوم439/21 ، من هذا السياق تم تقسيم هذا المبحث المعنون بالإطار المؤسساتي الى مطلبين حيث تناولنا المجلس الوطني للأمن المعلوماتي في المطلب الأول وتطرقنا إلى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ومكافحته في المطلب الثاني .

المطلب الأول

المنظومة الوطنية لأمن الأنظمة المعلوماتية

أنظمة المعلومات هي جملة من الموارد التى تسمح بجمع وتخزين ومعالجة وتوزيع المعلومات وإسترجها عند الحاجة تساعد في إتخاذ القررات أو القيام بأي وظيفة تفيد حركة المجتمع ، وهي انظمة مركبة من فرعين البنية التنظمية والاشخاص المرتبطين بالنظام ، و فرع تقني من التكنولوجيا والعتاد المادي واللامادي البرمجية، نظرا لتحديات الكبرى التى تواجهها الجزائر لحماية البنى التحتية للمعلومات الوطنية الحساسة والمعلومات الشخصية و لتحقيق إستقلالية رقمية تسمح بتأمين فضاءها الرقمي.

[1] مرسوم رئاسي رقم 439/21 المؤرخ 2021/12/07 يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ،ج ج،ج،ر، بتاريخ 2021/12/11، العدد ستة وثمانون،ص5

إستحدث المرسوم 05/20 منظومة وطنية لأمن الأنظمة المعلوماتية كأداة للدولة في مجال أمن الأنظمة المعلوماتية ذات ثنائية مؤسساتية متكاملة مجلس وطني يقوم بإعداد إستراتجية الوطنية لأمن الأنظمة المعلوماتية ووكالة وطنية تقوم بالتنسيق تنفيذ الإستراتجية .([1])

الفرع الأول

المجلس الوطني لأمن الأنظمة المعلوماتية

يعد المجلس الوطني للأمن الأنظمة المعلوماتية الذي يدعى في صلب النص المجلس إحدى مكونات المنظومة، جاء هذا في المادة 03 الفقرة 2 من المرسوم 05/20 و هو أعلى هيئة على مستواها رئيسه المباشر وزير الدفاع الوطني أو ممثله ويساعده ممثلين الأول لرئاسة الجمهورية والثاني للوزير الأول كما يضم تشكيلة متنوعة من الوزراء من معظم القطاعات، حيث نجد الوزير المكلف بالشؤون الخارجية والوزير المكلف بالداخلية كذلك كل من وزير الطاقة والعدل والمالية و يستطيع أن يسخر أي شخص أو مؤسسة أو هيئة تعينه في أعماله ، ومن مهامه هذه البت في الإستراتيجية التى يتم إقتراحها من الوكالة و دراسة مخطط عملها وتقرير نشاطاتها والموافقة عليها، ودراسة جميع التقارير المتعلقة بتنفيذ الإستراتجية،([2]) ويتولى الإتفاقيات و الموافقة على التعاون الدولي في مجال أمن الأنظمة المعلوماتية أيضا من مهامه إعطاء الموافقة على سياسة التصديق الإلكتروني و يبدي رأيه في التشريعات الخاصة بأمن الأنظمة المعلوماتية.[(3)]

لإنجاز مهام المجلس على أحسن وجه وضعت تحت سلطة و تصرف رئيس المجلس الأمانة التقنية يسيرها أمين عام معين طبقا للتنظيم المعمول به من قبل وزارة الدفاع الوطني،([4]) تقوم هذه الأخيرة بعدة أعمال تحت سلطة رئيس المجلس منها الإعداد لمشروع النظام الداخلي للمجلس و التنسيق مع الوكالة.

[1] - المادة 03الفقرة 2-3 المصدر السابق ، ص06

[2] - المادة 05 الفقرة 2-3 من المصدر نفسه ، ص 06

[3] المادة 04 الفقرة 2 -3 من المصدر نفسه ، ص06

[4] المادة 08 الفقرة 2 -3 رقم 05/20 المصدر نفسه ، ص06

تتمع الأمانة التقنية بعدة صلاحيات منها جمع الوثائق الخاصة بمهام و أشغال المجلس مع جمع أي معلومة أو وثيقة من أي جهة كانت ،كما تهتم هذه الأخيرة بأشغال الأمانة وتسير الموارد البشرية والمادية مع القيام بحفظ جميع الوثائق والأرشيف ويحدد تنظيمها وسيرها بموجب قرار من وزير الدفاع الوطني .([1])

يجتمع المجلس كلما دعت الضرورة بناء على إستدعاء الرئيس حيث يقوم هذا الأخير بإعداد جدول أعمال الإجتماعات و يتم إرسال الإستدعاءات قبل خمسة (05) أيام على الأقل قبل إنعقاد الإجتماع يتخذ المجلس قراراته بالأغلبية و حين تتساوى الأصوات يكون صوت الرئيس الفاصل أي المرجح، تدون نتائج الإجتماع في محضر ، ينتج عن هذه الأعمال قرارات و آراء و توصيات. ([2])

الفرع الثاني

وكالة أمن الأنظمة المعلوماتية

عرف المشرع الجزائري وكالة أمن الأنظمة المعلوماتية التى تدعى في صلب النص على أنها مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية و الإستقلالية المالية مقرها في مدينة الجزائر .([3])

أولا : مهام وكالة أمن الأنظمة المعلوماتية

يقع على الوكالة عبء كبير و ذلك لما أسند إليها من مهام فهي مكلفة بتحضير عناصر الإستراتجية وعرضها على المجلس مع تنسيقها وتنفيذها ،كما تقترح كيفيات إعتماد مزودي الخدمات في مجال أمن الأنظمة المعلوماتية ومتابعتهم ، وفي حالة وقوع حوادث سيبرانية الناتجة عن الهجمات و الإختراقات التى تستهدف المؤسسات أين تقوم بإجراء تحقيقات رقمية ، حيث تسهر على جمع وتحليل وتقيم المعطيات المتصلة بمجال أمن الأنظمة المعلوماتية مستخلصة المعلومات المناسبة لتأمين منشآت المؤسسات الوطنية و ضمان اليقظة التكنولوجية في هذا المجال.

---

[1] المادة 09 الفقرة 2 –3 من المصدر السابق ، ص ص 06- 07

[2] - صونيا مقري ، وليد لعامر ، "المنظومة الوطنية لأمن الأنظمة المعلوماتية كآلية مؤسساتية لمكافحة الجريمة المعلوماتية وفقا للمرسوم " 05/20 ، **مجلة البحوث في العقود وقانون الأعمال** ، م:10،العددالثاني ، 2025، ص 138

[3] المادة 17 المصدر نفسه ، ص07

تعد وجها للدعم من خلال تقديم المشورة و المساعدة للإدارات والمؤسسات والهيئات العمومية والخاصة من أجل وضع إستراتجية أمن الأنظمة المعلوماتية، و مرافقة الهياكل المختصة لإعطاء علاج للحوادث المتصلة بأمن الأنظمة المعلوماتية ،([1]) ليس هذا فقط بإمكانها إقتراح تدابير التطوير و المشاركة في التظاهرات العلمية الخاصة بمجال أمن الأنظمة المعلوماتية، كما تعطي توجيهات بخصوص تكوين أعوان المؤسسات العمومية في نفس الميدان ، ولها دور في إقتراح مشاريع إتفاقيات التعاون الدولي و الإعتراف المتبادل و مشاريع نصوص قانونية و تنظيمية في مجال أمن الأنظمة المعلوماتية بعد موافقة المجلس و إعداد تقارير دورية عن نشاطها وتحيين حالات الخلل و النقص الموجود في الأنظمة المعلوماتية. ([2])

ثانيا : تنظيم وسير وكالة أمن الأنظمة المعلوماتية

تقوم بإدارة وكالة أمن الأنظمة المعلوماتية لجنة التوجيه رئيسها مدير عام معين من طرف وزارة الدفاع طبقا للتنظيم المعمول به مستعينا بلجنة علمية،([3]) وتعمل تحت سلطته وتصرفه مديريات ومصالح تقنية وإدارية و مركز عملياتي وطني لأمن الأنظمة المعلوماتية،([4]) تتكون لجنة التوجيه من تشكيلة مزدوجة من كل وزارة حيث نجد وزارة الشؤون الخارجية و وزارة الداخلية وكل من وزارة العدل، المالية ، الطاقة التعليم العالي ، الإتصالات و وزارة الصناعة و التجارة ، بالإضافة الى بعض الأسلاك الأمنية منها مصالح الأمن وسلطة الضبط للبريد و الإتصالات الإلكترونية و كذلك السلطة الوطنية للتصديق الإلكترونية والهيئة الوطنية لحماية البيانات ذات الطابع الشخصي ، بإمكان اللجنة الإستعانة بأي شخص أو مؤسسة من شأنها أن تعينها في أعمالها و يمكنها الرجوع الى المدير العام للوكالة لأخذ إستشارة، كما تقوم أمانة اللجنة بالإهتمام بمصالح الوكالة ، ويتم تحديد القائمة الإسمية لأعضاء لجنة التوجيه بموجب قرار وزير الدفاع الوطني بناء على إقتراح السلطات التى ينتمون إليها .([5])

[1] صونيا مقري ، وليد لعامر ، المرجع السابق، ص 139

[2] صونيا مقري ، وليد لعامر ، المرجع نفسه، ص 139

[3] المادة 21 من المصدر السابق ، ص 8

[4] المادة 20 من المصدر نفسه ، ص 8

[5] المادة 22 من المصدر نفسه ، ص 8

أ – مهام لجنة التوجيه :

من أجل تنفيذ الإستراتجية الوطنية لأمن الأنظمة المعلوماتية تقوم اللجنة بالدراسة و الإقتراح عناصر الإستراتجية والبرامج السنوية ومتعددة السنوات وتقيم كل ما توصلت اليه الوكالة من نتائج مجموع أعمالها ، محددة الطرق والوسائل اللازمة للإستجابة للحاجات الوطنية للأمن المعلوماتي؛ مع ضبط السبل اللازمة لترقية البحث والتطوير في نفس المجال المذكور أعلاه بالإضافة الى التداول لكل المسائل الخاصة بالجانب المالي للوكالة سوء نفقات أو إرادات أو مرتبات المستخدمين و تكوين الخاص بهم والموافقة على النظام الداخلي للوكالة ، ([1]) ويتم إستدعاء أعضاء لجنة التوجيه من قبل رئيسها أربع مرات في السنة في دورة عادية كما تجتمع في مرة غير عادية إذا اضطرت الحاجة لذلك حسب ما يقرره نظامها الداخلي وتدون جميع أعمال لجنة التوجيه في محضر ويرسل في شكل تقرير الى وزارة الدفاع الوطني .([2])

ب –المدير العام لوكالة أمن الأنظمة المعلوماتية:

جاء في نص المادة 28 من مرسوم رئاسي 05/20 أنه يعين المدير العام لوكالة أمن الأنظمة المعلوماتية طبقا للتنظيم المعمول به في وزارة الدفاع الوطني ويتم إنهاء مهامه بنفس الشكل ، هذا الأخير يقوم بتنفيذ الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية والبرامج المقررة من طرف لجنة التوجيه فهو المسؤول عن سير الوكالة ، حيث يكلف بإعداد برامج الوكالة وتحضير ميزانيتها و يقوم بعرضهما على لجنة التوجيه فالأولى من أجل إعطاء الموافقة أما الثانية للمداولة والتنفيذ ، له عدة صلاحيات يبرم العقود و الإتفاقيات التى لها صلة بالوكالة فهو المتصرف الأساسي والممثل القانوني لها و الآمر بالصرف فهو أعلى هرم في السلم التدرجي لمستخدمي الوكالة الوطنية، يعد المدير العام للوكالة تقريرا سنويا عن نشاطات الوكالة ويرسلها الى رئيس المجلس.[(3)]

ج– اللجنة العلمية لوكالة أمن الأنظمة المعلوماتية:

تتألف اللجنة العلمية للوكالة من عشرة (10) أعضاء يتم إختيارهم من بين الأساتذة والباحثين في مجال أمن الأنظمة المعلوماتية لمدة ثلاث سنوات قابلة للتجديد من قبل لجنة التوجيه و ينتخب الرئيس من بينهم ، وتتولى أمانتها مصالح الوكالة .([4])

[1] المادة 23 من المصدر السابق ، ص 8

[2] صونيا مقري ، بن لعامر وليد ، المرجع السابق ، ص141

[3] المادة 28 من المصدر نفسه ، ص8

[4] المادة 31 من المصدر نفسه ، ص9

يلجأ اليها المدير العام للوكالة من أجل إستشارتها في المسائل ذات الطابع العلمي، فهي تندرج في إطار مهام الوكالة المتعلقة بنشاطات البحث و التطوير في المجال الأمني كما تبدي رأيها مع إعطاء التوصيات حول كيفيات تنفيذ مشاريع البحث و التطوير كما تشارك في التظاهرات العلمية وتنظيمها، كذلك فيما يخص التكوين و التأهيل للمستخدمين المكلفين بأمن الأنظمة المعلوماتية في الإدارات أو المؤسسات أو الهيئات، فهي دائمة التوصيات ، و إبداء الرأي في كل المسائل ذات الطابع العلمي التى يعرضها عليها المدير العام للوكالة و تقوم بالمصادقة على النظام الداخلي لها خلال دورتها الأولى،([1]) ولها صلاحيات الإستعانة بأي شخص ذو خبرة علمية يمكنه الإفادة و المساهمة في مجال الأمن المعلوماتي .([2])

المطلب الثاني

الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال

تغير سلوك الإجرام أصبح ذكيا و ليس عنيفا لا يترك كدمات وفي المقابل لم يتوانى المشرع الجزائري وساير التطور والتطلع مدركا بأن القواعد العامة لا تكون كافية لمواجهة هذا التغيير أين بادر الى سن قوانين خاصة تهدف إلى حماية شاملة ذات فعالية ،كان في مقدمتها القانون رقم 04/09 بتاريخ 05 أوت 2009 ، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام الإتصال .([3])

أعطى هذا القانون تعريفا لهذه الجرائم و حدد مجموعة من التدابير الوقائية و الأهم أنه أنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال، التي نحن بصدد تناولها في هذا المطلب مع الحديث عن المواكبة التي سايرت هذه الهيئة من تغيرات في إعادة التنظيم من خلال المراسيم .

[1] المادة 32 من المصدر السابق ، ص 9

[2] المادة 33 من المصدر نفسه ، ص 9

[3] شريف خالد ، "الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال في التشريع الجزائري" ، **مجلة البيان للدراسات القانونية** ، م:10،العدد الاول جوان 2025 ، ص 127

الفرع الأول

تشكيلة الهيئة الوطنية

بموجب المادة 13 من القانون رقم 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال تأسست هذه الهيئة الوطنية بإعتبارها سلطة إدارية مستقلة لدى وزارة العدل،([1]) إلا أن تشكيلها وتنظيمها وكيفية سيرها جاء متأخرا من خلال المرسوم الرئاسي رقم 261/15 المؤرخ في 08أكتوبر 2015 و هذا الأخير أعطاها الشخصية المعنوية وذمة مالية مستقلة.

عرفت المادة الثانية من هذا المرسوم الهيئة الوطنية على أنها سلطة إدارية مستقلة تتمتع بالشخصية المعنوية و الإستقلال المالي توضع لدى الوزير المكلف بالعدل وتمارس مهامها تحت رقابة السلطة القضائية،([2]) وهي إحدى الآليات المؤسساتية الهامة في هذا المجال تضطلع بمجموعة من المهام الإستشارية ، الرقابية و التقنية الحيوية و تتشكل الهيئة من لجنة مديرة يتولى رئاستها الوزير المكلف بالعدل و تضم في عضويتها كل من وزير الداخلية ، البريد ، قائد الدرك و المدير العام للأمن الوطني ، ممثل عن رئاسة الجمهورية وممثل عن وزارة الدفاع وقاضيان من المحكمة العليا يعينهما المجلس الأعلى للقضاء ومديرية عامة يديرها مدير عام ، مديرية للمراقبة واليقظة الإلكترونية كجهاز تنفيذي و مديرية للتنسيق التقني ومركز للعمليات التقنية وملحقات جهوية عبر مختلف مناطق الوطن.([3])

أن هذه التشكيلة طرأت عليها عدة تغييرات عبر مراسيم متعددة فبصدور المرسوم 172/19 تم تقليص التشكيلة و تمثلت في المديرية العامة وتضم كل من المديرية التقنية ومديرية الإدارة والوسائل ومجلس التوجيه موجها لعمل الهيئة ومشرف ومراقبا له، أما بالنسبة للتشكيلة التي أتى بها المرسوم183/20 في مادته الخامسة تتكون من مجلس التوجيه و المديرية العامة تحت السلطة المباشرة لرئيس الجمهورية.

---

[1] المادة 13 من القانون 04/09 ،بتاريخ 05غشت2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ، ج،ر، ،العدد سبعة واربعون بتاريخ 16غشت 2009، ص 8

[2] المادة 2 من المرسوم الرئاسي رقم 261/15 يحدد تشكيلة وتنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ج،ر،ج،ج،العدد ثلاثة وخمسون، ص16

[3] المادة 6 من المصدر نفسه ، ص17

أما الإعادة للتنظيم الهيئة التي جاء بها المرسوم الرئاسي 439/21 المؤرخ2021/11/07 حيث لم يمس التكوين و إنما التشكيلة حيث يلاحظ أنه أسندت مهام مباشرة فيما يخص تولي رئاسة مجلس التوجيه التى كان يتولها رئيس الجمهورية أصبحت تحت سلطة الأمين العام لرئاسة الجمهورية ،([1]) وأيضا المهام التي كانت من إختصاص بعض الوزراء تم توليها من طرف أمناء عامين للوزراء كأنه تفويض مهام أو تقليل حمل ، من هذا السياق سوف نتطرق للحديث عن المهام التي جاء بها المرسوم 439/21 المؤرخ في 07 نوفمبر 2021 .

الفرع الثاني

مهام الهيئة الوطنية

تضطلع الهيئة الوطنية لعدة مهام فهي التي تحدد الإستراتجية الوطنية للوقاية و المكافحة وتقوم بتحيين المعايير القانونية أما فيما يخص المراقبة فتقوم بممارسة الرقابة الوقائية و الإستباقية على الاتصالات الإلكترونية كل هذا تحت إشراف سلطة القاضي المختص أي سلطة قضائية فالغاية منها كشف الجرائم الإرهابية و التي تمس بأمن الدولة، ويكون بالتنسيق مع المصالح المختصة لوزارة الدفاع الوطني ، كما تحظى بمهمة جمع المعطيات الرقمية أين تقوم بحفظها وتحليل مصدرها و تمد يد العون لسلطات القضائية والشرطة والعدالة فتزودهم بالمعلومات سواء عند الطلب أو تلقائيا و تنفيذ طلبات المساعدة القضائية الأجنبية و تعمل على تطوير التعاون الدولي وتبادل المعلومات ، كما لها دور فعال في تكوين المحققين المختصين في مجال التحريات التقنية وتأهيلهم، كما أنها تقوم بدور توعوي و تحسيسي حول مخاطر هذه التقنيات من خلال المشاركة في التظاهرات الوطنية وتنظيم حملات توعية،([2]) وتتكون الهيئة من مجلس التوجيه والمديرية العامة تحت سلطة رئيس الجمهورية. ([3])

[1] المادة 06 من المرسوم الرئاسي رقم 439/21 المؤرخ 07 نوفمبر سنة 2021 ، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ومكافحتها ، ج،ر،ج،ج ،العدد ستة وثمانون صادرت بتاريخ 11نوفمبر 2021 ، ص06

[2] المادة 04 من المصدر السابق ، ص05

[3] المادة 05 من المصدر نفسه ، ص 06

أولا : مجلس التوجيه

هو أعلى سلطة في الهيئة مهامه التوجيه والإشراف و المراقبة الشاملة لعمل و نشاط هذه الأخيرة يتولى الدراسة والبت في كل قضية و مسألة تدخل مجال إختصاصه، لا سيما المتعلقة بشروط اللجوء للمراقبة الوقائية للإتصالات الإلكترونية ، كما يقوم بالمداولة حول الإستراتجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ومكافحتها ، يعنى بدراسة عمل الهيئة ومشروع الميزانية والنظام الداخلي والموافقة عليهم ، فمهامه ليست محصورة في الجانب التنظيمي فقط بل يقوم بتقييم حالة التهديد في مجال الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال من أجل تحديد العمليات والأهداف المنشودة بدقة،كما يبدي رأيه في كل مسألة تتصل بمهام الهيئة مع إعطاء إقتراحات مفيدة للعمل الهيئة .([1])

يجتمع المجلس بناءا على إستدعاء الأمين العام لرئاسة الجمهورية في دورة عادية مرة واحدة في السنة ، و يمكنه أن يجتمع في دورة غير عادية إذا إضطرت الظروف أو بطلب من أحد أعضائه أو من المدير العام للهيئة.([2])

ثانيا : المديرية العامة.

يدير المديرية العامة مدير عام يعين بموجب مرسوم رئاسي و تنهى مهامه بنفس الأشكال القانونية فهي وظيفة عليا في الدولة،([3]) حيث يتولى مسؤولية السير الحسن للهيئة وأدائها الفعال، له عدة مهام منها التخطيط والإستراتجية فهو الذي يقوم بإقتراح عناصرها ومخطط عمل الهيئة والعمل على تنفيذه، يعد مشروع النظام الداخلي و يقوم بإعداد ميزانية الهيئة فهو الآمر بالصرف يمارس السلطة السلمية على جميع المستخدمين، و هو الممثل القانوني ينوب عن الهيئة أمام السلطات والمؤسسات الوطنية و الدولية و كذلك أمام القضاء، من مهامه أيضا تحضير إجتماعات مجلس التوجيه و يتحكم في سير أعمال الهيئة وتنسيقها ومتابعتها ومراقبتها ، ويسهر على إحترام قواعد السر المهني ويقوم بإجراءات التأهيل وأداء اليمين للمستخدمين المعينين يساهم في تحيين المعايير القانونية.

[1] المادة 07 من المصدر السابق ، ص 6

[2] المادة 08 من المصدر نفسه ، ص07

[3] المادة 09 من المصدر نفسه ، ص07

يعد التقارير السنوية و الدورية لنشاطات الهيئة فالأولى ترفع إلى رئيس الجمهورية و الثانية إلى رئيس مجلس التوجيه ، كما يقوم بإخطار رئيس الجمهورية فوريا عن كل حادثة تمس أمن الدولة وكذلك إخطار رئيس أركان الجيش الوطني الشعبي إذا تعلق الأمر بالدفاع الوطني،([1]) تضم المديرية العامة مديريتين الأولى للمراقبة الوقائية و اليقظة الإلكترونية والثانية مديرية الإدارة والوسائل كما تتمتع بمصلحتين مصلحة للدراسات والتلخيص ومصلحة للتعاون واليقظة الإلكترونية إضافة الى ذلك تحوز على ملحقات جهوية .([2])

أ- مديرية المراقبة الوقائية واليقظة الإلكترونية

تقوم بتنفيذ عمليات المراقبة الوقائية للإتصالات الإلكترونية لغرض الكشف عن الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال بإذن قانوني مكتوب صادر عن السلطة القضائية وتحت مراقبتها ضف إلى ذلك تنفيذ طلبات المساعدة القضائية الأجنبية في مجال إختصاص الهيئة حينها تجمع المعطيات المفيدة لتحديد مكان المجرمين الإلكترونيين والتعرف عليهم ، كما تمد يد العون حين الطلب أو تلقائيا للسلطات القضائية والمصالح الشرطة والعدالة من خلال تزويدهم بمعلومات القيام بالتدقيق والتفتيش في أي مكان أو هيكل أو جهاز بإستثناء التابعة لوزارة الدفاع الوطني،كما تشارك في التظاهرات والحملات التوعية و التحسيسية حول استخدام التكنولوجيا ومخاطرها مع تنشيط عمل ملحقات الجهوية و إحترام قواعد السر المهني في نشاطاتها وإنجاز مهام اليقظة الإلكترونية،([3]) ولها إرتباط مباشر مع مقدمو الخدمات، حيث تستطيع مديرية المراقبة أن تضع التجهيزات والوسائل والأجهزة التقنية لتنفيذ مهامها مع إلزام المتعامل ومقدم الخدمة المساعدة الضرورية لها لإنجاز مهامها.

ب- مديرية الإدارة والوسائل

تهتم مديرية الإدارة والوسائل بتسيير الموارد البشرية والوسائل المالية والمادية للهيئة فتقوم بتموينها وإسنادها تقنيا، كما تهتم بصيانة العتاد والوسائل و المنشآت وتعد إحتياجات الهيئة في إطار تحضير تقديرات الميزانية.([4])

[1] المادة 10 من المصدر السابق ، ص 7

[2] المادة 11 من المصدر نفسه ،ص 7

[3] المادة 14 من المصدر نفسه ، ص07

[4] المادة 16 من المصدر نفسه ، ص08

ج- مصلحة الدراسات والتلخيص

هي العصب الفكري للهيئة التي ترسم معالم دربها ، حيث تقوم بإعداد مشروع مخطط عملها بالتنسيق والتشاور مع الهياكل الأخرى للهيئة وتلخيص الوثائق، ولها مهمة إجراء الدراسات البحوث المعمقة بكافة نشاطات الهيئة، ولها دور في توثيق الرصين في إعداد التقارير و الحصائل السنوية ، وتضمن حفظ الوثائق والأرشيف و لها مسؤولية قانونية تتمثل في مراقبة الإجراءات المتعلقة بالطلبات القضائية([1])

د- مصلحة التعاون واليقظة التكنولوجية:

الغرض من إنشاء هذه المصلحة فكرة التشارك والتعاون لتنفيذ عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ومكافحتها مع كل الشركاء دون الإغفال عن المتابعة المستمرة للتطورات المتسارعة في التكنولوجيا لضمان مواءمة نشاطات الهيئة. ([2])

هـ- الملحقات الجهوية:

تقوم الملحقات الجهوية بعمليات المراقبة الوقائية للإتصالات الإلكترونية الغاية منها الكشف عن الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ومكافحتها ، معتمدة في ذلك على إجراء شرعي حيث لا تتم هذه الأخيرة إلا بإذن مكتوب من السلطة القضائية وتحت رقابتها مباشرة. ([3])

و- سير الهيئة :

تلجأ الهيئة لسير نشاطها على أكمل وجه بالإستعانة بالقضاة وأعوان الشرطة القضائية من كافة الأسلاك الأمنية و توظف فئات أخرى من المستخدمين ،حيث أن هذه الفئات تتطلع على المعلومات السرية لذا وجب عليها الإلتزام بالسر المهني وأداء القسم أمام المجلس القضائي المختص إقليميا قبل تنصيبهم ، ([4]) أما في ما يخص إقتناء العتاد والأجهزة والحلول الخاصة بالمراقبة الوقائية فالمرسوم 381/24 المؤرخ 27 نوفمبر 2024 يتمم و يعدل المرسوم 439/21 أسندت للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ومكافحتها دون سواها أما آليات التنفيذ حددتها المادة الأولى أن التفاصيل وكيفية تطبيق هذا الإجراء يتم من خلال قرار مشترك بين الأمين العام لرئاسة الجمهورية ووزير المالية . ([5])

---

[1] المادة 17 من المرسوم الرئاسي رقم 439/21 ، المصدر السابق ، ص08

[2] المادة 18 من المصدر نفسه ، ص08

[3] المادة 19 من المصدر نفسه ، ص08

[4] المادة 22 من المصدر نفسه ، ص09

[5] المادة 01 من المرسوم الرئاسي رقم 381/24 المؤرخ 27 نوفمبر سنة 2024 ، يتمم المرسوم الرئاسي رقم 439/21 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ومكافحتها ، ج،ر،ج،ج ،العدد ثمانون ، ص 07

خلاصة الفصل الثاني:

قدمنا في هذا الفصل رؤية واضحة و تصورا متكاملا لحماية الأمن المعلوماتي من خلال ثلاثة آليات تقنية جزائية ومؤسساتية، حيث تناولنا في المبحث الأول آليات الحماية التقنية والجزائية أين قسمنا هذا المبحث الى مطلبين تطرقنا لآليات التقنية في المطلب الأول و الذي بدوره جزئناه الى فروع فكان الحديث عن التشفير في الفرع الأول الذي يضمن سرية المعلومات من خلال تحويل البيانات من شكلها القابل للقراءة الى شكل غير مفهوم ، فالغرض منه ليس الإخفاء فحسب بل ليكون مانعا لجهة غير مخولة للإطلاع أو التعديل ، أما الوظيفة المتمثلة في منع الوصول غير المصرح به وترقب وتحكم في حركات البيانات الواردة والصادرة وحماية الشبكات الداخلية من التهديدات الخارجية فهي من وظائف وأهداف الجدار الناري الذي تعرضنا اليه في الفرع الثاني فهو شبيه الحاجز الأمني يعمل على منع الاتصالات الضارة ويسمح فقط بمرور البيانات المعتمدة و الآمنة.

وتناولنا في الفرع الثالث لنظام كشف التطفل الذي يرصد الأنشطة المشبوهة ، حيث انه إذا تم كشف التطفل مبكرا و بسرعة يمكن تحديد المتطفل وإخراجه قبل أن تحصل سرقة أو تدمير فتكون عملية إستباقية ، كما عرجنا في الفرع الرابع الى التوقيع الإلكتروني الذي يثبت هوية المرسل وسلامة المحتوى ويعطي تأكيد الموافقة .

بما أن التكنولوجيا في تطور مستمر فإن الآليات التي تم ذكرها تكون على سبيل المثال لا الحصر إلا أنه في بعض الأحيان قد تعجز هذه الآليات التقنية في صد الإعتداء، مما يتيح للمتطفل فرصة تجاوز خط الدفاع، وهذا الإخفاق سوف نتناوله في المطلب الثاني وتحديدا في الفرع الأول حين يتم هذا التجاوز يبقى أمام المتسلل أمرين إما الدخول الى المعلومات و المعطيات المخزنة داخل نظام الحاسب الآلي بدون موافقة المسؤول عن النظام ، حينها تأخذ سلوك جرمي تسمى عملية الولوج غير مشروع يجرمها القانون الجزائري و يشدد عقوبتها بالقانون 06/24 المعدل والمتمم 156/66 من خلال المادة 394 مكرر أما الأمر الآخر والذي تناولناه في الفرع الثاني جريمة البقاء في المنظومة وهي سلوك جرمي مستمر و تواجد داخل نظام المعالجة الآلية للمعطيات لها عدة صور وضاعف لها المشرع الجزائري العقوبة في حالة إذا نتج عنها حذف أو تغير للمعطيات ، أما في حالة تخريب نظام التشغيل للمنظومة تكون العقوبة من سنة (01) الى ثلاثة سنوات (03) وغرامة من 10000دج إلى 30000دج .

لنتناول آخر فرع من هذا المطلب للحديث عن جريمة تأتي على أشكال ثلاثة من السلوكات الإدخال، التعديل و المحو ، إلا أنه لا يشترط إجتماعهم لخلق جريمة فسلوك واحد كافي لقيامها تسمى هذه الأخيرة جريمة إدخال معطيات في نظام المعالجة الآلية للمعطيات وإزالتها ، وهي إضافة برامج أو معلومات مزيفة الغرض منها السيطرة على المنظومة.

لننهي هذا الفصل من خلال المبحث الثاني الذي جاءنا فيه كل ما هو مستحدث وجديد نقصد الإطار المؤسساتي حيث خصص المطلب الأول لدراسة المجلس الوطني للأمن المعلوماتي تم تقسيمه الى فرعين حيث تناولنا في الفرع الأول المجلس وهيكله الذي يعد إحدى مكونات المنظومة وأعلى هيئة ومن مهامه البت في الإستراتيجية التي تقترحها الوكالة تم إنشاء هذه المنظومة من خلال المرسوم 05/20 بتاريخ 20 جانفي 2020 ، أما الفرع الثاني فأخذنا الحديث عن الوكالة الوطنية للأمن المعلوماتي التي هي في الأساس مؤسسة عمومية ذات طابع إداري وتتمتع بالشخصية المعنوية مهمتها تحضير الإستراتجية وعرضها على المجلس، كما تقوم بتحقيقات الرقمية في حالة الهجمات على الأنظمة لها عدة مهام تم التطرق لها ، أما عن التنظيم و التسيير فوكلت إلى لجنة التوجيه التي هي تحت سلطة مدير عام معين من طرف وزارة الدفاع هذه الأخيرة لها مهام أسندت لها دراسة و إقتراح عناصر الإستراتجية والبرامج السنوية وتبرز اللجنة العلمية لوكالة أمن الأنظمة المعلوماتية كفريق عمل متكون من الأساتذة والباحثين حيث تعطي توصيات وتقوم بتكوين المستخدمين ومهام أخرى .

أما المطلب الثاني تم التركيز على الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال في الفرع الأول أعطينا نبذة حياتية للهيئة الوطنية و ما مرت به من تقلبات وتغيرات ، حيث كانت نشأتها بقانون رقم 04/09 بتاريخ 05غشت 2009 تم تشكيلها بعد مرور 06 سنوات من إنشاءها بمرسوم رئاسي رقم 261/15 ، ليتم تقليص التشكيل بعد ذلك بمرسوم رئاسي رقم 172/19 ثم يعاد تكوينها لتصبح متكونة من مجلس التوجيه والمديرية العامة تحت سلطة رئيس الجمهورية وهذا أيضا كان بمرسوم رئاسي 183/20 لينتهي بنا المطاف للمرسوم الرئاسي رقم 439/21 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال الذي أعطى رئاسة مجلس التوجيه للأمين العام لرئاسة الجمهورية لقد مرت الهيئة بمحطات.

أما الفرع الثاني من هذا المطلب الأخير أحصينا مهام الهيئة المتمثلة في تحديد الإستراتجية الوطنية للوقاية والمكافحة والرقابة الوقائية و الإستباقية على الاتصالات الإلكترونية تحت إشراف القاضي المختص وتتكون هذه الأخيرة من مجلس التوجيه والمديرية العامة .

خـــــاتمة

على ضوء ما تطرقنا له في دراستنا للمذكرة الموسومة تحت عنوان الإطار القانوني للأمن المعلوماتي في التشريع الجزائري ، حيث تم تقديم التأصيل المفاهيمي عبر تحديد مفهوم الأمن المعلوماتي من ثلاثة زوايا جانب أكاديمي ، قانوني و تقني من هذه التعاريف نستنتج على أنه لا يقتصر كونه حاجز تقني بل هو نسيج متكامل من الإستراتجيات والتدابير التي تتشابك لتشكل دفاعا متعدد المستويات فالغرض واحد والهدف هو الحماية من خلال العناصر الثلاثة السرية السلامة والتكامل والإتاحة والتوافر.

الجزائر لا تعيش بمعزل عن العالم فهي عضو في المجتمع الدولي و لا تستطيع مجابهة هذه التحديات بمفردها ، فتأمين الفضاء الإلكتروني الذي لا يعترف بالحدود يقودها على التعاون الدولي من خلال الإنضمام إلى الإتفاقيات و المعاهدات المتعلقة بمكافحة الجريمة السيبرانية مثل إتفاقية الأمم المتحدة وقد أحسنت صنعا الجزائر حين وقعت على هاته الأخيرة و أكثر من ذلك حيث لعبت دورا محوريا في صياغتها وإعدادها وكان هذا بتاريخ 2025/10/25 فهذه الإتفاقيات أهم مصدر قانوني ملزم للأمن المعلوماتي وفي نفس السياق أصدر المشرع الجزائري مرسوم رقم 07/26 المؤرخ في 07جانفي 2026 يقضي بإنشاء هيكل مسؤول عن أمن الأنظمة المعلوماتية وحماية المعطيات في كل مؤسسة، إدارة أو هيئة عمومية، بوصفه مصدر داخلي يساير التطور الغرض منه الحماية فالتهديدات في إزدياد و الدافع إستباقي فرقمنة كل القطاعات تفرض ذلك وأيضا دافع تنظيمي فالحلول الأمنية المستقلة بذاتها تضعف المنظومة و أخيرا الدافع للإلتزامات القانونية الدولية وهذا ما جعلنا نلاحظ عزوف بعض الدول عن التعاون الدولي القضائي بحجة عدم تطابق التشريعات فإحداث هذا الهيكل يتدارك هذا الإشكال ويفرض الإستجابة.

إن ما يستخلص من خلال هذه الدراسة أن الأمن المعلوماتي ليس نتاجا جهد منعزل أو بعد واحد بل هو منظومة متكاملة الأبعاد التقنية والقانونية والمؤسساتية والبشرية فلا يمكن فصل واحد منها عن الأخرى، فالإخلال بأي بعد يختل منه توازن المنظومة ويعيد فتح الثغرات التي يسعى لها المتسلل لإستغلالها ، إن التحدي الأكبر ليس في تطوير الأدوات التقنية فقط بل في تنمية الوعي المجتمعي، و ثقافة الأمن المعلوماتي فالموظف المدرب يقف حاجزا منيعا أمام الهجمات، بينما الموظف المهمل قد يكون ممر عبور الى أعمق أسرار الدول ، إن المورد البشرية إذا أحسنت توجيهها وتدريبها تظل الحلقة الأقوى في الدفاع، و إن أهملت تكون الحلقة الأضعف التي تنهار عندها كل الحصون .

إن الأمن المعلوماتي في العصر الرقمي المضطرب ليس ترفا تقنيا ولا رفاهية بل هو إستثمار مستقبلي يصون كرامة الأفراد ويحافظ على السيادة الوطنية ، فالدول والمؤسسات والأفراد المدركين لأهمية هذا المجال و يحكمون بناء منظومتهم الوقائية و يعملون على تطويرها وتحديثها بشكل مستمر و تطوير تشريعاتهم هم وحدهم القادرون على التعامل مع هذا التحول الرقمي بثقة، وآمان وضمان إستمرارية نشاطاتهم وحماية مكتسباتهم من عواصف التهديدات ، إن تطوير هذه المنظمة وتنسيق جهود هيئاتنا الوطنية و مواءمة تشريعاتنا للمعايير الدولية، و العمل على برامج التدريب المؤسسي للأمن المعلومات فهو السبيل والطريق الأمثل لبناء فضاء رقمي آمن تسوده الثقة وتساهم فيه التقنيات الحديثة في رفاهية الإنسان و تقدم المجتمع لا تهديده أو إبتزازه ، تحقيق الأمن المعلوماتي يبدأ من الحفاظ على السيادة الوطنية من خلال تحقيق أمن الدولة ثم أمن المجتمع وأفراده .

قائمة المصادر والمراجع

أولا : المصادر

1-القرآن الكريم

2-إبن منظور جمال الدين محمد بن مكرم الانصاري ، لسان العرب ، م:1 ط السادسة ، دار صادر،بيروت 2011.

ثانيا :الدستور

1-الدستور 2020 المعدل والمتمم،ج ج ر العدد إثناني وثمانون بتاريخ 30ديسمبر2020

ثالثا: الإتفاقيات

1-إتفاقية المجلس الأروبي المتعلقة بمكافحة الجريمة الإلكترونية ، بودابست 2001/11/23.

2-الإتفاقية العربية لمكافحة جرائم تقنية المعلومات 21ديسمبر 2010.

3-إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية 24 ديسمبر 2024.

رابعا:القوانين العادية:

1-القانون رقم 02/26 المؤرخ 17فبراير2026 الذي يحدد القواعد العامة المتعلقة بخدمات الثقة للمعاملات الالكترونية ،ج ج،ج ر، العدد الرابع عشر 18 فبراير 2026

2-القانون رقم 14/25 المؤرخ 03غشت 2025يتضمن قانون الإجراءات الجزائية ،ج ج،ج ر،العدد اربعةوخمسون بتاريخ 13 غشت 2025.

3- القانون رقم 11/25 المؤرخ 24يوليو2025 يعدل ويتمم القانون رقم 07/18 المؤرخ10يونيو 2018و المتعلق بحماية الأشخاص الطبيعين في مجال معالجة المعطيات ذات الطابع الشخصي ،ج ج،ج ر العدد ثمانية وأربعون بتاريخ 24 يوليو 2025.

4-القانون رقم 06/24 المؤرخ 28ابريل 2024 المعدل والمتمم للأمر 156/66 المؤرخ 08يونيو 1966المتضمن قانون العقوبات ج ج،ج ر، العدد ثلاثون بتاريخ 30ابريل 2024.

5-القانون رقم 04/15 الموافق 01فبراير 2015 يحدد القواعد العامة المتعلقة بتوقيع الالكتروني والتصديق الإلكترونيين،ج ج،ج ر، العدد السادس بتاريخ 10فبراير 2015 ملغى.

6-القانون رقم 04/09 المؤرخ 05غشت2009 يتضمن القواعد العامة الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها ،ج ج،ج ر، العدد سبعة واربعون بتاريخ 16غشت 2009.

خامسا:المراسيم

1-المرسوم الرئاسي رقم 07/26 المؤرخ 07جانفي 2026 المتضمن إنشاء هيكل مسؤول عن أمن أنظمة المعلوماتية،ج ج ،ج ر، العدد الرابع 07 جانفي 2026.

2-المرسوم الرئاسي رقم 381/24 المؤرخ 27 نوفمبر 2024 يتمم المرسوم الرئاسي رقم 439/21 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها ج ج،ج ر، العدد ثمانون بتاريخ 2024/12/04.

3-المرسوم الرئاسي رقم 439/21 المؤرخ 2021/12/07 يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها ،ج ج،ج ر،العدد ستة وثمانون بتاريخ 2021/12/11.

4-المرسوم الرئاسي رقم 183/20 المؤرخ 13يوليو 2020يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها ،ج ج،ج ر،العدد أربعون 18يوليو2020.

5-المرسوم الرئاسي رقم 05/20المؤرخ 20جانفي يتعلق بوضع منظومة وطنية لامن الانظمة المعلوماتية ج ج،ج ر ، العدد الرابع بتاريخ 26 جانفي 2020.

6-المرسوم الرئاسي رقم 172/19 المؤرخ 06يونيو 2019 يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها ،ج ج،ج ر، العدد سبعة وثلاثون بتاريخ 09 يونيو 2019 .

7-المرسوم الرئاسي رقم 261/15 المؤرخ 08 اكتوبر 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها ، ج ج،ج ر، العدد ثلاثة وخمسون بتاريخ 16 اكتوبر 2015 .

سادسا:الكتب العامة

1- خضر مصباح إسماعيل الطيطي ، أساسيات أمن المعلومات والحاسوب،ط الأولى دار الحامد *عمان الأردن* 2009.

2-فارس محمد العمارات ، ابراهيم الحمامصة ، الامن السيبراني المفهوم وتحديات العصر ، ط الاولى ، دار الخليج للنشر والتوزيع ، عمان الأردن 2022.

3-منير الجنبيهي ، ممدوح الجنبيهي ، أمن المعلومات الإلكترونية ، دار الفكر الجامعي ، د ر ط ، الإسكندرية مصر 2005.

سابعا: الكتب المتخصصة

1-زبيحة زيدان ، الجريمة المعلوماتية في التشريع الجزائري والدولي ، دار الهدى ، د ر ط عين مليلة الجزائر 2011.

2-محمدخليفة ، الحماية الجنائية لمعطيات الحاسب الألي في القانون الجزائري والمقارن ، دار الجامعة الجديدة د ر ط الإسكندرية مصر ، 2007.

ثامنا :الأطروحات :

1-مالك محمد ،إستراتجية إدارة أمن المعلومات نظمية على إستشراف تطبيقات المعيار الدولي نموذجا ،رسالة دكتوراه تخصص علوم الاعلام والاتصال ، كلية علوم الاعلام والاتصال جامعة الجزائر 3 2016/2015.

تاسعا:مذكرات الماستر :

1-بورغداد وصال ، كواشي عبير،حماية خصوصية المستهلك الالكتروني في القانون الجزائري ، مذكرة شهادة الماستر في الحقوق تخصص قانون اعمال جامعة محمد البشير الابراهيمي، برج بوعريريج،2025/2024.

2-بوطمين وائل خليل الرحمان ، البعد السيبراني للامن القومي الجزائري ،دراسة مقاربة لنماذج دولية ، مذكرة شهادة الماستر في ميدان الحقوق والعلوم السياسية ، المدرسة الوطنية العليا للعلوم السياسية الجزائر 2025/2024.

3-بويديوة يمينة ،رمطين رابح ،الحق الدستور في البيئة ،مذكرة شهادة الماستر تخصص دولة ومؤسسات كلية الحقوق والعلوم السياسية ،جامعة 20اوت 1955سكيكدة ،دورة جوان 2023.

4-حمودي كاهنة، نظام أمن المعلومات في الجزائر ، مذكرة شهادة الماستر في العلوم السياسية والعلاقات الدولية ،كلية الحقوق والعلوم السياسية جامعة مولود معمري تيزي وزو2016.

5-عثماني رجاء ،بوحفص شيماء ، الحماية القانونية للحق في حرمة الحياة الخاصة ،مذكرة شهادة الماستر فيالحقوق تخصص قانون عام ، كلية الحقوق والعلوم السياسية ،جامعة بلحاج بوشعيب عين تموشنت 2023/2022.

6- عليلي عماد الدين ،بن قسيس زين الدين ، جرائم الخيانة الوطنية وتسريب المعلومات والوثائق السرية على ضوء القانون 06/24المعدل والمتمم لقانون العقوبات ،مذكرة شهادة الماستر في القانون ، كلية الحقوقوالعلوم السياسية ،جامعة 08ماي 1945قالمة 2025/2024.

- **عاشرا:المقالات العلمية :**

1-ادريس عطية ،مكانة الامن السيبراني في منظومة الامن الوطني الجزائري ،دراسة قانونية ، كلية الحقوق والعلوم السياسية ،جامعة العربي تبسي تبسة الجزائر 2019/12/01.

2-افتيسان وريدة ،بن ناصر وهيبة ، دسترة مبدأ الامن القومي التجربة الجزائرية نموذجا ،مجلة الدراسات القانونية صنف ج جامعة يحي فارس بالمدية ،م:08العدد الثاني ،جوان 2022.

3-الحمزة منير،لعجال حمزة ،التلوث الإلكتروني في الفضاء الرقمي ،المجلة الجزائرية للامن الانساني م:05العددالاول2020.

4-العياشي زرزار، حمزة بن وريدة، الحوسبة السحابية ،المفهوم والخصائص،مجلة الارصاد للدراسات الاقتصاديةوالادارية م:02،العددالثاني ديسمبر 2019.

5-اوبراهم صونية ،ملاك فانزة ، الامن المعلومات في ظل الإقتصاد الرقمي ،مجلة البحوث القانونية الاقتصادية ،م:08 ،العددالثاني ،جوان 2025.

6-بارة سمير ، الأمن السيبراني في الجزائر السياسات والمؤسسات ،المجلة الجزائرية للأمن الانساني،جامعة قاصدي مرباح ورقلة ،العدد الرابع ،جويلية 2017.

7-بن طيب ابراهيم ،اهمية أمن نظم المعلومات لدى المؤسسات الاقتصادية الحديثة ،مجلة التنمية والاقتصاد التطبيقي، المسيلة ، العدد الثالث ، مارس 2018.

8-بن علية سميرة ،سالمي عبد المجيد ،التطبيقات الالكترونية السياحية في الجزائر ،دراسة لغوية سيميائية، جامعة الجزائر 2، العدد الاول ، 2019.

9-جلال جناجرة،امن الشبكات وحمايتها قسم تكنولوجيا المعلومات ،جامعة فلسطين تقنية 2022.

10-حزام فتيحة ، حماية الانظمة الرقمية بين الاليات التقنية واجهزة الحماية ، مجلة الحقوق والعلوم الانسانية م:13العدد الثالث،اكتوبر 2020.

11-حواس فتيحة ، التوقيع الالكتروني (الخصوصيات والتطبيقات)،مجلة الدراسات القانونية المقارنة م:07العدد الاول 2021.

12-دويب العيد ،مفهوم الامن في الفكر الديني دراسة لابعاد الامن الانساني في الاسلام ،مجلة الدراسات القانونية والسياسية ،م:01 العدد خمسة، جانفي 2017.

13-رجب عبد الحميد حسنين،امن شبكات المعلومات الالكترونية :المخاطر والحلول ،جامعة الحصن ابوظبي الامارات العربية ،العدد ثلاثون ،ديسمبر2012.

14-سعيد مسعود الكثيري، الجريمة الالكترونية في ضوء اتفاقية بودابست الاطار المفاهيمي ،مجلة البحوث القانونية والاقتصادية ،م:09 ،العددالاول ،جانفي 2026.

15-شريف جيجان ، الامن السيبراني الصيني دراسة في دوافع والتحديات ، مجلة قضايا سياسية،جامعة النهرين ، العدد خمسة وستون ،2022.

16-شريف خالد، الجرائم المتصلة بتكنولوجيات الاعلام والاتصال في التشريع الجزائري ،مجلة البيان للدراسات القانونية ،م:10العددالاول ،جوان 2025.

17-شريف كامل شاهين ، امن المعلومات ، المجلة العربية للمعلوماتية وأمن المعلومات،م:01العددالاول اكتوبر 2020.

18-صونيا مقري ،وليد لعامر ، المنظومة الوطنية لامن الانظمة المعلوماتية كالية مؤسساتيةلمكافحة الجريمة المعلوماتيةوفقا للمرسوم 05/20،مجلة البحوث في العقود وقانون الاعمال م:10العددالثاني 2025

19-عماد حسين، محمد الفريحات،الجهود العربية والافريقية لمواجهة الجرائم الالكترونية في الفترة 2010-2023،مجلة ابن خلدون للدراسات والابحاث ،م:03 العدد الخامس ،ماي 2023.

20-غيتاوي عبدالقادر ،دليمي رشيد ، الطبيعة القانونية للمال العام ،مجلة القانون والمجتمع ، كلية الحقوق والعلومالسياسية جامعة ادرار ،2017/06/01.

21-فاطمة الزهراء رمضاني ، التعليق على نص المادة 34من التعديل الدستوري الجزائري ،مجلة العلوم القانونية والسياسية جامعة تلمسان، العدد الاول ، افريل 2021.

22-فرسان دليلة ، التنمر الالكتروني بين حرية التعبير والتشكيل القيمي ،دفاتر البحوث العلمية ،كلية علوم الاعلام والاتصال جامعة الجزائر ،م:10، العدد الاول 2022.

23-فريدة حمودي ، الامن المعلوماتي في الجزائر بين التطورات التكنولوجية وضعف البيئة الرقمية المجال المصرفي نموذجا ،دراسة قانونية ، مجلة الابحاث القانونية المعمقة ، العدد واحد واربعون ، 2020/08/17.

24-فصيح عبد القادر ، بن عمر محمد ، التوقيع الالكتروني ودوره في الاثبات ، مجلة العلوم القانونية والاجتماعية ،جامعة زيان عاشور الجلفة ، العدد الثالث ،د س ن.

25-فيلالي أسماء ، وشليل عبد اللطيف ، تهديدات أمن المعلومات وسبل التصدي لها ، مجلة البشائر الاقتصادية ،جامعة ابوبكر بلقايد تلمسان ،م:04،العدد الثالث ،د س ن.

26-قدايفية أمينة ، استراتجية الامن المعلوماتي ،مجلة الابعاد الاقتصادية ،جامعة امحمد بوقرة بومرداس الجزائر م:06العدد الاول 2016.

27-قطاف سليمان ،بوقرين عبد الحليم ، الاليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل اتفاقية بودابست والتشريع الجزائري ، المجلة الاكاديمية للبحوث القانونية والسياسية ،جامعة عمار ثليجي الاغواط الجزائر ،م:06،العدد الاول 2022.

28-ليتيم فتيحة ، ليتيم نادية ، الامن المعلوماتي للحكومة الالكترونية وارهاب القرصنة ، مجلة الفكر كلية الحقوق والعلوم السياسية جامعة محمد خيضر بسكرة ، العدد الثاني عشر 2015/03/25.

29-مسكية محمد، الفضاء السيبراني وتحديات الامن القومي للدول، مجلة العلوم القانونية والاجتماعية جامعة زيان عاشور الجلفة الجزائر ،م:07،العدد الرابع ،ديسمبر 2022.

30-هاني مطر ابوسعود،عباسة طاهر ، ارتباطات الامن المعلوماتي بالامن القومي ،مجلة الدراسات الحقوقية م:07،العدد الثاني ،جوان 2020.

31-يانبي شين،فيرين باكسون ،راندي كاتسا، بترجمة طه زروقي ، ما الجديد في أمن الحوسبة السحابية مجلة المعالم ،2011.

إحدى عشر:المواقع الانترنت

1-موقع العطاء الرقمي ،وزارة الاتصالات وتقنية المعلومات ،امن التطبيقات ،تاريخ النشر 2025/05/06،تاريخ التصفح2026/05/07،على الساعة 00:01 على الوصلة https://attaa.mcit.gov.sa/library/view/2178

2-موقع بكه للتعليم ،امن المعلومات واهميته والانواع والعناصر والاستراتجيات والبرامجوالاهداف،تاريخ النشر جوان2025تاريخ التصفح 2026/05/07على الساعة 00:18 على الوصلة bakkah.com /ar/knowldge.center

3-موقع جمعية أمن المعلومات ،الاستجابة للحوادث الامنية ،تاريخ النشر 2018/10/23،تاريخ التصفح2026/05/07على الساعة 01:25 على الوصلة Hemaya.org.sa/?p=**8095**

4-موقع الدرع الرقمي للمؤسسات السعودية في مواجهة التهديدات المتقدمة ،اساسيات تحليل الهجمات السيبرانية ،تم الاطلاع عليها بتاريخ 2026/03/13على الساعة 18:15 على الوصلة **https://www.rmg-sa.com**

5-موقع وزارة الشؤون الخارجية والجالية الوطنية بالخارج ،وقعت الجزائر معاهدة الامم المتحدة ،لمكافحة الجريمة السيبرانيةبتاريخ 2025/10/25،تم الاطلاع عليها بتاريخ 2026/03/13على الساعة العاشرة وخمسة واربعون دقيقة 10:45 على الوصلة **https://www.mfa.gov.dz/ar/press-and-information/news-and-press-releases/mrmagramane-signed-the-united-nations-convention-on-c**

إثنى عشر:المحاضرات :

1-حسيبة قيدوم ،محاضرات في الانظمة المعلوماتية،مطبوعة موجهة لطلبة السنة الثانية ماستر تخصص اتصال تنظيمي كلية علوم الاعلام والاتصال ،جامعة الجزائر 3 2021/2020.

2-بوازدية جمال ، الامن السيبراني ،محاضرات مقدمة لطلبة السنة الثانية ماستر تخصص دراسات واستراتجية وامنية ،كلية العلوم السياسية والعلاقات الدولية ،جامعة الجزائر 2020،2021/3.

3-بوكورو منال ، محاضرات في مقياس الحريات العامة مطبوعة بيداغوجية ،في مقياس الحريات العامة موجهة لطلبة السنة الثانية ماستر حقوق قانون عام ،جامعة الاخوة منتوري قسنطينة1، 2020/2019.

ملخص:

يمتاز هذا العصر بالتدفق العالي للبيانات والمعلومات معتمدا في ذلك على التكنولوجيا حيث أنه ألغى فكرة الحدود الزمنية والمكانية ، إلا أنه هذه البيانات والمعلومات وأثناء نقلها أو تبادلها في الفضاء الرقمي أو الوسائط الإلكترونية قد تتعرض لمخاطر وتهديدات تنتهك حرمتها وخصوصيتها ، ومنه فالأمن المعلوماتي هو مجموعة من الضوابط والإجراءات وجملة من الأساليب الوقائية التى تعمل على درء هذه التهديدات والمخاطر، فهي تهدف إلى توفير حماية أمنية لمجموع المعلومات المتعامل بها في البيئة الرقمية من خلال ضمان سريتها وصحتها وعدم القدرة للوصول إليها من أجل تغيرها أو إستبدالها أو عدم إتاحتها معتمدة في ذلك على الاليات التقنية كحاجز أولي منيع الى جانب اليات الجزائية المتمثلة في التجريم و العقوبات الرادعة لإنتهاكات الأمن المعلوماتي و الآليات المؤسساتية المتمثلة فالهيئات والهياكل ، إلا أن فعالية الأمن المعلوماتي تتطلب تكاملا بين الإطار التشريعي و الآليات التقنية والهياكل المؤسساتي ، وهذا محور دراستنا.

الكلمات المفتاحية : الأمن المعلوماتي – الأساليب الوقائية – التشفير– وكالة أمن الأنظمة

Abstract

This era is characterized by a high flow of data and information driven by technology, which has effectively eliminated the concepts of temporal and spatial boundaries. However, as this data is transmitted or exchanged within cyberspace and electronic media, it is increasingly exposed to risks and threats that violate its integrity and privacy.

Consequently, **Information Security** emerges as a comprehensive set of controls, procedures, and preventive methods designed to thwart these threats. It aims to provide robust protection for information handled within the digital environment by ensuring its **confidentiality**, **integrity**, and **availability**, while preventing unauthorized access, modification, or substitution.

To achieve this, it relies on **technical mechanisms** as a primary line of defense, alongside **penal mechanisms**—comprising criminalization and deterrent sanctions for security breaches—and **institutional mechanisms** represented by specialized bodies and frameworks. Ultimately, the effectiveness of information security requires a seamless integration between the legislative framework, technical tools, and institutional structures; this integration forms the core focus of our study.

فهرس المحتويات