الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et populaire

Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique

Université de Ghardaïa.

Faculté de Droit et des Sciences olitiques.
Département de Droit .

وزارة التعليم العالي و البحث العلمي

جامعة غرداية

كلية الحقوق والعلوم السياسية

قسم الحقوق

شهادة تصحيح

يشهد ....الأستاذ مرسلي محمد.....

بصفته رئيسا:.....في لجنة المناقشة لمذكرة

الماستر

الطالب(ة):...كيس فريد.....رقم التسجيل:19193908949....

الطالب(ة):...باموس مسعود.....رقم التسجيل:24079085501....

تخصص :....قانون جنائي.....دفعة:.2024.....لنظام(ل م د).

أن المذكرة المعنونة بـ: مبدأ الأمن القانوني في الفضاء الرقمي

.....

.....

تم تصحيحها من طرف الطالب / الطالبين وهي صالحة للإبداع.

غرداية في:.....

إمضاء الأستاذ رئيس اللجنة المكلف بمتابعة التصحيح

الأستاذ مرسلي محمد

رئيس القسم

رئيس قسم الحقوق

أبو القاسم عيسى

جامعـــــــــــة غردايـــــــــــــة

كلية الحقوق والعلوم السياسية

قسم الحقوق

مبدأ الأمن القانوني في الفضاء الرقمي

مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي

حقوق تخصص قانون جنائي وعلوم جنائية.

إعداد الطلبة:

- كيس فريد.
- بامون مسعود.

إشراف الأستاذ الدكتور:

عبد الرحيم لحرش.

لجنـة المناقشـة:

اسم ولقب الأستاذ	الرتبة	الجامعة	الصفة
مرسلي محمد	أستاذ محاضر "أ"	جامعة غرداية	رئيسا
بوحادة محمد	أستاذ محاضر "أ"	جامعة غرداية	عضوا مناقشا
لحرش عبد الرحيم	أستاذ محاضر "أ"	جامعة غرداية	مشرفا مقررا

نوقشت بتاريخ: 2025/05/29م

السنـــة الجامعيـــة

1445-1446هـ/2024-2025م

جامعـــــــــة غردايـــــــــــة

كلية الحقوق والعلوم السياسية

قسم الحقوق

مبدأ الأمن القانوني في الفضاء الرقمي

مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي

حقوق تخصص قانون جنائي وعلوم جنائية.

إعداد الطلبة:

- كيس فريد.
- بامون مسعود.

إشراف الأستاذ الدكتور:

عبد الرحيم لحرش.

لجنـة المناقشـة:

اسم ولقب الأستاذ	الرتبة	الجامعة	الصفة
مرسلي محمد	أستاذ محاضر "أ"	جامعة غرداية	رئيسا
بوحادة محمد	أستاذ محاضر "أ"	جامعة غرداية	عضوا مناقشا
لحرش عبد الرحيم	أستاذ محاضر "أ"	جامعة غرداية	مشرفا مقررا

نوقشت بتاريخ: 2025/05/29م

السنـــة الجامعيـــة

1445-1446هـ/2024-2025م


بسم الله الرحمن الرحيم

أَعُوذُ بِاللهِ مِنَ الشَّيْطَانِ الرَّجِيم:

{وَإِذْ قَالَ إِبْرَاهِيمُ رَبِّ اجْعَلْ هَذَا بَلَدًا آمِنًا وَاجْنُبْنِي وَبَنِيَّ أَنْ نَعْبُدَ الأَصْنَامَ}

صَدَقَ اللهُ العَظِيم، الآيَةَ 126، سُورَةُ البَقَرَة.

شكـــــر وعرفـــــان

نحمد الله عز وجل على إتمام هذا العمل

كما أتقدم بشكري الخالص إلى الأستاذ المشرف عبد الرحيم لحرش الذي أفادني بتوجيهاته ونصائحه جزاها الله ألف خير.

كما أتوجه بجزيل الشكر

الى جميع أساتذة قسم الحقوق اذ كان لنا الشرف العظيم في تعلمنا على أيديهم.

الى كل من ساعدني من قريب أو من بعيد في انجاز هذا البحث ولو بالكلمة طيبة

✍ **فريد، مسعود.**

إهـــــداء

إلهي لا يطيب الا بشكرك ولا يطيب النهار الا بطاعتك..

ولا تطيب اللحظات الا بذكرك..

ولا تطيب الآخرة الا بعفوك.. ولا تطيب الجنة الا برؤيتك الله جل جلاله

الى من بلغ الرسالة وأدى الأمانة..

ونصح الامة.. الى نبي الرحمة ونور العالمين..

سيدنا محمد صلى الله عليه وسلم

الى كل من كانوا سندا لي في الحياة والدي وأصدقائي وأساتذتي

أهدي هذا العمل المتواضع

✍ فريد

إهـــــــداء

الى صاحب السيرة العطرة، والفكر المستنير، فلقد كان له الفضل الأول في بلوغي التعليم العالي والدي الحبيب، أطال الله في عمره،

الى من وضعتني على طريق الحياة، وجعلتني رابط الجأش، وراعتني حتى صرت كبيرا امي الغالية، طيب الله ثراها

الى جميع أساتذتي الكرام، ممن لم يتوانوا في مد يد العون لي

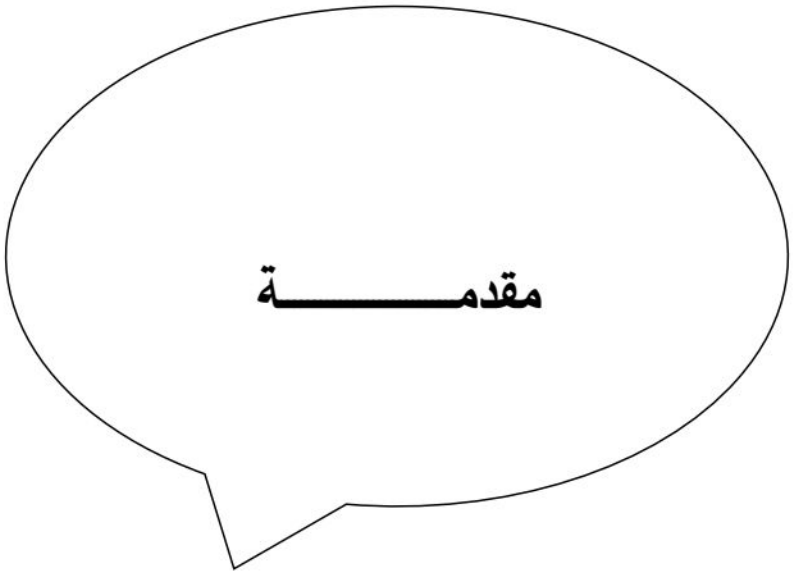
أهدي إليكم بحثي.

✍ مسعود

قائمة الرموز والمختصرات

باللغة العربية

- ✓ ق إ ج ج: قانون الإجراءات الجزائية الجزائري.
- ✓ ج ر: الجريدة الرسمية.
- ✓ مج: مجلد
- ✓ ع: عدد
- ✓ ص: الصفحة.
- ✓ د س ن: دون سنة نشر.
- ✓ د ب ن: دون بلد نشر.


مقدمـــــــــة

مقدمـــــــة

لقد حقق العالم تقدما تكنولوجيا ضـــخما في مجال المعلوماتية، شـــمل مختلف القطاعات فيها القطـاع القانوني، بغية حماية القانون والقاعدة القانونية من التغيير أو الحذف، وكذا حماية أمن الأفراد. حيث ســـعى المجتمع الدولي لتوظيف هذا التقدم التكنولوجي بوضـــعه لطرق مميزة للاسـتفادة منه. غير أن هذا التوظيف لم يكن مطلقا، بل فرضـت عليه قيود تهدف أسـاسـا الى حماية أمن الدول وأفرادها.

الأمن القانوني هو مبدأ من مبادئ القانون، يقوم على ضـــمان وضـــوح القواعد القانونية واستقرارها، وتوفير الحماية القانونية للأفراد ضد أي تعسف أو غموض في التطبيق. إلا أن هذا المبدأ يتطلب جملة من الشـــروط، من بينها أن يكون القانون مفهوما يمكن التنبؤ به، ومعياري، مستمدا من القانون الطبيعي للسلامة والاستقرار.

وفي ظل بروز البيئة الرقمية واجه هذا المبدأ تحديات كبرى اوجبت تأطير تكنولوجيات الاعلام والاتصال بأطر قانونية وتشريعية حديثة وفعالة.

ولمواجهة هذه التحديات، ســـعت العديد من الدول بما فيها العربية والغربية، الى تطوير اســـتراتيجيات وطنية لحماية القضـــاء الرقمي، بما يحوي من بيانات ومعاملات، في شـــكل تشريعات متخصصة في الامن السيبراني، وابرام اتفاقيات إقليمية ودولية، لتعزيز التعاون الدولي وضمان الحماية القانونية في العالم.

تنبع أهمية هذا الموضوع في ارتباطه المباشر بحياة الافراد وحقوقهم في ظل ما يشهده العالم من تزايد في الجرائم في المجال الرقمي، وتنامي الاعتماد على الأنظمة الرقمية في إدارة الشـــأن العام. بما في ذلك القطاعات القضـائية والإدارية. كما كان لتطور تكنولوجيا الاعلام والاتصـال دور كبير في ظهور بيئة رقمية، فرضـــت على مبدأ الامن القانوني، اســـتدعى ضـــرورة وجود تأطير قانوني محكم لحماية الحقوق والحريات الأساسية.

مقدمـــــــة

وجاء اختيار موضـــوع " مبدأ الأمن القانوني في الفضـــاء الرقمي" اســـتجابة لعدة اعتبارات علمية وواقعية، أبرزها:

- التحول الرقمي المتسارع الذي يشهده العالم في مجال تكنولوجيا الاعلام والاتصال
- الحاجة الضـــرورية لتحديث الأطر القانونية، لضـــمان اســـتقرار القواعد القانونية وحماية المتقاضين في البيئة الرقمية.
- الوقوف على القصور الذي تعانيه بعض التشريعات الوطنية في مواجهة التحديات التقنية الجديدة، مما يهدد مبدأ الامن القانوني ويضعف ثقة المواطن في قضائه.
- أهمية تعزيز التعاون الدولي والإقليمي في مجال الامن الرقمي القانوني، لحماية الأنظمة القضائية من التهديدات العابرة للحدود.

يهدف هذا الموضـــوع الى تفكيك مبدأ الامن القانوني الى العناصـــر المشـــكلة له، وإبراز قيمته القانونية في الوقت الراهن.

تناولت العديد من الدراســـات الاكاديمية في الســـنوات الأخيرة قضـــايا التحول الرقمي وأثره على الأنظمة القانونية، نذكر منها:

- "زهدور إنجي هند نجوى ريم ســـــندس، **اســـــتراتيجيات الوقاية القانونية والأمنية من الأمن الرقمي**، المجلة الدولية لنشـــــر البحوث والدراســـــات، مج2، ع16، كلية الحقوق والعلوم السياسية، جامعة محمد بن أحمد، وهران، الجزائر، فبراير 2021، حيث تناولت مبحثين الأول التكنولوجيا الرقمية الآمنة ضـد المد الإجرامي الالكتروني، والمبحث الثاني المواجهة الدولية والجزائرية لتعزيز الأمن الرقمي.
- بن شـــــعاعة حليمة، شـــــنين ســـــناء، **أثر التطور التكنولوجي على تحقيق مبدأ الأمن القانوني وأهم التحديات التي تعترضـــــه**، جامعة قاصـــــدي مرباح، ورقلة، جامعة عمار ثليجي بـالأغواط، د س ن، حيـث تنـاولـت الـدراســـــة في المبحـث الأول أثر التطور

التكنولوجي على تحقيق مبدأ الأمن القانوني، وفي المبحث الثاني التحديات التي تعترض تحقيق مبدأ الأمن القانوني.

واجه هذا الموضوع العديد من التحديات والصعوبات، أبرزها:

- حداثة الموضـــوع وقلة الدراســـات المتخصـــصـــة التي تناولته بعمق، شـكلت عائقا في الحصول على معلومات يستند اليها
- تفاوت مســـتويات النضـــج القانوني في التعامل مع التحول الرقمي بين الدول، صـــعب اجراء مقارنات دقيقة ومتكافئة
- صـــعوبة فهم المصـــطلحات لتداخل الجوانب القانونية بالتقنية، خصـــوصـــا في مجال الرقمنة.

أصبحت تكنولوجيا الاعلام والاتصال في الوقت الراهن أداة أساسية لتسيير الشأن العام، وتعزيز فعالية الأداء القانوني في البيئة الرقميةـــ ما صعب تحقيق الامن القانوني الذي واجهته تحديات في تكييف التشريعات، وعلى هذا الأساس يطرح الموضوع التساؤل الاتي:

الى أي مدى تســاهم تكنولوجيا الاعلام والاتصــال في تحقيق الأمن القانوني في العصــر الرقمي؟ وما هي فعالية الاســتراتيجيات والتشــريعات المعتمدة في حماية الفضــاء الرقمي على المستوى الدولي؟

وتندرج ضمن هذه الإشكالية أسئلة فرعية:

- ما هو مفهوم الأمن القانوني؟ وما علاقته باستخدام تكنولوجيا الإعلام والاتصال؟
- ما هي إجراءات الحماية القانونية المعتمدة لتحقيق الأمن القانوني في العصر الرقمي؟
- ما هي أبرز الاستراتيجيات الدولية لحماية الفضاء الرقمي؟
- ما دور الاتفاقيات والمؤسسات المتخصصة في تعزيز الأمن الرقمي في العالم العربي؟
- ما هي الاستراتيجيات التقنية والأمنية المتبعة لتعزيز الأمن الرقمي في الدول العربية؟

مقدمـــــة

- ما الأطر القانونية المعتمدة في الدول الغربية لحماية الفضاء الرقمي؟

نظرا لأن الموضوع "مبدأ الأمن القانوني في الفضاء الرقمي" هو فكرة قانونية بطبعها، تعمل ضمن بيئة تكنولوجيا حديثة ودقيقة، توجب علينا استعمال مناهج للبحث:

المنهج الوصـــفي التحليلي: الهدف منه اظهار الأفكار الرئيســـية لمبدأ الأمن القانوني وإطاره النظري والقـانوني في المجـال التقليـدي، ثم نقـل النتـائج إلى المجـال الرقمي وعرض النتـائج القانونية.

كذلك المنهج المقارن: الذي قورنت من خلاله القوانين والاســـتراتيجيات الرقمية التي أقرت في الدول الغربية والعربية لتوجيه الأمن القانوني في الفضـــاء الرقمي، وقُدمت الأمثلة التي بينت الفروق والتكامل في النتائج. وأيضـاً اسـتخدم المنهج النقدي، حيث جرى تحليل كل النصـوص القانونية.

بغرض الإلمام بجميع جوانب الموضوع اعتمدنا الخطة التالية: أين قمنا بتقسيم موضوع الدراسة إلى فصلين: الفصل الأول تحت عنوان **تكنولوجيا الاعلام والاتصال لتحقيق الامن القانوني** حيث قمنا بتقسيمه إلى مبحثين. المبحث الأول استعمال تكنولوجيا الإعلام والاتصال لتحقيق الأمن القانوني أما المبحث الثاني مصادر تهديد الخصوصية الرقمية.

أما الفصل الثاني فاخترنا له عنوان **إستراتيجية الدول لحماية الفضاء الرقمي**، وقمنا بتقسيمه إلى مبحثين: المبحث الأول الإستراتيجية المتبعة في الدول العربية، أما المبحث الثاني استراتيجية الوقاية القانونية من مهددات الأمن الرقمي .

الفصل الأول

تكنولوجيا الاعلام والاتصال

لتحقيق الامن القانوني

شهد العالم في العقود الأخيرة طفرة هائلة في تكنولوجيا الإعلام والاتصال، حيث أصبحت وسائل الاتصال الحديثة والإنترنت ركيزة أساسية في مختلف المجالات الاقتصادية والاجتماعية والسياسية، ولقد غيرت هذه التكنولوجيا طريقة تفاعل الأفراد مع بعضهم البعض، وساهمت في تسهيل المعاملات التجارية، وتعزيز حرية التعبير، ونشر المعرفة على نطاق واسع. ومع ذلك، فإن هذا التطور السريع رافقه العديد من التحديات القانونية والأمنية التي تهدد استقرار المجتمعات الرقمية وحقوق الأفراد والمؤسسات، ولعل أبرز هذه التحديات هي الحاجة إلى تحقيق الأمن القانوني، وهو مفهوم يشير إلى ضرورة ضمان وضوح القوانين واستقرارها، بحيث يتمكن الأفراد والجهات الفاعلة من التنبؤ بنتائج أفعالهم القانونية في البيئة الرقمية. فمع تزايد الجرائم الإلكترونية، مثل الاختراقات، وسرقة البيانات، والاحتيال الإلكتروني، والتضليل الإعلامي، برزت الحاجة إلى تطوير سياسات وتشريعات تكفل الحماية القانونية للأفراد والمؤسسات.

علاوة على ذلك، فإن حماية الفضاء الرقمي أصبحت قضية عالمية تتطلب تعاونًا دوليًا، حيث تبنت الدول المختلفة استراتيجيات متباينة لمواجهة التهديدات السيبرانية. ففي الدول الغربية، مثل الولايات المتحدة والاتحاد الأوروبي، تم وضع تشريعات صارمة وتعزيز البنية التحتية الأمنية لمكافحة الجرائم الرقمية وحماية حقوق المستخدمين. أما في الدول العربية، فإن الجهود لا تزال في طور التطوير، حيث تسعى الحكومات إلى بناء أطر قانونية وتنظيمية فعالة تتناسب مع طبيعة التحديات الرقمية المتزايدة.

بناءً على ذلك، يهدف هذا الفصل إلى دراسة العلاقة بين تكنولوجيا الإعلام والاتصال وتحقيق الأمن القانوني، من خلال استعراض مفهوم الأمن القانوني، والتدابير المتخذة لحماية الفضاء الرقمي. كما سيتم تحليل الاستراتيجيات الدولية في هذا المجال، مع التركيز على الفروقات بين الدول الغربية والعربية في التعامل مع المخاطر الأمنية والتحديات القانونية في البيئة الرقمية.

المبحث الأول: استعمال تكنولوجيا الإعلام والاتصال لتحقيق الأمن القانوني

في ظل التحولات الرقمية المتسارعة، بات من الضروري مواكبة التغيرات التي فرضتها تكنولوجيا الإعلام والاتصال على المنظومة القانونية، خاصة ما يتعلق بتحقيق الأمن القانوني. إذ يُعدّ هذا الأخير ركيزة لضمان استقرار العلاقات القانونية وشفافية المعاملات، ويزداد دوره أهمية مع توسّع استخدام الوسائل الرقمية. وعليه، يتناول هذا المبحث مفهوم الأمن القانوني، ثم يستعرض مختلف الإجراءات التقنية والقانونية التي تُعتمد لحمايته في بيئة رقمية متطورة.

المطلب الأول: التطور التكنولوجي وأثره على مبدأ الأمن القانوني

من المعروف أن مفهوم الأمن القانوني ليس من المفاهيم المتفق عليها بصورة موحدة، وبالتالي فإنه من الصعب إعطاء تعريفا محددا لما يتصف به من سمة التغيير فهو ليس مفهوما جامدا بل يرتبط مفهومه بتطور الظروف والأوضاع والعوامل المحلية والدولية، وكذا حاجات المجتمع المتجددة.[1]

الفرع الأول: مفهوم الأمن القانوني

لعل التعريف المتفق عليه لمبدأ الأمن القانوني هو الذي يقصد به وجود نوع من الثبات النسبي للعلاقات القانونية واستقرار المراكز القانونية لغرض إشاعة الأمن والطمأنينة بين أطراف العلاقات القانونية سواء أكانت أشخاصا قانونية خاصة أو عامة، حيث تستطيع هذه الأطراف ترتيب أوضاعها وفقا للقواعد القانونية القائمة وفق مباشرتها لأعمالها دون أن تتعرض المفاجآت أو أعمال لم تكن في الحسبان وهي صادرة عن إحدى سلطات الدولة. ويكون من شأنها زعزعة ركن الاستقرار والاطمئنان بالدولة وقوانينها[2].

[1]. جاوزني اسماعيل، **الأمن القانوني وعناصرها**، مجلة تحولات العدد الثاني جوان 2001، ص 191.

[2]. الخداري عبد الحق، **مبدأ الأمن القانوني ودوره في حماية حقوق الانسان**، مجلة الحقيقة، سنة 2016، ص 223.

أولا: التعريف الفقهي للأمن القانوني

يتفق الفقهاء بأن فكرة الأمن القانوني يصعب حصرها لسعة المجالات التي تتعلق بها، إذ أنها تختلف من مجتمع إلى آخر، فقد ذهب بعضهم إلى تعريف بأنه "معرفة الأفراد لمراكزهم القانونية على نحو دقيق ومؤكد وواضح، إذ يمكنهم ذلك من معرفة ما لهم من حقوق وما عليهم من واجبات، وهو ما يتيح لهم التصرف باطمئنان استنادا إليها دون خوف أو قلق من نتائج هذا التصرف في المستقبل"[1].

ثانيا: التعريف القضائي للأمن القانوني

باعتبار أن مبدأ الأمن القانوني مبدأ دولي، عرفته المحكمة الأوروبية لحقوق الإنسان والتي أكدت على ضرورة صياغة القانون بدرجة تمكن الشخص المعني من توقع النتائج المترتبة عن نشاط معين، أما مجلس الدولة الفرنسي فقد عرفه بأنه: "مبدأ يقضي أن يكون المواطنون، دون عناء كبير، في مستوى تحديد ما هو مباح وما هو ممنوع من طرف القانون المطبق وللوصول إلى هذه النتيجة، يتعين أن تكون القواعد المقررة واضحة، ومفهومة، وألا تخضع في الزمان إلى تغييرات متكررة أو غير متوقعة"[2].

ثالثا: خصائص الأمن القانوني

يمتاز مبدأ الأمن القانون بخصائص نذكرها فيما يلي:

1. مبدأ العمومية والطبيعة الآمرة

المقصود بالعمومية التوجه خطابها إلى الكافة، فلا تقتصر على شخص معين بالذات، ولا تصدر بشأن رابطة معينة بالذات، مما يضمن عدم حصول أمان لفئة دون الأخرى، كما يقوم على الطابع الآمر أي أنه يطبق من طرف السلطة لعامة للدولة ويمتد حتى إلى القاضي الذي

[1]. سعدي بن علي بن حسن المعمري، رضوان أحمد الحاف، **مبدأ الأمن القانوني ومقومات الجودة التشريعية**، مجلة البحوث القانونية والاقتصادية، ع79، مارس 2022، ص14-15.

[2]. المرجع نفسه، ص16.

يحظر عليه المساس بمحتواه، ويسري على المشرع أيضا الذي يجد نفسه ملزما باحترام مبدأ الأمن القانوني وعدم الخروج عن مقتضياته[1].

2. المرونة والعالمية

طابع المرونة يظهر في التفاعل بين المشرع والمخاطب بالقانون أي أنه قابل للتغيير أي أنه لا يقتصر على المتطلبات الكلاسيكية مثل حماية الحقوق المكتسبة إنما يمتد إلى حماية التوقعات المشروعة تحت مسمى "مرونة المبدأ القانوني"، كما يتصف بالطابع الدولي من خلال اتجاه جل الدول إلى اعتباره منطلقا أساسي في تحقيق الاستقرار وضمانه وذلك بالنص ليه ضمن التشريعات الدولية[2].

3. الثبات والديمومة

يظهر ذلك من خلال استقرار القاعدة القانونية ووضوحها، وديمومتها وثباتها، على الأقل إبقاء الدول لقوانينها فترة معينة من الزمن دون مفاجأة مواطنيها في التعديل كل مرة، أو إصدارها لقانون يمس علاقاتهم، مما ينجم عنه عدم استقرار[3].

الفرع الثاني: دور التكنولوجيا في تطوير القانون

على إثر التطور التكنولوجي الحاصل في العالم ظهرت نصوص قانونية تنظم آثار التقنيات الحديثة في شتى المجالات، سواء الاقتصادي أو الاجتماعي أو السياسي وحتى الثقافي، ما اصطلح عليه قوننة التكنولوجيا.

---

[1]. أفتيسان وريدة، بن ناصر وهيبة، **دسترة مبدأ الأمن القانوني: التجربة الجزائرية نموذجا**، مدلة الدراسات القانونية (صنف ج)، مج 08، ع02، جامعة يحي فارس المدية، الجزائر، 2015، ص975-976.

[2]. المرجع نفسه، ص977.

[3]. المرجع نفسه.

أولا: توجه النصوص القانونية نحو التقنيات الحديثة

لقد ساهم التطور التكنولوجي في تغيير هام في نصوص القانون من حيث الوظيفة التي تؤديها، حيث تغيرت عما كانت عليه باعتبارها قواعد آمرة ومكملة، بل ظهر نوع آخر كالنصوص ذات الطابع التقني مثل قوانين التجارة الالكترونية وقانون الانتخاب الالكتروني[1]، وقد نتج عن ذلك التطور ظهور العديد من المجالات الجديدة كالحق في حماية المعطيات الشخصية، وتجريم التعسف في استعمال وسائط الاتصال الحديثة، وقانون الملكية الفكرية، وقانون التجارة الالكترونية[2].

ثانيا: علم التنظيم

لم تصبح مهمة النصوص القانونية البت في مختلف الخصومات التي تقع بين الأفراد بل تعدت ذلك وأصبحت تعالج مختلف المراكز القانونية التي يحتلها الفرد، ويعد رد فعل الفرد من مختلف العوامل كوسائل التواصل الاجتماعي، فالتطور التكنولوجي له سلبيات يمكن أن تؤثر على عمل القاضي وقت بته في الدعوى، أين يجد نفسه مجبرا على التماشي مع مختلف التطورات التكنولوجية[3].

الفرع الثالث: ارتباط الأمن القانوني بالأمن التقني مظهر من مظاهر التكنولوجيا

الكلام عن موضوع التطور التكنولوجي ودوره في توفير الأمن القانوني يمنح للأشخاص الثقة ويشجعهم على إبرام التصرفات الالكترونية، ولا يكون إلا بالإلمام بمختلف الضوابط الالكترونية التي تبعث الثقة في محتوى التصرف الالكتروني، عن طريق ربط التصرفات القانونية مع الأشخاص الصادرة عنهم، كما تساهم وسائل التطور التكنولوجي في تطور المصطلحات

---

[1]. بوجمعة فاطمة الزهراء، **تأثير التطور التكنولوجي وتقنيات المعلومات على تحقيق الأمن القانوني**، مجلة الفكر المتوسطي، مج11، ع01، الجزائر، 2002، ص469.

[2]. عجة الجيلالي، **مدخل للعلوم القانونية، نظرية القانون**، ج1، برتي، الجزائر، 2009، ص181.

[3]. شعاعة حليمة، شنين سناء، **أثر التطور التكنولوجي على تحقيق مبدأ الأمن القانوني وأهم التحديات التي تعترضه**، جامعة قاصدي مرباح، ورقلة، جامعة عمار ثليجي بالأغواط، د س ن، ص5.

القانونية[1]، إن الهدف من ربط النصوص القانونية بالتطور التكنولوجي تأمين وحماية محتوى الوسائط الالكترونية والذي لا يتحقق إلا بتحدي النصوص القانونية للأخطار المسيطرة على الوضع في المواقع الافتراضية[2].

المطلب الثاني: الخصوصية المعلوماتية والفضاء الرقمي

يُعدّ الأمن القانوني من الركائز الأساسية لاستقرار المجتمعات، حيث يضمن وضوح القوانين واستقرارها، مما يسهم في تعزيز الثقة بين الأفراد والمؤسسات، ومع التطور التكنولوجي السريع ازدادت الحاجة إلى تبني إجراءات حماية متقدمة للحفاظ على هذا الأمن في البيئة الرقمية.[3]ومن بين هذه الإجراءات، تأتي القوانين والتشريعات الرقمية التي تواكب التحديات الحديثة، مثل قانون حماية البيانات الشخصية (GDPR)، إلى جانب تعزيز العقوبات على الجرائم السيبرانية، وإلزام الشركات بالشفافية، وإنشاء هيئات رقابية مختصة لمراقبة الامتثال للقوانين الرقمية. وبالإضافة إلى الإجراءات القانونية، تعتمد الدول على تقنيات متطورة لتعزيز الأمن، مثل تشفير البيانات لحمايتها من الاختراق، واستخدام الذكاء الاصطناعي لرصد التهديدات، وتطوير أنظمة المصادقة والأمان كالمصادقة الثنائية والقياسات الحيوية، إلى جانب برامج الحماية من الفيروسات والهجمات السيبرانية.[4]

الفرع الأول: الحق في الخصوصية المعلوماتية والمخاطر التي تواجهه

سنتطرق إلى مفهوم الخصوصية المعلوماتية والمخاطر الاتي تواجهها في البيئة الالكترونية.

---

[1]. كنوفي وسيلة، **جدلية القانون والتكنولوجيا بين التكامل والتحايل**، المجلة الجزائرية للعلوم القانونية والسياسية، مج57، ع5، الجزائر، 2020، ص86.

[2]. بن شعاعة حليمة، شنين سناء، مرجع سابق، ص8.

[3]. عبد العزيز الغنام، **الأمن السيبراني وحماية البيانات في العصر الرقمي**، دار الفكر العربي، 2022، ص. 35.

[4]. مسعودي هشام، آراء **الفكر القانوني حول مصطلح الأمن القانوني دراسة في الإشكالية والمفهوم**، مجلة الاجتهاد القضائي، مج12، ع 02، مخبر أثر الاجتهاد القضائي على حركة التشريع، جامعة محمد خيضر، بسكرة، أكتوبر 2020، ص69.

أولا: مفهوم الحق في الخصوصية المعلوماتية

لقد نصت الدساتير والشرائع على الحق في الخصوصية وصنفته من بين الحقوق الأساسية الملازمة للشخص الطبيعي، وهو حق الفرد في تقرير متى وإلى أي حد يمكن اطلاع الغير على شؤونه الخاصة، ويمكن القول بأن الحق في الحياة الخاصة يهدف إلى حماية جميع المعلومات المتعلقة بهوية الإنسان وخصوصياته ومسكنه ومراسلاته واتصالاته وأسراره، ولا يحق لأي أحد اختراقها إلا بصورة مشروعة أي في الحالات التي ينص عليها القانون[1].

ثانيا: المخاطر التي تواجه الخصوصية في الفضاء الرقمي

يمكن إجمال هذه المخاطر فيما يلي:

1. الحرص على الاهتمام بالملفات الشخصية

تحرص الدول على الاهتمام بالملفات الشخصية كالهوية وجواز السفر والإقامة وغيرها، وتدون في سجلات تسير من قبل الإدارة الحكومية، بحيث تسجل فيها البيانات الشخصية كالاسم ومحل الإقامة وتاريخ الميلاد واسم العائلة، كما تحفظ أجهزة الأمن سجلات الجرائم، وتدون تلك المعلومات على ورق يتم حفظه بالأرشيف ولا تكشف إلا لأشخاص محددين بطلب رسمي ولأهداف واضحة، لكن في الآونة الأخيرة والتحول إلى الرقمية التي جعلت من البيانات الشخصية قابلة للنسخ والتوزيع والتبادل بكل يسر، وبرزت معه مخاطر معالجة البيانات الكترونيا، ما دفع بالدول الأوروبية إلى تقنين استعمال البيانات الشخصية من قبل الإدارات الحكومية والشركات الكبرى، وذلك لخوفهم من استعمالها بشكر مضر[2].

---

[1]. علال نزيهة، **الإطار القانوني لحماية المعطيات ذات الطابع الشخصي في الفضاء الالكتروني في ظل القانون رقم 18-07**، دائرة البحوث والدراسات القانونية والسياسية، مج04، ع2، المركز الجامعي مرسلي عبد الله، تيبازة، الجزائر، 2020، ص54.

[2]. علال نزيهة، المرجع نفسه، ص55.

2. انتشار النقل الرقمي للبيانات

لما أصبحت المعلومات تنقل بشكل رقمي مما سهل عملية التجسس الالكتروني، لعدم قدرة شبكات الاتصال على توفير الأمان المطلق لسرية ما ينقل عبرها من بيانات، وإمكانية استخدام الشبكات في الحصول على المشروع على المعلومات عن بعد، وبالرغم من التقدم التكنولوجي إلا أن تقارير الخصوصية سلمت بأن حياة الأفراد وأسرارهم في البيئة الرقمية معرضة للاعتداء في ظل عدم تكامل حلقات الحماية[1].

3. من الناحية الاقتصادية

لقد أصبحت البيانات تغذي الابتكار في معظم القطاعات الصناعية، والتجارية الخدماتية، فعملية معالجتها تخدم الأداء وتزيد من الإنتاجية في كافة قطاعات الدولة، وظهرت أهمية الإدارة الفاعلة على تطوير الأنظمة والتطبيقات لتحسين نوعية الحياة وتحقيق الأرباح الاقتصادية، فقد أدركت الشركات أن البيانات الشخصية أصبحت ذهب العصر، فقامت بجمع البيانات الشخصية ومعالجتها والإشراف عليها واستثمارها بما يعود عليها بالنفع، ومساعدتها للوصول إلى أسواق جديدة، ومنه ظهر الخطر بما اصطلح عليه بتجارة البيانات الشخصية واستخدام البيانات للوصول إلى الأفراد واستهدافهم بالإعلانات الترويجية، ولعل الأخطر من ذلك الاعتداء على الأشخاص والأموال في عمليات احتيال مصرفية[2].

الفرع الثاني: معالجة البيانات ذات الطابع الشخصي

سنتطرق إلى مفهوم البيانات الشخصية ومعالجتها.

أولا: مفهوم المعطيات ذات الطابع الشخصي

عرفها القانون الجزائري بأنها كل معلومة متعلقة بشخص معرف أو قابل للتعريف "الشخص المعني" بصفة مباشرة أو غير مباشرة، بالرجوع إلى رقم التعريف أو عنصر أو عدة

[1]. علال نزيهة، المرجع السابق، ص55.

[2]. جبور منى الأشقر، جبور محمد، **البيانات الشخصية والقوانين العربية، الهم الأمني وحقوق الأفراد**، ط1، المركز العربي للبحوث القانونية والقضائية، لبنان، 2018، ص12.

عناصر تخص هويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية[1].

أما الشرع المغربي فقد عرف المعطيات ذات الطابع الشخصي بأنها كل معلومة كيف كان نوعها بما في ذلك الصورة والصوت المتعلقة بشخص ذاتي معرف أو قابل للتعرف عليه أو ما يطلق عليه "بالشخص المعني"[2]، أما بالنسبة للمشرع التونسي فقد عرفها بأنها كل البيانات مهما كان مصدرها أو شكلها التي تجعل من الشخص الطبيعي معرفا أو قابلا للتعريف باستثناء المعلومات المتصلة بالحياة العامة والمعتبرة قانونا[3].

ثانيا: مفهوم المعالجة الآلية للمعطيات ذات الطابع الشخصي

جاء في الفقرة 3 من المادة 3 من القانون 18-07 أن: "كل عملية أو مجموعة عمليات منجزة بطرق أو وسائل آلية أو بدونها على معطيات ذات طابع شخصي، مثل الجمع أو التسجيل أو التنظيم أو الحفظ أو الملائمة أو التغيير أو الاستخراج أو الاطلاع أو الاستعمال أو الإيصال عن طريق الإرسال أو النشر أو أي شكل آخر من أشكال الإتاحة أو التقريب أو الربط البيئي وكذا الإغلاق أو التشفير أو المسح أو الإتلاف".

كما عرفها المشرع التونسي بأنها العمليات المنجزة سواء بطريقة آلية أو يدوية من طرف شخص طبيعي أو معنوي هدفها جمع المعطيات الشخصية أو تسجيلها أو تنظيمها أو تغييرها أو

---

[1]. المادة **3 ف1**، القانون رقم **18-07**، المؤرخ في **25** رمضان عام **1439هـ**، الموافق **10** يونيو سنة **2018**، **يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي**، ج ر ع **34**، الصادرة بتاريخ **25** رمضان **1439هـ**، الموافق **10** يونيو سنة **2018**.

[2]. القانون المغربي رقم **08-09**، **يتعلق بحماية الأشخاص الذاتيين اتجاه معالجة المعطيات ذات الطابع الشخصي**، ج ر **5711**، بتاريخ **23** فبراير **2009**، ص52.

[3]. قانون تونسي أساسي، ع **63**، المؤرخ في **27** جويلية **2004**، **يتعلق بحماية المعطيات الشخصية**، الفصل4، ص2.

استغلالها أو استعمالها أو إرسالها أو نشرها أو إتلافها أو الاطلاع عليها وحتى جمع البيانات المتعلقة باستغلال قواعد البيانات أو الفهارس والسجلات أو البطاقات أو الربط البيني[1].

المبحث الثاني: مصادر تهديد الخصوصية الرقمية

مع تزايد التهديدات السيبرانية، باتت حماية الفضاء الرقمي أولوية دولية تستدعي تنسيق الجهود بين الدول. وقد عملت عدة أطراف، خاصة في الغرب، على تطوير استراتيجيات فعالة لضمان الأمن السيبراني ومواجهة المخاطر الرقمية.

المطلب الأول: اختراق النظم المعلوماتية

أصبحت التقنيات الجديدة تقدم العديد من الإيجابيات للخصوصية، إلا أنها تحمل في ثناياها العديد من المخاطر مع الحجم الهائل من المواد الالكترونية المتعلقة بالحياة الخاصة للناس والمخزنة ضمن تلك التقنيات، حيث أن وضع حماية لتلك الخصوصية يجب أن يراعى فيه استخدام تقنيات جديدة.

الفرع الأول: الدخول غير المشروع للنظام

يقصد به الاعتداء على وسائل الاتصال بالانترنت والتي تعتبر من قبيل نوعية الاختراق والتي تبدأ بالدخول إلى المعطيات الشخصية المخزنة في القرص الصلب الذي يحفظ فيه ويخزن ما يتم تحميله من على شبكة الانترنت وانتهاكها، ويفترض الدخول غير المشروع حدوث اتصال بين الفرد في العالم المادي والانترنت مما يستلزم الحصول على كلمة المرور[2] ويأخذ ثلاثة صور وهي:

- الدخول غير المشروع.
- الدخول غير المشروع بقصد ارتكاب جرائم.

---

[1]. القانون التونسي المتعلق بحماية المعطيات الشخصية، مصدر سابق.

[2]. فضل سليمان أحمد، **المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية**، دار النهضة العربية، القاهرة، 2013، ص314.

- التعديل غير المشروع.

يصـــطلح عليه الاختراق، هنا يقوم المخترق بجمع المعلومات التي تتمثل في عنوان IP التابع للسيرفر الذي يحتوي الموقع المستهدف، زيادة على جمع أسماء السكيرابتات المركبة في الموقع ويقوم بفحصـها وفي حالة وجود ثغرات برمجية فيها تسمح للهاكرز بفعل أشياء ممنوعة فالهجوم هو مرحلة اســتغلال الثغرات ويكون غالبا على شــكل روابط، منها يقوم الهاكرز بالدخول إلى لوحة تحكم المدير أو تطبيق الأوامر على الســيرفر أو رفع ملفات كالشــل[1]، ويمكن للمخترق التعرف على أي مستخدم على شبكة الانترنت من خلال برامج التجسس[2].

الفرع الثاني: التلصص

قبل ظهور الانترنت كان من الصعب قيام شخص بالتلصص على بريد شخص آخر وهو في منزله لم يتحرك، أو أن يسـتخدم اسـما مسـتعارا أو يوقع به، أو أن يتخل في موضــع شخص آخر إلا أنه مع الثورة تكنولوجيا المعلومات والانترنت مما أعطى مجالا أوسع لاستخدام الانتحال في مجال الاسم بل وحتى الهيئة، حيث يطل الإنسـان يتعامل بصـفة محتال باسـتمرار وبدون مشكلة[3].

الفرع الثالث: الفيروسات

يعرف الفيروس بأنه برنامج مشــفر للحاســب الآلي يتم تصــميمه لغاية محددة وهي إلحاق أكبر ضرر ممكن بأنظمة الحاسب الآلي، يقدر على ربط نفسه ببرامج أخرى ويعيد إنشاء نفسه حتى يبدو أنه يتكاثر ويتوالد ذاتيا، وينتشر بسرعة كبيرة من نظام لآخر، إما بواسطة قرص

---

[1]. سليم وليد السيد، **ضمانات الخصوصية في الانترنت**، دار الجامعة الجديدة، الإسكندرية، 2012، ص208.

[2]. بوكرة رشيدة، **تحديات العصر الرقمي في مواجهة خطط حماية الحق في الخصوصية**، مجلة حقوق الإنسان والحريات العامة، (م.ح.إ.ح.ع)، مج07، ع02، جامعة مستغانم، 2022، ص73.

[3]. سليم وليد السيد، مرجع سابق، ص209.

ممغنط، أو عبر شبكة الاتصالات ويمكن أن ينتقل عبر الحدود من أي مكان في العالم، ويتمثل تأثيره على الخصوصية في أن يدمر المعطيات الشخصية[1].

المطلب الثاني: اعتراض ومراقبة الاتصالات

لقد حققت الابتكارات في مجال التكنولوجيا تأثيرا إيجابيا على حرية التعبير، وعززت المشـــاركة الديمقراطية والاتصـــالات الرقمية، وأدت إلى تحســـين قدرات الجهات الفاعلة الحكومية وغير الحكومية على مراقبة واعتراض الاتصالات وجمع كم هائل من المعطيات الشخصية.

الفرع الأول: تخصيص وحدات أمنية متخصصة في الجرائم السيبرانية

أنشأت العديد من الدول وحدات متخصصة في التحقيقات الرقمية ضمن أجهزتها الأمنية، بحيث تضـم خبراء في تحليل البيانات وتتبع الجرائم الإلكترونية، مما يسـهم في تحسـين سـرعة وكفاءة التعامل مع التهديدات السيبرانية[2].

تمثل المراكز الوطنية للأمن الســـيبراني حجر الأســـاس في حماية البنية التحتية الرقمية، حيث تعمل على تطوير سياسات واستراتيجيات فعالة لمواجهة التهديدات السيبرانية المتزايدة. في ظل التحول الرقمي المتســارع، أصــبح من الضــروري توفير آليات دفاعية متطورة لضــمان حماية البيانات والأنظمة الحساسة.

1. أبرز الجهود لتعزيز الأمن السيبراني

لعل من أبرز الجهود التي قامت بها الدول لتعزيز الامن الســـيبراني تطوير أنظمة دفاعية متقدمة، وتقديم الدعم التقني، إضافة إلى مراقبة وتحليل الهجمات السيبرانية.

أ. تطوير أنظمة دفاعية متقدمة

تعتمد الدول على تطوير تقنيات متقدمة مثل الذكاء الاصـطناعي والتعلم الآلي لرصـد الأنشـطة المشـبوهة والاسـتجابة للهجمات بسـرعة وكفاءة. تشـمل هذه الأنظمة جدران الحماية المتطورة،

---

[1]. بوكرة رشيدة، مرجع سابق، ص74.

[2]. مارك أندرسون، **الأمن السيبراني والسياسة العالمية**، جامعة أكسفورد، 2021، ص142.

وتحليل سلوك المستخدم، وأنظمة كشف التسلل التي تعمل في الزمن الحقيقي لمنع الاختراقات قبل حدوثها.

ب. تقديم الدعم التقني

تلعب المراكز الوطنية دورًا حيويًا في تقديم الدعم التقني والتدريبي للشركات والمؤسسات الحكومية لضمان الامتثال لمعايير الأمن السيبراني. يشمل ذلك توفير الاستشارات، وتنفيذ اختبارات الاختراق، وإجراء تدريبات عملية لموظفي تكنولوجيا المعلومات لتعزيز قدرتهم على التعامل مع التهديدات السيبرانية بفعالية.

ج. مراقبة وتحليل الهجمات السيبرانية

تعمل المراكز على مراقبة النشاط السيبراني على مدار الساعة من خلال مراكز العمليات الأمنية (SOC)، حيث يتم تحليل الهجمات السيبرانية وتحديد أنماطها واتخاذ إجراءات وقائية لمنع وقوعها في المستقبل. تستخدم هذه المراكز تقنيات التحليل الجنائي الرقمي للكشف عن مصادر التهديدات وتحليل نقاط الضعف في الأنظمة المستهدفة[1].

نظرًا لأن التهديدات السيبرانية لا تعترف بالحدود، فإن التعاون الدولي أصبح ضرورة استراتيجية لمكافحة الجرائم الإلكترونية وحماية البنية التحتية الرقمية. يتطلب ذلك تنسيقًا واسع النطاق بين الدول والمنظمات الدولية لضمان استجابة فعالة للهجمات المتطورة.

2. أشكال التعاون الدولي في مجال الأمن السيبراني

تنوعت أشكال التعاون الدولي في مجال الأمن السيبراني، تمثلت في إبرام اتفاقيات تبادل المعلومات، ودعم مشاريع الأمن السيبراني العالمية، إضافة إلى التدريبات والمناورات السيبرانية المشتركة، وتعزيز التشريعات الدولية.

[1]. **تقرير الإتحاد الأوروبي حول إستراتيجية الأمن السيبراني**،2023، ص34.

أ. اتفاقيات تبادل المعلومات

تعمل الدول على توقيع اتفاقيات ثنائية ومتعددة الأطراف لتبادل المعلومات حول الهجمات السيبرانية وأساليب التصدي لها. تساهم هذه الاتفاقيات في تسريع الاستجابة للحوادث السيبرانية وتوفير بيانات استخباراتية دقيقة حول الجهات الفاعلة في التهديدات.

ب. دعم مشاريع الأمن السيبراني العالمية

تشارك الدول في تمويل ودعم المشاريع المتعلقة بالأمن السيبراني في منظمات مثل الأمم المتحدة والاتحاد الأوروبي، حيث يتم وضع أطر تنظيمية وسياسات دولية لتعزيز الأمن الرقمي. تشمل هذه الجهود توفير المساعدات التقنية للدول النامية، وتعزيز قدرات الاستجابة للحوادث السيبرانية على المستوى العالمي[1].

ج. التدريبات والمناورات السيبرانية المشتركة

تنظم الدول تحالفات أمنية لتنفيذ مناورات سيبرانية تحاكي الهجمات الحقيقية، مما يساعد على اختبار جاهزية الفرق الأمنية وتحسين التنسيق بين الجهات المختصة. تهدف هذه التدريبات إلى تطوير استراتيجيات دفاعية أكثر تكيفًا مع التهديدات المستجدة.

د. تعزيز التشريعات الدولية

يسهم التعاون الدولي في وضع تشريعات موحدة لمكافحة الجرائم السيبرانية، مما يسهل ملاحقة المجرمين الرقميين قانونيًا وتقديمهم للعدالة، خاصة في ظل تزايد الهجمات التي تستهدف البنى التحتية الحيوية مثل القطاعات المالية والطاقة.[2]

يمثل تعزيز الأمن السيبراني والتعاون الدولي ركيزتين أساسيتين في مواجهة التهديدات الرقمية المتزايدة.

---

[1]. أحمد سمير، **الجرائم الإلكترونية: الأبعاد القانونية والتقنية**، دار الفكر القانوني، 2020، ص95.

[2]. **تقرير الأمم المتحدة عن الجريمة السيبرانية**، 2022، ص57.

من خلال تطوير أنظمة دفاعية متقدمة، ودعم المؤسسات، وتحليل الهجمات، إلى جانب تعزيز التعاون بين الدول عبر اتفاقيات تبادل المعلومات والمناورات المشتركة، يمكن بناء بيئة سيبرانية أكثر أمانًا واستدامة.

الفرع الثاني: أبرز التشريعات والمبادرات الغربية

لعدل أن أغلب دول العالم بادرت إلى تعزيز الأمن السـيبراني من خلال إنشـاء مواقع وبرامج لذلك.

أ. اللائحة العامة لحماية البيانات (GDPR)

اللائحة العامة لحماية البيانات (General Data Protection Regulation – GDPR) هي أكثر القوانين صـرامة في مجال حماية البيانات، تبناها الاتحاد الأوروبي عام 2016 ودخلت حيز التنفيذ في مايو 2018، تنص على حماية البيانات على إرشادات صارمة بشأن جمعها ومعالجتها وتخزينها، وفض غرامة كبيرة في حالة عدم الامتثال[1].

ب. أهداف اللائحة

- تنظيم كيفية جمع ومعالجة وتخزين البيانات الشخصية داخل الاتحاد الأوروبي.
- فرض عقوبات مالية صارمة تصل إلى 20 مليون يورو أو 4% من الإيرادات السنوية العالمية لأي شركة تنتهك اللائحة.
- منح الأفراد حقوقًا موسعة مثل حق الوصول إلى بياناتهم الشخصية، حق المحو، وحق نقل البيانات[2].

[1]– معايير الأمن السيبراني: الولايات المتحدة الأمريكية وأوروبا والشرق الأوسط، منشورة على الموقع: https://ceinterim.com

[2]. **موقع الاتحاد الأوروبي–تفاصيل عن GDPR=https=//gdpr.ev.**

ج. التأثير العالمي للائحة GDPR

- أجبرت الشـــركات العالمية خارج أوروبا على الامتثال لمتطلباتها عند التعامل مع بيانات مواطني الاتحاد الأوروبي.
- ســـاهمت في اعتماد تشـــريعات مماثلة في العديد من الدول، مثل قانون خصـــوصـــية المستهلك في كاليفورنيا (CCPA) في الولايات المتحدة[1].

د. قانون الأمن السيبراني الأمريكي (CISA – 2018)

- أصـــــدرت الولايـات المتحـدة قـانون الأمن الســـيبراني (Cybersecurity and Infrastructure Security Agency Act – CISA) عام 2018، وهو يهدف إلى:
- إنشـــاء وكالة الأمن الســـيبراني وأمن البنية التحتية (CISA) لحماية شـــبكات وأنظمة المعلومات الحيوية.
- تعزيز التعاون بين الحكومة الفيدرالية والقطاع الخاص في مجال الأمن السيبراني.
- تطوير أنظمة متقدمة لرصد التهديدات الإلكترونية والاستجابة السريعة لها[2].

هـ. قانون الخدمات الرقمية (DSA) وقانون الأسواق الرقمية (DMA) – الاتحاد الأوروبي

- قانون الخدمات الرقمية (DSA – Digital Services Act) يهدف إلى:
- يهدف إلى محاربة الأخبار المضللة والمحتوى غير القانوني على المنصات الرقمية.
- زيادة الشفافية في استخدام البيانات من قبل شركات التكنولوجيا الكبرى.
- إلزام الشركات بالإفصاح عن آليات الإعلانات الموجهة والخوارزميات المستخدمة[3].

---

[1]. قائمة التحقق من الامتثال للائحة العامة لحماية البيانات (GDPR)، منشورة على الموقع: https://www.ibm.com .

[2]. بوصبع سلاف، **أثر سياسات الأمن السيبراني على الأمن القومي الأمريكي، قراءة في التجربة وفي إمكانية التطبيق على الحالة الجزائري**، مجلة السياسة العالمية، مج8، ع2، جامعة أمحمد بوقرة بومرداس، الجزائر، 2024، ص144.

[3]– مراعاة قانون الخدمات الرقمية (DSA)، منشور على الموقع: https://www.ad-dawra.com .

و. قانون الأسواق الرقمية (DMA – Digital MarketsAct) يركز على

- تنظيم عمل الشركات الرقمية الكبرى مثل جوجل، أمازون، وفيسبوك.
- منع الاحتكار وضمان بيئة تنافسية عادلة في الاقتصاد الرقمي.
- إجبار الشركات الكبيرة على منح المستخدمين مزيدًا من التحكم ببياناتهم[1].

الفرع الثالث: دور المنظمات الدولية في حماية الفضاء الرقمي

يتجلى دور المنظمات الدولية في حماية الفضاء الرقمي من خلال ما يلي:

أ. الاتحاد الأوروبي (EU)

-يعد الاتحاد الأوروبي من أبرز الجهات التنظيمية التي تضـــع معايير قانونية لحماية الفضـــاء الرقمي.

إلى جانب اللائحة العامة لحماية البيانات (GDPR)، يعمل الاتحاد على:

. إصدار استراتيجيات الأمن السيبراني الأوروبية لتعزيز حماية الشبكات الحيوية.

ـــــ إطلاق مبادرات مثل "سـايبرريزيلينس" (Cyber ResilienceAct) لزيادة صـلابة الأنظمة الرقمية ضد الهجمات السيبرانية[2].

ب. الأمم المتحدة (UN)

تلعب الأمم المتحدة دورًا محوريًا في تنسيق الجهود الدولية لحماية الفضاء الرقمي، من خلال:

ـــــ المكتب الدولي للأمن الســـيبراني (ITU – International Telecommunication Union)، الذي يضع معايير دولية للأمن السيبراني وتعزيز التعاون بين الدول[3].

ـــ "مجموعة العمل المفتوحة بشأن الأمن السيبراني" (OEWG – Open-endedWorking Group)، التي تسعى إلى إرساء قواعد دولية لمحاربة الجرائم السيبرانية.

---

[1]. قانون الأسواق الرقمية ما التزامات عمالقة التكنولوجيا في أوروبا؟ مقال منشور على الموقع: https://asharq.com.

[2]. موقع الإتحاد الدولي للاتصالات، **تقارير حول الأمن الرقمي** **https://www.itu.int** .

[3]. نادر أبو زيد، **التشفير والأمن السيبراني دراسة تحليلية**، مجلة دراسات الحماية الرقمية، ع 5، 2021، ص87.

ـ مشروع "مكافحة الجريمة السيبرانية" (Cybercrime Convention)، الذي يسعى إلى تعزيز التعاون في التحقيقات الإلكترونية والمحاكمات المرتبطة بالجرائم الرقمية[1].

تمثل السياسات الغربية في مجال الأمن الرقمي نموذجًا متقدمًا لحماية البيانات وتعزيز الأمن السيبراني. ومن خلال قوانين مثل GDPR في الاتحاد الأوروبي وCISA في الولايات المتحدة، إضافةً إلى الدور الفعّال للمنظمات الدولية، يتم تحسين مستوى الحماية الرقمية عالميًا. ومع ذلك، لا تزال التحديات قائمة، خاصة مع تطور أساليب الجرائم الإلكترونية والحاجة المستمرة لتحديث التشريعات واستراتيجيات الحماية.

[1]. نادر أبوزيد، المرجع السابق، ص88.

خلاصة الفصل الأول

يظهر مما تقدم أن تكنولوجيا الإعلام والاتصال قد أضحت حجر الزاوية في مسار إنجاز الأمن القانوني داخل البيئة الرقمية، لما توفره من أدوات فعالة في تيسير الوصول إلى القواعد القانونية والمعلومات القضائية، وتعزيز شفافية الإجراءات الإدارية والعدلية، وضمان دوام المرفق العام. وقد مكنت هذه التقنيات من تقليل الفجوة بين المواطن ومؤسسات الدولة، من خلال رقمنة المعاملات، وتوفير منصات إلكترونية تمكن الأفراد من ممارسة حقوقهم ومتابعة التزاماتهم القانونية بكفاءة وفاعلية.

بيد أن هذا التحول الرقمي، رغم ما يحمله من مزايا جمة، يفرض على المنظومات القانونية تحديات متعددة، سواء على الصعيد التشريعي أو الأمني. فمن الناحية القانونية، يتطلب استعمال هذه التكنولوجيات تحديث الإطار التشريعي بما يواكب المستجدات الرقمية، ويوفر ضمانات فعالة لحماية الحقوق الأساسية، وعلى رأسها الحق في حماية المعطيات الشخصية، وحرمة الحياة الخاصة، وضمانات المحاكمة العادلة عبر الوسائل الإلكترونية. أما من الناحية الأمنية، فيستلزم الأمر تطوير نظم الحماية الرقمية، وتقوية القدرات الوطنية في مجال الأمن السيبراني، لمواجهة مخاطر الاختراق والتلاعب بالمعلومات.

وعليه، فإن تكنولوجيا الإعلام والاتصال ليست مجرد أدوات تقنية، بل هي دعامة مؤسسية وقانونية يجب توظيفها في إطار استراتيجي شامل يأخذ بعين الاعتبار التوازن الدقيق بين متطلبات التطور التكنولوجي وضمانات الحماية القانونية. ومن خلال تبني هذه الأدوات بشكل مدروس، يمكن للدول أن تعزز من سيادة القانون، وترسّخ أسس الأمن القانوني في البيئة الرقمية، بما يضمن حماية الحقوق والحريات، ويعزز ثقة المواطن في النظام القانوني والقضائي. وبذا، يتحقق الانتقال من مجرد رقمنة الشكل إلى تحديث فعلي للجوهر القانوني، بما يتماشى مع تحديات العصر الرقمي.

الفصل الثاني
إستراتيجية الدول لحماية الفضاء الرقمي

في العصر الرقمي الذي نعيشه اليوم، أصبح الفضاء الإلكتروني يشكل أحد الأبعاد الأساسية التي تؤثر على حياتنا اليومية، وعلى مستوى الدول من حيث الأمن، الاقتصاد، والتطور التكنولوجي. نتيجةً لهذه الأهمية المتزايدة، تركز الدول على تبني استراتيجيات لحماية الفضاء الرقمي من التهديدات المتزايدة والمتنوعة مثل الجرائم الإلكترونية، الهجمات السيبرانية، وانتهاك الخصوصية. وتعكس هذه الاستراتيجيات التنوع في التصورات والتوجهات بين الدول، وفقًا لبيئاتها القانونية، التقنية، والثقافية.

في هذا الفصل، نعرض مقارنة بين الاستراتيجيات التي تتبعها الدول العربية والدول الغربية لحماية الفضاء الرقمي. حيث يتناول المبحث الأول استراتيجيات الدول العربية، بدءًا من الأطر التشريعية وصولًا إلى الاستراتيجيات الأمنية والتقنية.

بينما يتناول المبحث الثاني استراتيجيات الدول الغربية، مع التركيز على الأطر القانونية والتشريعية، وكذلك الأساليب الأمنية المتبعة في هذه الدول.

المبحث الأول: الإستراتيجية المتبعة في الدول العربية

تعتبر الدول العربية في طور تطوير أطرها القانونية والتقنية لحماية الفضـــاء الرقمي، حيث تســـعى إلى مواجهة التحديات المرتبطة بالتحول الرقمي والنمو التكنولوجي الســـريع. تختلف الاســتراتيجيات المتبعة بين الدول العربية بناءً على الظروف الســياســية والاقتصــادية والتطور التكنولوجي. وفي هذا المبحث، سـيتم تسـليط الضـوء على الأطر التشـريعية والقانونية التي تم اعتمادها في الدول العربية لحماية الفضـاء الرقمي، بالإضـافة إلى دراسـة الاسـتراتيجيات التقنية والأمنيـة التي تتبعهـا تلـك الـدول، مع التطرق أيضًـــا إلى التعـاون الـدولي في مجـال الأمن السيبراني[1].

المطلب الأول: الأطر التشريعية والقانونية لحماية الفضاء الرقمي

في السنوات الأخيرة، شـهدت الدول العربية تحولًا تدريجيًا نحو تحديث وتطوير الأطر التشـريعية والقانونية لحماية الفضاء الرقمي.

يعد هذا التحول جزءًا من جهود الدول لمواكبة النمو الســـريع للتكنولوجيا الرقمية والتهديدات المتزايدة من الهجمات السيبرانية، التي تضر بالأفراد والمؤسسات.

يعكس هذا التوجه السـعي نحو حماية الأمن السـيبراني، تأمين البيانات الشـخصـية، وضـمان الحقوق الرقمية للمواطنين في العالم الرقمي المتطور. تواصـل الدول العربية تعزيز التشـريعات لتوفير بيئة قانونية قادرة على مواجهة التحديات الناشئة في الفضاء الرقمي.

الفرع الأول: حماية البيانات الشخصية في الدول العربية

حماية البيانات الشـخصـية باتت من الأولويات الكبرى لدى العديد من الدول العربية، خاصـة مع التوسـع الكبير في جمع البيانات عبر الإنترنت من قبل الشركات والمؤسسات الحكومية. تهدف

[1]. أنور محمد، **أنظمة الكشف عن التسلل في الأمن السيبراني**، مراجعة الأمن السيبراني، 2021، د ب ن، ص130.

هذه التشريعات إلى ضمان حماية الأفراد من استخدام بياناتهم الشخصية بطرق غير قانونية أو ضارة[1].

أولا: مكافحة الجرائم السيبرانية في القانون الجزائري

لقد أقر المشـرع الجزائري على غرار التشـريعات الأخرى مسـايرة التطورات المسـتمرة للجرائم السيبراني

1. مكافحة الجرائم السيبرانية في إطار القواعد العامة

حاول المشرع الجزائري التماشي مع ما هو معمول به في مجال محاربة الإجرام السيبراني من خلال القانون 04-15 المتضمن تعديل قانون العقوبات، مع تزايد الاعتداءات على الأنظمة المعلوماتية بعد تطور آليات الاتصال وظهور المواقع الالكترونية تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات"، وطبقا لنص المادة 394 مكرر منه والتي نصـت على ما يلي: "يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50.000 إلى 100.00دج كل من يدخل أو يبقى عن طريق الغش في كل جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك، وتضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشـتغال المنظومة"[2]، كما قام المشـرع بتعديل جديد على قانون العقوبات بالقانون رقم 06-23 حيث تم تشديد العقوبة على كل الجرائم الواردة فيها[3].

أما تعديل القانون رقم 16-02 المؤرخ في 19 يونيو 2016 المعدل لقانون العقوبات قد أضاف المادة 87 مكرر 11 التي تعاقب كل جزائري أو أجنبي يرتكب أفعالا إرهابية أو يدبرها أو يعد

---

[1]. أنور محمد، المرجع السابق، ص136.

[2]- القانون رقم **04-15**، المؤرخ في **10** نوفمبر **2004**، المعدل والمتمم للأمر رقم **66-155**، **المتضمن قانون العقوبات**، ج ر ع **71**، الصادرة بتاريخ **10** نوفمبر **2004**.

[3]- بوزنون سعيد، **مكافحة الجريمة الالكترونية في التشريع الجزائري**، مجلة العلوم الإنسانية، مج ب، ع52، جامعة الإخوة منتوري، قسنطينة، 2019، ص49.

لها أو يشارك فيها، .... ويستخدم تكنولوجيات الإعلام والاتصال لارتكاب الأفعال المذكورة في المادة[1].

كما استحدث المشرع الجزائري القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بموجب الأمر رقم 21-11 المتمم للأمر رقم 66-155 المتضمن ق إ ج ج والذي تضمن المواد من 211 مكرر22، إلى 211 مكرر29 حيث يمارس وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وكذا قاضي التحقيق ورئيس القطب صلاحيتهم عبر كامل الإقليم الوطني[2].

2. مكافحة الجرائم السيبرانية في إطار القوانين الخاصة

أقر المشرع الجزائري قوانين خاصة لمكافحة الجرائم السيبرانية من خلال الأمر رقم 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة على مجموعة من المصنفات الأدبية والفنية وقد نص على نوعين منها وهي برامج الحاسوب في المادة 04 وقواعد البيانات في المادة 05 منه[3].

كما جاء القانون رقم 08-01 المتعلق بالتأمينات الاجتماعية المتمم لأحكام القانون 83-11 المعنون "بأحكام جزائية" وتضمن المواد من 93 مكرر2 إلى 93 مكرر6، وحصر جرائم المعلوماتية المرتكبة على البطاقة الالكترونية في:

- التسليم والاستلام بهدف الاستعمال غير المشروع للمؤمن له اجتماعيا أو المفتاح الالكتروني لهيكل العلاج أو مهنيي الصحة[4].

---

[1]- القانون رقم **16-02**، المؤرخ في **19** جوان **2016**، المعدل والمتمم للأمر **66-155**، المتضمن قانون العقوبات، ج ر ع **37**، الصادرة بتاريخ **22** جوان **2016**.

[2]- الأمر رقم **21-11**، المؤرخ في **25** أوت **2021**، المتمم للأمر رقم **66-155**، **المتضمن ق إ ج ج**، ج ر ع **65**، الصادرة بتاريخ **26** أوت **2021**.

[3]- الأمر رقم **03-05**، المؤرخ في **19** جمادى الأولى سنة **1424**هـ، الموافق **19** يوليو عام **2003**، **يتعلق بحقوق المؤلف والحقوق المجاورة**، ج ر ع **44**، الصدارة في **23** يوليو **2003**.

[4]- القانون رقم **08-01**، المؤرخ في **23** يناير **2008**، يتمم القانون رقم **83-11**، المؤرخ في **02** يوليو **1983**، **المتعلق بالتأمينات الاجتماعية**، ج ر ع **04**، الصادرة في **27** يناير **2008**.

- القيام بتعديل أو حذف كلي أو جزئي بطريق الغش للمعطيات التقنية أو الإدارية المدرجة في البطاقة الالكترونية.
- إعداد أو تعديل أو نسخ البرمجيات بطريق غير مشروع بالوصول أو استعمال المعطيات المدرجة في البطاقة الالكترونية للمؤمن له اجتماعيا.

وبموجب القانون رقم 09-04 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وهو القانون المنظم للفضاء الالكتروني ومكافحة المجال الإجرامي المتصل به، ثم جاء بعده القانون رقم 15-04 الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين حيث ساهم في حماية الوثيقة الالكترونية من خلال إضفاء الرسمية عليها، بدعها جاء القانون رقم 18-04[1] المتعلق بالقواعد العامة المتعلقة بالبريد والاتصالات الالكتروني إذ أنه عمل على وضع مجموعة آليات للتصدي للجرائم المتعلقة بالعالم الافتراضي حيث استحدث سلطة ضبط أوكل لها مهام السهر على احترام متعاملي البريد والاتصالات الالكترونية، كما جرم انتهاك سرية المراسلات المرسلة عن طريق البريد أو الاتصالات الالكترونية أو إفشاء مضمونها أو نشرها أو استعمالها دون ترخيص من المرسل[2].

لقد نص المشرع الجزائري في المادة 3 من القانون رقم 18-05، على أنه: "تمارس التجارة الالكترونية في إطار التشريع والتنظيم المعمول بهما.

غير أنه، تمنع مل معاملة عن طريق الاتصالات الالكترونية تتعلق بما يأتي:

- المنتجات التي تمس بحقوق الملكية الفكرية أو الصناعية أو التجارية،
- كل سلعة أو خدمة محظورة بموجب التشريع المعمول به،....."[3].

[1]- القانون رقم **18-04**، المؤرخ في **10** ماي **2018**، **يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية**، ج ر ع **27**، الصادرة في **13** ماي **2018**.

[2]- الدام محمد، مرجع سابق، ص54-55.

[3]- القانون رقم **18-05**، المؤرخ في **10** ماي **2018**، **المتعلق بالتجارة الالكترونية**، ج ر ع **28**، الصادرة في **16** ماي **2018**.

وجاء القانون 18-07 المتعلق بحماية الأشـخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشـخصـي من أجل سـد الفراغ التشـريعي إذ يهدف إلى تحديد قواعد حماية هؤلاء الأشـخاص من أي انتهاكات مهما كان مصـدرها أو شـكلها ويشـدد على أنه لا يمكن معالجة البيانات ذات الطابع الشخصي إلا بموافقة أصحابها[1].

ثانيا: قانون حماية البيانات الشخصية في مصر

يعد قانون حماية البيانات الشـخصـية في مصـر، الذي تم إصـداره في عام 2020 تحت رقم 151، خطوة محورية في حماية حقوق الأفراد الرقمية وضـمان خصـوصـيتهم في العصـر الرقمي. يهدف هذا القانون إلى تنظيم عملية جمع واستخدام وتخزين البيانات الشخصية، ويضع إطارًا قانونيًا يشدد على كيفية تعامل المؤسسات المختلفة مع البيانات التي تخص الأفراد، سواء كانت تلك المؤسسات حكومية أو خاصة.

ويشمل القانون العديد من المواد التي تحدد بوضوح حقوق الأفراد في معرفة كيفية استخدام بياناتهم، مع ضـرورة الحصـول على موافقتهم الصـريحة قبل جمع أو معالجة هذه البيانات. كما ينص القانون على فرض عقوبات صـارمة على الشـركات والمؤسـسـات التي تقوم بتسـريب البيانات الشـخصـية أو استخدامها بطرق غير قانونية، مما يعزز من حماية الأفراد ويحسن من بيئة الأمان الرقمي.

يُعتبر هذا القانون جزءًا من التزام مصـر المتزايد بتطبيق المعايير العالمية في مجال حماية الخصوصية وحماية البيانات الشخصية، وهو يأتي في وقت يشهد فيه العالم تزايدًا في المخاوف بشأن كيفية التعامل مع البيانات الشـخصـية في ظل الثورة الرقمية. ويشمل القانون أيضًـا إنشاء هيئة حماية البيانات الشـخصـية، التي تُعنى بالإشـراف على تنفيذ التشـريعات المتعلقة بحماية البيانات، والتأكد من أن المؤسـسـات تتبع أفضـل الممارسـات في مجال الأمان وحماية

[1]- بوعكة كمال، **الحماية القانونية للأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي**، المجلة الجزائرية لقانون الاعمال، جامعة محمد بوضياف، المسيلة، مج 01، ع02، 2020، ص52.

الخصـوصـية. كما يُلزم القانون الشـركات بتطبيق إجراءات أمنية صـارمة لحماية البيانات من المهاجمين السـيبرانيين ويعزز من الشـفافية في التعامل مع البيانات. من خلال هذه الخطوات، تسعى مصر إلى تعزيز الثقة في البيئة الرقمية، وتشجيع الأفراد على استخدام التقنيات الحديثة دون القلق بشأن تعرض بياناتهم الشخصية للتهديد أو الاستغلال غير القانوني[1].

ثانيا: قانون حماية الخصوصية في الأردن

جاء في المادة 8 من القانون رقم لسـنة 2020 الاشـتراطات الخاصـة بمعالجة البيانات الشخصية وهي كالتالي:

"يحظر القيام بمعالجة البيانات الشـخصـية دون موافقة صـاحبها، ما لم تكن المعالجة ضـرورية لأي مما يأتي:

- تنفيذ عقد يكون الشخص المعني بالمعالجة طرفا فيه.
- اتخاذ خطوات بناء على طلب الشخص المعني بالمعالجة بهدف إبرام عقد.
- تنفيذ التزام يرتبه القانون خلافا لالتزام عقدي أو صدور أمر من محكمة مختصة.
- حماية المصالح الحيوية للشخص المعني بالمعالجة"[2].

ثالثا: قانون الإمارات للأمن السيبراني[3]

في عام 2019، أطلقت دولة الإمارات العربية المتحدة "قانون الأمن السـيبراني" في خطوة استراتيجية تهدف إلى تعزيز حماية الفضـاء الرقمي وحماية البنية التحتية الوطنية من التهديدات والهجمات الإلكترونية المتزايدة في العصر الرقمي. يُعتبر هذا القانون بمثابة إطار قانوني شامل يعمل على تنظيم وضـبط الأنشـطة المتعلقة بالأمن السـيبراني داخل الدولة، ويشـمل تحديد المسـؤوليات والواجبات لكافة المؤسـسـات الحكومية والخاصـة التي تشـارك في تأمين الفضـاء

[1]- قانون رقم **151، يتضمن حماية البيانات الشخصية في مصر (PDPL)**، 2020، ص12.

[2]- قانون حماية البيانات الشخصية رقم ( ) لسنة 2020، الأردن، منشور في الموقع:https://lob.gov.jo .

[3]. أنور محمد، مرجع سابق، ص131.

الرقمي. كما يولي القانون أهمية خاصة لحماية البيانات الحساسة، مثل المعلومات الحكومية والبيانات التجارية الهامة، والتي يُعتبر الحفاظ عليها من أولويات الأمن الوطني[1].

رابعا: السعودية واستراتيجية الأمن السيبراني

تم تبني استراتيجية شاملة للأمن السيبراني تهدف إلى تعزيز قدرة الدولة على مواجهة التهديدات السيبرانية المتزايدة في ظل التوسع الرقمي المستمر. تسعى المملكة من خلال هذه الاستراتيجية إلى بناء بنية تحتية قوية تواكب التطورات التقنية الحديثة وتؤمن الفضاء الإلكتروني ضد الهجمات المتطورة والمتعددة. جزء من هذه الاستراتيجية هو تحديث التشريعات المتعلقة بالأمن السيبراني، ومنها "قانون مكافحة جرائم المعلومات" الذي تم إقراره لتعزيز مكافحة الجرائم الإلكترونية وتحديد عقوبات صارمة ضد المهاجمين السيبرانيين. يركز هذا القانون بشكل خاص على حماية المعلومات الحساسة مثل البيانات المالية والصحية للمواطنين، وهي من أكثر الأنواع المستهدفة من قبل المهاجمين نظرًا لقيمتها العالية[2].

الفرع الثاني: التعاون الإقليمي والدولي في مجال الأمن السيبراني

لا تقتصر جهود الدول العربية على تطوير التشريعات الداخلية فقط لحماية الفضاء الرقمي، بل تسعى العديد من هذه الدول إلى تعزيز التعاون الإقليمي والدولي لمكافحة الجرائم الإلكترونية العابرة للحدود. يعكس هذا التعاون ضرورة التنسيق بين الدول على مستوى عالمي لمواجهة التهديدات المتزايدة في الفضاء السيبراني، ويعزز من فعالية التدابير الأمنية المتبعة. نظرًا للطبيعة العابرة للحدود التي تتميز بها الجرائم الإلكترونية، فإنه من الضروري أن تكون هناك استراتيجيات تعاون تشمل تبادل المعلومات والتنسيق بين الأجهزة الأمنية على المستوى الإقليمي والدولي.

---

[1]– الأمن السيبراني في الإمارات العربية المتحدة، أولوية متزايدة في العصر الرقمي، مقال منشور على الموقع: https://dralaanasr.com .

[2]– الاستراتيجية الوطنية للأمن السيبراني في المملكة، مقال منشور على الموقع : https://my.gov.sa .

أولا: جهود الأمم المتحدة في مجال مكافحة الجريمة السيبرانية

لقد قدمت الأمم المتحدة جهودا قيمة في مجابهة الجريمة السيبرانية ومن أهم المؤتمرات التي عقدتها بهذا الشأن نذكر:

1. المؤتمر السابع لمنع الجريمة ومعاملة المجرمين

عقد في مدينة ميلانو الإيطالية في الفترة ما بين 26 أوت إلى 06 سبتمبر 1985 حيث لجنة الخبراء العشرين بدراسة موضوع حماية نظم المعالج الآلي والاعتداء على الحاسب وإعداد تقرير لعرضه على المؤتمر الموالي.

2. المؤتمر الثامن للأمم المتحدة

عقد في هافانا الكوبية، من 27 أوت إلى 07 سبتمبر 1990، وفيه أقرت المعاهدات النموذجية لتسليم المجرمين، وتبادل المساعدات في المسائل الجنائية ونقل الإجراءات والإشراف على المجرمين المحكوم عليهم بأحكام مشروطة أو المفرج عنهم إفراجا مشروطا[1].

أما في مجال الجرائم المتعلقة فلقد أشار هذا المؤتمر إلى إجراءات الواجب اتخاذها منها:

- تحديث القوانين وأغراضها الجنائية من أجل تطبيق أفضل القوانين على نحو ملائم.
- مصادرة العائد من الأنشطة غير المشروعة.
- اتخاذ تدابير الأمن والوقاية مع خصوصية الأفراد.
- رفع الوعي لدى الجماهير والقضاة على أهمية مكافحة هذا النوع من الجرائم.
- حماية مصالح وحقوق ضحايا جرائم الحاسوب[2].

3. المؤتمر الثالث عشر للأمم المتحدة لمنع الجريمة

انعقد في الدوحة من 12 و19 أفريل 2015، ومن أهم توصياته في مجال مكافحة الجريمة السيبرانية:

---

[1]- بيدي آمال، **جهود الأمم المتحدة في مكافحة الجريمة السيبرانية**، مجلة البحوث في الحقوق والعلوم السياسية، مج 08، ع01، جامعة تيارت، 2022، ص306.

[2]- بيدي آمال، المرجع السابق، ص306.

-وجوب استحداث أدوات وبرامج من أجل تسهيل مكافحة الجريمة السيبرانية.

-بناء قدرات أجهزة إنقاذ القانون ونظم العدالة الجنائية في مجال التحري عن الجرائم السيبرانية.

-التأكيد على أهمية اشراك القطاع الخاص في مجال مكافحة الجريمة السيبرانية[1].

ثانيا: الاتحاد الدولي للاتصالات

يعمل الاتحاد على مساعدة الحكومات في الاتفاق على مبادئ مشتركة تفيد الحكومات والصناعات التي تعتمد على تكنولوجيا المعلومات والبنية التحتية للاتصالات ويتضمن تحقيق أهداف هي:

- وضع استراتيجيات لتطوير نموذج التشريعات السيبرانية يكون للتطبيق محليا وعالميا بالتوازي مع التدابير القانونية.
- وضع استراتيجيات لتهيئة الأرضية الوطنية والإقليمية المناسبة لوضع الهيكلي التنظيمية والسياسات المتعلقة بجرائم الانترنت.
- وضع استراتيجية لتحديد الحد الأدنى المقبول عالميا في موضوع معايير الأمن ونظم تطبيقات البرامج والأنظمة.
- وضع استراتيجيات لوضع آلية عالمية للمراقبة والإنذار والرد مع ضمان قيام التنسيق عبر الحدود.
- وضع استراتيجيات لإنشاء نظام هوية رقمي عالمي وتطبيقه.
- تطوير استراتيجية عالمية لتسهيل بناء القدرات البشرية لتعزيز المعرفة في مختلف القطاعات وفي جميع المجالات المعلوماتية.

[1]- المرجع نفسه.

- تقديم المشورة بشأن إمكانية اعتماد إطار استراتيجي من أجل التعاون الدولي في مكافحة الجرائم[1].

ثالثا: اللجنة الاقتصادية والاجتماعية للاسكوا

تأسست الاسكوا عام 1973 من طرف المجلس الاقتصادي والاجتماعي للأمم المتحدة بقرار (LV1818) كبديل لمكتب الأمم المتحدة في بيروت (يونيسوب) ويعتبر الأمن السيبراني من أهم القضايا التي عالجها ومن بين مخرجاته ما يلي:

-في سنة 2014 تم عقدت اللجنة ورشة عمل في مسقط بعمان بالتعاون مع المركز الإقليمي للأمن السيبراني وكان هدفها بناء القدرات الوطنية في الدول العربية لتعزيز الامن السيبراني في مواجهة الجرائم السيبرانية.

-في سنة 2018 استضافت اللجنة حوارا إقليميا واجتماعيا للخبراء بشأن حوكمة الانترنت والأمن السيبراني[2].

رابعا: المنظمة العالمية للملكية الفكرية

اهتمت هذه المنظمة بالمجال السيبراني من خلال توفير الحماية القانونية للبرامج المعلوماتية وقواعد البيانات، إذ أنه تم الانفاق على توفير الحماية بواسطة الاتفاقيات الدولية منها "التريبس" و"اتفاقية برن" اللتان حثتا الدول الأعضاء فيهما على ضرورة تطوير التشريعات خاصة حقوق المؤلف، وإقرار عقوبات على أعمال التزوير في المعاملات التجارية والقرصنة[3].

---

[1]- الدام محمد، مرجع سابق، ص40.

[2]- حاجي نعيمة، **الجريمة السيبرانية والجهود الدولية لمكافحتها**، مجلة النبراس للدراسات القانونية، مج 06، ع01، جامعة العربي التبسي، تبسة، 2021، ص70.

[3]- بن جدو بن علية، **تحديات الأمن السيبراني لمواجهة الجريمة الالكترونية**، المجلة الجزائرية للأمن الإنساني، مج07، ع02، جامعة باتنة 1، 2002، ص310.

المطلب الثاني: الاستراتيجيات التقنية والأمنية والتعاون الدولي

تسعى الدول العربية إلى تطوير وتنفيذ استراتيجيات تقنية وأمنية متكاملة لمواكبة التحديات المتزايدة في مجال الأمن السيبراني، وذلك لضمان حماية الفضاء الرقمي من الهجمات السيبرانية المتنوعة. في هذا السياق، تتبنى العديد من الدول العربية تقنيات حديثة واستراتيجيات شاملة تهدف إلى تعزيز أمن الشبكات والمعلومات وحماية البيانات الشخصية للأفراد والمجتمعات. تتنوع هذه الاستراتيجيات ما بين الإجراءات التقنية المتقدمة، تطوير الكوادر المتخصصة، وتعزيز التعاون الدولي لمكافحة التهديدات السيبرانية.

الفرع الأول: الاستراتيجيات التقنية لحماية الفضاء الرقمي

تتنوع الاستراتيجيات التقنية لحماية الفضاء الرقمي نذكر منها:

أولا: أنظمة الكشف عن الهجمات السيبرانية

تعتبر أنظمة الكشف عن الهجمات السيبرانية من الأدوات الأساسية التي تعتمد عليها العديد من الدول العربية لحماية شبكاتها الرقمية ضد التهديدات المتزايدة والمعقدة، وتشمل هذه الأنظمة أنظمة الكشف عن التسلل (IDS)وأنظمة الوقاية من التسلل (IPS)، التي تعد من الحلول المتقدمة للكشف المبكر والوقاية الفعالة من الهجمات الإلكترونية، وتعمل أنظمة IDS على مراقبة الشبكات والأنظمة للكشف عن الأنشطة المشبوهة والتسلل غير المصرح به، حيث تقوم بتحليل الحركة على الشبكة ومقارنتها بأنماط معروفة للهجمات بهدف تحديد أي نشاط غير عادي قد يشير إلى محاولة اختراق أو هجوم. من ناحية أخرى، توفر أنظمة IPS طبقة إضافية من الأمان من خلال التفاعل الفوري مع الهجمات المكتشفة، حيث تقوم هذه الأنظمة بالتفاعل بشكل مباشر مع الهجمات وتعطيلها أو الحد من تأثيرها قبل أن تتسبب في أضرار جسيمة. هذا التكامل بين الكشف والوقاية يساهم في تمكين المؤسسات الحكومية والخاصة من تحديد الهجمات أو الأنشطة المشبوهة في الوقت الفعلي، مما يمكنها من اتخاذ الإجراءات المناسبة بسرعة وفعالية[1].

[1]– أنظمة كشف التسلل IDS، مقال منشور على الموقع: https://majed.blog .

ثانيا: التوقيع الرقمي والتشفير السيبراني

لقد أصبح النشاط الرقمي يلازم خصوصية وأمان الحريات، والحق بعد التطور المذهل والهائل للتقنيات الرقمية وارتفاع نسبة استعمال الانترنت ومواقع التواصل الاجتماعي، هذه الأيقونة أصبحت تستغل بطرق غير مشروعة وتعدت حدود الشخصية والخصوصية، إذ أصبح الاطلاع والعبث بمعلومات الغير وليس هذا فقط بل إلحاق الأذى من طرف المخترقين غير المصرح بهم بذلك، الأمر الذي ساعد على ارتكاب الجرائم التي تعدت الدول[1].

1. التوقيع الالكتروني

يقصد بالتوقيع الرقمي آلية يتم استخدامها في الأنظمة الالكترونية الهدف منها تحديد هوية المستخدم والتأكد منها، لضمان عنصر الأمان والسرية، كما يساعد على حظر القيام بأي تعديلات في الوثائق بعد وضع التوقيع، وتظهر أهمية التوقيع الالكتروني في التصديق بأن الرسالة لم يحدث بها أي تغيير ويصعب تزوير التوقيع والعبث به، وقد ورد موضوع التوقيع الالكتروني في القانون الجزائري في المادة 2/327 من القانون رقم 05-10، المؤرخ في 2005/06/20، المتضمن تعديل القانون المدني[2].

أما المشرع الفرنسي فقد أقر قبل المشرع الجزائري التوقيع الالكتروني ابتداء من 13 مارس 2000 من خلال القانون رقم 230 لسنة 2000 حيث صدر في صورة تعديل للنصوص المنظمة للإثبات في القانون المدني الفرنسي تزامنا مع كثرة استخدام المحررات الالكترونية، ويعتد معيار التوقيع القمي Digital Signature Standard (DSS) على أسلوب التشفير الذي يستخدم خوارزمية التوقيع الرقمي (DSA) وهي صيغة من التواقيع الالكترونية التي صادقت عليها و م أ.

---

[1]. زهدور إنجي هند نجوى ريم سندس، **استراتيجيات الوقاية القانونية والأمنية من مهددات الأمن الرقمي**، المجلة الدولية لنشر البحوث والدراسات، مج2، ع16، كلية الحقوق والعلوم السياسية، جامعة محمد بن أحمد، وهران، الجزائر، فبراير 2021، ص219.

[2]. المرجع نفسه.

2. التشفير من تقنيات الأمن المعلوماتي

يرتبط التوقيع الالكتروني بالتشـــفير (Encryption) وهو عملية تغيير البيانات ولا يتمكن من قراءتها سوى الشخص المستقبل باستخدام مفتاح فك التشفير، فالطريقة الشائعة للتشفير تتمثل في وجود مفتاحين، المفتاح العام Public-key ومفتاح خاص Private-key يتوفر لدى الشخص الذي أنشأه فقط، يمكن أي شخص يملك المفتاح العام أن يرسل الرسائل المشفرة دون أن يستطيع فك شيفرة الرسالة إلا الشخص الذي يملك المفتاح الخاص، لذا يعتبر التشفير إجراء تقنيا يسمح بزيادة الأمان والثقة في التجارة الالكترونية كما يضمن السرية الكاملة والحيلولة دون تعديلها أو اختراقها وتتلخص أغراض التشفير فيما يلي:

- توثيق الموقع.
- توثيق الرسالة.
- الفعالية[1].

ثالثا: آلية المصادقة الالكترونية المستحدثة

بما أن المعاملات الالكترونية تقوم أساسا على مبدأ الثقة والأمان، رأت التشريعات إلى ضرورة خلق طرف محايد يعمل على ترسيخ تلك الثقة من أجل حماية المعلومات والعمل على تأكيد مصداقيتها، لذا عمدت الهيئات المختصة إلى إسناد مهمة حماية البيانات إلى جهات معتمدة تعمل على تصديق وتوقيع المعاملات الالكترونية من أجل الوصول إلى بيئة الكترونية آمنة.

[1]. بيل جيتس، **المعلوماتية بعد الانترنت**، سلسلة عالم المعرفة، المجلس الوطني للثقافة والفنون والآداب، الكويت، 1998، ص47.

1. مفهوم آلية التصديق الالكتروني

حيث أن الفقهاء لم يتفقوا على وضع تعريف شامل للتوثيق الالكتروني حيث عرفه البعض على أساس أنه وسيلة فنية آمنة للتحقق من صحة التوقيع الالكتروني أو المحرر، ونسبه إلى شخص أو كيان معين، عبر جهة موثوق بها يطلق عليها "مقدم خدمات التصديق الالكتروني"[1]. بالنسبة للمشرع الجزائري فقد ميز بين نوعين من الجهات المكلفة بالتصديق من خلال المادة 11/2 و12 من القانون رقم 15-04 حيث سمى الأولى الطرف الثالث الموثوق، والجهة الثانية مؤدي خدمات التصديق الالكتروني[2].

وجاء في المادة 2 من قانون الأونسترال النموذجي للأمم المتحدة عام 2001 أن القائم على خدمات التصديق شخص يصدر الشهادات ويجوز له تقديم خدمات أخرى متصلة بالتوقيعات الالكترونية، أما قانون التوجيه الأوروبي رقم 1999/93 المتعلق بالتوقيعات الالكترونية فقد عرف مقدم خدمات التصديق بأنه كل كيان أو شخص طبيعي أو معنوي يقوم بتقديم شهادات توثيق الكترونية متصلة بالتوقيع الالكتروني[3].

2. مسؤولية سلطات التصديق الالكتروني

لقد أقر المشرع الأوروبي أن التوقيع الالكتروني يتمتع بذات الحجية التي يتمتع بها التوقيع التقليدي، وأمام ذلك نظم لتوجيه الأوروبي مسؤولية الجهات المصدرة لشهادة التوثيق بنصوص خاصة وأقام المسؤولية على قاعدتين الأولى المسؤولية المفترضة لجهات التصديق الالكتروني والثانية جوزا تحديد نطاق صلاحية الشهادة، وجاء في المادة 6 من قانون التوجيه الأوروبي أن المكلف بخدمة التوثيق الالكتروني المصدرة للشهادة يكون مسؤولا عن الضرر الذي يسببه للشخص الطبيعي أو المعنوي الذي اعتمد تلك الشهادة[4].

---

[1]- منصور محمد حسنين، **الإثبات التقليدي والالكتروني**، دار الفكر الجامعي، الإسكندرية، 2006، ص286.

[2]- القانون رقم **15-04**، المؤرخ في **2015/02/01**، **الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين**، ج ر ع **06**، الصادرة بتاريخ **2015/02/10**.

[3]. زهدور إنجي هند نجوى ريم سندس، مرجع سابق، ص224.

[4]. المرجع نفسه، ص226.

رابعا: التحليل البياني للكشف عن التهديدات

تعرف التهديدات السيبرانية بأنها استغلال الحاسبات وتكنولوجيا المعلومات في تدمير البنية المعلوماتية للخصوم، وكذا تعطيل شبكات الدفاع الجوي واختراق أنظمة المعلومات للبريد الالكتروني لمكاتب رؤساء الدول والتجسس عليهم، حيث أن تلك التهديدات السيبرانية تهدد المجتمع وأمن الاقتصاد الوطني والجانب الأمني والعسكري للدول وفق أهداف مسطرة[1] ، فالتحليل البياني للكشف عن التهديدات أصبح أداة محورية في تعزيز الأمن السيبراني في الدول العربية، وتشمل المخاطر الرقمية كل ما يمكن أن يعرض الأنظمة والشبكات للخطر، نذكر منها الهجمات الفيروسية، التصيد الاحتيالي والاختراقات والتي مع وجودها يصبح التحليل الأمني أمرا لا غنى عنه، مثل أن تحلل البيانات تحديد رسائل البريد الالكتروني المشبوهة ويتم إزالتها قبل وصولها إلى المستخدم، ومن فوائد التحليل البياني ودورها في تعزيز الأمن السيبراني نذكر:

- الكشف المبكر من خلال التعرف على التهديدات الالكترونية قبل وقوعها، مما يقلل من احتمالية الأضرار.
- التخصيص مما يمكن النظام من تعلم خصائص كل شبكة وتحديد السلوكيات غير الطبيعية.
- المرونة حيث وانه بفضل تحليل البيانات يمكن للأنظمة التكيف مع التهديدات الجديدة والتعامل معها بكل كفاءة[2].

خامسا: تشكيل فرق سيبرانية وطنية

تشكيل فرق سيبرانية وطنية يمثل خطوة استراتيجية حيوية لمواجهة التهديدات السيبرانية المتزايدة التي تؤثر على الأمن الوطني في العصر الرقمي. في ظل تزايد الهجمات الإلكترونية

[1]– عطية إدريس، **مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري**، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي، تبسة، الجزائر، مقال منشور على الموقع: https://asjp.cerist.de ، ص108.

[2]– كيفية تعزيز الأمن السيبراني باستخدام التحليل البياني المتقدم، مقال منشور على الموقع: http://omalytica.com .

التي تستهدف الحكومات والشركات والأفراد على حد سواء، قامت العديد من الدول العربية بتأسيس فرق سيبرانية وطنية متخصصة لضمان حماية البنية التحتية الرقمية وحفظ سرية المعلومات. تتألف هذه الفرق من خبراء متخصصين في الأمن السيبراني، الذين يتمتعون بمهارات فنية عالية للتعامل مع الحوادث الأمنية الإلكترونية بفعالية وسرعة.

تتضمن مهام هذه الفرق مراقبة الشبكات الوطنية، الكشف عن الهجمات السيبرانية والتعامل معها فور وقوعها، بالإضافة إلى تقديم الاستشارات الأمنية والتوجيهات للقطاعات المختلفة، سواء كانت حكومية أو خاصة، لضمان تطبيق أفضل الممارسات في مجال الأمن السيبراني. كما تساهم هذه الفرق في تطوير استراتيجيات أمنية وطنية شاملة تستند إلى أحدث التوجهات التقنية وتستجيب للتهديدات المستمرة والمتطورة. من ناحية أخرى، تلعب فرق الأمن السيبراني دوراً مهماً في نشر الوعي الأمني بين موظفي المؤسسات العامة والخاصة، من خلال تنظيم ورش عمل ودورات تدريبية لتعليم كيفية تأمين الشبكات وحماية البيانات من الهجمات المحتملة. هذا التوجه الاستراتيجي يسهم في تعزيز قدرة الدولة على التصدي للهجمات السيبرانية وحماية الأمن القومي في ظل التحول الرقمي السريع[1].

الفرع الثاني: التعاون الدولي في مجال الأمن السيبراني

لا تقتصر استراتيجيات الدول العربية على الإجراءات المحلية فقط، بل تسعى العديد من هذه الدول إلى تعزيز التعاون الإقليمي والدولي في مواجهة التهديدات السيبرانية العابرة للحدود. فالتعاون الدولي يعتبر عاملًا أساسيًا في التصدي للهجمات السيبرانية التي تتجاوز الحدود الجغرافية. وفي هذا السياق، تتبنى الدول العربية سياسات تعاون متعددة مع المنظمات الدولية والإقليمية في مجال الأمن السيبراني.

[1]. زهرة، ر، **الذكاء الاصطناعي في كشف التهديدات السيبرانية، الذكاء السيبراني**،2021، ص 198-210.

لقد اهتم المجتمع الدولي بموضوع مكافحة الجرائم السيبرانية لما تكتسيه من خطورة، حيث قامت العديد من دول العالم بالتوقيع على الاتفاقيات لتعزيز التعاون من أجل التصدي لها نذكر أهمها فيما يلي:

1. الاتفاقية الأوروبية لحماية الأفراد وقت معالجة البيانات الشخصية

صدرت في عام 1981 عن المجلس الأوروبي "اللجنة الوزارية"، وفي عام 1985 صدرت عنه التوصية رقم (R20/85) المتعلقة بالبيانات الشخصية في أغراض التسوق المباشر، بعدها صدر التوجيه الأوروبي سنة 1955 الخاص بحماية الأشخاص الطبيعيين في مواجهة معالجة البيانات الشخصية، ثم التوجيه الأوروبي رقم (EC97/66) سنة 1997 بخصوص معالجة تلك البيانات والخصوصية في مجال الاتصالات، وصار نافذا في 1998/10/15، وفي 12 يوليو 2002 صدر التوجيه (EC2002/58) الخاص بمعالجة البيانات ذات الطابع الشخصي والحياة الخاصة في إطار الانترنت[1].

ثانيا: معاهدة الويبو الخاصة بحق المؤلف

أبرمت عام 1996، وصارت نافذة عام 2002، وهي اتفاق خاص في إطار اتفاقية برن تناولت حماية المصنفات وحقوق المؤلفين في البيئة الرقمية، تمنح هذه المعاهدة بعض الحقوق للمؤلفين ومدة الحماية بموجب المعاهدة 50 سنة على الأقل لأي مصنف، وتتضمن موضوعين يتعين حمايتهما وهما:

-برامج الحاسوب.

-البيانات وقواعد البيانات إذا اعتبرت ابتكارات فكرية بسبب اختيار ترتيبها[2].

[1]- بساعد سامية، **حماية البيانات الشخصية للمستهلك من مخاطر الدفع الالكتروني**، مجلة الحقوق والعلوم الإنسانية، مج15، ع01، جامعة زيان عاشور، الجلفة، 2022، ص1413.

[2]- الدام محمد، **الأمن السيبراني**، مذكرة تخرج ضمن متطلبات نيل شهادة الماستر في الحقوق، تخصص جريمة وأمن، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر، الوادي، 2022-2023، ص42.

2. اتفاقية بودابست (Budapest Convention)

تعتبر اتفاقية بودابست بشأن الجرائم الالكترونية مراجعة جماعية للجرائم الالكترونية من قبل الدول الأعضاء في البلدان من أوروبا وبعض الدول غير الأعضاء، وهي أول معاهدة متعددة الجنسيات لفهم "معالجة الجريمة السيبرانية بحذافيرها"، وقد كان لها تأثير عميق بشأن التشريعات الدولية لمكافحة جرائم الانترنت، ولعبت دورا مهما على المستوى الدولي للتصدي للجرائم السيبرانية، حيث بدأ مجلس أوروبا يعمل في جرائم الكمبيوتر منذ السبعينات أي في عام 1989، اعتمد تقرير المشاكل عن الجريمة ذات الصلة بالحاسوب لتطوير القانون الجنائي ضد تلك الجرائم، وقوانين الإجراءات الجنائية المتعلقة بتقنية المعلومات في عام 1995، وبين عامي 1997 و2001 تم تطوير اتفاقية بشأن جرائم الانترنت وتم التفاوض من قبل "لجنة الخبراء حول الجريمة" في الفضاء السيبراني، المعينين من قبل لجنة الوزراء، وفي فبراير 2001 طالب وزراء العدل ووزراء الداخلية للدول الثماني الكبار من الخبراء في اجتماع ميلانو بإيطاليا وضع توصيات تخص اقتفاء المجرمين على شبكة المعلومات، مع ضرورة احترام الخصوصية، وفي 23 نوفمبر 2001 وقع في بودابست 30 دولة الاتفاقية الأوروبية لمكافحة جرائم الانترنت[1].

تلتزم الدول الأعضاء في المنظمة باتخاذ تدابير تشريعية ملائمة لتجريم تسع جرائم في المعلوماتية وهي[2] الدخول غير القانوني المتعمد، الاعتراض القانوني المتعمد دون حق، التدخل المتعمد في المعطيات بالتدمير أو الحذف أو التشويه أو التبديل أو التعديل أو التعطيل، والتدخل المتعمد في الأنظمة، وإساءة استخدام الأجهزة، والتزوير المتعمد باستخدام الكمبيوتر. والاحتيال المتعمد، والجرائم المتعلقة بدعارة الأطفال، إضافة إلى الجرائم المتعلقة بحق المؤلف[3].

---

[1]– قطاف سليمان، بوقرين عبد الحليم، **الآليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل اتفاقية بودابست والتشريع الجزائري**، مخبر البحث في الحقوق والعلوم السياسية، جامعة عمار ثليجي بالأغواط، المجلة الأكاديمية للبحوث القانونية والسياسية، مج6، ع1، 2022، ص338.

[2]– المواد من 2 إلى 13، اتفاقية بودابست، مصدر سابق.

[3]– طه وليد، **التنظيم التشريعي للجرائم الالكترونية في اتفاقية بودابست**، قطاع التشريع بوزارة العدل، جمهورية مصر، د س ن، ص من 23 إلى25.

الفرع الثالث: المنظمة الدولية للشرطة الجنائية الإنتربول في مكافحة الجرائم السيبرانية

لقد أنشئت المنظمة الدولية للشرطة الجنائية (الانتربول) عام 2004، خاصة بمكافحة جرائم التكنولوجيا، وقامت بالتعاون مع مجموعة الدول الثمانية الكبرى (G8) وذلك بوضع استراتيجيات لمواجهة هذا النوع من الجرائم وذلك ب:

- إنشاء مركز اتصالات أمني يعمل 24 ساعة 7 أيام في الأسبوع على مستوى مصالح لشرطة في الدول الأعضاء.
- استخدام أحدث الوسائل في عملية المكافحة، مثل قاعدة البيانات المركزية للصور الإباحية المحولة من قبل الدول وتستخدم برناج Excalibur لتحليل ومقارنة تلك الصور أوتوماتيكيا.
- تزويد شرطة الدول الأعضاء بكتيبات إرشادية حول جرائم المعلوماتية وكيفية التدريب على مكافحتها[1].

ومنه فإن شركة الانتربول تعد منظمة عالمية لمكافحة الجرائم الدولية العابرة للحدود، ومنها الجرائم السيبرانية، هذا ما جاء في الدورة 77 للجمعية العامة للمنظمة، حيث دعا أمينها العام جميع حكومات الدول لدعم وتطور نظم تبادل المعلومات حول المشتبه فيهم ومحاربة الإرهاب المتنامي في العالم[2]

المبحث الثاني: استراتيجية الوقاية القانونية من مهددات الأمن الرقمي

في المقابل، تتبنى الدول الغربية استراتيجيات أكثر تطورًا في مجال حماية الفضاء الرقمي، نظرًا لما تحققه من تقدم تكنولوجي ووجود بنى تحتية قوية في هذا المجال. تتسم الاستراتيجيات الغربية بوجود تشريعات صارمة تتعلق بحماية البيانات وحقوق الأفراد، بالإضافة إلى استخدام تقنيات متطورة لمواجهة التهديدات السيبرانية. في هذا المبحث، سيتم تحليل الأطر القانونية

[1]- الدام محمد، المرجع السابق، ص45.

[2]- المرجع نفسه.

والتشريعية المتبعة في الدول الغربية لحماية الفضاء الرقمي، بالإضافة إلى استعراض الأساليب الأمنية المتبعة والتعاون الدولي في مجال الأمن السيبراني.

المطلب الأول: المواجهة الدولية والجزائرية لتعزيز الأمن الرقمي

تحظى حماية الأمن الرقمي عناية كبيرة من طرف الدول الأجنبية والجزائر بالخصـــوص، إذ توليها في الوقت الحاضـــر اهتماما اســـتثنائيا في ميدان المعلومات، هذا ما حاولنا التطرق إليه بشيء من التفصل في هذا المطلب.

الفرع الأول: الأساليب التقنية لحماية المعطيات

من أبرز خصـائص الـــ GDPR هو تأكيده على حقوق الأفراد الأسـاسـية فيما يتعلق ببياناتهم الشـخصـية. تشـمل هذه الحقوق حق الوصـول إلى البيانات، الذي يمكن الأفراد من معرفة من يمتلك بياناتهم وكيفية استخدامها، وحق التصحيح الذي يسمح بتعديل البيانات غير الدقيقة. بالإضـــافة إلى ذلك، هناك "الحق في أن يتم نســـيانهم" الذي يتيح للأفراد طلب حذف بياناتهم الشخصية إذا لم تعد هناك حاجة لتخزينها أو استخدامها، مما يضمن حماية أكبر ضد الاستخدام غير المصرح به للبيانات الشخصية.[1]

1. الشفافية والإفصاح

يجب على الشركات والمؤسسات التي تقوم بجمع واستخدام البيانات الشخصية أن تلتزم بمبدأ الشـفافية. وهذا يعني أنه يتعين عليهم توفير معلومات واضـحة ودقيقة للأفراد حول كيفية جمع واســتخدام بياناتهم. يتضـــمن ذلك تفاصـــيل عن الأغراض التي من أجلها يتم جمع البيانات، الأشـخاص الذين سـيحصـلون على هذه البيانات، والفترة الزمنية التي سـيتم خلالها تخزينها. تهدف هذه الشـفافية إلى بناء الثقة بين الأفراد والشـركات وضـمان أن يكون الأفراد على دراية كاملة بكيفية تعامل مؤسساتهم مع بياناتهم الشخصية.

[1]. علي ح. فاضل مرجع سابق، ص 257.

2. المسؤولية والعقوبات

يعد مبدأ المسؤولية من الجوانب الحاسمة في GDPR، حيث يُلزم النظام الشركات والمؤسسات باتخاذ تدابير أمنية وحماية فعالة لضمان سلامة البيانات الشخصية. في حال عدم الامتثال لهذه القوانين، فإن الـــ GDPR ينص على فرض عقوبات مالية ضخمة. يمكن أن تصل الغرامات إلى 4% من الإيرادات العالمية السنوية للشركة أو 20 مليون يورو (أيّهما أكبر)، مما يشكل رادعًا قويًا ضد الانتهاكات. وبذلك، يسعى النظام إلى ضمان أن تلتزم المؤسسات بالمعايير الأمنية العالية فيما يتعلق بحماية البيانات.

3. حماية البيانات من المصدر (Data Protection by Design)

يعد مبدأ "حماية البيانات من المصدر" أحد الركائز الأساسية في الـ GDPR. يتطلب هذا المبدأ من الشركات والمؤسسات تطبيق سياسات وإجراءات أمنية لحماية البيانات الشخصية منذ البداية، أي من مرحلة جمع البيانات وحتى استخدامها وتخزينها. على المؤسسات أن تدمج تدابير حماية البيانات في تصميم أنظمتها وأدواتها، وليس مجرد إضافة هذه التدابير في مرحلة لاحقة[1].

يهدف هذا المبدأ إلى تقليل المخاطر التي قد تهدد خصوصية الأفراد من خلال تصميم الأنظمة بطريقة تضمن حماية البيانات منذ أول لحظة يتم فيها جمعها.

4. نقل البيانات عبر الحدود

يحدد الـــ GDPR أيضًا قواعد صارمة فيما يخص نقل البيانات الشخصية خارج الاتحاد الأوروبي. يتعين على الشركات التي تنقل البيانات إلى دول أخرى ضمان أن هناك مستوى مناسب من الحماية للبيانات في تلك الدول، ويشمل ذلك ضرورة حصول هذه الشركات على ضمانات كافية مثل التوقيع على بنود تعاقدية أو ضمانات قانونية أخرى. يهدف هذا إلى حماية الأفراد في حال تم نقل بياناتهم إلى دول قد لا تتوفر فيها نفس معايير حماية البيانات الموجودة في الاتحاد الأوروبي.

[1]. أنور محمد، مرجع سابق، ص147.

5. دور الوكيل المعتمد لحماية البيانات (DPO)

في العديد من الحالات يطلب الـ GDPR من الشركات تعيين "مسؤول حماي
ة البيانات" أو (Data Protection Officer) DPO لضـمان الامتثال للقانون. يكون دور الـ DPO هو تقديم الاسـتشـارات المتعلقة بحماية البيانات، بالإضـافة إلى مراقبة التزام الشـركة بالقوانين والتشريعات المعمول بها. في حالة وجود مشاكل أو انتهاكات محتملة، يكون الـ DPO هو المسؤول عن الإبلاغ عنها والتعامل مع أي إجراءات تصحيحية قد تكون مطلوبة.

6. تعزيز الثقة وحماية الحقوق الفردية

بجانب الجوانب القانونية والتنظيمية، يهدف GDPR إلى تعزيز الثقة بين الأفراد والشركات. من خلال ضمان الشفافية والمسؤولية وحماية الحقوق الأساسية، يسعى الاتحاد الأوروبي إلى خلق بيئة يشـعر فيها الأفراد بالأمان بشـأن كيفية التعامل مع بياناتهمالشـخصـيةبذلك، يشـكل الـ GDPR نموذجًا قويًا للأنظمة القانونية التي يمكن أن تلهم بقية دول العالم لضـمان حماية حقوق الأفراد في عصر البيانات الرقمية[1].

الفرع الثاني: الولايات المتحدة وتشريعات حماية البيانات

في الولايات المتحدة، تتبنى الحكومة مجموعة من القوانين التي تهدف إلى حماية البيانات الرقمية وضمان أمن الفضاء السيبراني، وتتنوع هذه التشريعات في نطاقاتها وأهدافها. تهدف كل منها إلى معالجة جانب معين من جوانب حماية البيانات الشخصية أو تعزيز الأمن في الفضاء الرقمي. من بين أبرز هذه التشريعات:

1. قانون حماية الشبكات الحاسوبية (CISPA)

يُعد قانون حماية الشبكات الحاسوبية (CISPA) أحد التشريعات الهامة التي تم سنها بهدف حماية البنية التحتية السيبرانية للولايات المتحدة من الهجمات الإلكترونية. يركز CISPA بشكل رئيسـي على تعزيز التعاون بين الحكومة والشـركات الخاصـة في تبادل المعلومات المتعلقة

[1]. الاتحاد الأوروبي، **النظام العام لحماية البيانات (GDPR)**، جريدة قوانين الاتحاد الأوروبي، 25 مايو 2018، ص11.

بالتهديدات الأمنية، ويهدف إلى تسهيل هذا التعاون من خلال تبادل البيانات في الوقت الفعلي. ينص القانون على ضرورة مشاركة معلومات عن الهجمات السيبرانية والتعامل معها بشكل منسق لضمان استجابة سريعة وفعالة. كما يتيح للقطاعين العام والخاص التعاون في مواجهة التهديدات المتزايدة على الشبكات الحاسوبية، مما يعزز قدرة الولايات المتحدة على التصدي للهجمات السيبرانية. ومع ذلك، تعرض CISPA لانتقادات من قبل جماعات حقوق الإنسان والمنظمات المدافعة عن الخصوصية، حيث يعتبر البعض أن هذا التعاون قد يؤدي إلى انتهاك خصوصية الأفراد، نظراً لإمكانية جمع بيانات شخصية بشكل مفرط[1].

2. قانون حماية المعلومات الصحية (HIPAA)

قانون حماية المعلومات الصحية (HIPAA) هو تشريع مهم في الولايات المتحدة يهدف إلى ضمان حماية البيانات الصحية الحساسة للأفراد، من خلال توفير إطار قانوني يفرض معايير دقيقة للأمان وحماية الخصوصية. يتمثل الهدف الأساسي لهذا القانون في الحفاظ على سرية البيانات الصحية الشخصية، سواء كانت في مرحلة التخزين أو النقل أو المعالجة. يتم تطبيق HIPAA على مجموعة واسعة من المؤسسات، بما في ذلك المستشفيات، العيادات، شركات التأمين، وأي جهة تقدم خدمات رعاية صحية، حيث يتعين عليها اتخاذ تدابير أمنية صارمة للحفاظ على خصوصية المرضى. يفرض القانون متطلبات شاملة تتعلق بالتحكم في الوصول إلى المعلومات الصحية، بما في ذلك تحديد من يحق لهم الاطلاع على البيانات وكيفية معالجتها. بالإضافة إلى ذلك، فإن HIPAA ينص على فرض عقوبات مالية شديدة على المؤسسات التي تتقاعس عن الالتزام بالمعايير الأمنية، مما يعزز من أهمية تطبيقه بشكل صارم. كما يساهم القانون في تعزيز الثقة بين المرضى ومقدمي الرعاية الصحية، حيث يضمن

[1]. اتحاد الأمن السيبراني الأمريكي، **قانون حماية الشبكات الحاسوبية (CISPA)**، مجلة الأمن السيبراني. 2020، ص22.

للمرضـــى حق الوصـــول إلى معلوماتهم الصـــحية وتصـــحيحها إذا لزم الأمر، مما يعزز من الشفافية ويعزز حماية حقوق الأفراد في إدارة بياناتهم الصحية[1].

3. قانون حماية الخصوصية على الإنترنت للأطفال (COPPA)

يُعد قانون حماية الخصـوصـية على الإنترنت للأطفال (COPPA) من أبرز التشـريعات التي تهدف إلى حماية بيانات الأطفال الشـخصـية في الفضـاء الرقمي. ينظم هذا القانون كيفية جمع واستخدام البيانات الشخصية للأطفال تحت سن 13 عامًا عبر الإنترنت. يتطلب COPPA من الشـركات التي تجمع بيانات شـخصـية للأطفال الحصـول على موافقة الوالدين قبل جمع أي بيانات، ويشـمل ذلك معلومات مثل الاسـم، العنوان، البريد الإلكتروني، وبيانات الموقع. علاوة على ذلك، يُلزم القانون الشـركات بتوفير إشـعارات واضـحة ومفهومة للآباء حول كيفية جمع البيانات، وطريقة اسـتخدامها، والخيارات المتاحة لهم للتحكم في تلك البيانات. كما يُعطي الآباء حق الوصـول إلى هذه البيانات وحذفها إذا لزم الأمر. يهدف COPPA إلى حماية الأطفال من الاسـتغلال التجاري المحتمل عبر الإنترنت وضـمان عدم جمع بياناتهم الشـخصـية دون موافقة وعي الوالدين.

4. قانون حماية خصوصية المعلومات المالية (GLBA)

قانون حماية خصـوصـية المعلومات المالية (GLBA) هو قانون أمريكي آخر يركز على حماية المعلومات المالية الشخصية للأفراد. ينظم GLBA كيفية تعامل المؤسسات المالية، مثل البنوك وشـركات التأمين، مع البيانات الشـخصـية للعملاء. يشـترط القانون على هذه المؤسـسـات اتخاذ تدابير أمنية لضـمان سـرية وسـلامة البيانات المالية. يتطلب GLBA من الشـركات أن تقدم إشعارات واضحة للعملاء حول سياسات الخصوصية الخاصة بها، ويسمح للعملاء باختيار ما إذا كانوا يرغبون في مشـــاركة بياناتهم مع أطراف ثالثة. بالإضـــافة إلى ذلك، يُلزم القانون

[1]. وزارة الصحة الأمريكية، **قانون حماية المعلومات الصحية (HIPAA)**، تقرير حقوق البيانات الصحية، 2019، ص10.

المؤسسات المالية بتطبيق إجراءات أمنية تمنع الوصول غير المصرح به إلى البيانات الشخصية، مما يعزز الأمان ويعطي العملاء الثقة في أن بياناتهم ستظل محمية.

5. قانون مراقبة الخصوصية وحماية الأمن الوطني (FISA)[1]

قانون مراقبة الخصوصية وحماية الأمن الوطني (FISA) هو قانون آخر يتعلق بحماية الخصوصية، لكن ضمن سياق الأمن الوطني. يهدف هذا القانون إلى تنظيم جمع المعلومات الاستخباراتية المتعلقة بالأفراد، سواء داخل الولايات المتحدة أو خارجها، وهو يتعامل بشكل خاص مع عمليات التنصت والمراقبة على الاتصالات الدولية. يسمح FISA للحكومة الأمريكية بالوصول إلى البيانات والاتصالات عبر الإنترنت بهدف حماية الأمن الوطني، ولكن هذا قد يؤدي إلى تضارب مع الحقوق الفردية في الخصوصية. ولذا، أثيرت العديد من المخاوف حول مدى تأثير هذا القانون على خصوصية الأفراد وحقوقهم في الحماية من المراقبة غير المصرح بها.

6. قانون حماية بيانات المستهلك (CCPA)

على مستوى الولايات، يُعد قانون حماية بيانات المستهلك في كاليفورنيا (CCPA) أحد أقوى القوانين في الولايات المتحدة الذي يركز على حماية الخصوصية. يهدف CCPA إلى منح الأفراد في ولاية كاليفورنيا حقوقًا أقوى في التحكم في بياناتهم الشخصية. يسمح القانون للمستهلكين بطلب الاطلاع على البيانات التي تم جمعها عنهم من قبل الشركات، كما يحق لهم طلب حذف هذه البيانات أو منع بيعها لأطراف ثالثة.

---

[1]. الاتحاد الأوروبي للأمن السيبراني، **اتفاقية بودابست لمكافحة الجرائم الإلكترونية**، تقرير التعاون الدولي في مجال الأمن السيبراني.2020، ص54.

بالإضـافة إلى ذلك، يُلزم الشـركات بالإفصـاح عن كيفية جمع واسـتخدام بيانات المسـتهلكين. يُعتبر CCPA خطوة كبيرة نحو منح الأفراد المزيد من القوة في إدارة بياناتهم الشخصية وضمان الحفاظ على خصوصيتهم.

7. تشريعات أخرى لحماية الخصوصية في قطاع التعليم

يوجد أيضًا مجموعة من التشريعات الأخرى التي تهدف إلى حماية البيانات الشخصية في قطاع التعليم. من أبرز هذه التشـريعات قانون حقوق التعليم وخصـوصـيته (FERPA)، الذي يضـمن حماية خصـوصـية السـجلات التعليمية للطلاب في المؤسـسـات التعليمية. يحدد FERPA كيفية استخدام البيانات الأكاديمية للطلاب ويمنع الإفصاح عنها دون موافقة الأفراد المعنيين أو أولياء الأمور. كما ينظم كيفية التعامل مع هذه البيانات، مما يعزز حماية خصـــوصـــية الطلاب في الفضاء الأكاديمي[1].

تعتبر الولايات المتحدة من الدول التي تمتلك مجموعة من التشــريعات المعقدة والمتنوعة لحماية البيانات الرقمية.

ورغم أن هذه التشـــريعات تغطي العديد من المجالات مثل الصـــحـة، الأمن الســـيبراني، وخصوصية الأطفال، إلا أن النظام الأمريكي لا يتمتع بإطار قانوني شامل يشمل جميع جوانب حماية البيانات الشخصية كما هو الحال مع الـــ GDPR في الاتحاد الأوروبي. لذلك، تعتبر الولايات المتحدة بحاجة إلى تطوير قوانين أكثر تكاملاً وشـــمولية لمواكبة التحديات الرقمية المتزايدة وضمان حماية فعالة للحقوق الفردية في الفضاء الرقمي.

[1]. وكالة حماية البيانات الشخصية الأمريكية، **قانون حماية الخصوصية على الإنترنت للأطفال (COPPA)**، تقرير حماية الخصوصية،2019، ص32.

المطلب الثاني: الأساليب والتقنيات الأمنية والتعاون الدولي

تعتمد الدول الغربية على تقنيات أمنية متقدمة لحماية الفضاء الرقمي مثل الذكاء الاصطناعي وتحليل البيانات الكبيرة (Big Data) للكشف عن التهديدات والهجمات المتطورة. هذه التقنيات توفر أدوات قوية للتنبؤ بالهجمات وتحليل أنماط السلوك غير الطبيعي في الشبكات. على سبيل المثال، يمكن للذكاء الاصطناعي تحليل كميات ضخمة من البيانات في وقت قياسي للكشف عن الأنماط التي قد تشير إلى وجود هجمات محتملة، مثل الهجمات ذات الأهداف الخفية أو الهجمات متعددة المراحل التي قد تكون صعبة الكشف باستخدام التقنيات التقليدية[1].

الفرع الأول: برامج الحماية

بالإضافة إلى ذلك، تعتمد الدول الغربية على مجموعة من الأساليب التقنية لتعزيز أمان الشبكات وحمايتها من الهجمات الإلكترونية المتزايدة، مثل:

1. الجدران النارية (Firewalls)

تعتبر الجدران النارية أحد أهم أدوات الأمان الأساسية في حماية الشبكات من الهجمات. تعمل الجدران النارية على مراقبة وتصفية حركة المرور بين الشبكة الداخلية والعالم الخارجي، مما يتيح التحكم في البيانات المتدفقة ويساعد في منع الوصول غير المصرح به إلى الشبكات[2]

2. أنظمة منع التسلل (IDS) وأنظمة الكشف عن التسلل (IPS)

تستخدم هذه الأنظمة لمراقبة حركة البيانات في الشبكة والكشف عن الأنشطة المشبوهة أو الغير مصرح بها. تهدف هذه الأنظمة إلى التعرف على المحاولات التي قد تشير إلى هجوم، مثل محاولات الوصول غير المصرح به أو محاولات اختراق. كما يمكن لتلك الأنظمة اتخاذ إجراءات تلقائية لتقليل الضرر في حال تم تحديد التهديد[3].

---

[1]. فيليبس س، **التشفير المتقدم في العصر الرقمي**، مجلة الأمان الرقمي، 13(2)، 2019، ص 101-110.

[2]. جورج، ل، **تحليل البيانات الكبيرة واستخدامها في الأمن السيبراني**، مجلة تكنولوجيا المعلومات، 2023، ص 28-42.

[3]. أليسون، مرجع سابق، ص.49

الفرع الثاني: الآليات القانونية في مواجهة الجرائم السيبرانية

من المهم الإشارة إلى أن التعاون الدولي يعتبر جزءًا أساسيًا من حماية الفضاء الرقمي. حيث تسعى الدول الغربية، مثل الولايات المتحدة ودول الاتحاد الأوروبي، إلى تعزيز التعاون مع دول أخرى من خلال إبرام اتفاقيات دولية تهدف إلى تبادل المعلومات والخبرات في مجال الأمن السيبراني. على سبيل المثال:

أولا: الآليات القانونية في مواجهة الجرائم السيبرانية في التشريع الجزائري

تدخل المشرع الجزائري بآليات جديدة لمواجهة الجريمة السيبرانية تمثلت فيما يلي:

أولا: الحماية بموجب الدستور والقانون المدني

كفل دستور الجزائر لسنة 2020 حماية الحقوق الأساسية، بحيث تضمن الدولة عدم انتهاك حرمة الإنسان، وتم ذلك من خلال نصوص تشريعية في قانون العقوبات والإجراءات الجنائية وقوانين أخرى خاصة من أهمها:

- المادة 35، الحريات الأساسية.
- المادة 47 "لكل شخص الحق في حماية حياته الخاصة وشرفه.

لكل شخص الحق في سرية مراسلاته واتصالاته الخاصة في أي شكل كانت.

لا مساس بالحقوق المذكورة في الفقرتين الأولى والثانية إلا بأمر معلل من السلطة القضائية.

حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي.

يعاقب القانون على كل انتهاك لهذه الحقوق".

- المادة 6/54: "الحق في نشر الأخبار والأفكار والوصر والآراء في إطار القانون، واحترام ثوابت الأمة وقيمها الدينية والأخلاقية والثقافية"[1].

[1]- قطاف سليمان، بوقرين عبد الحليم، مرجع سابق، ص344-345.

تبعا على الأهمية الدستورية لحرمة حياة الأشخاص فقد نص المشرع على كل من يقع عليه اعتداء غير مشروع حق التعويض وذلك من خلال المادة 124 من التقنين المدني بقولها: "كل عمل أيا كان يرتكبه المرء يسبب ضررا للغير يلزم من كان سببا في حدوثه بالتعويض"[1].

ثانيا: الفرق بين الأطر القانونية في الولايات المتحدة والاتحاد الأوروبي

على الرغم من التشابه بين الأطر القانونية في الولايات المتحدة والاتحاد الأوروبي في حماية البيانات الشخصية والأمن السيبراني، هناك بعض الفروقات الجوهرية:

التركيز على حماية الأفراد في الاتحاد الأوروبي مقابل التركيز على الأمن في الولايات المتحدة: تختلف السياسات المتعلقة بحماية الخصوصية والأمن بين الاتحاد الأوروبي والولايات المتحدة بشكل ملحوظ، حيث يتبنى كل منهما نهجًا مميزًا في التعامل مع هذه القضايا. في الاتحاد الأوروبي، يُعتبر الحق في الخصوصية جزءًا أساسيًا من حقوق الإنسان، ويُعزز ذلك من خلال اللائحة العامة لحماية البيانات (GDPR)، التي تمنح الأفراد في الاتحاد الأوروبي حقوقًا قوية في التحكم في بياناتهم الشخصية. بموجب هذا القانون، يمكن للأفراد الوصول إلى بياناتهم، تصحيحها، حذفها، وحتى نقلها إلى أطراف أخرى، مما يضمن لهم درجة عالية من السيطرة على معلوماتهم الشخصية. كما يُجبر هذا القانون الشركات على الامتثال لإجراءات صارمة لحماية البيانات، ويشمل ذلك فرض عقوبات مالية ثقيلة على أي خرق لهذه القوانين، مما يعكس اهتمام الاتحاد الأوروبي الكبير بحماية خصوصية الأفراد[2].

في المقابل، تركز التشريعات في الولايات المتحدة بشكل أكبر على حماية الأمن السيبراني وحماية البنية التحتية من الهجمات الإلكترونية. على سبيل المثال، يعتبر قانون حماية الأمن السيبراني (CISPA) واحدًا من أبرز القوانين التي تهدف إلى تعزيز قدرة الحكومة الأمريكية على التصدي للتهديدات الإلكترونية وحماية الشبكات الحساسة. يُمكّن هذا القانون الحكومة من

[1]– بوضياف اسمهان، **الجريمة الالكترونية والإجراءات التشريعية لمواجهتها في الجزائر**، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، مج 03، ع03، جامعة محمد بوضياف، المسيلة، 2018، ص362.

[2]. مارتن، ج. المرجع السابق، ص69.

جمع البيانات المتعلقة بالتهديدات السيبرانية من الشركات الخاصة لمواجهة الهجمات الإلكترونية بشكل سريع وفعال. إلا أن هذه التدابير قد تثير بعض المخاوف المتعلقة بالخصوصية الفردية، حيث قد يتم جمع بيانات الأفراد دون موافقتهم أو دون ضمانات كافية لعدم استخدامها بشكل مفرط.

إذن، بينما يُولي الاتحاد الأوروبي أهمية كبيرة لحماية حقوق الأفراد وحفظ خصوصيتهم في إطار تشريعات قانونية صارمة، فإن الولايات المتحدة تركز بشكل أساسي على تعزيز الأمن الوطني وحماية البنية التحتية في مواجهة التهديدات الإلكترونية. هذا التوجه يعكس اختلافًا جوهريًا في الفلسفة القانونية بين النظامين، حيث يرى الاتحاد الأوروبي أن حماية الخصوصية يجب أن تكون أولوية لا يمكن التنازل عنها، بينما تعطي الولايات المتحدة الأولوية للأمن السيبراني، حتى لو كان ذلك على حساب بعض جوانب الخصوصية الفردية[1].

ثالثا: التعاون بين القطاعين العام والخاص

التعاون بين الحكومة والشركات الخاصة في الولايات المتحدة، كما يظهر في قوانين مثل الـــ CISPA، يركز على تعزيز جهود الأمن السيبراني من خلال التعاون المشترك لمكافحة الهجمات الإلكترونية. بينما في الاتحاد الأوروبي، على الرغم من وجود برامج تعاون مماثلة، إلا أن التشريعات تُعطي الأولوية لحماية الأفراد وحقوقهم في التحكم في بياناتهم، مما يعكس توازنًا أكبر بين الأمان وحماية الخصوصية.

بالتالي، الفرق بين نهج الاتحاد الأوروبي والولايات المتحدة في هذا السياق يعود إلى الفلسفة الأساسية التي توجه كل من النظامين التشريعيين: الاتحاد الأوروبي يركز بشكل أكبر على حقوق الأفراد في الخصوصية، بينما الولايات المتحدة تركز على الأمن السيبراني والتعاون بين الحكومة والقطاع الخاص لمكافحة التهديدات السيبرانية[2].

[1]. مارتن، ج. المرجع السابق، ص68.

[2]. المرجع نفسه، ص38.

الفرع الثالث: تحديات تطبيق الأطر القانونية

تُشكّل الأطر القانونية والتشريعية لحماية الفضاء الرقمي عنصرًا أساسيًا لضمان أمان المعلومات وحماية الأفراد من الجرائم الإلكترونية. ومع ذلك، تواجه هذه التشريعات تحديات متعددة تعيق فعاليتها في مواجهة التهديدات المتزايدة.

أولا: التحديث المستمر للتشريعات

مع التطور السريع لتكنولوجيا المعلومات، تظهر أساليب جديدة لارتكاب الجرائم الإلكترونية، مما يتطلب تحديثًا دوريًا للتشريعات لمواكبة هذه التغيرات.

ومع ذلك، غالبًا ما تكون العمليات التشريعية بطيئة مقارنة بسرعة التطور التكنولوجي، مما يؤدي إلى فجوات قانونية يستغلها المجرمون. على سبيل المثال، مع ظهور تكنولوجيا البلوك تشين والعملات الرقمية، أصبح من الضروري وجود تنظيمات جديدة في مجال التعاملات المالية الرقمية.[1]

ثانيا: الاختلافات بين الدول

تختلف التشريعات المتعلقة بحماية البيانات الشخصية، والتجارة الإلكترونية، وحقوق الملكية الفكرية بين الدول، مما يعقد التعاون الدولي لمكافحة الجرائم السيبرانية العابرة للحدود. هذا التباين يؤدي إلى مشكلات في تنسيق الجهود ومشاركة المعلومات بين الدول المختلفة. على سبيل المثال، يمكن أن تحدث معاملة تجارية عبر الإنترنت بين أطراف من دول مختلفة، ما يؤدي إلى تساؤلات حول القانون الذي ينبغي أن يحكم هذه العلاقة[2].

ثالثا: التهديدات المتطورة

تتزايد الهجمات الإلكترونية في تعقيدها وابتكارها، مما يتطلب من التشريعات أن تكون أكثر مرونة في التعامل مع هذه التهديدات الجديدة. يجب أن تتضمن الأطر القانونية آليات تسمح

[1]. إليسون، ر، **أنظمة الكشف عن التسلل، تطوير وتقنيات حديثة**، مجلة أمن البيانات، 9(4)، 2020، ص 77-90.

[2]. المرجع نفسه، ص91.

بالتكيف السريع مع التهديدات المتغيرة باستمرار. على سبيل المثال، مع تزايد استخدام الشبكات الافتراضية الخاصة (VPN) وتقنيات إخفاء الهوية، تصبح ملاحقة الجناة أكثر صعوبة، مما يستلزم تطوير قوانين جديدة تكون قادرة على مواجهة هذه التهديدات بشكل فعال.

رابعا: صعوبة إنفاذ القوانين

الطبيعة العابرة للحدود للفضاء الرقمي تجعل من الصعب ملاحقة الجناة أو تطبيق الأحكام القضائية.

الجرائم الإلكترونية مثل الاحتيال والقرصنة تحدث غالبًا من دول ذات قوانين ضعيفة أو غير متعاونة، ما يجعل إنفاذ القانون على المستوى الدولي تحديًا كبيرًا. هذا التحدي يتطلب تعزيز التعاون الدولي وتطوير آليات قانونية جديدة للتعامل مع الجرائم الإلكترونية العابرة للحدود.

خامسا: حماية الخصوصية وحقوق الأفراد

مع جمع البيانات واستخدامها بطرق غير قانونية، تتعرض حقوق الأفراد للانتهاك. يجب أن يكون هناك توازن بين حماية المجتمع من الجرائم الإلكترونية وحماية خصوصية الأفراد وحقوقهم. ينبغي أن تضمن التدابير القانونية الفعالة القدرة على ملاحقة المجرمين دون المساس بالحقوق الأساسية للأفراد.[1]

سادسا: تحديات القضاء والتحقيق

يمكن أن تواجه الأجهزة القضائية صعوبة في التعامل مع الجرائم الإلكترونية بسبب التعقيدات التقنية المرتبطة بها. قد يحتاج القضاة والمحققون إلى التدريب المستمر والتحديث القانوني لفهم ومواجهة التحديات الجديدة المرتبطة بالجرائم الإلكترونية.

تُعد الأطر القانونية والتشريعية لحماية الفضاء الرقمي ضرورية لضمان أمان المعلومات وحماية الأفراد من الجرائم الإلكترونية. ومع ذلك، يتطلب التصدي للتحديات المستمرة تحديث التشريعات.

[1]. إليسون، ر. المرجع السابق، ص98.

خلاصة الفصل الثاني

من خلال استعراض استراتيجيات الدول العربية والدول الغربية لحماية الفضاء الرقمي، يتضح أن هناك تفاوتًا في مستوى التطور والتنفيذ بين هذه الدول. بينما تسعى الدول العربية لتطوير الأطر التشريعية والتقنية لمواكبة التحديات الجديدة في الفضاء الرقمي، تعتمد الدول الغربية على بنى تحتية قوية واستراتيجيات قانونية وتقنية متقدمة لمواجهة هذه التهديدات. يتطلب الأمر من الدول العربية العمل على تعزيز التعاون الدولي واستخدام تقنيات متطورة في مجال الأمن السيبراني، في حين تستمر الدول الغربية في تحديث قوانينها وأساليبها الأمنية لمواكبة التحولات الرقمية السريعة.

الخاتمـــــــة

الخاتمـــــة

وفي ختام بحثنا، توصلنا إلى أن مبدأ الأمن القانوني في الفضاء الرقمي أصبح أحد المرتكزات الأساسية لضمان حماية الحقوق والحريات في ظل التطور التكنولوجي المتسارع، ولا سيما في مجال تكنولوجيا الإعلام والاتصال، وتوصلنا إلى النتائج التالية:

1. أن تعزيز هذا المبدأ يقتضـــي وجود بيئة قانونية مرنة ومتكاملة قادرة على التكيف مع التحديات الرقمية المعاصـرة، بما يضـمن الشـفافية، ويوفر الولوج العادل إلى المعلومة القانونية، ويكفل الحماية الفعّالة للمعطيات الشخصية.
2. اتضح من خلال المقارنة بين التجربتين الغربية والعربية أن الدول الغربية، بفضل أطرها التشريعية المحكمة ومؤسساتها المختصة، استطاعت تحقيق تقدم ملحوظ في مجال حماية الفضاء الرقمي، من خلال اعتماد سياسات متقدمة كالنظام الأوروبي العام لحماية البيانات والتعاون الدولي في مكافحة الجرائم السيبرانية. أما على الصعيد العربي، فرغم الجهود المبذولة، لا تزال المنظومات القانونية والمؤسساتية تعاني من محدودية في التنسيق والتكامل، مما يستدعي ضرورة إعادة تقييم الاستراتيجيات المتبعة وتعزيز القدرات التشريعية والتقنية.
3. ان تكريس مبدأ الأمن القانوني في البيئة الرقمية يستوجب تبني رؤية تشريعية شاملة تتماشى مع المعايير الدولية، وتطوير الأطر القانونية الوطنية، وتفعيل التعاون الإقليمي والدولي، إضافة إلى تعزيز الثقافة القانونية الرقمية لدى الأفراد والمؤسسات، من أجل بناء فضاء رقمي آمن يكرّس سيادة القانون ويحمي الحقوق والحريات في العصر الرقمي.

ونظرا لنقص بعض العناصر ارتأينا اقتراح بعض المقترحات المتمثلة فيما يلي:

4. اختيار الأشخاص محل الثقة للقيام بمعالجة البيانات وامتلاكهم الكفاءة العالية في استخدام الحاسوب.

5. عقد ندوات إعلامية لتوضـيح محتوى القانون الخاص بحماية البيانات الشـخصـية للأفراد والهيئات والتأكيد على المخاطر الناجمة عن استعمالها بطرق غير مشروعة.
6. ضـــرورة عقد مؤتمرات دولية للتحذير من اختراق البيانات الشـــخصـــية للأفراد وتشـــديد العقوبة على مرتكبيها.
7. العمل على سن قانون دولي موحد للأمن السيبراني تتساوى فيه العقوبات.

قائمة المصادر والمراجع

قائمة المصادر والمراجع

باللغة العربية

I. المصادر

القوانين:

1. الأمر رقم **03-05**، المؤرخ في **19** جمادى الأولى سنة **1424هـ**، الموافق **19** يوليو عام **2003**، **يتعلق بحقوق المؤلف والحقوق المجاورة**، ج ر ع **44**، الصدارة في **23** يوليو **2003**.
2. الأمر رقم **21-11**، المؤرخ في **25** أوت **2021**، المتمم للأمر رقم **66-155**، **المتضمن ق إ ج ج**، ج ر ع **65**، الصادرة بتاريخ **26** أوت **2021**.
3. القانون رقم **04-15**، المؤرخ في **10** نوفمبر **2004**، المعدل والمتمم للأمر رقم **66-155**، **المتضمن قانون العقوبات**، ج ر ع **71**، الصادرة بتاريخ **10** نوفمبر **2004**.
4. القانون رقم **08-01**، المؤرخ في **23** يناير **2008**، يتمم القانون رقم **83-11**، المؤرخ في **02** يوليو **1983**، **المتعلق بالتأمينات الاجتماعية**، ج ر ع **04**، الصادرة في **27** يناير **2008**.
5. القانون رقم **15-04**، المؤرخ في **2015/02/01**، **الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين**، ج ر ع **06**، الصادرة بتاريخ **2015/02/10**.
6. القانون رقم **16-02**، المؤرخ في **19** جوان **2016**، المعدل والمتمم للأمر **66-155**، المتضمن قانون العقوبات، ج ر ع **37**، الصادرة بتاريخ **22** جوان **2016**.
7. القانون رقم **18-04**، المؤرخ في **10** ماي **2018**، **يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية**، ج ر ع **27**، الصادرة في **13** ماي **2018**.
8. القانون رقم **18-05**، المؤرخ في **10** ماي **2018**، **المتعلق بالتجارة الالكترونية**، ج ر ع **28**، الصادرة في **16** ماي **2018**.
9. القانون رقم **18-07**، المؤرخ في **25** رمضان عام **1439هـ**، الموافق **10** يونيو سنة **2018**، **يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي**، ج ر ع **34**، الصادرة بتاريخ **25** رمضان **1439هـ**، الموافق **10** يونيو سنة **2018**.

II. المراجع

الكتب:

10. أحمد سمير، **الجرائم الإلكترونية: الأبعاد القانونية والتقنية**، دار الفكر القانوني، 2020.
11. أنور محمد، **أنظمة الكشف عن التسلل في الأمن السيبراني**، مراجعة الأمن السيبراني، 2021، د ب ن.
12. سليم وليد السيد، **ضمانات الخصوصية في الانترنت**، دار الجامعة الجديدة، الإسكندرية، 2012.
13. طه وليد، **التنظيم التشريعي للجرائم الالكترونية في اتفاقية بودابست**، قطاع التشريع بوزارة العدل، جمهورية مصر، د س ن.

قائمة المصادر والمراجع

14.عبد العزيز الغنام، **الأمن السيبراني وحماية البيانات في العصر الرقمي**، دار الفكر العربي، 2022.

15.عجة الجيلالي، **مدخل للعلوم القانونية، نظرية القانون**، ج1، برتي، الجزائر، 2009.

16.فضل سليمان أحمد، **المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية**، دار النهضة العربية، القاهرة، 2013.

17.مارك أندرسون، **الأمن السيبراني والسياسة العالمية**، جامعة أكسفورد،2021.

18.منصور محمد حسنين، **الإثبات التقليدي والالكتروني**، دار الفكر الجامعي، الإسكندرية، 2006.

المجلات:

19.أفتيسان وريدة، بن ناصر وهيبة، **دسترة مبدأ الأمن القانوني: التجربة الجزائرية نموذجا**، مجلة الدراسات القانونية (صنف ج)، مج 08، ع02، جامعة يحي فارس المدية، الجزائر، 2015.

20.إليسون، ر، **أنظمة الكشف عن التسلل، تطوير وتقنيات حديثة**، مجلة أمن البيانات، 9(4)، 2020.

21.بساعد سامية، **حماية البيانات الشخصية للمستهلك من مخاطر الدفع الالكتروني**، مجلة الحقوق والعلوم الإنسانية، مج15، ع01، جامعة زيان عاشور، الجلفة، 2022.

22.بن جدو بن علية، **تحديات الأمن السيبراني لمواجهة الجريمة الالكترونية**، المجلة الجزائرية للأمن الإنساني، مج07، ع02، جامعة باتنة 1، 2002.

23.بوجمعة فاطمة الزهراء، **تأثير التطور التكنولوجي وتقنيات المعلومات على تحقيق الأمن القانوني**، مجلة الفكر المتوسطي، مج11، ع01، الجزائر، 2002.

24.بوزنون سعيد، **مكافحة الجريمة الالكترونية في التشريع الجزائري**، مجلة العلوم الإنسانية، مج ب، ع52، جامعة الإخوة منتوري، قسنطينة، 2019.

25.بوصبع سلاف، **أثر سياسات الأمن السيبراني على الأمن القومي الأمريكي، قراءة في التجربة وفي إمكانية التطبيق على الحالة الجزائري**، مجلة السياسة العالمية، مج8، ع2، جامعة أمحمد بوقرة بومرداس، الجزائر، 2024.

26.بوضياف اسمهان، **الجريمة الالكترونية والإجراءات التشريعية لمواجهتها في الجزائر**، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، مج 03، ع03، جامعة محمد بوضياف، المسيلة، 2018.

27.بوعكة كمال، **الحماية القانونية للأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي**، المجلة الجزائرية لقانون الاعمال، جامعة محمد بوضياف، المسيلة، مج 01، ع02، 2020.

28.بوكرة رشيدة، **تحديات العصر الرقمي في مواجهة خطط حماية الحق في الخصوصية**، مجلة حقوق الإنسان والحريات العامة، (م.ح.إ.ح.ع)، مج07، ع02، جامعة مستغانم، 2022.

29.بيدي آمال، **جهود الأمم المتحدة في مكافحة الجريمة السيبرانية**، مجلة البحوث في الحقوق والعلوم السياسية، مج 08، ع01، جامعة تيارت، 2022.

قائمة المصادر والمراجع

30.جاوزني اسماعيل، **الأمن القانوني وعناصرها**، مجلة تحولات العدد الثاني جوان 2001.

31.جبور منى الأشـقر، جبور محمد، **البيانات الشـخصـية والقوانين العربية، الهم الأمني وحقوق الأفراد**، ط1، المركز العربي للبحوث القانونية والقضائية، لبنان، 2018.

32.جورج، ل، **تحليل البيانات الكبيرة واستخدامها في الأمن السيبراني**، مجلة تكنولوجيا المعلومات، 2023.

33.حاجي نعيمة، **الجريمة السـيبرانية والجهود الدولية لمكافحتها**، مجلة النبراس للدراسـات القانونية، مج 06، ع01، جامعة العربي التبسي، تبسة، 2021.

34.الخداري عبد الحق، **مبدأ الأمن القانوني ودوره في حماية حقوق الانسان**، مجلة الحقيقة، سنة 2016.

35.زهدور إنجي هند نجوى ريم سـندس، **اسـتراتيجيات الوقاية القانونية والأمنية من مهددات الأمن الرقمي**، المجلة الدولية لنشـر البحوث والدراسـات، مج2، ع16، كلية الحقوق والعلوم السـياسـية، جامعة محمد بن أحمد، وهران، الجزائر، فبراير 2021.

36.سعدي بن علي بن حسن المعمري، رضوان أحمد الحاف، **مبدأ الأمن القانوني ومقومات الجودة التشريعية**، مجلة البحوث القانونية والاقتصادية، ع79، مارس 2022.

37.شعاعة حليمة، شنين سناء، **أثر التطور التكنولوجي على تحقيق مبدأ الأمن القانوني وأهم التحديات التي تعترضه**، جامعة قاصدي مرباح، ورقلة، جامعة عمار ثليجي بالأغواط، د س ن.

38.علال نزيهة، **الإطار القانوني لحماية المعطيات ذات الطابع الشخصي في الفضاء الالكتروني في ظل القانون رقم 18-07**، دائرة البحوث والدراسـات القانونية والسـياسـية، مج04، ع2، المركز الجامعي مرسـلي عبد الله، تيبازة، الجزائر، 2020.

39.فيليبس س، **التشفير المتقدم في العصر الرقمي**، مجلة الأمان الرقمي، 13(2)، 2019.

40.قطاف سـليمان، بوقرين عبد الحليم، **الآليات القانونية الموضـوعية لمكافحة الجرائم السـيبرانية في ظل اتفاقية بودابسـت والتشـريع الجزائري**، مخبر البحث في الحقوق والعلوم السـياسـية، جامعة عمار ثليجي بالأغواط، المجلة الأكاديمية للبحوث القانونية والسياسية، مج6، ع1، 2022.

41.كنوفي وسيلة، **جدلية القانون والتكنولوجيا بين التكامل والتحايل**، المجلة الجزائرية للعلوم القانونية والسياسية، مج57، ع5، الجزائر، 2020.

42.مسعودي هشام، **آراء الفكر القانوني حول مصطلح الأمن القانوني دراسة في الإشكالية والمفهوم**، مجلة الاجتهاد القضائي، مج12، ع 02، مخبر أثر الاجتهاد القضائي على حركة التشريع، جامعة محمد خيضر، بسكرة، أكتوبر 2020.

43.نادر أبو زيد، **التشفير والأمن السيبراني دراسة تحليلية**، مجلة دراسات الحماية الرقمية، ع 5، 2021.

التقارير:

قائمة المصادر والمراجع

44. الاتحاد الأوروبي للأمن السيبراني، **اتفاقية بودابست لمكافحة الجرائم الإلكترونية**، تقرير التعاون الدولي في مجال الأمن السيبراني، 2020.

45. بيل جيتس، **المعلوماتية بعد الانترنت**، سلسلة عالم المعرفة، المجلس الوطني للثقافة والفنون والآداب، الكويت، 1998.

46. **تقرير الإتحاد الأوروبي حول إستراتيجية الأمن السيبراني**،2023.

47. زهرة، ر، **الذكاء الاصطناعي في كشف التهديدات السيبرانية، الذكاء السيبراني**،2021.

48. عطية إدريس، **مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري**، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي، تبسة، الجزائر، مقال منشور على الموقع: https://asjp.cerist.de.

المواقع:

49. اتحاد الأمن السيبراني الأمريكي، **قانون حماية الشبكات الحاسوبية (CISPA)**، مجلة الأمن السيبراني. 2020.

50. الاتحاد الأوروبي، **النظام العام لحماية البيانات (GDPR)**، جريدة قوانين الاتحاد الأوروبي، 25 مايو 2018.

51. الاستراتيجية الوطنية للأمن السيبراني في المملكة، مقال منشور على الموقع : https://my.gov.sa .

52. الأمن السيبراني في الإمارات العربية المتحدة، أولوية متزايدة في العصر الرقمي، مقال منشور على الموقع: https://dralaanasr.com .

53. أنظمة كشف التسلل IDS، مقال منشور على الموقع: https://majed.blog .

54. قانون الأسواق الرقمية ما التزامات عمالقة التكنولوجيا في أوروبا؟ مقال منشور على الموقع: https://asharq.com.

55. قائمة التحقق من الامتثال للائحة العامة لحماية البيانات (GDPR)، منشورة على الموقع: https://www.ibm.com .

56. كيفية تعزيز الأمن السيبراني باستخدام التحليل البياني المتقدم، مقال منشور على الموقع: http://omalytica.com .

57. مراعاة قانون الخدمات الرقمية (DSA)، منشور على الموقع: https://www.ad-dawra.com .

58. معايير الأمن السيبراني: الولايات المتحدة الأمريكية وأوروبا والشرق الأوسط، منشورة على الموقع: https://ceinterim.com

الهيئات:

59. **موقع الاتحاد الأوروبي-تفاصيل عن GDPR=https=//gdpr.ev.**

60. موقع الإتحاد الدولي للاتصالات، **تقارير حول الأمن الرقمي https://www.itu.int** .

61. وزارة الصحة الأمريكية، **قانون حماية المعلومات الصحية (HIPAA)**، تقرير حقوق البيانات الصحية، 2019.

62. وكالة حماية البيانات الشخصية الأمريكية، **قانون حماية الخصوصية على الإنترنت للأطفال (COPPA)**، تقرير حماية الخصوصية، 2019.

قائمة المصادر والمراجع

مذكرات الماستر

63.الدام محمد، **الأمن السيبراني**، مذكرة تخرج ضمن متطلبات نيل شهادة الماستر في الحقوق، تخصص جريمة وأمن، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر، الوادي، 2022-2023.

القوانين الأجنبية

64.قانون حماية البيانات الشخصية رقم ( ) لسنة 2020، الأردن، منشور في الموقع:https://lob.gov.jo .

65.قانون تونسي أساسي، ع **63**، المؤرخ في **27** جويلية **2004**، **يتعلق بحماية المعطيات الشخصية**، الفصل4.

66.قانون رقم **151**، **يتضمن حماية البيانات الشخصية في مصر (PDPL)**، 2020.

67.القانون المغربي رقم **08-09**، **يتعلق بحماية الأشخاص الذاتيين اتجاه معالجة المعطيات ذات الطابع الشخصي**، ج ر **5711**، بتاريخ **23** فبراير **2009**.

فهـرس المحتويـــات

فهرس المحتويات

فهرس المحتويات

فهرس المحتويات

الملخص:

يهدف هذا البحث إلى دراسة مبدأ الأمن القانوني في الفضاء الرقمي، في ظل التحول التكنولوجي المتسارع وتزايد الاعتماد على تكنولوجيا الإعلام والاتصال. يتناول الفصل الأول أهمية استخدام هذه التكنولوجيا لتعزيز الأمن القانوني، من خلال استعراض الإطار المفاهيمي، ودور التشريعات، والتحديات التي تواجه تطبيق الإجراءات القانونية في البيئة الرقمية. أما الفصل الثاني، فيتناول الاستراتيجيات الوطنية لحماية الفضاء الرقمي، مركزًا على الأطر التشريعية والتطورات التقنية في الدول العربية والغربية، خاصة في مجالات حماية البيانات الشخصية، والتعاون الدولي في مجال الأمن السيبراني، والفروق بين السياسات المعتمدة في المنطقتين.ويخلص البحث إلى أن تحقيق الأمن القانوني في الفضاء الرقمي يتطلب تكييف الأنظمة القانونية مع التحولات الرقمية، وتعزيز الأطر المؤسساتية والتقنية، وتشجيع التعاون الإقليمي والدولي لمواجهة التهديدات السيبراني.

الكلمات المفتاحية:

الأمن القانوني – الأمن السيبراني – حماية البيانات الشخصية – الفضاء الرقمي

Abstract

This research aims to study the principle of legal security in the digital space, in light of the rapid technological transformation and increasing reliance on information and communication technology. The first chapter addresses the importance of using this technology to enhance legal security, by reviewing the conceptual framework, the role of legislation, and the challenges facing the implementation of legal procedures in the digital environment. The second chapter addresses national strategies for protecting the digital space. Focusing on legislative frameworks and technological developments in Arab and Western countries, particularly in the areas of personal data protection, international cooperation in cyber security, and the differences between the policies adopted in the two regions. The study concludes that achieving legal security in the digital space requires adapting legal systems to digital transformations. Strengthening institutional and technical frameworks, and encouraging regional and international cooperation to confront cyber threats.

Key words:

- Legal security - Cyber security - Personal data protect – Digital space –

انتهى بفضل الله وتوفيقه.