وزارة التعليم العالي والبحث العلمي

جامعة يحي فارس -المدية

كلية الحقوق والعلوم السياسية

قسم الحقوق

مذكرة بعنوان:

الأمن المعلوماتي

ودوره في حماية الحياة الخاصة

مذكرة لنيل شهادة الماستر

الميدان حقوق وعلوم سياسية

تخصص: قانون جنائي وعلوم جنائية

إعداد الطالبين:

- عبد المالك حربي.

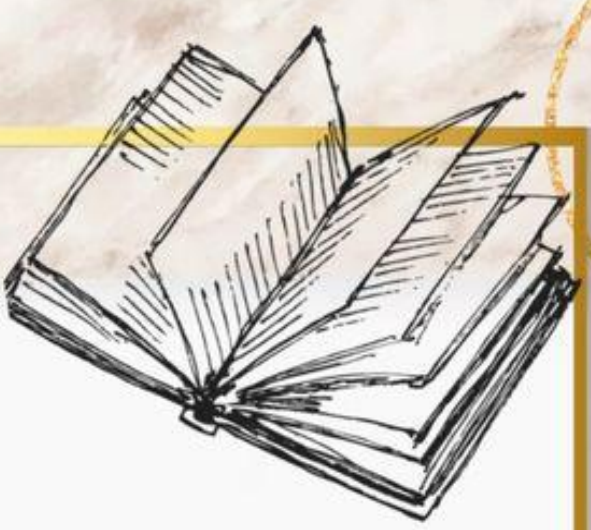
- عيسى بلولو.

إشراف الأستاذ(ة):

- د/ بركان فضيلة.

السنة الجامعية: 2025/2024


بسم الله الرحمن الرحيم



شكر وعرفان

قال تعالى: "يٰأَيُّهَا ٱلَّذِينَ آمَنُواْ لَا تَدْخُلُواْ بُيُوتًا غَيْرَ بُيُوتِكُمْ حَتَّىٰ تَسْتَأْنِسُواْ وَتُسَلِّمُواْ عَلَىٰ أَهْلِهَا ذٰلِكُمْ خَيْرٌ لَّكُمْ لَعَلَّكُمْ تَذَكَّرُونَ ﴿٢٧﴾ فَإِن لَّمْ تَجِدُواْ فِيهَآ أَحَدًا فَلَا تَدْخُلُوهَا حَتَّىٰ يُؤْذَنَ لَكُمْ وَإِن قِيلَ لَكُمُ ٱرْجِعُواْ فَٱرْجِعُواْ هُوَ أَزْكَىٰ لَكُمْ وَٱللَّهُ بِمَا تَعْمَلُونَ عَلِيمٌ ﴿٢٨﴾ لَّيْسَ عَلَيْكُمْ جُنَاحٌ أَن تَدْخُلُواْ بُيُوتًا غَيْرَ مَسْكُونَةٍ فِيهَا مَتَاعٌ لَّكُمْ وَٱللَّهُ يَعْلَمُ مَا تُبْدُونَ وَمَا تَكْتُمُونَ ﴿٢٩﴾ "

سورة النورالاية: 27،28،و29.

الحمد لله الذي أنار لنا درب العلم والمعرفة،

وأعاننا على أداء هذا الواجب ووفقنا لإنجاز هذا العمل..

أشكر كل من ساهم في إخراج هذا العمل وعلى رأسهم

الأستاذة المشرفة * بركان فضيلة *

التي لم تبخل علينا بتوجيهاتها ونصائحها القيمة..

والتي كانت عونا لنا في إتمام هذا البحث..

إلى كل من أشعل شمعة في دروب عملنا..

وإلى من أعطانا من حصيلة فكره لينير دربنا..

نرجوا من الله عز وجل أن ينفعنا بهذا العمل..

وأن ييسر خطانا ويوفقنا لما فيه خير وصلاح لأمتنا..





الإهـداء

"الحمد لله والصلاة والسلام على المصطفى "ﷺ

أما بعد أود أن أهدي هذا العمل المتواضع إلى:

من ساندتني في صلاتها ودعائها وشاركتني أفراحي وأحزاني ..

إلى أمي الغاليةأطال الله في عمرها..

إلى عماد البيت ونوره الذي منحني الرعاية والحب والعطاء..

أبي الغالي حفظه الله ورعاه..

إلى إخوتي وأخواتي..

إلى رفيقة دربي وسندي في الحياة زوجتي

إلى كل عائلتي.. وأصدقائي..

إلى كل من وسعتهم ذاكرتي ولم تسعهم مذكرتي

إلى كل من علمني حرفا أهدي هذا العمل..



*** عبد المالك ***



الإهــداء

إلى كل من زرعا لي نورا وهاجا في طريقي وقلبي

إلى من ربياني صغيرا. أهدي ثمرة جهدي إلى من علمتني

ومنحتني الأفضل

إلى " أمي " ..

أهدي ثمرة جهدي إلى من منحني الحماية والرعاية والحب والعطاء

الذي منحني القوة والعزيمة لمواصلةمشواري الدراسي إلى " أبي"

كما أهدي عملي هذا إلى إخوتي وأخواتي.

إلى رفيقة دربي وسندي في الحياة زوجتي

إلى كل الأهل والأقارب.

إلى زملائي الذين رافقوني طوال مشواري الدراسي

كل من ساعدني من قريب أو بعيد.



*** عيسى ***

مقـــدمـــة

مقدمة:

شهد العالم خلال العقود الأخيرة ثورة رقمية غير مسبوقة، مست مختلف مجالات الحياة، وأسهمت في تطوير أنماط جديدة من التواصل والعمل والمعاملات. إلا أن هذا التوسع في الاعتماد على الوسائل التكنولوجية صاحبه بروز مخاطر تهدد أحد أهم حقوق الإنسان الأساسية، وهو الحق في الحياة الخاصة، لاسيما في ظل تطور وسائل التتبع، وجمع البيانات، والقرصنة، ما جعل من حماية الخصوصية الرقمية قضية مركزية في العصر الحديث.

وفي هذا الإطار، برز الأمن المعلوماتي كأداة أساسية لمواجهة هذه التهديدات، إذ يهدف إلى حماية المعلومات ونظم المعالجة من أي اختراق أو اعتداء قد يؤدي إلى انتهاك الخصوصية أو الإضرار بالمصالح الفردية والمؤسسية. غير أن الأمن المعلوماتي في حد ذاته لا يكفي، ما لم يكن مدعومًا بآليات متقدمة من الأمن السيبراني، تُمكن من التصدي للهجمات الإلكترونية المعقدة، وتمنح الأفراد والمجتمعات حماية فعلية في البيئة الرقمية.

إن العلاقة بين الأمن المعلوماتي وحماية الحياة الخاصة لم تعد مجرد مسألة تقنية، بل أصبحت قضية قانونية وأخلاقية تُطرح على مختلف التشريعات الوطنية والدولية، التي باتت مطالبة بإرساء قواعد قانونية حديثة، مرنة وفعالة، تواكب هذا الواقع المتسارع، وتؤمن التوازن بين متطلبات الأمن واحترام الحقوق والحريات.

إلا أن فعالية الأمن المعلوماتي، حتى مع الدعم الذي توفره آليات الأمن السيبراني، تبقى محل تساؤل في ظل تزايد التهديدات الرقمية التي تمس الحياة الخاصة، مما يثير الحاجة إلى تقييم مدى نجاعة هذه الوسائل القانونية والتقنية في تحقيق الحماية المطلوبة.

وعليه، نطرح الإشكالية الرئيسية التالية:

- إشكالية البحث:

إلى أي مدى يساهم الأمن المعلوماتي، مدعومًا بآليات الأمن السيبراني، في حماية الحياة الخاصة في البيئة الرقمية ؟.

❖ **الفرضيات:**

وللإجابة عن هذه الإشكالية، ينبثق عنها عدد من التساؤلات الفرعية، منها:

- ما الإطار المفاهيمي للأمن المعلوماتي، وما علاقته بالأمن السيبراني؟

- كيف تنظم التشريعات الوطنية والدولية حماية الخصوصية في البيئة الرقمية؟

- ما مدى فاعلية الآليات التقنية والتشريعية المعتمدة في حماية البيانات الشخصية؟

- ما التحديات التي تواجه الدول في تطبيق الحماية المعلوماتية للخصوصية؟

وتُقترح الفرضيات التالية كبنية مبدئية للبحث:

- الفرضية الأولى: الأمن المعلوماتي يشكّل أداة فعالة نظريًا في حماية الخصوصية، لكنه يواجه تحديات كبيرة في مجال تطبيقه.

- الفرضية الثانية: العلاقة بين الأمن السيبراني والخصوصية الرقمية علاقة تكاملية، تتطلب تنسيقًا تشريعيًا وتقنيًا لتحقيق التوازن.

❖ **أهمية البحث:**

من الناحية العلمية

- المساهمة في إثراء الدراسات القانونية المتعلقة بالأمن المعلوماتي وحماية الخصوصية الرقمية.

- تقديم مقاربة مقارنة بين التشريع الجزائري والمعايير القانونية الدولية في مجال حماية الحياة الخاصة.

من الناحية العملية

- تحديد أوجه القصور والتحديات في التشريع الوطني لمواجهة الجرائم الإلكترونية المتعلقة بالخصوصية.

- اقتراح توصيات عملية لتعزيز الأطر القانونية والتقنية لحماية الحياة الخاصة في البيئة الرقمية

❖ **أهداف البحث:**

- تحليل المفاهيم القانونية والفنية المتعلقة بالأمن المعلوماتي وأمن الحياة الخاصة في البيئة الرقمية.

- تبيان مدى تأثير الأمن المعلوماتي في حماية الحقوق الفردية، خصوصًا الحق في الحياة الخاصة.

- دراسة الإطار القانوني الجزائري والتنظيمات الدولية لحماية الخصوصية الرقمية ومكافحة الانتهاكات.

- تقييم دور آليات الأمن السيبراني في تعزيز الحماية القانونية للمعلومات والبيانات الشخصية.

❖ **أسباب إختيار الموضوع:**

- أسباب ذاتية:

اهتمام الباحث بالقضايا الحديثة في القانون الجنائي المتعلق بجرائم المعلوماتية وحماية الحقوق الرقمية.

الرغبة في الإسهام الأكاديمي في موضوع يجمع بين القانون والتقنية الرقمية، ويساهم في تطوير التشريع الوطني.

التطلع لفهم معمق للآليات القانونية والأمنية التي تحمي الحياة الخاصة، والاستفادة منها في المجال المهني والأكاديمي.

- أسباب موضوعية:

أهمية الموضوع في ظل التطور السريع لتقنيات المعلومات وانتشار الجرائم الإلكترونية التي تهدد الخصوصية.

الحاجة إلى دراسة دور الأمن المعلوماتي والآليات القانونية المتاحة لحماية الحياة الخاصة في البيئة الرقمية.

نقص الدراسات القانونية المقارنة التي تجمع بين التشريع الوطني والمعايير الدولية في هذا المجال.

❖ **المنهج المتبع:**

بهدف الإجابة على اشكالية البحث فإنه تم الإعتماد على المنهج التحليلي الوصفي، وذلك بالرجوع إلى المراجع العربية والقوانين لإستنباط أهم المفاهيم المتعلقة بالأمن المعلوماتي والحياة الخاصة، ومحاولة إستخلاص العلاقة بينهما.

❖ **هيكل البحث:**

للإحاطة بموضوع بحثنا وللإجابة على إشكالية الدراسة الأساسية والأسئلة الفرعية، وفي سبيل التوصل إلى الأهداف الموجودة لهذه الدراسة مع مراعاة المنهج العلمي المستخدم، وعدم الخروج عن المحاور الأساسية لمذكرتنا، قسمنا هذه المذكرة إلى فصلين.

فقد خصصنا الفصل الأول للحديث عن الأمن المعلوماتي، فقسمناه إلى مبحثين تناولنا في المبحث الأول: ماهية الأمن المعلوماتي ومجلاته، وفي المبحث الثاني تناولنا دور الأمن السيبراني في دعم الأمن المعلوماتي.

أما الفصل الثاني فخصصناه لدراسة حماية الحياة الخاصة، فقسمناه إلى مبحثين، تطرقنا في المبحث الأول إلى الإطار القانوني لحماية الحياة الخاصة في البيئة الرقمية، فتناولنا في المبحث الثاني آليات تعزيز الأمن المعلوماتي لحماية الحياة الخاصة.

وننهي بحثنا هذا بخاتمة موجزة نورد فيها أهم النتائج التي توصلنا إليها والتوصيات التي يمكن إقتراحها

❖ **صعوبات البحث:**

يسعى أي طالب لإنجاز مذكرة متقنة ومستوفية لجميع جوانب الدراسة، غير أن الدراسة لأي موضوع تواجهه مجموعة من العقبات والصعوبات، وفي هذه الدراسة واجهنا صعوبات تتمثل في:

ندرة المصادر العربية المتخصصة، وتعقيد التداخل بين الجوانب التقنية والقانونية، وسرعة التطور التشريعي، بالإضافة إلى محدودية الدراسات المقارنة بين التشريعات الوطنية والدولية.

الفصل الأول:

الأمن المعلوماتي

أدى التطور التكنولوجي إلى اتساع مفهوم الأمن، خاصة مع المخاطر التي تحدثها تقنية المعلومات وتحديدها بالمساس بسلامة المعلومات وأمن أنظمة معالجتها، أو فيما يعرف بمخاطر المعلوماتية.

ولمواجهة هذا الخطر ظهر مفهوم جديد للأمن وهو ما يعرف بالأمن المعلوماتي والسلامة المعلوماتية، حيث كان هذا الأخير أكثر موضوعات في عصر المعلومات إثارة للجدل القانوني، ونتساءل لماذا كان أحدث وآخر إفرازات عصر المعلومات، من بين موضوعاتها وتحدياتها وقطاعاتها أكثرها إثارة للجدل وأكثرها محلا للاهتمام؟ وعن مدى الالتزام بالحماية ضد هذه المخاطر؟.

وإن استظهار واستطلاع بداية تطور ونماء التقنية المعلوماتية وتطور تأثر النظام القانوني بموضوعاتها وفقا لما سيتم توضيحه لاحقا، يظهر أن الخصوصية وحماية الحياة الخاصة من مخاطر التقنية كانت أولى الموضوعات اهتماما في أواخر الستينيات، ثم تبعها الاهتمام بجرائم الكمبيوتر ومن ثم الملكية الفكرية لمصنفات المعلوماتية وتحديد البرامج اعتبارا من الصنف الثاني للسبعينيات ومطلع الثمانينات، ومن ثم مسائل الموقع الإلكتروني والتجارة الإلكترونية مترافقة مع مسائل أمن الأعمال المصرفية والمالية مترافقة مع أمن المعلومات في بداية مطلع التسعينيات.

هذا الموضوع الذي تسعى الدول والحكومات والمؤسسات والأفراد إلى تحقيقه من جراء ما شوهد من أخطار وخسائر نتيجة الاختراقات المعلوماتية بمختلف أشكالها.

المبحث الأول: المفاهيم والأسس العامة الأمن المعلوماتي

لقد كان للتطور التكنولوجي والتقدم العلمي والتقني في مجال أمن وتقنيات المعلومات بالغ الأثر في حماية الأجهزة والوسائل العلمية التي تحقق قدرا من الحماية تتماشى مع التقدم العلمي والتطور الخطير في أساليب الاختراق التي تستهدف أنظمة المعلومات وما تتضمنه من معلومات، حيث احتلت المعلومات في الوقت الحاضر مكانا متميزا لما لها من قيمة مادية ومعنوية، ومن الخطورة أن لا تحاطه بحماية قانونية وإن توفرت الحماية الفنية، ولكن قبل الخوض في عناصر تلك الحماية لابد أن نقوم أولا بتحديد ماهية السلامة الأمن المعلوماتي، يتطلب ذلك بيان كل من مفهوم الأمن المعلوماتي وأهميته، إلى جانب بيان العناصر والوسائل التي يقوم عليها الأمن المعلوماتي، باعتبارها مقومات أساسية تحتاج للتوضيح.

المطلب الأول: مفهوم الأمن المعلوماتي

هناك عدة مفاهيم جاءت لتوضيح المقصود بالسلامة المعلوماتية أو ما يعرف بالأمن المعلوماتي، من زاوية أكاديمية هو "العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها من أنشطة الاعتداء عليها".[1]

أما من الناحية التقنية فيقصد به: الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية،[2] والخارجية.

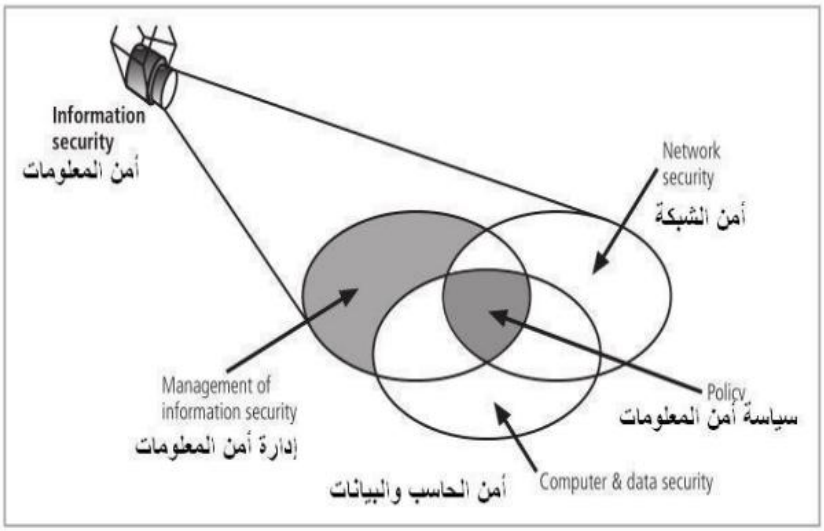
أما من الناحية القانونية فإن أمن المعلومات هو: "محل دراسات وتدابير حماية سرية وسلامة المحتوى وتوفر المعلومات، ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة"،[3] وهو لا شك هدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظم معالجتها.

يتضح من هذه التعاريف أن السلامة المعلوماتية لا تنحصر عناصرها فقط على أمن وسلامة الأنظمة المعلوماتية، بل هي تخص أمن وسلامة الأنظمة والمعلومات والمعطيات بصفة شاملة أو عامة،

[1] د. هالة كمال أحمد نوفل، بحث حول "استطلاع رأي النخبة حول جرائم اختراق البيئة المعلوماتية الافتراضية واستشراف الاتجاهات الحديثة في مجال أمن المعلومات"، مقدم للمؤتمر السادس لجمعيات المكتبات والمعلومات السعودية - البيئة المعلوماتية الآمنة، المفاهيم والتشريعات والتطبيقات، المنعقد بمدينة الرياض في 6-7 أبريل 2010، ص11.
[2] د. خالد ممدوح إبراهيم، أمن المعلومات الإلكترونية، الدار الجامعية، الإسكندرية، 2008، ص27.
[3] د. عبد الرحمان شعبان عطيات، أمن الوثائق والمعلومات، ط1، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004، ص122.

إذ تشمل إضافة إلى التجنب الأمني سرية وضمان تواجد تلك المعطيات في صيغة صحيحة أو في شكلها الصحيح وحماية المعلومات ذات قيمة مهما كان نوعها[1].

الشكل رقم 01: مجالات أمن المعلومات[2]



لكن عند الحديث عن السلامة المعلوماتية وحتى يتضح المقصود بذلك لابد من تحديد العناصر المشكلة لها فيما يخص المقصود بسلامة المعلومات (المرقمنة)، وسلامة الأنظمة المعلوماتية، وهذا ما سوف أتولى توضيحه فيما يأتي:

الفرع الأول: تعريف الأمن المعلوماتي التعريف يسبق المفهوم

ويهدف الإحاطة بمفهوم المعلومات (أولا) نحاول أن نجد تعريف محدد وشامل وكذا تمييزها عن بعض المصطلحات التي قد تتداخل معها (ثانيا).

كما أن مصطلح المعطيات قد يتداخل أو يتشابه في معناه مع مصطلحي المعلومات والبيانات، لذلك سوف يتم تبيان ما المقصود بهاته المصطلحات كلا على حدا:

أولا- المقصود بالمعلومات:

هناك عدت مفاهيم وردت بشأن تعريف المعلومات سواء من الناحية الفقهية أو من الناحية القانونية، نوجزها فيما يلي:

[1] د. عبد الرحمان شعبان عطيات، مرجع سابق، ص123.
[2] Michael whitman and Hathord, Principles of information security, 5th Ed, usa, 2012, p4.

- **التعريف الفقهي للمعلومات:**

انقسم الفقه في تعريف المعلومات إلى اتجاهين اثنين الأول يعرفها تعريفا واسعا والاتجاه الثاني يعرفها تعريفا ضيقا:

- **المفهوم الواسع للمعلومات:**

من أبرز الفقهاء الذين تزعموا هذا الاتجاه نجد الفقيه الفرنسي (CATALA) الذي عرف المعلومات على أنها: "كل رسالة يمكن نقلها إلى الغير بأي وسيلة من الوسائل".[1]

ونظرا لمرونة هذا التعريف واستيعابه لكل الوسائل النقل الرسالة أو المعلومة ومنها الوسائل المعلوماتية وكل جديد في مجال التكنولوجيا الرقمية، فإن بعض الفقهاء الفرنسيين قد تبنوا نفس التعريف ومنهم الفقيه (M.VASSEUR)الذي عرف المعلومات بأنها : النقل المادي المجرد لأحداث معينة تم الحصول عليها من مصادر متنوعة.[2]

ونفس الشيء بالنسبة لتعريف الفقيه (GALLOUX) الذي عرف المعلومات على أنها: "الهيئة أو الحالة الخاصة للمادة أو الطاقة التي يمكن نقلها أو إبلاغها للغير".[3]

وبالرغم من أسبقية هذا الاتجاه في وضع التعريف القانوني للمعلومات في وقت لم تكن فيه المعلوماتية قد حظيت بالاهتمام الفقهي والتشريعي، إلا أن هناك من انتقد هذه التعاريف، وأخذ عليها أنها لم تهتم بمحتوى المعلومة التي تحملها الرسالة أو قيمتها المالية، أو مدى الاستفادة منها بقدر انشغالهم بإمكانية نقلها أو تداولها بين مختلف الوسائل، فليس كل رسالة تنقل إلى الغير تمثل معلومة تستوجب الحماية، وإنما الحماية تشمل بعض المعلومات التي لها ميزة أو قيمة معية وليس كل المعلومات.

- المفهوم الضيق للمعلومات:

نظرا للانتقادات التي وجهت للمفهوم الواسع للمعلومات أخذ غالبية الفقه يتجهون إلى وضع تعريف للمعلومات بما يناسب الاتجاهات الحديثة التي تركز على القيمة المالية التي تحملها المعلومة أكثر من تركيزها على وسائل تناقلها.

[1]CATALA, Ebauche d'une théorie juridique de l'information D 1984, P 87.
[2]MICHEL Vasseur: Des responsabilités en cours par le banquier a raison des informations avais et conseil dispenses a ses client revue banque, 1983948
[3]GALLOUX (J-C): Ébauche d'une définition juridique de l'information, D 1994, chron, p229.

من بين تلك التعريفات ما جاء به الفقيه الفرنسي Elis DRAGON على أنها: كل رسالة ذات معنى تنقل إلى الغير وتتوقف قيمتها المالية على نوعية مضمونه الإعلامي.[1]

وهذا ما يذهب إليه جانب كبير من الفقه المصري إلى الأخذ بالمفهوم الضيق للمعلومات، حيث عرفها البعض على أنها كل رسالة تحمل معنى وتتحدد قيمتها المالية حسب كثافة ونوعية مضمونها الإعلامي،[2] وفي ذات المعنى يعرفها البعض الآخر: كل رسالة تحمل معنى ودلالة، وتتوقف قيمتها المالية على ثقلها الإعلامي.[3]

كما يعرفه البعض الآخر على أنها كل ما يقوم بمال من أرقام وبيانات وغير ذلك، مادام يمثل معارف ذات قيمة مالية.[4]

ومن بين أهم التعريفات الجامعة والمانعة نجد من عرفها على أنها: مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح لأن تكون محلا للتبادل والاتصال أو التفسير والتأويل أو المعالجة سواء بواسطة الأفراد أو الأنظمة الإلكترونية، وهي تتميز بالمرونة بحيث يمكن تغييرها وتجزئتها وجمعها ونقلها بوسائل وأشكال مختلفة.[5]

وما يمكن استخلاصه من التعاريف السابقة أن المعلومات هي عبارة عن رسالة ذات معنى ولها قيمة مالية، وقد تتخذ عدت صور مهما كان شكلها (عادية أو مشفرة) ويمكن نقلها واسترجاعها أو تداولها بمختلف الوسائل.

ثانيا- التعريف التشريعي للمعلومات:

ورد في عدة نصوص قانونية استعمال كلمة " معلومات" أو كلمات أخرى قريبة منها مثل "بيانات" أو معطيات ففي القانون الجنائي الفرنسي، (23) مثلا نجده يعاقب على بث معلومات خاطئة (المواد 322/14 و411/10) دون أن يقدم تعريفا للمعلومات، كما يعاقب أيضا على إفشاء معلومات ذات طبيعة سرية، وذلك من خلال جريمة إفشاء سر المهنة (م13/226).[6]

وبالإضافة إلى المجال الجنائي هناك نصوص أخرى حيث عرفتها اتفاقية بودابست لمكافحة الجريمة المعلوماتية بتعريف المعلومات أو المعطيات المعلوماتية على أنها:

[1] ELISE Dragon, Etude sur le statut juridique de l'information, D. 1998, chron, p 65.
[2] د. محمود عبد المعطى خيال: التأمين على المعلومات، ط 1999، القاهرة، ص 12.13.
[3] د. أيمن إبراهيم العشماوي، المسئولية المدنية عن المعلومات دار النهضة العربية، القاهرة، 2004، ص 34.
[4] الحسين محمد حسام لطفي، عقود خدمات المعلومات دراسة في القانونين المصري والفرنسي القاهرة، 1994، ص 65.
[5] د. خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، المرجع السابق، ص 27.
[6] د. أيمن إبراهيم العشماوي، المرجع السابق، ص 28.

كل تمثيل للوقائع أو المعلومات أو المفاهيم تحت أي شكل، وتكون مهيأة للمعالجة الآلية بما في ذلك برنامج معد من ذات الطبيعة ويجعل الحاسب يؤدي المهمة.[1]

كما نجد عدة دول عربية والتي أخذت بالتعريف الذي نص عليه في قانون الأونيسترال النموذجي للتجارة الإلكترونية، فمثلا نجد قانون التجارة الإلكترونية البحريني لعام 2002 المادة الأولى منه تعرفها على أنها: "النصوص والصور والأصوات والرموز وبرامج الحاسب والبرمجيات وقاعدة البيانات".[2]

وكذلك بالنسبة لمشروع قانون التجارة الكويتي من خلال المادة الثانية على أنها : مفردات يتم تبادلها على شكل رقمي أو تماثلي أو بما يشابهها في ذلك الصوت والصورة والبيانات والرموز بأنواعها وأنظمة الحاسب وقواعد البيانات والنصوص ولقد فسرت المذكرة الإيضاحية للقانون هذا التعريف، ونوهت إلى أن هذا المصطلح يشمل أي شكل من المفردات اللغوية أو غير اللغوية مقروءة أو مسموعة أو منظورة، ويتم تبادلها بشكل رقمي أو تماثلي، إضافة إلى فتح المجال أمام أي شكل تقني مشابه ومستحدث ويكون قابلا للتداول.[3]

ونجد كذلك الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الموقعة بالقاهرة بتاريخ 2010 تعرف البيانات على أنها: "كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة تقنية المعلومات، كالأرقام والحروف والرموز وما إليها...".[4]

أما بالنسبة للمشرع الجزائري فلقد نص حديثا على تعريف للمعلومات أو بالأصح المعطيات من خلال الأمر رقم 06-09 المتعلق بمكافحة التهريب المادة 02/ط على أنها: "المعلومات: كل المعطيات المعالجة أو غير المعالجة، المحللة أو غير المحللة وكل وثيقة أو تقرير وكذا الاتصالات الأخرى بمختلف أشكالها بما فيها الإلكترونية ونسخها المحقق في صحتها المصادق على مطابقتها".[5]

[1] الحسين محمد حسام لطفي، مرجع سابق، ص68.
[2] القانون الأردني، مشروع قانون التجارة الإلكترونية.
[3] أيمن عبد الله فكري، مرجع سابق، ص 45.
[4] الفقرة الثالثة من المادة الثانية من "الاتفاقية العربية لمكافحة جرائم تقنية المعلومات"، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010 و المصادق عليها من قبل الجزائر بموجب المرسوم الرئاسي رقم 14-252 المؤرخ في 08 سبتمبر 2014، ج.ر عدد 57 لتاريخ 28 سبتمبر 2014.
[5] الأمر رقم 06-09 المؤرخ في 15 يوليو 2006 المتعلق بمكافحة التهريب، الجريدة الرسمية عدد 47 بتاريخ 19 يوليو 2006.

وعرف معطيات معلوماتية على أنها أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها.[1]

ومن الملاحظ أن هناك علاقة بين المعلومات والمعطيات إذ تعتبر هذه الأخيرة وفقا للمشرع الجزائري أنها عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة، وبذلك ترجع للفرق الموضح تاليا بأن البيانات أو المعطيات هي المادة الخام للمعلومات.

كذلك القانون الجنائي المعدل والمتمم بموجب القانون 04-15 نجد المواد 394 مكرر وما بعدها والتي تتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات على أن تضاعف العقوبة في حالة تغيير أو حذف المعطيات المنظومة إذا ترتبت عن فعل الدخول أو البقاء عن طريق الغش في كل أو جزء منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك، وبذلك نجد المشرع الجزائري يتحدث عن المعطيات بصفة عامة وبأي شكل هي عليه.

- المعلوماتية والمعلومة:

تعرف المعلوماتية على أنها علم المعلومات الخاضعة للمعالجة الإلكترونية،[2] وأن المعلومة إجمالا هي كل مادة معرفة قابلة لأن تتمثل في إشارات متعارف عليها من أجل حفظها أو معالجتها أو بنها، ورغم اختلاف التعريفات إلا أن المهم في ذلك أن تكون المعلومة خاضعة لنظام المعالجة الآلية على أن يكون هذا النظام أمن ومحمي.

ويقصد بالمعالجة الآلية: مجموعة العمليات المحققة بواسطة الوسائل الأوتوماتيكية و التي لها علاقة بجمع و تسجيل و تعديل وحفظ و تحطيم وبث المعطيات واستغلالها بوجه عام.[3]

والمعلوماتية في نهاية الأمر لا تخرج عن استعمالات الكمبيوتر و ما تفرضه من تقنيات حتمتها مظاهر التقدم في هذا المجال، ولا تخرج هذه الاستعمالات بدورها عن مستويين، فالأول يعرف بالمعالجة الآلية للبيانات أي استعمال جهاز الحاسوب في حزن المعلومة ومعالجتها دون أن يرتبط بشبكة الاتصالات، والثاني يعرف بتبادل المعطيات الالكترونية أي نقل المعلومة من موقع على موقع باستعمال وسائل

[1] الحسين محمد حسام لطفي، مرجع سابق، 67.
[2] القاضي علي كحلون، الجوانب القانونية لقنوات الاتصال الحديثة والتجارة الإلكترونية، دار إسهامات في أدبيات المؤسسة، تونس، 2002، ص347.
[3] Art 5 de la loi français n" 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

الاتصال الحديثة،[1] أي الربط بين عدد من الحواسيب في أماكن مختلفة، و هو ما يفترض ارتباط جهاز الحاسوب بشبكات الاتصال وقواعد البيانات.

ولا شك أن المعالجة الآلية للبيانات أو المعلومات وفي جميع أشكالها قد يتم فيها خرق لقواعد الأمن المعلوماتي والسلامة المعلوماتية، بل إنها تسهل الاعتداء على المعلومات وأنظمة معالجتها بفضل الإمكانات الكبيرة في عالم الاتصالات وتقنية المعلومات التي أضحت تغزو جميع الميادين. وتعرف ظاهرة الإجرام المعلوماتي بأنها الأفعال غير المشروعة المرتبطة بنظم الحواسيب،[2] وأن محلها هو دائما معطيات الحاسب بدلالاتها المختلفة والواسعة.

ثالثا- التمييز بين المعلومات والبيانات والمعطيات:

هناك علاقة بين مصطلح المعلومات ومصطلح البيانات أو المعطيات، إذ كثيرا ما يقع الخلط بين هذه المصطلحات، ولذلك من الأحسن إبراز الفرق، فتعرف البيانات على أنها: مجموعة من الحقائق التي تعبر عن مواقف وأفعال معينة حدثت في الماضي أو الحاضر أو ستحدث في المستقبل سواء كان التعبير بالكلمات، أو الأشكال، أو الرموز،[3] أما المعلومات فهي بيانات خضعت للتشغيل والتحليل والتفسير لتحقيق أغراض معينة وتمكينهم من الحكم السديد على الظواهر والمشاهدات.[4]

لذلك يرى البعض أن البيانات هي معلومات في حالة كمون و المعلومات هي بيانات في حالة حركة ونشاط، ولذلك فإن البيانات تمثل حقائق رقمية أو غير رقمية، والمعلومات هي كل نتيجة مبدئية أو نهائية مترتبة على تشغيل البيانات، أو تحليلها أو استقراء دلالتها أو استنباط ما يمكن استنباطه منها وحدها أو متداخلة مع غيرها، فالمعلومة وفقا للرأي السابق تأتي في مرحلة تالية ومتأخرة على البيانات،[5] ويعتبر البعض الآخر كذلك البيانات عبارة عن بعض المعطيات المجردة التي يتم تجميعها وتصنيفها وتوصيف محتواها داخل الحاسب الآلي أو أية وسيلة أخرى من وسائل الاتصال الحديثة حيث تساعد بعد تحليلها على إعطاء المعلومات.[6]

[1] على كحلون، مرجع سابق، ص 348.
[2] فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية، رسالة لنيل درجة الدكتوراه في الحقوق جامعة عين شمس، كلية 35 الحقوق، مصر 2012، ص 35.
[3] أيمن عبد الله فكري، جرائم نظم المعلومات، مرجع سابق، ص 39.
[4] د. إبراهيم أحمد الصعيدي : نظام التشغيل الإلكتروني للبيانات مطبعة المعرفة، 1981، ص 13.
[5] د. أيمن عبد الله فكري، مرجع سابق، ص 40.
[6] عبد الرشيد مأمون ومحمد سامي عبد الصادق حقوق المؤلف و الحقوق المجاورة في ضوء قانون حماية حقوق الملكية الفكرية الجديد رقم 82 لسنة 2002، الكتاب الأول، دار النهضة العربية، القاهرة، 2004، ص 120.

وقد وفق جانب من الفقه حين فرق بين المعلومات والبيانات بالقول: "إن المعلومات هي نتيجة معالجة البيانات وذلك لأننا نستخدم البيانات لاستنتاج المعلومات،[1] وبذلك تشكل البيانات المادة الخام التي يتم تجهيزها للحصول على المعلومات، فالمعلومة لذا أصحاب الرأي السابق تأتي في مرحلة تالية ومتأخرة على البيانات، لذا تعد المعلومة القيمة المضافة، أما البيانات فهي المادة الخام بالنسبة لها.

أما المعطيات فقد ورد تعريف لها في الحكم الفرنسي الصادر في 1981 بأنها: "إعادة إبراز المعلومات وفقا للشكل الإصلاحي بغرض تسهيل معالجتها بوسائل إنسانية أو آلية،[2] فما يميز المعطيات هي شخصيتها الشكلية سواء كانت في شكلها الخام أو المعالجة أو المبرمجة.

ومن ذلك يمكن اعتبار مصطلح البيانات أو المعطيات كمصطلح عام يشمل كل الحقائق والعمليات التي يمكن معالجتها لاستنتاج منتج نهائي في شكل معلومات.

- تحديد طبيعة وشروط المعلومات:

تتطلب السلامة المعلوماتية وقواعد الأمن المعلوماتي تحديد كل من الطبيعة القانونية للمعلومات،والشروط الواجب توافرها في المعلومة حتى تحض بالحماية على النحو الآتي:

- **الطبيعة القانونية للمعلومات:**

يوجد خلاف فقهي حول الطبيعة القانونية للمعلومات، حيث يعتبرها جانب من الفقه أنها تعد أموالا منقولة وانه يمكن تقويمها بالمال انطلاقا من القيمة الاقتصادية لها، وبالتالي تصح أن تكون محل الحقوق المالية وعلى الأخص حق الملكية، وعلى أساس أنه يمكن استغلالها في تحقيق أرباح مادية أو تحسين أداء المشروعات الانتخابية، وبالتالي يجوز أن يرد عليها جميع أنواع التعاملات التجارية،[3] وباعتبار المعلومات مال مقوم سواء كانت مبتكرة أو غير مبتكرة، فهي تتمتع بالحماية القانونية، ذلك لأنها إذا كانت مبتكرة فهي محمية بمقتضى قانون حماية الملكية الفكرية، وإذا كانت غير ذلك فهي محمية بموجب القواعد العامة في القانون المدني باعتبارها مال منقول.

[1] محمد سامي عبد الصادق المرجع السابق، ص 39، 40.
[2] د. أيمن عبد الله فكري، مرجع سابق، ص 40.
[3] خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، مرجع سابق، ص 34.

ويرى جانب من الفقه الفرنسي أن المعلومات أموالا ذات طبيعة خاصة انطلاقاً من أن غياب الكيان المادي للمعلومات، لا يجعلها محلا لحق مالي من نوع الحقوق المتعارف عليها في الفقه، والتي ترد على كيانات مادية، وإن جاز اعتبارها محلا لحق ملكية أدبية أو فنية أو صناعية.[1]

وبالتالي فإن المعلومات التي لا تكون محلا للحقوق الأدبية أو الفنية أو الصناعية، يلزم بالضرورة استبعادها عن طائفة الأموال، ولا يعنى هذا الاستبعاد أن تظل هذه المعلومات بدون حماية في حالة ما تعرضت لسوء استعمال كالاستيلاء عليها أو استخدامها استخداما غير مشروع، فإن المسؤولية في هذه الحالة تقوم وفق قواعد المسؤولية المدنية المستندة إلى نص المادة 1382 من القانون الفرنسي.[2]

وفي حالة الاعتراف بالخطأ تكون المحكمة قد اعترفت بوجود الحق وهو المعلومات،[3] ومعناه أن يكون للمعلومات طبيعة خاصة تسمح بأن يكون الحق الوارد عليها من نوع الملكية العلمية.

- **الشروط الواجب توافرها في المعلومة:**

حتى تحضا المعلومة بحماية قانونية فلا بدا أن تتوفر على مجموعة من الشروط متفق عليها والمتمثلة فيما يأتي:

- أن يتوفر في المعلومة التحديد والابتكار:

الخاصية الأولى التي تتميز بها المعلومة هي أن تكون محددة ومبتكرة وإلا اعتبرت غير حقيقية، فإذا ما اعتبرنا المعلومة تعبير وصياغة محددة تجعل الرسالة ما قابلة للتبليغ عن طريق علامات أو إشارات معينة، ومن الضروري أن تكون محددة وبصفة خاصة في مجال الاعتداءات على الأموال، فهذا النوع من الاعتداءات يفترض دائما وجود شيء محدد.[4]

أما بخصوص الابتكار فهو كذلك أمر أساسي، فأي معلومة غير مبتكرة تعد معلومة شائعة وعامة ومتاحة للكل وليس خاصة بشخص معين.

[1] خالد ممدوح إبراهيم، مرجع سابق، ص 34.

[2] art 1382 Du C.C.F dispose que: « Tout fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute du quel il est arrivé à le réparer ».

[3] خالد ممدوح ابراهيم، مرجع سابق، ص 35.

[4] Pierre Catala, les transformations de droit par informatique, Emergences du droit de l'informatique, 1983, P264.

- أن يتوفر في المعلومة السرية والاستئثار:

السرية صفة ضرورية لحصر نطاق المعلومة وجعل حركة الرسالة أو تداول المعلومة محدد في دائرة من الأشخاص أوفي نطاق مجال معين، حيث أنه لا يمكن أن تتحدث عن الجرائم الخاصة بالسرقة والنصب وخيانة الأمانة، إذا انعدم هذا الحصر، وكذلك لأن المعلومة غير السرية تقبل التداول ومن ثم تكون بمنأى عن أي حيازة، كما في حالة الرقم السري الخاص باستعمال بطاقات الائتمان.[1]

ويقلل الطابع السري في هذه الحالات المختلفة من استخدام المعلومات ويقصرها فقط على دائرة المؤتمنين عليها والدين يجدون أنفسهم هكذا منتفعين بحق الاستئثار عليها.[2]

الفرع الثاني: أهمية الأمن المعلوماتي

مع التطور السريع لتكنولوجيا المعلومات والاتصالات، أصبح الأمن المعلوماتي ضرورة ملحة لحماية الأفراد والمؤسسات من المخاطر المتزايدة، حيث تمثل المعلومات رأس مال حيوي يجب الحفاظ

عليه من العبث أو السرقة أو الضياع،[3] ونظرا لهذا تطرقنا لأهمية الأمن المعلوماتي كالآتي:

- حماية سرية المعلومات: يعد الحفاظ على سرية المعلومات وحمايتها من الوصول غير المصرح به أحد أهم أهداف الأمن المعلوماتي، من خلال تقنيات مثل التشفير، وإدارة حقوق الوصول[4].

- ضمان سلامة البيانات: يهدف الأمن المعلوماتي إلى حماية المعلومات من التعديل أو التزوير أو الإتلاف، مما يضمن سلامة ودقة البيانات خلال تخزينها أو نقلها.[5]

- الحفاظ على استمرارية الأعمال: يلعب الأمن المعلوماتي دورًا أساسياً في حماية استمرارية المؤسسات وضمان عدم تعطل العمليات الحيوية نتيجة الهجمات السيبرانية أو الكوارث المعلوماتية.[6]

- حماية الخصوصية الشخصية: مع الانتشار الكبير للمعاملات الإلكترونية، أصبح الأمن المعلوماتي أساسياً لحماية البيانات الشخصية للأفراد من السرقة أو سوء الاستخدام.[7]

[1] د. خالد ممدوح إبراهيم، مرجع سابق، ص 31.
[2] محمد سامي الشواء، ثروة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، 1994، ص 176.
[3] حسن شوقي، "الأمن المعلوماتي في عصر العولمة"، دار الفكر العربي، 2018، ص 15.
[4] سامي عبد العزيز، "أمن المعلومات: المبادئ والمفاهيم"، دار الصفاء للنشر والتوزيع، 2019، ص 35.
[5] عبد الله أبو الروس، "تأمين نظم المعلومات"، مكتبة الأنجلو المصرية، 2017، ص 50.
[6] محمد فتحي، "الإدارة الإلكترونية والأمن المعلوماتي"، دار الفكر الجامعي، 2016، ص 77.
[7] نادية حسن، "الجرائم المعلوماتية وحماية الخصوصية"، دار الجامعة الجديدة، 2020، ص 90.

- دعم الثقة في البيئة الرقمية: الأمن المعلوماتي يعزز الثقة في استخدام الإنترنت والتطبيقات الإلكترونية، مما يشجع الأفراد والمؤسسات على التعامل الرقمي بأمان.[1]

المطلب الثاني: عناصر ووسائل الأمن المعلوماتي

للأمن المعلوماتي عناصر أساسية ومبادئ وهي التي يقوم عليها موضوع الدراسة سواء بالنسبة للحماية الفنية والتقنية لها أو بالنسبة للحماية القانونية، ويبدو أن قواعد الأمن المعلوماتي تتعلق ابتداء بسرية المعلومات.

الفرع الأول: عناصر الأمن المعلوماتي

حدد بعض الباحثين والمهتمين بأمن المعلومات ثلاثة عناصر أساسية ينبغي توفيرها والاهتمام بها لفهم وتوفير أمن المعلومات وجاءت هذه العناصر تحت مسمى ثالوث أو مثلث الأمن المعلوماتي (The CIA Triad) وكان هذا سنة 1987.

ويمكن تعريف هذه العناصر على أنها "مجموعة من المكونات الواجب توفرها للحفاظ على المعلومات الثابتة والمنقولة من أي نوع من أنواع الاستغلال والاعتداء، بحيث لا يطلع عليها سوى الأشخاص المصرح لهم، حيث ان كل عنصر من هذه العناصر مهم للإبقاء على سرية وسلامة البيانات وان أي نقص في عنصر من هذه العناصر سيؤدي حتما إلى المساس بسرية وسلامة المعلومات ".

أ. وجاء نودج ثالوث أمن المعلومات (The CIA Triad) بثلاثة عناصر كالآتي:[2]

- سرية المعلومات (Data Confidetiality):

الغاية من هذا العنصر، هو التأكد من أن المعلومات السرية والحساسة لا تكشف ولا يتم الاطلاع عليها من قبل أشخاص غير مخولين أو غير mares مصرح لهم بذلك، وهذا يعني أن المعلومة مؤمنة، ولا يطلع عليها إلى من طرف الأشخاص أو الأقسام الذين لهم صلاحيات الإطلاع، ومن هنا يجب الحرص على درجة السرية، وتقسيم المعلومات حسب درجة أهميتها وحساسيتها، وفي المقابل يتم تصنيف الأشخاص الذين يحق لهم الوصول لهذه المعلومات وكذلك نوع هذا الوصول هل هو للإطلاع فقط أم للنسخ والتعديل، كما أن هؤلاء الأشخاص الذين يطلعون على معلومات معينة قد لا يكون لديهم الحق في الاطلاع على معلومات أخرى.

[1] عماد زكي، "أمن المعلومات وأمن الشبكات"، دار الكتب العلمية، 2015، ص 110.
[2] عبد الرحمان شارع العتيبي، دور الأمن السيبراني في تعزيز الأمن الإنساني، مذكرة ماجستير، جامعة نايف المعلوم الأمنية: كلية العلوم الاستراتيجية، قسم الأمن الإنساني، 2015، ص 14-15.

- توفر المعلومات (Data Availability):

يشير هذا العنصر إلى وجوب ديمومة وتوفر المعلومات أي أن تكون المعلومات متوفرة ومتاحة لدى الطلب من قبل الأشخاص المخولين بالإطلاع، وبمعنى آخر حماية المعلومة من أي خطر من أخطار الهجوم او التعدي وبأي أسلوب كان هذا التعدي.

- سلامة المعلومات وتكاملها (Data Integrity):

ويقصد بهذا العنصر أن تكون المعلومات سليمة في محتواها، ولم تتعرض لأي محاولة للإتلاف أو التغيير سواء كانت هذه المحاولة مقصودة أو غير مقصودة، ويوضح الشكل في الأسفل نموذج مثلث أمن المعلومات.[1]

الشكل رقم 02: يوضح نودج مثلث أمن المعلومات (The CIA Triad)[2]



[1] عبد الرحمان شارع العتيبي، مرجع سابق، ص15.

[2] http://wwwmarianowo.org/network-security-cia-seven-excitin-parts-of-attending-network-security-cia-225, page consulter le 27/04/2025, à 23:11.

ب- سداسي باركر لأمن المعلومات وفي سنة 2002 قدم دون باركر (Donn B.Parker):[1]

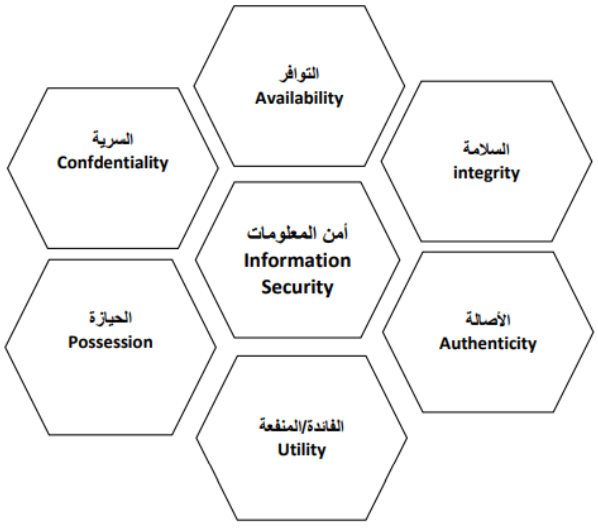
وهو باحث ومستشار في امن المعلومات وجهة نظر بديلة حول عناصر أمن المعلومات، فإضافة إلى العناصر الثلاثة السابقة التي جاءت في النموذج السابق أضاف باركر ثلاثة عناصر أخرى وهي:

- الحيازة (Possession): يعتبر عنصر الحيازة أو امتلاك التحكم واحدا من إضافات باركر للنموذج السابق، وتمت اضافة هذا العنصر انطلاقا من فرضية مفادها أن المعلومات يمكن ان يتحكم فيها فرد أو مجموعة من الافراد لا يمتلكون الحق في ذلك، فانطلاقا من هذا العنصر يمكن إعطاء صلاحيات التحكم في المعلومات للأشخاص المعنين فقط.

- الأصالة (Authenticity): يقصد بهذا العنصر التحقق من شخصية وهوية الأشخاص أو الجهات التي تطلع على المعلومات، وهل هم مخولون فعلا ولديهم صلاحيات الوصول والاطلاع على هذا النوع من المعلومات.

- المنفعة الفائدة (Utility): يساعد هذا العنصر في الإشارة إلى المعلومات ذات الفائدة والقيمة وهذا هو العنصر الأخير من سداسي باركر لأمن المعلومات، ويركز هذا العنصر على مفهوم يتم اغفاله تماما أو الخلط بينه وبين عنصر التوافر وهو فائدة هذه البيانات، فهذه الأخيرة قد تكون متاحة وقابلة للاستخدام ولكن ليس بالضرورة ان تكون في شكل مفيد ذو قيمة.

الشكل رقم 03: سداسي باركر (Parker) للأمن المعلوماتي[2]



[1]Umesh Hodeghtta and Umeshaa nayak, The info sec Hand book an introdution Security, Apress open, New york, p52.
[2] Georgie penbey, the parkerian Hexad, cia model expanded, P7.

- إشكاليات وتحديات أمن المعلومات:[1]

مع التزايد المستمر للتعقيد التقني والمصاعب القانونية وتوقعات حماية الخصوصية ارتفعت تحديات أمن المعلومات بشكل متسارع خلال السنوات الماضية إذ أن الانتشار الكبير لاستعمال التطبيقات القابلة للعمل مع شبكة الانترنت (Web Enabled) في تسعينيات القرن الماضي وتزايد حصة هذا الاستثمار في سوق الأسهم غالبا ما دفع بمرتبة عمليات أمن المعلومات إلى مستوى الأفضلية.

وتشمل التحديات التي تواجهها إدارات تقنيات امن المعلومات ما يلي:

- عدم الفهم والخلط أحيانا بين العديد من تقنيات أمن المعلومات المختلفة والمتضاربة.

- معرفة من يمكن له ومن لا يمكن له الوصول للمعلومات، والأنظمة والشبكات فأحيانا قد لا تبلغ سجلات الموظفين الدقيقة بسرعة إلى إدارة تقنية المعلومات.

- عدم وجود معايير شاملة ومتفق عليها للأمن المعلوماتي.

- تحديد مستوى الصلاحيات الصحيح لكل موظف وكل مستخدم للنظام لكي يقومون بإعمالهم من دون السماح للجميع بالنفاد الكامل لجميع الملفات والأنظمة.

- معرفة من يمكن أن تثق فيهم من الموردين والشركاء والزبائن من أجل التزويد بالمعلومات فليست كل المعلومات سواء فقد تحتوي مرفقات البريد الالكتروني على فيروسات أو رسائل، صور أو نصوص أو حتى (Stegnography) تسجيلات صوتية مخفية بتقنية.

- جلب مؤهلين وأخصائيين وخبراء في امن المعلومات.

- المحافظة على القدرة الهندسية للاستجابة السريعة ضد مختلف التهديدات والهجمات من الأفراد الذين يحاولون الوصول إلى معلومات قيمة.

- ضف إلى ذلك التحديات القانونية والتشريعية خاصة في دول العالم الثالث فأغلبية هذه الدول تفتقر للإطار القانوني والتشريعي لردع مرتكبي الجرائم المعلوماتية.[2]

[1] لورنس أوليفه، ترجمة محمد مراياتي، أمن تقنية المعلومات نصائح من خبراء المنظمة العربية للترجمة، ب س ن، ص 25-26.

[2] لورنس أوليفه، مرجع سابق، ص27. (بتصرف)

- Web Enabled:

هي عبارة عن مجموعة من تطبيقات الحاسوب والتي تم انشاؤها باستخدام لغة HTML ويمكن الوصول إليها انطلاقا من متصفحات الانترنت Stegnographyهو على طريقة أو تقنية إخفاء البيانات الرقمية داخل وسيط أخر كإخفاء رسالة نصية داخل صورة مثلا بشكل يمكن سوى المرسل والمستلم الاطلاع على المحتوى المحفى وأصل كلمة (Stegnography) هو الفريقي مشتق من الكلمة (Stegosgraphia) وهي مكونة من كلمتين stegos وتعني الصنف أو العطاء وGraphia وتعلى الكتابة أول تسجيل الاستخدام هذا المصطلح كان سنة 1499 من قبل يوهانس تريتيموس (Johannes Trithemius).

الفرع الثاني: وسائل الأمن المعلوماتي

وسائل أمن المعلوماتي والأنظمة المعلوماتية عبارة عن آليات وإجراءات وأدوات ومنتجات تستخدم للوقاية والتقليل من مخاطر المعلوماتية والتهديدات التي تتعرض لها الأنظمة المعلوماتية، ويتم الحفاظ على أمن المعلومات باتخاذ التدابير والاحتياطات وكافة الإجراءات الضرورية الممكنة، عن طريق الإدارات وبمشاركة كافة القطاعات لمنع وقوع الجريمة المعلوماتية، ولا شك مختلف وسائل الحماية التقنية و حتى القانونية تهدف الحماية وتأمين الحماية لعناصر النظام الأمني للمعلومات.[1]

ولوسائل الأمن أصناف متعددة سواء من حيث الطبيعة أو الغرض من أجل فرض الحماية وهي كالآتي:

1- وسائل الأمن المتعلقة بالدخول إلى الشبكة:

هي الوسائل التي تساعد في التأكد من أن الشبكة ومصادرها استخدمت بطريقة مشروعة من خلال تعين الوسائل التي تعتمد على تحديد حقوق المستخدمين، أو الإجراءات والأدوات والوسائل التي تتيح التحكم بمشروعية استخدام الشبكة.[2]

2-الوسائل التي تهدف إلى منع إنشاء المعلومات لغير المخول لهم:

وهذه الوسائل الهدف من ورائها الحفاظ على سرية المعلومات وهي تشمل:

- ✓ تشفير المعطيات والملفات.

[1] فهد عبد الله العبيد العازمي، مرجع سابق، ص 33.
[2] د. محمد محمود المكاوي، مرجع سابق، ص258.

- ✓ إجراءات حماية نسخ الحفظ الاحتياطية.
- ✓ الحماية المادية للأجهزة ومكونات الشبكة.

3- الوسائل الهادفة لحماية التكاملية و سلامة المحتوى:

هي وسائل الهدف من ورائها ضمان عدم تغير وتعديل محتوى المعطيات من قبل أشخاص أو جهات غير مخول لهم بذلك وهي تشمل التقنيات التالية:

- ✓ تقنيات الترميز.
- ✓ التوقيعات الالكترونية وأحسنها التوقيع الرقمي أو البصمة الرقمية التي تعتمد على تقنيات التشفير وضع برمجيات تحري الفيروسات وغيرها.[1]

4- وسائل الأمن المتعلقة بالتعريف بالشخص المستخدم وتوثيق الاستخدام والمشروعية

هي الوسائل التي تهدف إلى ضمان استخدام النظام أو الشبكة من قبل الشخص المخول بذلك وهي تشمل الوسائل التالية:

- ➢ كلمات السر بأنواعها.
- ➢ البطاقات الذكية المستخدمة للتعريف.
- ➢ وسائل التعريف البيولوجية التي تعتمد على سمات ذاتية معينة في شخص المستخدم متصلة ببنائه البيولوجي
- ➢ المفاتيح المشفرة وتضم ما يعرف بالأقفال الالكترونية التي تحدد مناطق النفاذ.[2]

5- الوسائل والأدوات الفنية لتوفير أمن المعلومات والاتصالات:

من بينها وعلى سبيل المثال ما يلي:

- استخدام تكنولوجيا الفخ الايجابي وهو فلتر يقوم بتصعيد التداخل في القنوات ويرفض دخول غير المشتركين إلى تلك القناة.

- تطبيق نظم إدارة وامن المعلومات والاتصالات.

- استخدام خطوط تليفونات واتصالات مأمنة لإستخدام تكنولوجيا التشفير والترميز.

[1] أيمن عبد الله فكري، مرجع سابق، ص 161.
[2] المرجع نفسه، من 161، 162.

- استخدام تكنولوجيا SSI وهي تكنولوجيا تتضمن بروتوكولا امنيا للأنترنت فيكون الدخول إلى النظام لمن هم مرخص لهم بذلك.

- استخدام تكنولوجيا التوقيع الرقمي في مهر الرسالة الالكترونية، للتحقق من نسب المستند الالكتروني أو الرسالة الالكترونية لصاحبها أو مرسلها.[1]

- استخدام وسائل التأكد من صحة وسلامة المراسلات الالكترونية.

- استخدام البرامج المضادة للفيروسات وتحديثها بانتظام.

- استخدام تكنولوجيا الجدران النارية، لحماية نظم الحاسبات والمعلومات.

- استخدام تكنولوجيا الكشف عن وسائل التنصت في النظم والشبكات.

- استخدام الـ COOKIES FILE لإزاحة الوسائل التي تستخدم في الدخول غير المشروع للنظام للتلصص عليه،[2] وإلى غير ذلك من الوسائل الفنية والتقنية الكثيرة التي يمكن استخدامها للوقاية أو على الأقل للتقليل من اختراق الأنظمة المعلوماتية ومكافحة الأفعال إجرامية بحسب العديد من الخبراء فإن الشخص الذي يملك جهاز كمبيوتر شخصي أو محمول عليه إتباع عدد من الوسائل الآمنة:

- ✓ عدم فتح أي ملف برسائل الكترونية غير معروفة.
- ✓ عدم تنزيل برامج مجهولة من مواقع منتديات غير معروفة.
- ✓ عدم إيقاف أو إطفاء برامج مكافحة الفيروسات والجدار الناري.
- ✓ عدم الإفصاح عن كلمة السر لأي شخص وعدم كتابتها على مقصوصات ورقية.
- ✓ اختيار كلمات سر غير متداولة وقوية ولا تدل على شخصية الشخص.
- ✓ عدم حفظ صورة شخصية في الأجهزة ونقلها لبطاقة الذاكرة.
- ✓ تحديث وتغيير كلمات السر بين فترة وأخرى.

وبالتالي فإن التطورات الحاصلة في مجال إعداد برامج وتقنيات الحماية من الأخطار والمشاكل التي تهدد الأنظمة المعلوماتية، تعتبر من العمليات المعقدة والصعبة التي تتطلب الكثير من الجهد والوقت والموارد المالية، ومن تقنيات الحماية المعلوماتية.

[1] محمد محمود المكاوي، مرجع سابق، ص 259.
[2] أيمن عبد الله فكري، مرجع سابق، ص 162.

قبل التحدث عن الجرائم المعلوماتية والأساليب الإجرامية الواقعة على المعلومات والأنظمة المعلوماتية، لابد من وقاية فنية وإجراءات تقنية للمحافظة على سلامتها من أي اعتداء أو اختراق أو تلاعب وتعديل أو اعتراض غير مشروع

وكذلك حتى تتحقق أهداف السلامة المعلوماتية فيما يتعلق بالسرية والموثوقية وكذا التكاملية وسلامة المحتوى كما تم توضيحه، لكن ما يمكن ذكره أنه لا يمكن حصر أو توقيف المخاطر الأمنية والسيطرة على الجرائم المعلوماتية بصفة دقيقة ولعدة أسباب منها أن الانترنت حديثة الانتشار، والكل يعلم أنه إذا حضر الانترنت قلت نسبة الأمن مهما كان الجهاز المتصل به، ونظرا للتطور التكنولوجي المتجدد والمستمر فإن المخاطر كذلك في استمرار، ولا تقف عند حد معين أو على نمط محدد فالخير والشر في صراع دائم لم يتوقف منذ القدم.[1]

وذلك لأنه كلما تم اكتشاف وسيلة أمنية لحماية المعلومات والأنظمة المعلوماتية، إلا وجدت ثغرة، يمكن النفاذ منها واختراق تلك الأنظمة والحصول على المعلومات، فمهما اخترع الإنسان من وسائل حماية فهو ليس بكامل، وبالتالي مهما تطورت التقنيات إلا وجدا ما يخترق تلك التقنيات، إلا أنه لا يمنع من أخذ بعض الاحتياطات والتدابير الأمنية على الأقل للمحافظة على المعلومات والأنظمة المعلوماتية السالفة الذكر.[2]

[1] محمد محمود المكاوي، الجوانب الأخلاقية والاجتماعية والمهنية للحماية من الجرائم المعلوماتية (جرائم الكمبيوتر والانترنت)، ط1، المكتبة العصرية للنشر والتوزيع، مصر، 2010، ص 250.
[2] أيمن عبد الله فكري، مرجع سابق، ص 163.

المبحث الثاني: دور الأمن السيبراني في دعم الأمن المعلوماتي

يرتبط الأمن ارتباطاً وثيقاً بأمن المعلومات، فالوصول إلى أمن المعلومات أو بثها أو حتى مجرد الإطلاع عليها هو ما يقف في الغالب وراء عمليات الاختراق للشبكات والحديث عن الأمن يستدعى تعريف الخطر أي التهديد الذي يتعرض له النظام بالإضافة إلى نقاط الضعف أو الثغرات التي تعتريه، ثم اتخاذ الإجراءات الأمنية المفروض اتخاذها ، لدفع الخطرمن الاختراق لأية معلومات أمنية أو شخصية تؤثر على المجتمع والدولة من مخاطر ذلك الفضاء السيبراني.[1]

المطلب الأول: تعريف الأمن السيبراني وأهدافه

الفرع الأول: مفهوم الأمن السيبراني

هو مكون من لفظين يعنيان " الأمن: وهو النقيض لكلمة الخوف، والأمن مصدر الفعل أمن أمناً وأماناً وأمنة: أي اطمئنان النفس وسكون القلب وزوال الخوف، ويقال: أمن من الشر، أي سلم منه. قال تعالى في كتابه العزيز: {وَإِذْ قَالَ إِبْرَاهِيمُ رَبِّ اجْعَلْ هَذَا البلَد آمِناً وَارْزُقْ أَهْلَهُ مِنَ الثَّمَرَاتِ}.

ويعرفه الاتحاد الدولي للاتصالات بأنه: "مجموعة من المهمات، مثل تجميع وسائل وسياسات وإجراءات أمنية ومبادئ توجيهية، ومقاربات لإدارة المخاطر، وتدريبات وممارسات وتقنيات تستخدم الحماية البيئة السيبرانية والمؤسسات والمستخدمين.[2]

كما تعددت التعاريف التي تناولت مصطلح السيبرانية كل حسب الزاوية التي نظر إليها منها، إلا أنها اشتركت في مضمون واحد متقارب في المعنى وهو استهداف مواقع إلكترونية من خلال وسائل إلكترونية أخرى، وهى مجموعة من الممارسات التي ترمى إلى حماية الأنظمة والشبكات والبرامج والجهات الرقمية أياً كان نوعها، وهذه الممارسات متنوعة إلى تدابير احتياطية استباقية قبل وقوع الخلل، وعلاجية بعد وقوع الخلل.[3]

ومفهوم الأمن السيبراني من المفاهيم التي لاقت اهتماماً كبيراً في الآونة الأخيرة نظراً لظهور تقنيات تكنولوجية جديدة، واستخدامها بشكل واقع في كافة المنشآت، وقد عرف NIST الأمن السيبراني

[1] نورة الصانع وآخرين، العلاقة بين الوعي بالأمن السيبراني والقيم الوطنية والأخلاقية والدينية التلاميذ المرحلتين الابتدائية والمتوسطة بمدينة الطائف، مجلة البحث العلمي في التربية، الطائف، 2020، ص278، 306.
[2] هشام محمد خليل، الجوانب الإجرامية للجوانب المعلوماتية، مجلس الأمن والقانون عدد 2، شرطة دبي، 2012، ص38.
[3] حسين بن سليمان بن راشد الطيار، الأمن السيبراني في منظور مقاصد الشارع: دراسة تأصيلية المملكة العربية السعودية، جامعة الطائف، مجلة جامعة الطائف للعلوم الإنسانية، المجلد 6، العدد 21، ص264.

بأنه حماية الأصول المعلوماتية من خلال معالجة التهديدات التي تتعرض لها المعلومات التي تتم معالجتها وتخزينها ونقلها بواسطة أنظمة المعلومات المتداخلة بين الشبكات.[1]

وقد عرفته الوكالة الفرنسية لأمن أنظمة الإعلام ANSSI وهي وكالة مكلفة بالدفاع السيبراني الفرنسي، بأنه فضاء التواصل المشكل من خلال الربط البيني العالمي للمعدات المعالجة الآلية للمعطيات الرقمية، وأنه لا يقتصر ذلك فقط على شبكة الإنترنت، إنما يشمل شبكات عالمية وخاصة مثل (GpsAcARsswiftpath)،[2] وعرفه الكاتبان Lento Martti وNettaanmakiPekka في كتابهما Automation and technology, Analyticssecurity cyber بأنه مجموعة من الإجراءات التي تتخذ في الدفاع ضد الهجمات السيبرانية، وعوقبها، وتنفيذ التدابير المضادة المطلوبة، وفي تكوين رؤى حول كيفية تحسين وحوكمة أمن معلومات المنشأة وجهود إدارة المخاطر[3].

يرتبط الأمن المعلوماتي بالجريمة الإلكترونية التي هي أساس الأمن المعلوماتي الذي يعمل على مكافحتها، وعي عبارة عن جرائم ذكية تنشأ في البيئة الإلكترونية أو الافتراضية، حيث يقوم بها أفراد أو منظمات لديهم درجة عالية من الذكاء ويمتلكون المعرفة والتقنية، مما يتسبب في خسائر فادحة للمجتمع، وتظهر أهميته في عالمنا المترابط بواسطة الشبكة العنكبوتية، حيث أصبح يمثل عنصرا مهما في الحياة الإنسانية على كافة المستويات السياسية والاقتصادية والاجتماعية، فهو الآن عصب الحياة الحالية التي تعتمد عليها الدول والأفراد في كل معاملاتها.[4]

الفرع الثاني: أهداف الأمن السيبراني

يهدف الأمن السيبراني إلى حماية المعلومات والأنظمة الرقمية من التهديدات والهجمات الإلكترونية، وذلك من خلال تحقيق مجموعة من الأهداف الأساسية التي تساهم في ضمان سلامة البيانات واستمرارية الأعمال كالتالي:[5]

[1]National institute of standards and technology (NIST) (2018), a Glossary of key information securityterms National Institute of standards and technologyinteragency or internal report. available at http://csrc.nist.gov/publications.

[2] تغريدة صفاء، لبنى خميس مهدي، أثر السيبرانية في تطور القوة، مجلة حامور أبي للدراسات، بغداد د، مركز حمورابي للبحوث والدراسات الاستراتيجية، ع33-34، السنة 2020، ص149.

[3] صباح مهدي هادي الشمري، زيد محمد علي اسماعيل، الأمن السيبراني كمرتكز جديد في الاستراتيجية العراقية، العراق، مجلة قضايا سياسية، 2012، العدد 62، جامعة النهرين، كلية العلوم السياسية، 2020، ص277.

[4] علاء الدين فرحان من الردعه النووي إلى الردع السيبراني دراسة لمدى تحقيق مبدأ الردع في القضاء السيبراني، الجزائر، جامعة بسكرة مجلة الفكرة المجلد 16، العدد 1، 2021، ص 2246.

[5] بكة التعليم، "أهداف الأمن السيبراني ومواطن أهميته"، شوهد بتاريخ: 2025/04/27، https://bakkah.com/ar/knowledgecenter.

- الحفاظ على سرية البيانات (Confidentiality): يقصد بها ضمان عدم الوصول غير المصرح به إلى المعلومات، مما يحمي البيانات الحساسة من التجسس أو التسريب. يتم تحقيق ذلك عبر تقنيات مثل التشفير، والمصادقة، وضوابط الوصول.

- ضمان نزاهة البيانات (Integrity): تتمثل في الحفاظ على دقة المعلومات وموثوقيتها، ومنع أي تعديل غير مصرح به. يُستخدم في ذلك تقنيات مثل تدقيق المجموع، والنسخ الاحتياطي، وتصحيح الأخطاء.

- توفير البيانات (Availability): يهدف إلى ضمان إمكانية الوصول إلى المعلومات واستخدامها عند الحاجة، من خلال حماية الأنظمة من الأعطال والهجمات مثل هجمات رفض الخدمة (DoS).

-المساءلة (Accountability): تتعلق بتتبع الأنشطة الرقمية وتوثيقها لضمان المساءلة القانونية، وذلك عبر سجلات التدقيق (Logs) وتقنيات التوثيق.

- حماية البنية التحتية الحيوية (Critical Infrastructure Protection): تتمثل في تأمين الأنظمة الحيوية مثل شبكات الكهرباء والمياه، لضمان استمرارية الخدمات الأساسية.

الشكل رقم 04: أهداف الأمن السيبراني[1]



[1] بكة التعليم، "أهداف الأمن السيبراني ومواطن أهميته"، شوهد بتاريخ: 2025/04/27، https://bakkah.com/ar/knowledgecenter.

بحيث تتمثل خطوات تحديد أهداف الأمن السيبراني كمايلي:[1]

يعد إنشاء قدرة وطنية لإدارة الحوادث مهمة طويلة الأجل تبدأ بإنشاء مجموعة فرق وطنية للاستجابة لحوادث الأنظمة الإلكترونية منها تحديد أو إنشاء قدرات وطنية ال فرقة Cer Incident Response Team[2] ووضع آليات داخل الحكومة الوطنية للتنسيق بين القطاعين المدني والحكومي.[3]

ولم تنشئ أغلب الدول العربية هيئة وطنية الأمن السيبراني باستثناء بعض الدول التي بعثت مثل هذه الهيئات بتسميات مختلفة، أما في بعض الدول العربية الأخرى، فنلاحظ إحداث مجالس وهيئات عدة لها دور هام في تحديد الرؤية الإستراتيجية الوطنية للأمن السيبراني وفي وضع البرامج العملية لتحقيقها، تتخذ في بعض الأحيان شكل مجالس، وفي أحيان أخرى شكل هيئات إدارية تابعة لرئاسة الجمهورية أو للوزارة المكلفة بالأمن أو بالدفاع الوطني أو بالعدل، مثلما هو الشأن في مصر متمثل في المجلس الأعلى للأمن السيبراني التابع لمجلس الوزراء، والجزائر متمثل في الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، أما في الكويت فتباشر الهيئة العامة للاتصالات وتقنية المعلومات الاختصاص المتعلق بمهام ومسئوليات الأمن السيبراني وغيرها في مجال حماية البيانات الشخصية، نلاحظ بأن بعض الدول العربية أحدثت هيئات وطنية لمراقبة البيانات الشخصية من ذلك الدول التالية: تونس والإمارات العربية المتحدة والمغرب ومصر والأردن، ولكن من المفيد التأكيد على عدم خضوع هذه الهيئات إلى نفس النظام القانوني، وعدم تمتعها بنفس الصلاحيات والامتيازات مع الملاحظ أن هناك بعض الدول العربية التي أوكلت مهمة مراقبة البيانات الشخصية إلى مصالح وزارة مثلما هو الشأن بالنسبة لدولة قطر، حيث جعل المشرع من الوحدة القانونية لوزارة الاتصالات المصلحة المختصة في هذا المجال.[4]

[1] على بهلوان، استخدام قاعدة البيانات ومنتج التطبيقات، القاهرة، دار الكتب العلمية للنشر والتوزيع، الطبعة الثانية، 2018، ص18.
[2] خالد ممدوح إبراهيم الجرائم المعلوماتية، الإسكندرية، دار الفكر الجامعي، الطبعة الأولى، 2019، ص37.
[3] عبد الفتاح بيومي حجازي مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي: دراسة قانونية متعمقة في القانون المعلوماتي، الإسكندرية، دار الفكر الجامعي، 2020، ص 32.
[4] الرؤية العربية للأمن السيبراني، الواقع – التحديات – الفرص، المنظمة العربية لتكنولوجيا الاتصال والمعلومات، تونس، 2021، ص25.

المطلب الثاني: العلاقة بين الأمن السيبراني والأمن المعلوماتي

الفرع الأول: الأمن السيبراني والأمن المعلوماتي وأوجه التشابه والاختلاف بينهما

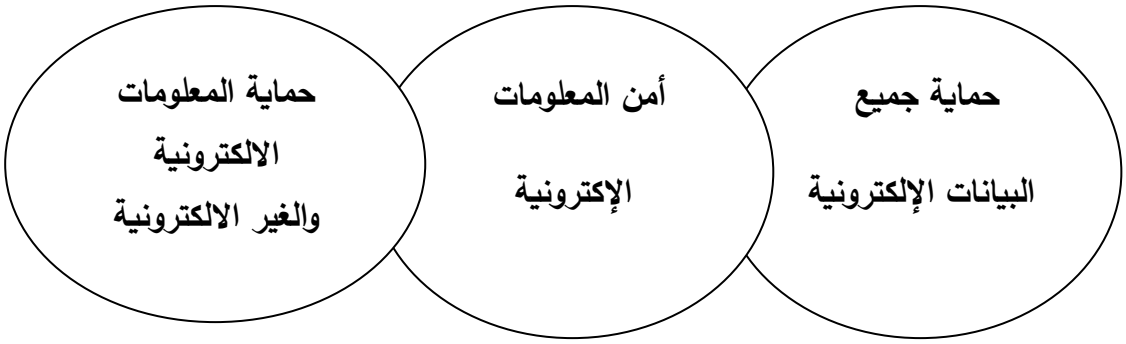
- الأمن السيبراني:

الأمن السيبراني يشير إلى حماية الأنظمة والشبكات والبرمجيات من الهجمات الرقمية أو الإلكترونية التي تستهدف الوصول إلى المعلومات أو تغييرها أو تدميرها.[1]

- الأمن المعلوماتي:

الأمن المعلوماتي يهتم بحماية المعلومات من أي تهديد قد يؤدي إلى فقدان سريتها أو سلامتها أو توفرها، سواء كانت هذه المعلومات محفوظة رقميا أو ورقيا.[2]

الشكل رقم 05: أمن المعلومات والأمن السيبراني[3]



- أوجه التشابه والاختلاف:

- تشابه: كلا المفهومين يسعيان إلى حماية المعلومات من التهديدات، ويهدفان لضمان السرية والسلامة والتوافر.

- اختلاف: الأمن السيبراني يركز على حماية الفضاء الإلكتروني (الشبكات والأنظمة الرقمية)، أما الأمن المعلوماتي فهو أوسع ويشمل حماية المعلومات بأشكالها كافة (رقمية وغير رقمية).[4]

[1] حسن عبد الله حسن، "مقدمة في الأمن السيبراني"، دار النشر للجامعات، 2021، ص 15.
[2] علي عبد العزيز، "أساسيات الأمن المعلوماتي"، مكتبة الأنجلو المصرية، 2020، ص 22.
[3] حسن عبد الله حسن، مرجع سابق، ص 16.
[4] يوسف عبد الله سلامة، "الأمن المعلوماتي والأمن السيبراني: دراسة مقارنة"، المجلة العربية للأمن السيبراني، العدد 5، 2022، ص. 101-103.

الفرع الثاني: الترابط بين الأمن السيبراني والأمن المعلوماتي ودورهما في حماية المنظومات المعلوماتية

- الأمن السيبراني كأداة لتحقيق الأمن المعلوماتي:

الأمن السيبراني يعتبر الوسيلة الحديثة لتحقيق متطلبات الأمن المعلوماتي في بيئة رقمية متطورة، من خلال استخدام برامج الحماية وجدران النار وأنظمة الكشف عن الاختراقات.[1]

- دور الأمن المعلوماتي في تعزيز السياسات السيبرانية:

وضع سياسات لحوكمة أمن المعلومات (مثل تصنيف البيانات، سياسات الاحتفاظ بالبيانات) يساهم بشكل مباشر في بناء بيئة إلكترونية آمنة ومستدامة.[2]

- ضرورة التكامل بين الأمن السيبراني والأمن المعلوماتي:

لا يمكن فصل الأمن السيبراني عن الأمن المعلوماتي، فكلاهما يكمل الآخر، لتحقيق حماية شاملة للمعلومات والأصول التقنية.[3]

- الأمن المعلوماتي: هو المجال الأشمل الذي يهتم بحماية المعلومات بجميع أشكالها، سواء كانت مخزنة ورقيًا أو إلكترونيًا أو حتى محفوظة شفهيًا.

- هدفه الرئيسي: ضمان سرية المعلومات وسلامتها وتوافرها.

- الأمن السيبراني: هو جزء متخصص من الأمن المعلوماتي، يركز تحديدًا على حماية المعلومات الرقمية والأنظمة والشبكات الإلكترونية التي تخزن أو تنقل هذه المعلومات.

- **هدفه الرئيسي:** حماية البيئة الرقمية ضد القرصنة والهجمات الإلكترونية.

إذن العلاقة بينهما هي علاقة شمول وجزئية، لأن الأمن السيبراني يعد فرعا من الأمن المعلوماتي، وكل أمن سيبراني هو أمن معلوماتي، ولكن ليس كل أمن معلوماتي هو أمن سيبراني.

[1] محمد سعيد مرسي، "الأمن السيبراني في المؤسسات الحكومية"، دار الفكر الجامعي، 2021، ص. 88-90.
[2] سعيد الحربي، "إدارة أمن المعلومات: نظرة شاملة"، مركز دراسات الشرق الأوسط، 2019، ص. 67-69.
[3] خالد منصور الخطيب، "التحديات المعاصرة في الأمن السيبراني"، المجلة الدولية لأبحاث المعلومات، 2021، العدد 10، ص. 45-47.

والأمن المعلوماتي يحمي المعلومات مهما كان شكلها، أما الأمن السيبراني يحمي المعلومات عندما تكون مرتبطة بالأنظمة الرقمية والإنترنت.[1]

والأمن السيبراني يمثل جزءًا فرعيا من مظلة الأمن المعلوماتي الأوسع. وبينما يركز الأمن المعلوماتي على حماية المعلومات بكل صورها، ينصب تركيز الأمن السيبراني على حماية البيانات والمعلومات الموجودة في الفضاء الرقمي من التهديدات والهجمات الإلكترونية.[2]

[1] خالد منصور الخطيب، مرجع سابق، ص. 45.
[2] علي عبد العزيز، "أساسيات الأمن المعلوماتي"، مكتبة الأنجلو المصرية، 2020، ص. 24.

يتشكل الأمن المعلوماتي من مجموعة الإجراءات والضوابط الهادفة إلى حماية المعلومات من المخاطر التي تهدد سريتها وسلامتها وتوافرها، ويقوم على عناصر أساسية تشمل السرية والتكاملية والتوافر. وتكمن أهميته في الحفاظ على بيانات الأفراد والمؤسسات، مما يساهم في تعزيز الثقة والاستقرار المعلوماتي، ويتم تحقيقه عبر وسائل تقنية مثل التشفير وأنظمة الحماية، وإدارية مثل السياسات الأمنية. أما الأمن السيبراني، فهو فرع متخصص من الأمن المعلوماتي يركز على حماية الأنظمة الإلكترونية والشبكات من الهجمات السيبرانية، ويهدف إلى ضمان أمن البيانات الرقمية ومنع الاختراقات والتلاعب بها. وتكمن العلاقة بين الأمن المعلوماتي والأمن السيبراني في أن الأمن السيبراني يعد وسيلة عملية لتحقيق جوانب الأمن المعلوماتي داخل البيئات الرقمية، حيث يتكاملان لضمان حماية شاملة للمعلومات على كافة المستويات.

الفصل الثاني

حماية الحياة الخاصة

أدى التطور المتسارع في تكنولوجيا المعلومات والاتصالات إلى تغييرات عميقة في مختلف جوانب الحياة، حيث أصبح العالم يعتمد بشكل متزايد على الفضاء الرقمي لتسيير شؤونه الاقتصادية والاجتماعية والإدارية. وقد نتج عن هذا التحول الكبير تدفق غير مسبوق للمعلومات والبيانات الشخصية عبر شبكات الاتصال، مما زاد من فرص جمعها ومعالجتها واستخدامها بطرق قد تهدد خصوصية الأفراد وحريتهم الشخصية.

في المقابل، برز مفهوم الأمن المعلوماتي كعنصر جوهري في حماية هذا الفضاء الرقمي من المخاطر المتعددة مثل الاختراقات، والهجمات السيبرانية، وتسريبات البيانات. لكن، وعلى الرغم من أن الهدف المعلن للأمن المعلوماتي هو حماية الأنظمة والمعلومات، إلا أن الإجراءات المتخذة لتحقيقه قد تتقاطع أحيانًا مع الحقوق الأساسية للأفراد، وفي مقدمتها الحق في حماية الحياة الخاصة.

إن التحدي الأكبر اليوم يكمن في إيجاد توازن دقيق بين مقتضيات الأمن من جهة، وضرورة احترام خصوصية الأفراد من جهة أخرى، في ظل بيئة رقمية معقدة تتطور باستمرار. ومن هنا تبرز أهمية دراسة هذا الموضوع، لفهم الإشكاليات القانونية والتقنية المرتبطة به، وتحليل الأطر التنظيمية التي تسعى إلى صيانة الحياة الخاصة دون الإخلال بالأمن المعلوماتي.

المبحث الأول: الخصوصية ومبادئ الحياة الخاصة في ظل الأمن المعلوماتي

تعد الخصوصية ومبادئ الحياة الخاصة من الركائز الأساسية لحماية الفرد وحرية اختياره. ومع تطور تقنيات الأمن المعلوماتي، أصبح من الضروري تعزيز سُبل حمايتها من المخاطر الإلكترونية والانتهاكات المتزايدة.

المطلب الأول: خصوصية الحياة الخاصة في ظل الأمن المعلوماتي

ارتبط مفهوم الخصوصية بمفهوم حماية المعلومات حديثا ووضع الخصوصية في إطار الحق في حماية البيانات الخاصة. وحدد المختصون أن الخصوصية في الحد الفاصل بين حق الفرد المطلق وبين حق المجتمع وفي عام 1980 ذهب القاصي الأمريكي (Brandis Louis) قاضي المحكمة العليا إلى أن الخصوصية هي حق الفرد في أن يترك ليكون وحيدا، لذا حددت الخصوصية كواحد من سمات المجتمع الديمقراطي في عام 1967 عرف (Alan Westin) الخصوصية بأنها رغبة الأفراد في الاختيار الحر للآليات التي يعبرون بها عن أنفسهم ورغباتها.

الفرع الأول: مفهوم الحياة الخاصة والخصوصية

أولا- مفهوم الحياة الخاصة:

تعرف الحياة الخاصة على أنها: " تمثل مجموعة من الحقوق التي تتعلق بالجانب الشخصي من حياة الإنسان، والتي لا يرغب في كشفها للآخرين، وهي تشمل الخصوصيات الجسدية، والعلاقات الأسرية، والاتصالات، والمراسلات، والمعتقدات، والأنشطة اليومية التي لا تهم المجتمع العام".[1]

ويضيف أن مفهوم الحياة الخاصة يشمل ثلاث فروع رئيسية:

- **الجانب الجسدي والشخصي:** حماية الجسد من التفتيش أو الكشف دون رضا.

- **الجانب العائلي:** صون العلاقات الأسرية، والزواج، والمسكن.

- **الجانب المعلوماتي:** حماية البيانات والمراسلات من الاطلاع أو الاستخدام دون إذن.

ثانيا- مفهوم الخصوصية:

ويمكننا هذا التعرف على عدة أنواع للخصوصية وهي:

[1] د. محمد عصفور، الحياة الخاصة في القانون الجنائي، دار الجامعة الجديدة، الإسكندرية، ط1، 2010، ص 45-47

- **خصوصية المعلومات (Information Privacy):** وتتضمن خصوصية المعلومات القواعد التي تحكم جمع وإدارة البيانات الخاصة (معلومات طبية، معلومات مالية، بطاقات هوية.
- **الخصوصية الجسدية أو المادية (Body Privacy):** وتتعلق بالحماية ضد أي اعتداءات تمس النواحي الجسدية مثل فحوصات الجينات وفحص المخدرات والمؤثرات العقلية.
- **خصوصية الاتصالات (Communication Privacy):** وتعني بسرية وخصوصية الاتصالات والمراسلات الهاتفية والبريد الإلكتروني وغيرها من الاتصالات.[1]

صاحب الانتشار الواسع للمعلومات في الوطن العربي انتشار شتى أنواع الجرائم الإلكترونية فحاولت هذه الدول إيجاد سبل تشريعية وإجرائية ناجعة لمواجهة الجرائم المعلوماتية من تلك الجهود القرار الصادر عن مجلس وزراء العدل العرب الخاص بإصدار القانون الجزائي الموحد كقانون عربي نموذجي.[2]

الفرع الثاني: وسائط الاختراق الالكتروني والجرائم الالكترونية التي تهدد الخصوصية

أولا- وسائط الاختراق الالكتروني لخصوصية الفرد

أ- البريد الإلكتروني Electronic Mail): وهو أكثر استخدامات الانترنت شيوعا يتكون المصطلح من جزأين رئيسيين هما رأس (Header) ونص (Body)، ويحتوي الرأس على معلومات حول المرسل والمتلقي والمعلومات اللازمة لتوصيل الرسالة إلى العنوان المناسب، ويحتوي النص على الرسالةالتي تم تكوينها.[3]

ويستطيع الجاني من خلال البريد الإلكتروني أن يرسل مادة معينة إلى شخص ما بغرض النيل من شرفه أو كرامته أو تعرضه إلى بعض الناس واحتقارهم فإذا ما استخدم البريد الإلكتروني للقيام بالأفعال السابقة عد مرتكبا الجريمة الذم والقدح، وبعد الهجوم عبر البريد الالكتروني والمواقع الإلكترونية من أفضل الطرق للهجمات على الأجهزة الإلكترونية بصورة عامة حيث أن عمليات

[1] سيفون باية، الأنترنت والصحافة الإلكترونية، دراسة في طبيعة العلاقة والتأثير، ط1، الجزائر، دار الخلدونية، 2016، ص154.
[2] المويشر، تركي بن عبد الرحمان، بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته، أطروحة دكتوراه في الفلسفة الأمنية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، السعودية، 2009، ص 175.
[3] الشوابكة محمد أمين، جرائم الحاسوب والانترنت الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2007، ص32، 33.

الاحتيال وعمليات السرقة الإلكترونية تكون في الغالب عبر البريد والمواقع الإلكترونية، وسرقة كلمة المرور (Password Sniffing) باستخدام برامج لاقطة (Sniffer) أثناء الاتصال بالانترنت.[1]

ب- شبكة الويب العالمية (World Wide Web): يمكن تعريف شبكة الويب العالمية (www) أو (Web) بأنها عبارة عن كم هائل من المستندات المحفوظة في شبكة الحاسوب، والتي تتيح لأي شخص أو لأي جهة الاطلاع على معلومات تخص جهات أخرى أو أشخاص آخرين قاموا بوضعها على هذه الخدمة، حيث تقدم خدمة معلومات واسعة النطاق من خلال خاصية الخطوط المحورية المتعددة والتي تسمح للمستخدمين بالارتباط عبر أنظمتها بالنصوص والملفات للحصول على المعلومات التي يعلق عليها النص المحوري (Texte Hyper).

ج- غرف المحادثات والدردشة (Chat Rooms): غرف المحادثة أو الثرثرة عبارة عن مساحات معروفة في القضاء الإلكتروني (Space Cyber) تتيح لمستخدمها الاشتراك في محادثات بين بعضهم البعض، بإرسال البريد الإلكتروني الذي يمكن قراءته من قبل الشخص المشترك في غرفة المحادثة وفي الواقع عندما تتخاطب عبر الانترنت فإن ما يحدث هو أنك تكتب رسالة باستخدام لوحة المفاتيح، حيث يمكن للآخرين رؤية ما يكتب.[2]

ثانيا- الجرائم الالكترونية التي تهدد الخصوصية: بتطور وشيوع استخدام الانترنت ووسائل التكنولوجيا تعددت أشكال الجرائم الإلكترونية التي يتعرض لها الأفراد والمنظمات والدول وتوضح أهمها كالتالي:

أ- سرقة المال المعلوماتي المعنوي (Identity Theft): أو سرقة الهوية وهي جريمة تأخذ صورة اختلاس البيانات والمعلومات والإفادة منها باستخدام السارق للمعلومات الشخصية مثل الاسم العنوان الأرقام السرية الخاصة بالمجني عليهم، والاستخدام غير الشرعي الشخصية المجني عليه ليبدأ بها عمليات السرقة المتخفية عبر الانترنت بحيث تؤدي بالغير إلى تقديم الأموال الإلكترونية أو المادية، إلى الجاني عن طريق التحويل البنكي،[3] هذا النوع من الجرائم يعتبر من أبرز أشكال الجرائم الإلكترونية وأكثرها خطورة، وتشير سرقة الهوية إلى تلك العمليات التي تتم من خلالها سرقة معلومات شخصية عن الهوية تستخدم للاحتيال والقيام بأعمال غير قانونية واستغلال هذه المعلومات لتحقيق مكاسب مالية فعند إصابة جهاز الحاسب الآلي بأحد البرامج الخبيثة، قد يقوم هذا البرنامج بالبحث في الجهاز عن بيانات شخصية، مثل الاسم أو العنوان أو مكان الميلاد أو رقم الهاتف أو رقم بطاقة الهوية أو أرقام بطاقات

[1] طالب أحسن مبارك، جرائم الاحتيال والعوامل الاجتماعية والنفسية المهيئة لها، جامعة نايف العربية للعلوم الأمنية، 2007، ص45.
[2] الشوابكة محمد أمين، مرجع سابق، ص 38، 45.
[3] المرجع نفسه، ص138.

الائتمان إلى آخره من معلومات، ثم يتم استخدامها في تزوير بطاقات الهوية وشهادات ميلاد وكشوف حسابات البنوك وسرقة الأموال.

ب- الاحتيال عبر الانترنت (Internet Fraud): الاحتيال الإلكتروني هو نوع من الاحتيال يتم فيه استخدام الانترنت ووسائطه المختلفة كالمواقع الإلكترونية والبريد الإلكتروني للقيام بعمليات احتيالية لتحقيق مكاسب مالية يتمثل الاحتيال بإغراء المتلقي بالاستجابة لطلبات المتصل في الحصول على معلومات شخصية أو العنوان البريدي الإلكتروني ليتمكن من الدخول واستخدام البريد الإلكتروني في أعمال تخصه باسم صاحب البريد الإلكتروني ويسبب تزايد أعداد المستخدمين للانترنت على مستوى العالم، ازدادت مخاطر تعرض الأفراد والشركات والمنظمات والحكومات العمليات الاحتيال عبر الانترنت.[1]

ج- الاختراق: يحدث الاختراق ثغرات في نظام الحماية الخاصة بالهدف، فيتمكن المخترق من الوصول إلى المعلومات بشكل غير قانوني فيقوم بالاستيلاء على المعلومات ونشرها بعد تحريفها، أو حذفها مكان الموقع بما يحقق أهداف تخريبية يسعى إليها المتصل بهجومات الاختراق (Penetration Attacks) في تلك الهجمات التي يتم من خلالها الدخول غير المشروع إلى الأنظمة الآلية وتخطي نظام التأمين الخاص بها، وفي حالات الاختراق الكامل يتمكن المهاجم من السيطرة الكاملة على الحاسب الآلي وتغيير البيانات أو تبديلها، أو زرع برامج خبيثة داخل الجهاز وفي بعض الحالات يقوم المخترق (Intruder) باستخدام الحاسب الآلي الذي تم اختراقه كأداة لشن هجوم إلكتروني على جهاز آخر خاصة وإن كانا متصلين بشبكة واحدة.[2]

د- جرائم الإضرار بالبيانات: تعتبر جريمة الإضرار بالبيانات من أخطر الجرائم الإلكترونية نظرا للخسائر التي تلحق بالأفراد أو المؤسسات، وتشمل الجريمة كل عملية الكترونية تهدف إلى تعديل أو محو أو سرقة أو إتلاف أو تعطيل العمل للمعلومات وقواعد البيانات الموجودة بصورة إلكترونية (Digital Form) على الحواسيب الآلية المتصلة بشبكات المعلومات أو مجرد محاولة الدخول بطريقة غيرمشروعة إليها.[3]

[1] الشوابكة محمد أمين، مرجع سابق، ص 185.
[2] شفيق نوران، أثر التهديدات الإلكترونية على العلاقات الدولية – دراسة في أبعاد الأمن الالكتروني، ط1، المكتب العربي للمعارف، القاهرة مصر، 2016، ص33، 34.
[3] محمد نصر الله، المسؤولية الجنائية لانتهاك الخصوصية المعلوماتية (دراسة مقارنة)، مركز الدراسات العربية والتوزيع، ط1، مصر، 2016، ص12.

تقع جريمة الإضرار أو الإتلاف في نطاق المعلوماتية عندما يتم الاعتداء على الوظائف الطبيعية للحاسب الآلي، وذلك بالتعدي على البرامج (Logical) والبيانات (Data) المخزنة والمتبادلة بين الحواسيب وشبكاته الداخلية (المحلية) أو العالمية (الانترنت). ويكون ذلك عن طريق التلاعب بالبيانات سواء بإدخال معلومات مصطنعة أو بإتلاف المعلومات المخزنة بالحواسيب والمتبادلة عبر الشبكة العالمية (Global Net) بمحوها أو تعديلها أو تغيير نتائجها أو التشويش على النظام المعلوماتي، الأمر الذي يؤدي إلى إعاقة سير عمل النظام الآلي.[1]

ه- الاعتداء على الملكية الفكرية الأسماء مواقع الانترنت: من صور الاعتداء الأخرى التي تمثل اعتداء على الملكية الفكرية للأسماء ما يحدث من اعتداءات على أسماء مواقع الانترنت (Domain Names) حيث أن القاعدة العالمية في تسجيل أسماء النطاقات والتي تتم أيضا باستخدام بطاقات الائتمان من خلال شبكة الانترنت.

من الجرائم الأخرى المتعلقة بأسماء النطاقات على شبكة الانترنت ما يعرف بإعادة التوجيه (Redirection) مثلما حدث الموقع شركة (Nike) في شهر يونيو عام 2000، حيث قامت جماعة من المحترفين بالدخول على موقع شركة تسجيل النطاقات الشهيرة والمعروفة باسم (Network Solutions) وتغيير بيانات النطاق الضعف إجراءات أمن المعلومات بالشركة في ذلك الحين. وبذلك تم إعادة توجيه مستخدمي الانترنت إلى موقع الشركة انترنت في أسكوتلندا.[2]

و- الالتقاط غير المشروع للبيانات: ويشمل الدخول غير المصرح به محاولة أي شخص الاستيلاء على أنظمة ومعلومات الغير ولو على سبيل إشباع الفضول والمتعة والإثارة أو تحديث أنظمة حماية الحاسبات الآلية.[3]

إن الدخول غير المشروع إلى النظام المعلوماتي أو البقاء فيه بدون إذن يتيح للمجرم المعلوماتي ممارسة نشاطاته الإجرامية من أجل تحقيق مكاسب شخصية متباينة ومتعلقة بذات المجرم بحيث تمكنه من التقاط البيانات المخزنة في قواعد البيانات أو المتبادلة عبر قنوات الانترنت واستخدامها بطرق غير مشروعة، ويتمكن المجرم المعلوماتي من النقاط البيانات بعد الدخول غير المشروع إلى النظام أو البقاء فيه إما عن طريق التجسس المعلوماتي (Informatique espionage) أو عن طريق الاحتيال الخداع Spoofing) أو عن طريق تفجير الموقع المستهدف.

---

[1] طالب أحسن مبارك، مرجع سابق، ص44.
[2] محمد نصر محمد، مرجع سابق، ص 13، 17.
[3] الشاعر عبد الرحمان بن ابراهيم، مواقع التواصل الاجتماعي والسلوك الإنساني، دار صفاء للنشر والتوزيع، عمان الأردن، 2015، ص53.

ز- التحويل الإلكتروني غير المشروع للأموال: اكتسب التعامل بالأموال في عصر المعلوماتية صفة البيانات الإلكترونية المخزنة في ذاكرة الحاسب الآلي، وأدت الثورة الرقمية إلى إمكانية إجراء تحويلات ومبادلات لهذه الأموال من أي مكان في العالم، وتكمن خطورة الأمر في إمكانية تلاعب الجاني بهذه البيانات المخزنة في ذاكرة الحاسب الآلي أو في برامجه وإجراء تحويلات في كل أو بعض أرصدة الغير أو فوائدها وتحويلها إلى حسابه أو حسابات أخرى.[1]

ح- الاحتيال باستخدام بطاقات الدفع الإلكتروني عبر الانترنت: يعتمد نظام بطاقة الدفع الإلكترونية على عمليات التحويل الإلكترونية من حساب بطاقة العميل بالبنك المصدر للبطاقة إلى رصيد التاجر بالبنك الذي يوجد به حسابه، وذلك من خلال شبكة التسوية الإلكترونية للهيئات الدولية وتعطي بطاقة الدفع الإلكتروني الحق للعميل في الحصول على السلع والخدمات عبر شبكة الانترنت عن طريق تصريح كتابي أو تليفوني يخصم القيمة على حساب بطاقة الدفع الإلكتروني الخاصة به.[2]

الفرع الثالث: أشكال التعدي على خصوصية الفرد

أولا- أشكال التعدي على خصوصية الفرد:

تتعرض عملية تبادل المعلومات على الشبكة العالمية لمحاولات هجوم بأشكال مختلفة، ويكون بعضها بشكل مباشر أو بشكل غير مباشر من خلال وسيط واحد أو أكثر وتعارف الخبراء على تسمية هذا الهجوم بالاختراق ومواقع التواصل الاجتماعي ليست بمنأى عن هذه الاحترافات فحسابات المستخدمين المواقع التواصل الاجتماعي عرضة للدخول إلها وانتحال شخصية منشتها وابتزازه وكثيرا من الحوادث حصلت نتيجة الدخول غير المشروع لمواقع الغير.[3]

فالاختراق هو المرور أو التسلل إلى نظام الحاسب الإلحاق الضرر بالمعلومات المخزنة فيه أو سرقتها والاستيلاء عليها أو نشر الفيروسات فيها ويمكن تقسيم الأشخاص الذين يقومون بعملية "الاختراق" إلى أربع فئات وهي:[4]

- الفئة الأولى: الفضوليون / المحترفون (Hackers): وهم الذين يقومون بالاستمتاع بتنفيذ المهمات الصعبة بل المستحيلة واقتحام اعقد الأنظمة على سبيل الهواية، بهدف إثبات الذات أو بنوايا إجرامية كتدمير البيانات أو الابتزاز.

[1] الشوابكة محمد أمين مرجع سابق، 166.
[2] المرجع نفسه، ص193.
[3] الشاعر عبد الرحمان، مرجع سابق، ص52.
[4] المرجع نفسه، ص53، 54.

- الفئة الثانية المتلصصون (Crackers): وهم الفئة التي تحاول الدخول إلى أنظمة الحاسوب الآلي بسوء نية وبشكل غير قانوني بغرض التخريب، وذلك بتغيير المعلومات أو بحذفها أو إضافة معلومات تخدم هدفا معينا.

- الفئة الثالثة: العابثون (Vandals) وهم الفئة التي تخترق النظام بدافع العبث، وينقسمون إلى مجموعتين هما مجموعة تشكل بعض المستخدمين الذين لهم حق الدخول في النظام، والمجموعة الثانية من الغرباء الذين لهم حق استخدام النظام أو الدخول فيه، وفي كلنا الحالتين يدخل العابثون بهدف العبث واللهو ويعتقدون أن ما يقومون به من أعمال غير معاقب عليها وهي مباحة.

ومن أهم صور الاعتداء الالكتروني على خصوصية بالأفراد نذكر ما يلي:

- الاعتداء على الحياة الخاصة للفرد: حظيت الحياة الخاصة للأفراد بحماية دستورية وقانونية في مختلف تشريعات الدول المتقدمة، لما لخصوصية الأفراد من أهمية قصوى على كيان الفرد والمجتمع معا، والحق في الخصوصية هو أحد الحقوق اللصيقة التي تثبت للإنسان، والتي غالبا ما يصعب حصر الجوانب المختلفة لها، والتمييز بحدود واضحة بين ما يعد من الحياة الخاصة للإنسان وما يعد من الحياة العامة له ولما كانت الحياة الخاصة للأفراد بصورتها المستحدثة والمتمثلة في بنوك المعلومات المرتبطة بالتكنولوجيا مهددة بالعديد من الانتهاكات والاعتداءات. ولاسيما بظهور شبكة الانترنت والأجهزة التكنولوجية الحديثة، فإن النصوص التقليدية تقف عاجزة أمام هذه الاعتداءات على خصوصية الأفراد وأسرارهم.[1]

- نشر وإعلان معلومات تتعلق بالحياة الخاصة للفرد: حيث يتم نشر معلومات حول الحياة الخاصة بالفرد عبر مختلف وسائل التكنولوجيا دون موافقته الصريحة، أو عدم الالتزام بحدود هذا الرضاء فيما يتعلق بالتعامل مع المعلومات الشخصية وطرق المعالجة الإلكترونية لها، وما يتعلق من معلومات مثل الحالة الصحية والاجتماعية والأسرية وفي هذا الشأن استقر القضاء على أن لكل شخص حقا مطلقا، وقاصر على صورته وعن استعمالها وأن الاعتداء على صورة الشخص يكون الاعتداء على جزء هام من الخصوصية، وهو الأمر الذي يستوجب المسؤولية والعقاب بحسب النشاط المخالف للحق في الخصوصية.[2]

- التنصت على الآخرين: يتنصت المجرم الالكتروني على الحياة الخاصة بالآخرين عن طريق استخدام برنامج معين يقوم بفتح منفذ في جهاز الشخص المعتدي عليه، يمكن من خلاله الاطلاع والاستماع إلى

[1] الشوابكة محمد أمين، مرجع سابق، ص 58، 59.
[2] محمد نصر محمد، مرجع سابق، ص30.

جميع المحادثات والمراسلات الصادرة من الشخص المعتدي عليه ويتم إدخال هذا الملف إلى الجهاز المعتدي عليه عن طريق البريد الإلكتروني أو عن طريق مواقع مغربة يزورها المعتدي عليه.[1]

- جرائم الذم والتحقير عبر الانترنت: تعد جرائم الذم والقدح والتحقير من أكثر الجرائم شيوعا في نطاق شبكة الانترنت، إذ يساء استخدامها للنيل من شرف الغير أو كرامته أو تعرضه إلى بعض الناس واحتقارهم بما يتم إسناده للمجني عليه على شكل رسالة بيانات.

وتتنوع صور الذم والقدح والتحقير بتنوع العرض من استخدام الانترنت والطريقة التي يستخدم بها، فقد يكون الدم والقدح والتحقير وجاهيا عبر وسائل الاتصال المباشر، أو قد يكون كتابيا أو قد يكون غيابيا، أو قد يكون بواسطة المطبوعات وجميع هذه الصور ترتكب عبر الانترنت من خلال المبادلات الإلكترونية الكتابية أو الصوتية أو التصويرية، وهي إما أن تكون بين طرفيات انترنت (Internet Terminal) متصلة (الحواسيب)، وإما أن تكون بواسطة طرفية انترنت منفصلة (مستقلة)، أو غير ما تبثه شبكات التواصل الاجتماعي من مضامين مباشرة أو غير مباشرة باستخدام الأجهزة الذكية.[2]

- التشهير Cyber Deramation: التشهير وتشويه السمعة في مواقع التواصل الاجتماعي سهل وميسر للعاملين وذلك بالقيام بنشر معلومات حصل عليها المتصل بطريقة غير مشروعة أو معلومات مغلوطة وتهدف إلى كسب مادي أو سياسي أو اجتماعي معين.

ثانيا- حجم الاختراق والتعدي على الخصوصية في الجزائر:

أسست الجزائر سنة 2009 قسم خاص لمكافحة الجريمة المعلوماتية متخصص في استغلال الأدلة المعلوماتية ضمن المديرية الفرعية للشرطة العلمية والتقنية، وتمكنت مصالح المديرية العامة للأمن الوطني خلال السداسي الأول من سنة 2013 معالجة ما مجموعه 383 قضية تتعلق بالجريمة الالكترونية، في حين تم معالجة 515 قضية خلال سنة 2012، ويتعلق الأمر بـ 126 قضية خاصة بالاستغلال غير القانوني للأداة المعلوماتية، و154 تتعلق بالهاتف النقال، و103 تخص الصور الفوتوغرافية والفيديو.

في هذا الصدد عالجت الخلية المركزية لمكافحة الجريمة الالكترونية خلال السداسي الأول من نفس السنة 15 قضية. تتعلق بانتهاك خصوصية الحياة الشخصية (معالجة 6 قضايا سنة (2012) وأربعة خاصة بالتشهير (8) قضايا سنة (2012) و 11 بسبب الابتزاز (4) قضايا سنة (2012)

[1] محمد نصر محمد، مرجع سابق، ص31.
[2] الشوابكة محمد أمين، مرجع سابق، ص30، 31.

وواحدة خاصة بانتحال الشخصية (4) قضايا سنة (2012) و 24 تتعلق بالقرصنة (10) قضايا سنة 2012)، ويشير القسم المختص في استغلال الأدلة المعلوماتية أن غالبية المخالفات تتعلق بالتكنولوجيات الجديدة سيما بواسطة الحواسيب والانترنت والهواتف النقالة، وتم كذلك تسجيل أزيد من 100 قضية خلال 9 أشهر من سنة 2014 ومعظمها تتعلق بالنصب والاحتيال على الأشخاص.

أما في السداسي الأول من سنة 2015 سجلت مصالح الأمن 417 قضية تتعلق بالجريمة الالكترونية، شملت انتحال الشخصية، النصب والاحتيال التزوير الإلكتروني تخريب بيانات شخصية وعامة الابتزاز بصور أو معلومات مقرصنة، التشهير، السرقة الالكترونية.

يلاحظ من الإحصائيات أن نسبة الجرائم الالكترونية شهدت ارتفاعا مستمرا، ففي السداسي الأول من سنة 2015 فاقت الجرائم الالكترونية ما تم تسجيله في السنوات (2012, 2013 و 2014) وهذا نظرا للارتفاع المتزايد لاستخدام شبكة الانترنت من قبل جميع الفئات الاجتماعية، وبالتالي ازدياد عدد ضحايا القرصنة والنصب والاحتيال ومختلف أشكال الجرائم الالكترونية الأخرى مع ارتفاع عدد مجرمي الانترنت.[1]

في حين سجلت سنة 2018 أكبر نسبة في قضايا القذف حيث احتلت نسبة 1354% بمجموع 42 جريمة شملت قذف أشخاص و تشويه سمعتهم تليا نسبة 741% بمجموع 23 جريمة تمثلت في قضايا السب سواء بطريقة كتابية أو عن طريق رسوم ومطبوعات غير البريد الالكتروني أو الصوتي، واحتلت قضايا التشهير نسبة 677 بمجموع 21 قضية وذلك بنشر معلومات مغلوطة عن أشخاص أو مؤسسات للتشهير بهم ونشر إشاعات و 17 قضية بنسبة 558% من صنف المساس بخصوصية الأشخاص دون علمه ورضاء ووضع تعليقات مسيئة لهم أو التهديد والابتزاز.[2]

من خلال النسب يتبين أن أكثر أشكال الجريمة الالكترونية في السنوات الأخيرة تمثل في جريمة القذف والسب وهذا نتيجة خاصية التخفي التي يمنحها القضاء الالكتروني للمجرمين، وكذا بسبب عدم التبليغ عن الجريمة من قبل الضحايا خاصة أن أغلب الجناة من فئة أقارب الضحية، وكذا نقص الوعي بالقوانين التي تشرع للأمن السيبراني وتعاقب كل من يسيء استخدام التكنولوجيا الحديثة.

[1] الشوابكة محمد أمين، مرجع سابق، ص32.
[2] محمد نصر محمد، مرجع سابق، 275، 276.

ثالثا- أشكال التهديدات التي تواجه أمن المعلومات:

يعرف أمن المعلومات بأنه العلم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها أو الحاجز الذي يمنع الاعتداء عليها، وذلك من خلال توفير الأدوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية والمعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين عبر الاتصالات، وضمان أصالة وصحة هذه الاتصالات مع الحماية من المخاطر المحتملة والناتجة عن استغلال ثغرات وضعف النظام.

تتزايد التهديدات التي تواجه أمن المعلومات نتيجة التطور المتسارع في الأساليب التي يمكن من خلالها الوصول لبيانات ومعلومات سرية خاصة بهدف تعديلها أو سرقتها أو حتى تدميرها. ويمكن تصنيف أساليب التهديد بهدف الحصول على المعلومات بأسلوب غير مصرح به إلى ما يلي:

أ- اختراق الشبكات (Hacking): تتم عملية الاختراق من خلال سرقة كلمة السر (Password Cracking) أو التعرض للاختراق أثناء محاولة معالجة اختراق سابق (Zero-Day Attack) أو هجمات حقن قواعد البيانات أو Language Injection AttackStructured Qucry.

ب- الهندسة الاجتماعية (Social Engineering): ليس المصطلح الهندسة الاجتماعية معنى متفق عليه، ولكن من أقرب التعريفات أن تقول إنها استخدام المهاجم الحيل نفسية كي يخدع مستخدمي الحاسوب ليمكنوه من الوصول إلى أجهزة الحاسوب أو المعلومات المخزنة فيها وخلافاً لما قد يتوهم بعض الناس، فإن الهندسة الاجتماعية يجب أن تكون على رأس قائمة وسائل الهجوم التي تتطلب حماية المعلومات منها،[1] والسبب في ذلك يرجع إلى الآتي:

- أن الهندسة الاجتماعية من أنجح الوسائل التي يستخدمها المهاجم لسهولتها مقارنة بالوسائل التقنية الأخرى.
- أن المتخصصين في مجال أمن المعلومات وكذلك مستخدمي الحاسوب لا يعيرون خطر الهندسة الاجتماعية في اهتمامهم.[2]

فالهندسة الاجتماعية يقصد بها تحفيز المستخدم على الإفصاح عن بيانات سريتها من خلال طرح أسئلة بهدف جمع معلومات دون إثارة أي شبهة، ويحتوي هذا الأسلوب على عدة تقنيات منها مايلي:

[1] شوابكة، مرجع سابق، ص170.
[2] الغثير خالد بن سليمان، أمن المعلومات بلغة مسيرة تقديم محمد بن إبراهيم السويل، مكتبة الملك فهد الوطنية، ط1، الرياض، 2009، ص31.

- **التوأمة الشريرة (Evil Twin):** أي ادعاء جهة معينة بأنها جهة موثوق منها من قبل المستخدم تطلب منه استخدام ملف مرفق يكون صارا به.
- **سرقة الهوية (Identity Theft):** أي ادعاء جهة معينة بأنها جهة أخرى معروفة من قبل المستخدم، بحيث يكون الطلب منه تقديم المعلومات بشكل مباشر.
- **التصيد (Phishing):** ويقصد منها وصول رسالة مزيفة من جهة غالبا مالية ومعروفة لطلب معلومات أو التحقق منها، ولتحقيق ذلك قد تحتوي هذه الرسائل على رابط مزيف لجهة معروفة.

ج- البرمجيات الضارة (Malwar): تتم عملية الاختراق من خلال برامج متخصصة لتسهيل التسلل إلى النظام أو الشبكة بهدف تدمير البيانات، وما أن يتم تثبيت البرمجية الضارة فإنه من الصعب جدا إزالتها، ويحتوي هذا الأسلوب على عدة تقنيات منها:[1]

- **حصان طروادة Trojan Horse:**برنامج يظهر بأنه يعمل بشكل معين ومفيد للمستخدم بينما هو في الواقع يقوم بعمل ضار وخفي عن المستخدم.
- **الفيروسات (Viruses):** برامج تدخل إلى الحاسوب وتتصل بالملفات المخزنة به ثم يكرر نفسه بحيث يتم تدمير هذه الملفات
- **برامج التجسس (Spywar):** برمجيات تؤدي إلى التجسس على المعلومات الشخصية دون علم مستخدم الحاسوب، وغالبا ما يتم تنزيلها بشكل سري من الانترنت.

رابعا- التعدي على الخصوصية والأمن المعلوماتي:

تعتبر جريمة الاعتداء على خصوصية الأفراد من أخطر الجرائم التي يمكن أن تقع عن طريق الانترنت نظرا لعدم وجود الحماية التقنية الفاعلة لما يتم تداوله من معلومات وأسرار ومراسلات عن طريق الانترنت، وتشمل جريمة الاعتداء على الحياة الخاصة الاعتداء بالتنصت أو التسجيل، أو نقل الحديث صدر عن شخص أو مراسلة دون رضاه بواسطة جهاز معين، أو النقاط أو نقل صورة شخص تواجد في مكان معين دون رضاه، والحاق الضرر المادي والمعنوي عليه، وتشير أحدث تقارير الخصوصية إلى أنه لا تزال أسرار الأفراد وخصوصياتهم في خطر. وتعتبر عملية حماية الخصوصية في البيئة الرقمية من أهم الوسائل والإجراءات التقنية بوصفها عملية تكاملية محكومة بإستراتيجية محددة العناصر، ومن الخطأ مجرد الاعتقاد بأن استخدام بعض التقنيات يحمي البيانات الشخصية حماية كاملة

[1] الغثير خالد بن سليمان، مرجع سابق، ص32.

وبالإضافة إلى ذلك يجب عدم إغفال أهمية الحماية القانونية والتشريعية وتكاملها مع الحماية التقنية والتنظيمية.[1]

المطلب الثاني: مبادئ الحماية القانونية للحق في الخصوصية في مواقع التوصل الاجتماعي

تدخل المشرع الجزائري لحماية الحق في الخصوصية من خلال إحاطته بمنظومة تشريعية، تكفل له حماية تشريعية وأساس قانوني يشكل ضمانة للأشخاص الطبيعيين للمطالبة بحماية حقوقهم من أي انتهاك لخصوصيتهم في مواقع التواصل الاجتماعي بسبب أخطاء ارتكبها المستخدمين لهذه المواقع كعدم حفظ البيانات الخاصة أو إنشاء سريتها بعد أن تم حفظها وتخزينها أو بسبب اختراق الغير لهذه المواقع، وقد استند المشرع الجزائري في هذه الإحاطة التشريعية إلى العديد من المبادئ.

الفرع الأول: مبادئ خاصة بضمان الأمن المعلوماتي للحق في الخصوصية

تعددت المبادئ المتعلق بضمان الأمن المعلوماتي للحق في الخصوصية منها مبدأ الشرعية ومبدأ سلامة المعطيات الشخصية وحساسيتها، ومبدأ الملائمة بين طبيعة المعطيات والهدف من تخزينها ومعالجتها، ونذكر منها على النحو الآتي:[2]

- مبدأ الشرعية:

جاء في نص المادة 47 من التعديل الدستوري لسنة 2020 أنه: 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. فمن نص المادة أعلاه يتضح أنه اعتراف الدستور بأن الحق في الخصوصية حق من الحقوق الأساسية ولا يهم الشكل الذي يكون فيه، ولا يمكن الاطلاع عليه إلا يعلم وإذن صاحبه، أو خرقه إلا في ظروف خاصة وبموجب أمر معلل من السلطة القضائية، ومثالها أن تقوم هذه الأخيرة بمناسبة التحقيق في جرائم التمييز وخطاب الكراهية بإصدار:[3]

- ✓ أمر تسليم أية معلومة أو بيان يكون مخزنا باستخدام وسائل تكنولوجيات الإعلام والاتصال.

[1] حمد نصر محمد، مرجع سابق، 282.
[2] المرجع نفسه، 290.
[3] الغثير خالد بن سليمان، مرجع سابق، ص55.

- ✓ أمر بالتقاط الفوري عليها إذا كان المحتوي يشكل جريمة من جرائم التمييز.
- ✓ أمر بالتدخل الفوري لسحب أو تخزين معلومات والمحتويات المقدم الخدمات ليتم الاطلاع عليها أو الجمل الدخول إليها غير ممكن.

ومنه يجب أن تشمل المعطيات الخاصة مضمون شرعي كما هو مبين أدناه:

- المعلومات والمعطيات الخاصة للأفراد الغير قابلة للنقل والتداول عبر الوسائط الالكترونية إلا يعلم ورغبة حائزها.

- المعلومات والمعطيات الخاصة بالأفراد السرية وتكون متداولة بين عدد محدد من الأشخاص، ويستوي في ذلك أن ترد على حدث أو حقيقة أو أن ترد على فكرة أو عمل ذهني.

- المعلومات والمعطيات الشخصية والمرتبطة بشخص المخاطب بها كحالته الصحية وذمته المالية وحالته الاجتماعية واسمه، وهي معلومات يملك صاحبها سلطة قانونية فلا يجوز الاطلاع عليها أو تناولها إلا بإذنه أو بموجب أمر من السلطة القضائية المختصة[1].

- مبدأ سلامة المعطيات الشخصية وحساسيتها:

حتى تحظى المعطيات الشخصية المخزنة والمعالجة في مواقع التواصل الاجتماعي بالحماية القانونية لابد أن تكون صحيحة كاملة ومدينة، خالية من أي غموض أو تدليس، وهذا الأمر يسري على جميع المعطيات الخاصة بالفرد سواء كانت اجتماعية أو دينية أو مالية، وفي هذا الخصوص عرف المشرع الجزائري المعطيات ذات الطابع الشخصي، بموجب نص المادة الثالثة من القانون رقم 18-07 المؤرخ في 10 يونيو 2018 والمتعلق بحاجة الأشخاص الطبيعيين في مجال معالجة المصليات ذات الطابع الشخصي، على أساس طبيعة البيانات الشخصية والتي يفترض بها أن تبقى سليمة تحت طائلة عربات جزائية وهي: رقم التعريف أو عناصر خاصة بالهوية البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية.[2]

[1] عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة الكترونيا الدراسة مقارنة، دار النهضة العربية، مصر،2010، ص 189.

[2] جمال مصالح عبد الحليم، الحماية الجنائية للحق في الخصوصية في مواجهة نظم المعلومات دار النهضة العربية 2016، مصر، ص 110.

- مبدأ الملائمة بين طبيعة المعطيات والهدف من تخزينها ومعالجتها:

اعتمد المشرع الجزائري في تأطيره القانوني للمعطيات الخاصة على مبدأ الملائمة بين البيانات الشخصية والهدف من تخزينها ومعالجتها، فمثلا تسجيل المعطيات الخاصة بالطلبة على مستوى المنصة الرقمية البروقرس بهدف الانتفاع بخدمات مؤسسات التعليم العالي، وتسجيل بيانات الأشخاص العاطلين عن العمل وغير المؤمنين في منصة منحة البطالة للحصول على منحة البطالة، وتسجيل التاريخ الصحيح للفرد للحصول على الضمان الاجتماعي، وتسجيل الناخبين في البطاقة الوطنية للناخبين لتنظيم عملية الانتخابات.

وهناك أيضا فكرة تسجيل المعطيات الخاصة في مواقع التواصل الاجتماعي للحصول على خدمة أو منتج عن بعد، فيضطر الفرد بإرسال معطياته الخاصة كرقم هاتف وعنوانه الشخصي واسمه إلى المورد الالكتروني ليتمكن من الحصول على الخدمة أو المنتج المروج له في الوسائط الالكترونية:

- معالجة بطريقة مشروعة ونزيهة.
- مجمعة لغايات محددة وواضحة ومشروعة وألا تعالج لاحقا بطريقة تتنافى مع هذه الغايات.
- ملائمة ومناسبة وغير مبالغ فيها بالنظر إلى الغايات التي من أجلها تم جمعها أو معالجتها.
- صحيحة وكاملة ومحينة إذا اقتضى الأمر.
- محفوظة بشكل يسمح بالتعرف على الأشخاص المعنيين خلال مدة لا تتجاوز المدة اللازمة لإنجاز الأغراض التي من أجلها تم جمعها أو معالجتها[1].

الفرع الثاني: مبادئ وأصناف الحماية القانونية الخاصة بضمان حقوق الأشخاص الطبيعيين المسجلة بياناتهم

أولا- المبادئ الخاصة بضمان حقوق الأشخاص الطبيعيين المسجلة بياناتهم

ويشمل مبدأ تمكين الأشخاص المعنويين أو الطبيعيين من ممارسة حقوقهم الأساسية في الوسائط الرقمية عامة ومواقع التواصل الاجتماعي خاصة وأبرزها على الإطلاق الحقوق المبينة أدناه[2]:

[1] جمال مصالح عبد الحليم، مرجع سابق، ص111.
[2] المرجع نفسه، ص111، 112.

- الحق في الحصول على المعلومة:

فمن حق الشخص المعني بمحتوى المعلومة سواء مباشرة أو عن طريق ممثله القانوني الاطلاع على مضمون المعلومات والبيانات التي تخصه والتي تم تخزينها ومعالجتها بأي شكل كان، فالصور والطرق مختلفة خاصة وأن المعطيات تخصه ولا تخص الغير ولا تمس بأي شكل كان النظام العام أو الآداب العامة وفي هذا الخصوص نصت المادة 55 من التعديل الدستوري لسنة 2020 التي تنص على: "يتمتع كل مواطن بالحق في الوصول إلى المعلومات والوثائق والإحصائيات والحصول عليها وتداولها، لا يمكن أن تمس ممارسة هذا الحق بالحياة الخاصة للغير وبحقوقهم وبالمصالح المشروعة للمؤسسات وبمقتضيات الأمن الوطني".

- حق تصحيح المعلومات الخاصة:

في كثير من الأحيان يلجأ الأفراد إلى تصحيح بعض المعطيات والمعلومات في صفحاتهم الخاصة في مواقع التوصل الاجتماعي، والتي يفترض بها أنها محجوبة عن بقية المستخدمين باستثناء المسؤولين عن الموقع، الذين ينبغي عليهم تمكينهم من ذلك، كما يتعين عليهم معالجة معطيات الأفراد مهما كان مصدرها أو شكلها، على النحو الذي يضمن لهم عدم المساس بحقوقهم وشرفهم وسمعتهم وكذا احترام الكرامة الإنسانية والحياة الخاصة.

- الحق في محو البيانات الشخصية:

تعتمد الكثير من مواقع التوصل الاجتماعي على خاصية الطف أو المسح أو الاتلاف، وهذا لتمكين أصحاب الصفحة ومالك المعلومة أو البيان من التخلص من المعلومات التي يرغب في حذفها مهما كان السبب، وهذا يعتبر ضمانة أساسية لحماية خصوصية الأفراد في منصات التواصل الاجتماعي، لأنه سيحجب المعلومة التي تخصه ليس فقط عن الغير بل أيضا عن مقدمي الخدمات.[1]

ثانيا- أصناف الحماية القانونية للحق في الخصوصية في مواقع التواصل الاجتماعي

تتنوع أصناف الحماية القانونية للحق في الخصوصية بين الحماية المعلوماتية كتدبير وقائي، والجزائية كتدبير ردعي عقابي.

[1] جمال مصالح عبد الحليم، مرجع سابق، ص112.

- الحماية المعلوماتية للحق في الخصوصية مواقع التواصل الاجتماعي كإجراء وقائي

توجد إلى جانب الحماية الجنائية حماية معلوماتية للحق في الخصوصية في مواقع التواصل الاجتماعي وذلك بهدف منع المتطفلين والقراصنة من الدخول الى شبكاتهم، لذا يجب اتخاذ كافة تدابير الحيطة والحذر عند استخدام الأجهزة الالكترونية عموما ومواقع التواصل الاجتماعي خصوصا.

فإن المقصود بالحماية المعلوماتية هي إنشاء برامج تقنية حمايته تعمل على حماية البيانات الرقمية من شتى أشكال الهجومات الالكترونية، ومن خلال هذا المبحث سيتم التعرف على أهم التطبيقات التي تحمي المعلومات الشخصية في البيئة الافتراضية ودورها الفعال في تحقيق الحماية ضمن الفروع التالية:

- ✓ **أنواع التطبيقات الالكترونية لحماية الخصوصية المعلوماتية:**

هناك العديد من التطبيقات التي يمكن الاعتماد عليها لحماية المصليات الخاصة، تختلف باختلاف درجة الحماية التي توفرها وعلى حسب نوعية الاختراقات وطبيعة الفيروسات المستعملة في الاختراق ومن أبرز هذه التطبيقات لدينا:

- ✓ **تطبيق ماي دانا مانجر my data manager :**[1]

بعد هذا التطبيق من بين أهم التطبيقات التي تساعد على حماية خصوصية المستخدم أثناء استخدام الأنترنت والتحكم باستهلاك البيانات، حيث يقوم هذا الأخير على تأمين استخدام الأنترنت من خلال إيجاد ما يعرف بالشبكة الخاصة الافتراضية VPN لتشفير البيانات الغير محمية إلى جانب مراقبته لكمية البيانات التي يستهلكها كل تطبيق.[2]

- ✓ **تطبيق المراسلة سيغنال signal:**

من أكثر التطبيقات التي تعمل على دعم الحفاظ وحماية الخصوصية المعلوماتية والأمان الرقمي، فهو يوفر ميزة التشفير من طرف الى طرف end to end enycryption لجميع المحادثات النصية والصوتية وكذلك محادثات الفيديو ... الخ، وقد حصل على الحديد من الموافقات من قبل الهيئات

[1] الموقع الرسمي للبرنامج ماي دانا ما تاجر تم الاطلاع على الموقع بتاريخ 28/05/2023 على الساعة 22:30 موجود على الرابط التالي: https://play.google.com/store/apps/details?id=com mobilia .android.malm&hl=ar&al US

[2] خلدون عمان سعيدة تطبيقات مفيدة لحماية الخصوصية الرقمية تؤمن تصفح الأنترنيت والتراسل ورسائل البريد الالكتروني ، مقال منشور بتاريخ 12 جانفي 2021، تم الاطلاع عليه بتاريخ 01/06/2023 على الساعة 10:00 موجودة في الرابط التالي:https:my-data-manager.ar.uptodown.com/android.

التي تهتم بحماية حق الخصوصية لمستخدميها مثل مؤسسة موزيلا، والتي تطور متصفح فاير فوكس ولجنة حماية الصحافيين.[1]

✓ **تطبيق fingersecurity:**[2]

يشكل هذا التطبيق نوع من الحماية الخاصة بخلق وقفل التطبيقات المتواجدة على مستوى الأجهزة التي تعمل بنظام التشغيل الأندر ويد عن طريق بسمة الأصبع، كما يحتوي ذات التطبيق على سيمات متعددة للبصمة يمكنك تثبيتها والاختيار من بينها الشكل الذي يساعد صاحب الجهاز ومن لهم الصفات التي يتصف بها هذا التطبيق أنه يمنح مدة زمنية معنية لمنع قفل التطبيقات المعنية به وبعد مرور تلك الفترة يطلب منك التطبيق إعادة إدخال البسمة من جديد للتأكد من صاحب الهاتف، كما يمنع من الإشعارات من الظهور ودعم حمايتها.

✓ **التشفيرEncryptions:**

يعتبر التشفير أحد برامج الوقاية والحماية من الهجمات السيبرانية، حيث تظهر مهمته في تشفير البيانات المتبادلة وضمان عدم المساس بمحتوى البيانات لأي تعديل أو تغيير، ولعل الخاصية الأساسية من التشفير تبرز في إمكانية تغيير البيانات المتبادلة عند حل التشفير عن طريق مفتاح التشفير من طرف المرسل أو من الطرف المستقبل، وجدير بالذكر أن نظام التشفير يحتوي على أسلوبين من الحماية منها ما هو متعلق بحماية الشبكة الخاصة الافتراضية من خلال تشفير كل الرسائل والبيانات المتجمعة في البيئة الافتراضية قبل تبادلها، في حين الأسلوب الثاني يبدوا في شكل نظام يسمى SSL[3].

- الحماية الجزائية للحق في الخصوصية في مواقع التواصل الاجتماعي كإجراء ردعي

لقد تضافرت جهود الدولة الجزائرية من أجل وضع تصور قانوني فعال في تعزيز الحق في الخصوصية ورفع مكانته، وتحقيق الحماية القانونية من جهة وصيانة البيانات والمعطيات من جهة أخرى وفي ظل الرقمنة تمكنت تقنية المعلوماتية الجديدة من الحصول على معلومات وتخزين وتحليل كم

[1] الموقع الرسمي للبرنامج سيدال تم الاطلاع على الموقع بتاريخ 02/06/2023 على الساعة 13:20 موجود على الرابط الثاني: : https//play.google.com/store/apps/details?id=ory thoughtcrime securesms &hl كنا ايكس - خلدون فنان سعيد المرجع السابق.

[2] خلدون غسان سعيد، المرجع السابق.

[3] حكيمة جاب الله انعكاسات الجريمة السيرانية على البيئة الرقمية دراسة في آليات واستراتيجيات مكافحتها، حوليات جامعة الجزائر 663 الجزائر المجد 35 العدد 03، 2021، ص 663.

هائل من البيانات الشخصية من قبل العديد من المؤسسات والوكالات الحكومية والغير الحكومية، مما رتب آثار جد سلبية على خصوصية الحياة الفردية للأشخاص، وهو ما سيتم التطرق له:[1]

✓ **جريمة الدخول والبقاء الغير مشروع:**

نص المشرع الجزائري على جريمة الدخول والبناء الغير مشروع في المادة 394 مكرر من قانون العقوبات، حيث يرتكز الركن المادي لهذه الجريمة في فعل الدخول أو البقاء الغير مشروع وهو دخول بطريقة الغش والاحتيال إلى ما يقوم به نظام المعالجة الآلية للمعطيات وهو عملية غير مصرح بها تكون هذه الأخيرة لإساءة استخدام الحاسب الآلي ونظامه عن طريق شخص غير مرخص له للوصول إلى المعطيات والمعلومات المخزنة بداخله، وفعل البقاء هو التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له حق في السيطرة على هذا النظام.[2]

✓ **جريمة الاعتداء العمدي على المعطيات الموجودة داخل النظام المعلوماتي:**

نص المشرع الجزائري على هذا النوع من الجرائم في المادة 394 مكرر 1 من قانون العقوبات، هذه الجريمة تتمثل في صورتين الأولى الاعتداء العمدي على المعطيات الموجودة داخل النظام، أما الثانية فهي المساس العمدي خارج النظام.

يتمثل الركن المادي للصورة الأولى من هذا النوع من الجرائم والذي يتجسد أساس في ثلاث أفعال وهي الإدخال المحو التعديل والملاحظ أن المشرع لم يشترط اجتماع هذه الأفعال معا لتكون صورة واحدة بهذه الجريمة، بل يكفي أن يكون فعلا واحدا صادرا عن الجاني كي يقوم الركن المادي، كما أن هذا التلاعب في المعطيات يقتصر على المعلومات التي يحتويها النظام سواء بإضافة ما هو جديد صحيحا كان أو غير ذلك، أو تعديل ما هو موجود بأي شكل من الأشكال، وقد ذكر المشرع العقوبة الواجب تطبيقها في المادة 394 مكرر1.[3]

أما الصورة الثانية وهي المساس العمدي للمعطيات خارج النظام، فقد جاء بها المشرع الجزائري في نص المادة 394 مكرر 2، وبذلك يكون قد كرس حماية جزائية للمعطيات في حد ذاتها لكونها أنه لم يشترط أن تكون المعلومة داخل نظام المعالجة الآلية أو قد تم معالجتهاآليا فالفقرة 01 من نفس المادة تنص على أن محل الجريمة يتمثل أساسا في المعطيات بغض النظر عن كيفية وطريقة

[1] عبد الله بن عبد الله السند الأحكام الفقهية للتعاملات الالكترونية دار الفكر الجامعي، 2004، مصر، ص 4000.
[2] خليفة التواجد الغير مشروع في أنظمة المعلوماتية، أطروحة دكتوراه، كلية الحقوق جامعة ناجي مختارة عناية الجزائر، 2011، ص 142.
[3] مختارية بوزيدي، المرجع نفسه، ص 16.

تخزينها سواء كانت مرسلة عن طريق منظومة معلوماتية أم معالجة آليا أو كانت ضمن أقراص لكونها استعملت لارتكاب جرائم منصوص عليها، أما بخصوص فقرتها الثانية فقد خصها بالأفعال المجرمة في حد ذاتها بغض النظر عن الغرض من هذه الجرائم، وهذا ما ميز المشرع الجزائري عن غيره. أما بخصوص العقوبة فهي واضحة في المادة 394 مكرر 2.[1]

إن الحماية القانونية التي أحاطها المشرع الجزائري بالمعطيات الشخصية للأشخاص الطبيعيين في مواقع التواصل الاجتماعي غير كافية بضمان أمنها المعلوماتي، بدليل التزايد المستمر للجرائم الماسة بالحق في الخصوصية الناتجة عن الاستخدام غير المشروع لمنصات التواصل الاجتماعي، وما تبعها عن ذلك من جرائم ذات الصلة بها.

الفرع الثالث: دور التطبيقات الالكترونية والحماية الجزائية في حماية الخصوصية المعلوماتية

تلعب التطبيقات الالكترونية دورا بارزا في تكريس وظيفة الأمن المعلوماتي من خلال التصدي للهجمات الالكترونية وحماية الخصوصية المعلوماتية، ويكمن هذا الدور الرئيسي في:

- اتخاذ التدابير اللازمة والضرورية لحماية المعلومات الحساسة من أي اختراق.
- ضمان سلامة المعلومات واستمرارها ضد أي تعديل أو تغيير أو محو غير مشروع أو تدمير.[2]
- مهمة الكشف عن الفيروسات ومكافحتها أو محاولة تدميرها قبل البدء في الاطلاع على البياناتا لشخصية الالكترونية أو تشويه البيانات المتوفرة في مختلف منصات التواصل الاجتماعي".[3]
- تشفير البيانات والمعلومات التي يتم تسجيلها في مواقع التواصل الاجتماعي.[4]
- تعمل التطبيقات الالكترونية الهادفة لحماية البيانات الشخصية على منع تحميل البرامج الخبيثة، التي يمكن أن تتواجد بذاكرة الحاسوب أو الهواتف الذكية.[5]

[1] مختارية بوزيدي، المرجع نفسه، ص 18.
[2] الجواد دلال صادق أمن المعلومات دار اليازوري العلمية للنشر والتوزيع 2000، عمان، ص 41.
[3] حزام فتيحة حماية الأنظمة الرقمية بين الآليات الثانية وأجهزة الحماية لقراءة في احكام المرسوم الرئاسي 20-05، مجلة الحقوق والعلوم الإنسانية الجزائر المجلد 13 العدد 03، 2020، ص 175.
[4] المرجع نفسه، ص 176.
[5] حكيمة جاب الله، المرجع السابق، ص 663.

المبحث الثاني: الإطار القانوني لحماية الحياة الخاصة في ظل الأمن المعلوماتي

يعد الإطار القانوني حجر الأساس في ضمان حماية الحياة الخاصة داخل البيئة الرقمية، خاصة مع تزايد انتهاك الخصوصية عبر الوسائل التقنية الحديثة.

المطلب الأول: التشريعات والتحديات الوطنية والدولية المنظمة لحماية البيانات الشخصية

في ظل التحولات الرقمية المتسارعة، لم تعد البيانات الشخصية مجرد معلومات معزولة، بل أصبحت مورداً استراتيجياً يوازي في قيمته الاقتصادية والأمنية الثروات الطبيعية. هذا التغير جعل مسألة حماية البيانات الشخصية في قلب منظومة الأمن المعلوماتي، حيث يتطلب تأمينها تشريعات قانونية صارمة موازية للإجراءات التقنية.

الفرع الأول: التشريعات الوطنية والدولية المنظمة لحماية البيانات الشخصية

أولا- التشريعات الوطنية لحماية البيانات الشخصية:

1- الجزائر:

القانون رقم 18-07 المؤرخ في 10 يونيو 2018 المتعلق بحماية الأشخاص الطبيعيين في ما يتعلق بمعالجة المعطيات ذات الطابع الشخصي،[1] يعد الإطار القانوني الأساسي لحماية البيانات الشخصية في الجزائر، ينص هذا القانون على مبادئ أساسية مثل الشفافية، والشرعية، والحد من جمع البيانات، والحق في الوصول والتصحيح، والحق في الاعتراض، والحق في الحذف. كما أنشأ السلطة الوطنية لحماية البيانات ذات الطابع الشخصي كهيئة مستقلة تشرف على تطبيق هذا القانون وتضمن احترام حقوق الأفراد.[2]

- المحتوى الأساسي للقانون:

المادة 4: تحدد نطاق تطبيق القانون على المعالجة الآلية وغير الآلية للمعطيات ذات الطابع الشخصي، سواء تمت من الأشخاص الطبيعيين أو من الأشخاص المعنويين.

المادة 32: تنص على إلزامية إعلام الشخص المعني قبل جمع معطياته الشخصية، مع توضيح الأغراض والجهات المستفيدة.

المادة 34: تمنح الحق للشخص المعني في الوصول إلى معطياته الشخصية وتصحيحها.

[1] الجريدة الرسمية الجزائرية، العدد 32، 10 جوان 2018، ص. 10–23.
[2] مختارية بوزيدي، مرجع سابق، ص 75.

المادة 36: تتيح للشخص المعني الحق في الاعتراض على معالجة معطياته لأسباب مشروعة.

2- تونس:

القانون الأساسي عدد 63 لسنة 2004 المؤرخ في 27 يوليو 2004 المتعلق بحماية المعطيات الشخصية،[1] يُعتبر الإطار القانوني الرئيسي لحماية البيانات الشخصية في تونس. ينظم هذا القانون جمع، ومعالجة، وتخزين، ونقل البيانات الشخصية، ويحدد حقوق الأفراد مثل الحق في الوصول، والتصحيح، والاعتراض، والحذف. كما أنشأ الهيئة الوطنية لحماية المعطيات الشخصية كهيئة مستقلة تشرف على تطبيق هذا القانون وتضمن احترام حقوق الأفراد.[2]

- المحتوى الأساسي للقانون:

الفصل 01: يقر بحق كل شخص في حماية معطياته الشخصية باعتبارها من الحقوق الأساسية المضمونة بالدستور، ولا يمكن أن تقع معالجتها إلا في إطار الشفافية والأمانة واحترام كرامة الإنسان ووفقا لمقتضيات هذا القانون.

الفصل 02: ينطبق هذا القانون على المعالجة الآلية وغير الآلية للمعطيات الشخصية سواء تمت من الأشخاص الطبيعيين أو من الأشخاص المعنويين.

الفصل 20: يجب على المسؤول عن معالجة المعطيات الشخصية إذا عهد ببعض أعمال المعالجة أو جميعها إلى الغير في إطار عقد مناولة أن يتحرى في اختيار من يعهد إليه بذلك.

ثانيا- التشريعات الدولية المنظمة لحماية البيانات الشخصية:

1- الاتحاد الأوروبي: اللائحة العامة لحماية البيانات (GDPR)

تعد اللائحة العامة لحماية البيانات (GDPR)، التي دخلت حيز التنفيذ في 25 مايو 2018، التشريع الأساسي في الاتحاد الأوروبي لحماية البيانات الشخصية،[3] تنطبق هذه اللائحة على جميع الدول الأعضاء في الاتحاد الأوروبي، وتحدد قواعد صارمة لجمع، ومعالجة، وتخزين، ونقل البيانات

[1] الجريدة الرسمية للجمهورية التونسية، عدد 63، 27 جويلية 2004، ص. 1931–1942.
[2] مختارية بوزيدي، مرجع سابق، ص77.
[3] GDPR Regulation (EU) 2016/679, Official Journal of the European Union, L119, 4 May 2016, pp. 1–88.

الشخصية. تُركز اللائحة على حقوق الأفراد، مثل الحق في الوصول، والتصحيح، والاعتراض، والحذف، وتفرض عقوبات مالية كبيرة على المخالفين.[1]

- المحتوى الأساسي للقانون:

المادة 5: تحدد المبادئ الأساسية لمعالجة البيانات الشخصية، مثل الشرعية والشفافية والحد من الغرض والبيانات.

المادة 6: توضح الأسس القانونية لمعالجة البيانات، مثل موافقة الشخص المعني أو تنفيذ عقد.

المادة 15: تمنح الحق للأفراد في الوصول إلى بياناتهم الشخصية.

المادة 17: تعرف بحق "النسيان" أو الحق في محو البيانات.

3- المبادئ التوجيهية لمنظمة التعاون والتنمية الاقتصادية (OECD):

أصدرت منظمة التعاون والتنمية الاقتصادية (OECD) في عام 1980 المبادئ التوجيهية لحماية الخصوصية وتدفق البيانات الشخصية عبر الحدود. تُعد هذه المبادئ مرجعًا هامًا للتشريعات الوطنية والدولية في مجال حماية البيانات الشخصية، وتُركز على مبادئ مثل الشفافية، والاختيار، والحد من جمع البيانات، والدقة، والأمن، والاحتفاظ بالبيانات.[2]

- المحتوى الأساسي للمبادئ:

المبدأ 1: تقر بضرورة وجود قوانين أو إجراءات لحماية الخصوصية.

المبدأ 2: تحدد شروط جمع البيانات، مثل الموافقة المسبقة.

المبدأ 3: تقر بحق الأفراد في الوصول إلى بياناتهم وتصحيحها.

المبدأ 4: تحدد شروط نقل البيانات إلى دول خارجية.

[1] اللائحة العامة لحماية البيانات(GDPR) ، الاتحاد الأوروبي، الموقع الرسمي: https://gdpr-info.eu/ gdpr-info.eu، تاريخ الإطلاع: 2025/05/11، على الساعة: 10:30.

[2] مبادئ الخصوصية لمنظمة التعاون الاقتصادي والتنمية، الموقع الرسمي: https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm، تاريخ الإطلاع: 2025/05/11، على الساعة: 18:00.

الفرع الثاني: تحديات تطبيق القوانين في مواجهة الجرائم الرقمية

تزايدت الجرائم الرقمية بشكل غير مسبوق في ظل التطور التكنولوجي المتسارع، مما أوجد تحديات قانونية وتقنية حقيقية أمام الجهات المختصة، ويعد الأمن المعلوماتي اليوم محورا أساسيا في مواجهة هذه الجرائم، وسط صعوبات تطبيق القوانين التقليدية على واقع رقمي معقد ومتغير.

وتتمثل هذه التحديات في الآتي:

- كيفية مواجهة الصعوبات الناجمة عن التكنولوجيا والبرمجيات وطرق تنفيذها، والقدرة على التحكم فيها، لا سيما مع خصائصها التي تتجاوز أحيانا قدرات الأفراد فتؤدي إلى ارتكاب جرائم دون قصد فتكون هناك إساءة استعمال.

- تكييف القوانين والتشريعات مع طبيعة التطورات التقنية، أي تحدي التوفيق بين عناصر الأمن المعلوماتي في شقيه التقني والتشريعي، وكذا التنظيمي أيضا أي تسيير المؤسسات.

- تحقيق الأمن المعلوماتي يواجه تحدي كبير، فالتحقق من هوية الأفراد الذي بعد مجسدا للمفهوم الأمني تجد العكس منه فوسائل الإعلام الجديد لا تشترط الكشف عن الهويات الحقيقية للأفراد مما يصعب من ملاحقة مرتكبي الجرائم في حال وقوعها وصعوبة تتتبع المصدر الحقيقي.

- تحدي السرية الذي يواجه بالرفض من قبل الباحثين عن الحقيقة أو قد يتعارض مع الحق في الوصول إلى المعلومة.

1- الإشكالات القانونية والتشريعية في مواجهة الجرائم الرقمية:

تواجه التشريعات الوطنية صعوبة في مواكبة التطور المتسارع للجرائم الرقمية، إذ أن أغلب النصوص القانونية المعمول بها لا تزال مستمدة من منظومات تقليدية أعدت لجرائم مادية واضحة الأركان، مما يجعلها عاجزة أحيانا عن ضبط الأفعال الإجرامية المرتكبة عبر الوسائط الرقمية.

ويتمثل أبرز إشكال تشريعي في غياب تعريف دقيق وموحد للجرائم الرقمية، فضلا عن ضعف الصياغة القانونية في كثير من القوانين الوطنية، والتي تستخدم مصطلحات فضفاضة مثل "الاعتداء على نظم المعالجة الآلية" دون تحديد كاف للوسائل أو النطاق التقني المقصود، كما يلاحظ غياب التجانس بين القوانين العربية في معالجة هذه الجرائم، مما يضعف التنسيق الإقليمي والدولي.[1]

[1] عبد العال، يوسف، الجرائم الإلكترونية في القانون المقارن، دار النهضة العربية، القاهرة، 2020، الصفحة 73-75.

- في الجزائر، نص القانون 09-04 لسنة 2009 على "الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال" دون تحديد دقيق لكل صنف.

- فالقانون الجزائري رقم 09-04 (2009) المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ما زال يواجه محدودية في التغطية القانونية لبعض أنواع الجرائم الحديثة مثل الابتزاز الإلكتروني عبر الميتافيرس.

- قصور الإطار القانوني الوطني والتشريعات التقليدية.

- غياب تعريف دقيق للجرائم الرقمية في بعض التشريعات.

- عدم مواكبة التطور التكنولوجي السريع مثل الذكاء الاصطناعي، العملات الرقمية، شبكات(VPN).

- تضارب القوانين بين الدول في البيئة الرقمية العابرة للحدود

- إشكالية تنازع الاختصاص القضائي بين الدول.

- عدم وجود اتفاقيات ثنائية أو جماعية كافية لتنظيم التعاون القضائي في مجال الجرائم الإلكترونية.[1]

❖ **صعوبة التكييف القانوني للجرائم الرقمية الحديثة:**

- الجرائم الرقمية لا تتخذ شكلا ماديا ملموسا، مما يعيق تطبيق قواعد القانون الجنائي التقليدي عليها.

- جرائم مثل سرقة البيانات أو اختراق البريد الإلكتروني يصعب تكييفها ضمن "السرقة" بمفهومها التقليدي.

- الحاجة إلى استحداث جرائم جديدة مثل "الابتزاز الرقمي"، و"التنصت السيبراني".[2]

- الجرائم الرقمية تشمل أفعالا جديدة مثل: التصيد الإلكتروني، الابتزاز الرقمي، سرقة الهوية، وهي أفعال يصعب إدراجها ضمن الأوصاف الجنائية التقليدية.

- على سبيل المثال، اختراق حساب إلكتروني لا يمكن تكييفه كـ «سرقة" تقليدية، مما يعرقل المتابعة القضائية.[3]

[1] بودابست، اتفاقية مجلس أوروبا حول الجرائم السيبرانية، 2001.
[2] جابر هدى، التكييف القانوني للجرائم الإلكترونية، مجلة الدراسات القانونية، عدد 12، 2021، ص 45.
[3] المرجع نفسه، ص 46.

❖ **إشكالية تنازع الاختصاص القضائي والتعاون الدولي:**

الجرائم الرقمية غالبا ما تكون عابرة للحدود، إذ قد يكون الجاني في بلد والمجني عليه في آخر، مما يؤدي إلى مشكلات في تحديد الاختصاص القضائي.

- اتفاقية بودابست (2001) تشكل إطارا دوليا مهما، لكنها لا تشمل دولًا عربية كثيرة، ما يضعف التنسيق القضائي الدولي.

- غياب آليات فعالة للتعاون الفوري بين الجهات القضائية، خصوصا في القضايا العاجلة[1].

2- التحديات التقنية والإجرائية أمام الأجهزة الأمنية والقضائية:

تعد الأجهزة الأمنية والقضائية الطرف المباشر في التعامل مع الجرائم الرقمية من لحظة وقوعها وحتى إصدار الحكم. غير أن هذه الأجهزة تواجه صعوبات عملية متزايدة بسبب الطبيعة الخاصة لتلك الجرائم،[2] وهو ما يبرز من خلال التحديات التالية:

- صعوبة تتبع الجناة وإثبات الهوية الرقمية:

الفاعل الرقمي لا يترك آثارا مادية يمكن تتبعها كالجاني التقليدي، بل غالبا ما يخفي هويته باستخدام أدوات مثل:

- ✓ برامج تغيير العناوين(VPN) .
- ✓ تقنيات التخفي عبر "الدارك ويب".
- ✓ استخدام خوادم وسيطة(Proxies)
- ✓ حسابات وهمية بأسماء غير حقيقية.

- ضعف الكفاءة التقنية للضبطية القضائية وأجهزة التحقيق:

غالبا ما تفتقر الأجهزة الأمنية إلى التكوين التقني الكافي لفهم طبيعة الجريمة الرقمية،[3] وهو ما يؤدي إلى:

- ✓ إغفال بعض الأدلة الرقمية خلال التحريات.

[1] اتفاقية بودابست بشأن الجريمة السيبرانية، مجلس أوروبا، 2001.
[2] عبد الحكيم الحناوي، الأمن السيبراني والجرائم المعلوماتية، منشورات الحلبي الحقوقية، بيروت، 2021، ص. 88.
[3] محمد فرحات، "التحقيق الجنائي في الجرائم المعلوماتية"، المجلة الجزائرية للقانون والاقتصاد، عدد 18، 2022، ص. 112.

- ✓ سوء توثيق البيانات الرقمية بطريقة غير مقبولة قضائيا.
- ✓ ضعف محاضر التحري وغياب المصطلحات الفنية الدقيقة.

- قابلية الأدلة الرقمية للتلف والتعديل:

الأدلة في الجرائم الرقمية غالبًا ما تكون إلكترونية (بريد إلكتروني، سجلات دخول، بيانات موقع، رسائل دردشة... إلخ)،[1] وهي:

- ✓ سهلة الحذف أو التلاعب.
- ✓ تحتاج إلى توثيق سريع لحفظها.
- ✓ تتطلب أدوات وتقنيات محددة لاستخراجها دون الإضرار بها.

- ضعف البنية التحتية والتنسيق بين المؤسسات:

لا تزال البنية التحتية للأمن السيبراني في العديد من الدول العربية ضعيفة،[2] ما يتجلى في:

- ✓ غياب قواعد بيانات مركزية مشتركة.
- ✓ تأخر الرد على طلبات التعاون الداخلي أو الدولي.
- ✓ تداخل الاختصاصات بين الجهات الأمنية، مما يُحدث تضاربًا في الإجراءات.

المطلب الثاني: الآليات الدولية والوطنية ودورها لضمان الأمن المعلوماتي

يشكل الأمن المعلوماتي أحد أهم التحديات في العصر الرقمي، مما يستدعي تضافر الجهود على المستويين الدولي والوطني. وتُعتمد آليات متعددة لضمان هذا الأمن، تشمل الأطر القانونية، والتدابير التقنية، والتعاون بين الدول والمؤسسات.

الفرع الأول: الآليات الدولية والوطنية لضمان وتعزيز الأمن المعلوماتي

في ظل التزايد المستمر للتهديدات السيبرانية، أصبح ضمان وتعزيز الأمن المعلوماتي ضرورة حيوية لحماية الأفراد والدول، وتتمثل الآليات المعتمدة في هذا المجال في جهود وطنية تشريعية وتقنية، إلى جانب تعاون دولي يهدف إلى وضع معايير موحّدة وتبادل الخبرات.

[1] جابر، هدى، "تحديات الإثبات في الجرائم الإلكترونية"، مجلة العلوم القانونية والسياسية، جامعة باتنة، عدد 15، 2021، ص. 97.
[2] المنتدى الاقتصادي العالمي، تقرير الجريمة الإلكترونية العالمية، 2023، ص. 26.

أولا- الآليات القانونية:

تتعدد ضمانات تعزيز الأمن المعلوماتي على المستوى الدولي الإقليمي والوطني، وهذا راجع للتهديدات المعلوماتية التي لم تستثن أية دولة، لذلك لبذل الجهود سواء من طرف المنظمات الدولية، الإقليمية والدولة في إطار سيادتها على إقليمها للتصدي للتهديدات التي تعتبر تعدي على خصوصية الإنسان وانتهاك حقه في سرية معلوماته.

1- على المستوى الدولي:

من بين الجهود الدولية التي تم اعتمادها من أجل دعم المنظومة القانونية لدرك مخاطر الجرائم الالكترونية على سبيل المثال:

- منظمة الأمم المتحدة (United Nations):

تبنت الأمم المتحدة منذ عام 1989 أدلة ومبادئ تتعلق باستخدام الحاسبات وحماية البيانات الشخصية، إلا أن هذه المبادئ كانت غير ملزمة للدول، مما قلل من فعاليتها. واصلت المنظمة جهودها من خلال مؤتمرات دولية، مثل مؤتمر البرازيل 2010 وقطر 2015، حيث دعت لتعزيز التعاون لمواجهة الجريمة المعلوماتية،[1] كما أصدرت قرارات عديدة، أبرزها القرار 57/239 و58/199، لتشجيع ثقافة عالمية للأمن المعلوماتي. وتضمنت الجهود أيضاً قرارات لمكافحة إساءة استخدام الإنترنت في الجرائم، خاصة المتعلقة بالمخدرات، مع التركيز على تدريب الكوادر القانونية. تؤكد هذه المبادرات حرص الأمم المتحدة على تعزيز التعاون الدولي ورفع الوعي العالمي بالأمن السيبراني.[2]

- الاتحاد الدولي للاتصالات (The International Telecommunication) (Union):

يسعى إلى تنظيم الاتصالات الدولية من خلال المعاهدات والأنظمة الملزمة و المعايير غير الملزمة، فاللوائح تمنع التدخل في خدمات الاتصالات للدول الأخرى ولكنها ترخص السيطرة على الاتصالات الدواعي أمنية،[3] فرغم الجهود التي يبذلها الاتحاد الدولي للاتصالات إلا أن بعض الأنظمة غير الملزمة تعتبر عائقا أمام فعالية دور الاتحاد في تعزيز الأمن المعلوماتي، هذا فضلا عن التذرع بالدواعي الأمنية واستغلال التحديات الأمنية للتنصت على الدول شعوباً وحكومات للتجسس عليها، فحتى

[1] مدير محمد الجنبيهي ممدوح محمد الجنبيهي، أمن المعلومات الالكترونية الإسكندرية دار الفكر 73 الجامعي، 2006، ص 73.

[2] فاروق خلف، الآليات القانونية لمكافحة الجريمة المعلوماتية، ورقة بحث مقدمة في الملتقى الوطني - الجريمة المعلوماتية بين الوقاية والمكافحة، جامعة محمد خيضر، بسكرة، 2015 ص 5.

[3]Report Catherine A. Theohary, John W. Rollins. Cyberwarfare and Cyberterrorism: In Brief, [N.P], Congressional Research Service, March 27, 2015. p A.

قادة الدول الكبرى تعرضوا للتنصت على مكالماتهم الهاتفية مثل: الرئيس الأمريكي (باراك أوباما) (Barack Obama) والمستشارة الألمانية أنجيلا ميركل) (Angela Merkel).

- حلف شمال الأطلسي (الناتو) (North Atlantic Treaty Organisation):

تم اتخاذ تدابير لمواجهة الهجمات الإلكترونية عبر تعزيز سياسة الدفاع السيبراني، حيث اعتمد حلف الناتو عام 2008 سياسة رسمية تؤكد على تقديم المساعدة عند الطلب والتعاون القائم على الثقة، مع مراعاة حساسية المعلومات. كما اعتُبرت التهديدات الإلكترونية سببًا محتملاً لتفعيل الدفاع المشترك بموجب المادة 5 من ميثاق الناتو، مما يعكس تصاعد هذه التهديدات وعجز الدول منفردة عن التصدي لها. ومن هنا برزت الحاجة إلى التعاون الدولي. ورغم اهتمام المنظمات الدولية بالأمن المعلوماتي، تظل الجهود غير ملزمة، مما يحد من فعاليتها على أرض الواقع.،[1] لكن ينقص هذه الجهود الدولية طابع الإلزامية لكي تتجسد هذه الجهود على أرض الواقع، وهذا راجع إلى:

أ - التفاوت الموجود بين الدول المتقدمة والدول النامية والدول المتخلفة، فهناكدول متطورة تقنيا تكنولوجيا ومعلوماتيا عكس دول أخرى.

ب - المنافسة وتضارب المصالح بين الدول فالدول اليوم تشهد نوع جديد من الحروب التي تتمثل في الحروب الالكترونية؛ لذلك ليس من مصلحة بعض الدول تعزيز المنظومة القانونية المتعلقة بالأمن المعلوماتي : كونها هي من تشن الهجومات الالكترونية على الدول التي تتعارض مع مصالحها.

2- على المستوى الإقليمي:

تم إبرام اتفاقية بودابست سنة 2001 من قبل مجلس أوروبا، وتُعد أول معاهدة دولية تهدف إلى توحيد قوانين الدول بشأن الجرائم الإلكترونية. تلزم الاتفاقية الدول الموقعة بسنّ تشريعات جنائية ضد أنواع محددة من الجرائم في الفضاء الإلكتروني، وتتميز بإمكانية انضمام دول غير أوروبية، كما فعلت الولايات المتحدة. وتُعد هذه الاتفاقية من أبرز المبادرات الداعمة للأمن المعلوماتي، نظرًا لطابعها الإلزامي الذي يسهم في توحيد الجهود الدولية لمكافحة الجريمة السيبرانية.،[2] فهي تعتبر من أهم الاتفاقيات الداعمة للأمن المعلوماتي، وتستمد أهميتها من الطابع الإلزامي لها من خلال توحيد القوانين المتعلقة بالجرائم الالكترونية بين الدول الموقعة عليها.

[1] مجلة الناتو، « التهديدات الجديدة الأبعاد الالكترونية، docu/int.nato.www//http: htm.ex-ind/AR/Threads Cyber/September/11/2006/review
بتاريخ: 2025/05/11، على الساعة: 20:10د.

[2] Report Catherine A. Theohary, John W. Rollins, Op.cit. p 7.

3- على المستوى الوطني على ضوء التشريع الجزائري:

التكييف المنظومة القانونية مع المتغيرات الراهنة لم يغفل المشرع الجزائري أهمية تعزيز الأمن المعلوماتي بتعديل قانون العقوبات، و من بعض التشريعات الأخرى. ويتمثل أهمها في:

- قانون رقم 04 - 15 المتعلق بقانون العقوبات:

نص المشرع في المادة 394 مكرر على معاقبة كل من يدخل أو يحاول الدخول إلى منظومة معلوماتية عن طريق الغش، حتى دون تعديل أو حذف للبيانات، تأكيدًا على حماية سرية وسلامة وإتاحة المعلومة. كما شدد على أن مجرد محاولة الاختراق تُعد جريمة، وتضاعف العقوبة، حسب المادة 394 مكرر 3، إذا استُهدفت مؤسسات الدفاع الوطني أو المؤسسات العامة نظرًا لحساسية بياناتها. كما نص في المادة 394 مكرر 6 على غلق المواقع التي تُستخدم لارتكاب جرائم إلكترونية، مما يعكس حرص المشرع على حماية الأمن المعلوماتي للدولة.

- قانون رقم 09 -04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها:

لقد تطرق للحالات التي تسمح بمراقبة الاتصالات الالكترونية للوقاية من الجرائم التي تمس أمن الدولة كالإرهاب أو الاقتصاد الوطني أو لصعوبة الوصول إلى الحقيقة في التحقيقات القضائية، وفي إطار تنفيذ طلب المساعدة القضائية الدولية، هذا وقد وضح إجراءات تفتيش وحجز المعطيات المعلوماتية في الفصل الثالث من القانون،[1] فالقانون رقم 09-04 يعتبر من القوانين التي فصلت كثيرا في كيفية التصدي للجرائم الالكترونية من خلال توضيح حالات مراقبة الاتصالات الالكترونية، والقواعد الإجرائية لتفتيش المنظومات المعلوماتية، و في التزام مقدمي الخدمات تقديم المساعدة للسلطات إذا اقتضت الضرورة ذلك.[2]

- قانون رقم 15-03 المتعلق بعصرنة العدالة:

إذ أكد المشرع في الفصل الخامس في المادة 17 على أنه: "يعاقب بالحبس من سنة (1) إلى خمس (5) سنوات و بغرامة تتراوح بين 100000 دج إلى 500000 دج كل شخص يستعمل بطريقة

[1] الجمهورية الجزائرية الديمقراطية الشعبية. "قانون رقم 09 - 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الجريدة الرسمية العدد 47، الصادرة بتاريخ 2009/08/16، ص6، 7.
[2] المرجع نفسه، ص 8.

غير قانونية العناصر الشخصية المتصلة بإنشاء توقيع الكتروني يتعلق بتوقيع شخص آخر"،[1] نظرا لسماح المشرع إمكانية إرسال الوثائق والإجراءات القضائية الكترونيا إذا استلزم الأمر ذلك، وسعي الجزائر نحو الإدارة الالكترونية لتلبية حاجات المواطنين في أسرع وقت، هذا ما دفع المشرع الجزائري لعدم إهمال عقوبة الاستعمال غير القانوني للتوقيع الالكتروني.

ثانيا- الآليات المؤسساتية:

لتعزيز آليات حق الإنسان في الأمن المعلوماتي لا بد من تأسيس مجموعة من الهيئات الداعمة لتطبيق النصوص التشريعية المتعلقة بحماية الأمن المعلوماتي لا يقتصر نشاطها على المستوى الوطني بل يتعداه إلى المستوى الدولي في إطار التعاون الدولي والتنسيق في هذا المجال، ويمكن إبراز أهم هذه المؤسسات في:

1- الآليات المؤسساتية الدولية لتعزيز الأمن المعلوماتي:

سارعت المنظمات الدولية، خاصة المعنية بمكافحة الجريمة المنظمة والإرهاب، إلى إنشاء هيئات متخصصة في الوقاية من الجرائم الإلكترونية. ويُعد الإنتربول من أبرز هذه الهيئات، نظرًا للطابع العابر للحدود لهذه الجرائم، حيث يلعب دورًا مهمًا في الدعم العملياتي والتحقيقات والابتكار والتدريب. وفي هذا الإطار، أنشأ الإنتربول "المجمع العالمي للابتكار" (IGCI) بسنغافورة سنة 2014 لتعزيز البحث والخبرة العالمية في هذا المجال. ويبرز من ذلك أهمية التعاون الدولي، نظراً لعدم قدرة الدول منفردة على مواجهة الجريمة الإلكترونية بشكل فعّال،[2]نظرا لكون الدولة بمفردها لا تستطيع القضاء على الجرائم الالكترونية فالحاجة ملحة كي يكون هناك تعاون دولي يتفق مع طبيعة هذا النوع من الجرائم التي تتميز مكافحتها بسرعة إجراءات التحقيق والتنسيق الجيد بين أجهزة الشرطة للعديد من الدول.

2- الآليات المؤسساتية الإقليمية لتعزيز الأمن المعلوماتي:

من أهمها وكالة تطبيق القانون الأوروبية المتخصصة في مكافحة الجريمة و الإرهاب في دول الاتحاد الأوروبي (أوروبول) (Europol)، حيث أعلنت في 2014/09/01 عن إنشاء قوة خاصة لمحاربة الجرائم المعلوماتية في دول الاتحاد الأوروبي و خارجه لتنضم دول أخرى إليها مثل كندا،

[1] الجمهورية الجزائرية الديمقراطية الشعبية " قانون رقم 15.03 يتعلق بعصرنة العدالة". الجريدة الرسمية العدد 06. الصادرة بتاريخ : 2015/02/10، ص6.

[2]International Criminal Police Organization, «Cybercrime », from: https://www.interpol.int/ar/Crime-areas/Cybercrime/Cybercrime, on: 09-02-2017.

استراليا والولايات المتحدة الأمريكية، وظيفتها التنسيق مع التحقيقات الدولية لمواجهة التهديدات الالكترونية التي تستهدف خاصة القطاع المالي ومكافحة المواقع الالكترونية التي تبيع الممنوعات،[1] وإن كانت صعوبة الإثبات بالأدلة الالكترونية - لتلك الجرائم - أهم تحد يواجه مهام هذه الأجهزة.

3- الآليات المؤسساتية الوطنية لتعزيز الأمن المعلوماتي:

إن تنامي تهديد الأمن القومي - لجميع الدول من طرف الحروب الالكترونية وما خلفته من الجرائم الالكترونية - جعل من الدول - على غرار الجزائر - حريصة على أمنها المعلوماتي بإنشاء هيئات هدفها الرئيسي ضمان أمنها المعلوماتي والوقاية من مختلف الجرائم الالكترونية.

والجزائر كغيرها من الدول سعت هي الأخرى لدعم الأمن المعلوماتي مؤسساتيا حيث يوجد:

3- على المستوى المركزي:

يوجد المعهد الوطني للأدلة الجنائية وعلم الإجرام الذي تم إنشاؤه بمرسوم رئاسي رقم 183-04 المؤرخ في 26 جوان 2004 والمكلف بالقيام بالخبرات التطبيقية المدعومة بالتكنولوجيا المناسبة بطلب من القضاة لتحديد هويات مرتكبي الجنايات والجنح خدمة للعدالة، والمشاركة بأبحاث للتقليل من جميع أشكال الإجرام،[2] كما يوجد مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني، والمصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني.

4- على المستوى المحلي:

لمكافحة الجريمة الإلكترونية محليًا، أنشأت المديرية العامة للأمن الوطني مخابر للشرطة العلمية عام 2007 في الجزائر العاصمة ووهران وقسنطينة، بهدف تتبع الأدلة الرقمية ودعم العدالة. كما تم استحداث خلايا لمكافحة الجرائم الإلكترونية سنة 2010، بدأ عددها بـ23 خلية قبل تعميمها على مستوى جميع الولايات. تضم هذه الخلايا عناصر مختارة وفق مؤهلات علمية وخبرة في الشرطة القضائية، ويتم تأهيلهم بدورات تكوينية متخصصة. ومع ذلك، يُشدد على ضرورة تنظيم دورات تدريبية دورية لتحديث مهاراتهم، نظراً للتطور السريع لأساليب الجرائم الإلكترونية.[3]

---

[1] فاروق خلف، مرجع سابق، ص 6.

[2] الدرك الوطني "المعهد الوطني للأدلة الجنائية وعلم الإجرام"، متحصل عليه من : http://www.mdn.dz/site_cgn/index.php?L=ar#undefined ، بتاريخ: 2025/05/11 على الساعة : 20:40د.

[3] عبد الرحمان حملاوي، "دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية ورقة بحث مقدمة في الملتقى الوطني الجريمة المعلوماتية بين الوقاية والمكافحة ، جامعة محمد خيضر، بسكرة 2015، ص8، 9.

ثالثا- الآليات الإجرائية:

يكشف الواقع حجم المخاطر والخسائر التي تترتب عن الحروب والجرائم الالكترونية، الأمر الذي يفرض على الأفراد المنظمات المختلفة، والدول الإسراع في تبني مجموعة من الإجراءات للمواجهة والوقاية من آثارها، وعلى العموم تنقسم هذه الإجراءات إلى:

1-الآليات التقنية هي عديدة، من أهمها:[1] توفير مصدر احتياطي للطاقة الكهربائية لضمان استمرار عمل مراكز الحاسب الآلي ينبغي التزويد المستمر لمراكز الحاسب الآلي بمصدر آخر للطاقة الكهربائية، ويستخدم لذلك مزود الكهرباء المستمر (UPS).

- استخدام وسائل التحقق من شخصية المستخدم عن طريق تعريف المستخدم بنفسه للنظام المعلوماتي من خلال إدخال الرقم السري الخاص به إلى النظام، أو إدخال بطاقة ممغنطة مخصص لها مكان في الحاسب الآلي، وجهاز الكشف عن بصمة الأصبع وكف اليد، ملامح الوجه والعينين.

- توظيف جدران الحماية: وهي عبارة عن أجهزة وبرامج تعمل على تصفية البيانات بين الشبكة الداخلية والشبكة الخارجية لحماية الأنظمة المعلوماتية الداخلية المتعلقة بالمنظمات والأفراد عبر التحقق من صلاحية المستخدم التشفير، وبرامج الحماية من الفيروسات.

- برامج مكافحة الفيروسات: تعتبر من أهم وسائل حماية أجهزة الحاسب الآلي بالبحث عن الفيروسات المعروفة وغير المعروفة التي تهدد أجهزة الحاسب الآلي والبرامج لاكتشافها قبل حدوث الأضرار، ومن ثم القضاء عليها.

نظرا لتزايد الاعتماد على البريد الالكتروني تزيد معه فرصة اختراق أمنه وسرية معلوماته، وعن البرامج التي توفر الحماية للبريد الالكتروني برنامج يوجد برنامج PGP Pretty Good Privacy، حيث يعمل على توفير خدمات الخصوصية، التحقق، تخزين الملفات باستخدام أفضل خوارزميات التشفير، ومن جانب آخر يمتاز بعدم سيطرة أية شركة حكومية عليه وإمكانية استخدامه من قبل الشركات والأفراد معا لضمان الاتصال مع الآخر بطريقة آمنة.[2]

2-الآليات التكوينية:

تحرص المديرية العامة للأمن الوطني في الجزائر على التكوين الجيد للعنصر البشري، فقد سطرت برنامجاً تكوينياً للإطارات والرتباء والأعوان، فمنذ سنة 2003 م إلى غاية 2010 م كانت

[1] منصور بن سعيد القحطاني، مرجع سابق، ص 48-59.
[2] خضر مصباح إسماعيل الطيطي، مرجع سابق ، ص 379، 380.

هناك 6 دورات تكوينية بالداخل بمشاركة خبراء أجانب ليتم تكوين 128 ضابطا و 4 دورات بخارج الجزائر استفاد منها 9 ضباط، ودورة واحدة وطنية بمشاركة كفاءات وطنية لتكوين 39 ضابطا،[1] في حين برز تشجيع للأفراد الذين يمتلكون مهارات ومواهب في العمل الالكتروني،[2] لأنه من متطلبات الحماية الالكترونية وجود عنصر بشري كفء له القدرة العالية على المناورة، يتميز بالذكاء وسرعة البديهة.

ثالثا- الآليات البحثية التوعوية:

حيث تبرمج المديرية العامة للأمن الوطني من أجل توعية المواطن بمخاطر الجرائم الالكترونية أيام دراسية لمختلف الأطوار الدراسية، والمشاركة في الملتقيات أو الندوات والمؤتمرات ذات الصلة بالأمن المعلوماتي والجريمة الالكترونية،[3] لذلك لا بد من توعية المواطن لماهية هذه الجرائم، والحروب الالكترونية وأسلحتها ومخاطرها، وعليه يتوجب أن تتضافر جهود العديد من المؤسسات للقيام بالدور التوعوي والبحثي منها الأسرة، المدرسة الجامعة منظمات المجتمع المدني ووسائل الإعلام.

رابعا- آليات حماية الخصوصية الرقمية في التشريع الجزائري:

أدت المعاملات الإلكترونية عبر وسائل الاتصال الحديثة كالحاسوب والهاتف إلى بروز تحديات ومخاطر تهدد المستخدمين، سواء كانوا أفرادًا أو مؤسسات. من أبرز هذه المخاطر انتهاك خصوصية البيانات الشخصية أو المالية، وجمع المعلومات من المكالمات أو الرسائل أو المواقع التي تمت زيارتها. تُرسل هذه البيانات إلى خوادم مثل "فرفاتا" وتُتاح عبر مواقع خاصة. كما تشمل التهديدات تزوير بطاقات الائتمان، اختراق البريد الإلكتروني، انتحال الهوية، والابتزاز والقرصنة، ما يعكس الحاجة لحماية أمن المستخدمين الإلكتروني بشكل صارم.[4]

الفرع الثاني: حماية الخصوصية الرقمية القانونية

- حماية الخصوصية الرقمية من خلال بعض التعديلات في القوانين العامة:

تطرق المشرع الجزائري لحماية الخصوصية بصورة ضمنية في إطار القواعد العامة المتعلقة بحماية الحياة الخاصة في صورتها التقليدية، كما أن انتشار التكنولوجية في عدة مجالات، ومنها مجال

[1] عبد الرحمان حملاوي، مرجع سابق، ص 7.
[2] عبد الكريم صالح المحسن، الاختراقات الالكترونية... قوة سياسية تتناسب مع الحروب الجديدة، متحصل عليه من: http://all4syria.info/Archive/237537، بتاريخ: 2025/05/11، على الساعة: 22:39د.
[3] عبد الرحمان حملاوي، مرجع سابق، ص 9.
[4] صغير يوسف، الجريمة المرتكبة عبر الانترنيت مذكرة ماجستير في القانون الدولي للأعمال، جامعة مولود معمري تيزي وزو، 2013/2014.

الخصوصية المعلوماتية، وفر للمشرع حماية أخرى عند المعالجة الآلية لكل البيانات المتعلقة بهذه الخصوصية مهما كان مجال استخدامها.[1]

- حماية الخصوصية الرقمية في التعديل الدستوري لسنة 2016:

الحماية القانونية للخصوصية لم تكن مجسدة في دستور 1996 بصورتها الحالية، بل وردت بصورة ضمنية في المادة 39، منه التي تنص في مضمونها على حماية الحقوق الأساسية للإنسان وعلى الحريات الفردية والجماعية.

- حماية الخصوصية الرقمية من خلال تعديل قانون العقوبات بقانون رقم 24-06:

تنبه المشرع الجزائري للأخطار والعقبات التي يمكن أن تنجم عن الجرائم الالكترونية أو المعلوماتية في مجال المعاملات الالكترونية المختلفة أين يتم الكشف عن الخصوصية الرقمية متعلقة بمعلومات خاصة به، أو معلومات أخرى متعلقة بتجارته أو أمواله، وذلك بإدراج القسم السابع مكرر الموسوم بـ: المساس بأنظمة المعالجة الآلية للمعطيات وتنص على هذه الجريمة.

- الحماية من خلال بعض القوانين المستحدثة في مجال البيانات الشخصية:

تمكن المشرع الجزائري من إصدار قوانين مستحدثة بهدف تخصيص حماية أكبر للخصوصية الرقمية، فبعدما بدأ هذا الأخير بتعديل الهرم التشريعي، فاستحدث قوانين عدة منها قانون رقم 09-04، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، وقانون رقم 15-12، المتعلق بحماية الطفل، وقانون رقم 18 05 المتعلق بالتجارة الإلكترونية، قانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعية في مجال معالجة المعطيات ذات الطابع الشخصي.[2]

- حماية الخصوصية الرقمية من خلال قانون رقم 09-04:

لقد أولى المشرع اهتماما للبيانات الشخصية عن طريق استحداث قانون رقم 09-04، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، وهنا يلتزم مقدم الخدمة بحفظ المعطيات المتعلقة بالخصوصية فوردت على سبيل الحصر في المادة 11 من هذا القانون، وذلك لمدة سنة واحدة، ومع ذلك فكل المتعاملين بالحواسب أو الهاتف النقالة أو غيرها من وسائل الاتصال الرقمية يخضع للعقوبات الجزائية عند جمع هذه البيانات عن الأشخاص لأكثر من سنة.

[1] عبد الرحمان حملاوي، مرجع سابق، ص11.
[2] المرجع نفسه، ص12.

- حماية الخصوصية الرقمية من خلال قانون رقم 15-12:

نظم المشرع الجزائري قانون رقم 15-12، في مجال حماية الحق في الخصوصية المتعلقة بالأطفال ضد حماية جرائم استغلال أو انتهاك حياة الأطفال الخاصة بواسطة نشر أو بث صور أو بيانات عبر كل وسائل الاتصال، بحيث يكون الطفل هدفا سهلا للمخترقين أو المنحرفين نظرا لسهولة تحديد موقعهم الجغرافي واستدراجهم نحو المجهول.[1]

- حماية الخصوصية الرقمية من خلال قانون رقم 18-05:

تتسم الحماية القانونية التي خصها المشرع الجزائري في المادة 26 من قانون رقم 18-05، المتعلق بالتجارة الإلكترونية بكونها حماية وقائية أكثر من جزائية، وبالتالي فهذا القانون لم ينظم ولا عقوبة جزائية ذات صلة بالبيانات الشخصية للأفراد، أي المتعلقة بخصوصية هؤلاء، فيعاب المشرع على هذا الإغفال القانوني الوارد في هذا المجال ، فانه بات من الضروري والحتمي عليه تضمين هذا القانون بمواد تحمي خصوصية المتعاملين عبر الانترنت من العبث بها على أوجه غير مشروعة.[2]

- حماية الخصوصية الرقمية من خلال قانون 18-07:

أما بالنسبة لقانون رقم 18-07، يمكن القول أنه استدراك للإغفال الذي وقع فيه المشرع في قانون رقم 18-05، ومن ضمن هذا القانون 76 مادة موزعة على سبعة أبواب تضمنت ونظمت حماية الحياة الخاصة للأشخاص وأسرهم في مجال معالجة المعطيات ذات الطابع الشخصي، ولعل من أبرز هذه المواد التي وضعها بخصوص هذه الحماية، فنجد المادة 02، من هذا القانون التي تنص في مضمونها على ضرورة أن تتم معالجة المعطيات ذات الطابع الشخصي مهما كان مصدرها أو شكلها، في إطار احترام الكرامة الإنسانية والحياة الخاصة والحريات العامة وألا يمس بحقوق الأفراد وشرفهم وسمعتهم.[3]

[1] عبد الرحمان حملاوي، مرجع سابق، ص12،13.
[2] المرجع نفسه، 13-14.
[3] المرجع نفسه، ص15.

أضحى موضوع الحياة الخاصة في ظل الأمن المعلوماتي من القضايا الجوهرية في خضم التحولات الرقمية المتسارعة وما آلت إليه من تطورات في مجال تكنولوجيا المعلومات والاتصالات، فيعتبر هذا الموضوع أحد أبرز التحديات القانونية والإنسانية في العصر الحديث. حيث أصبحت البيانات الشخصية عرضة للاستغلال، والخصوصية مهددة نتيجة الاستخدام غير المشروع أو غير المنظم للتقنيات الرقمية.

وعليه تبين من خلال هذا الفصل أن ضمان حماية الحياة الخاصة يتطلب تبني مبادئ واضحة تحكم جمع ومعالجة البيانات، إلى جانب ضرورة وجود إطار قانوني فعّال على الصعيدين الوطني والدولي. كما أن التوازن بين حماية الأمن المعلوماتي واحترام الحقوق الفردية لا يمكن تحقيقه إلا من خلال تشريعات دقيقة، وآليات رقابة فعّالة، وتعاون دولي مستمر، حيث تبقى حماية الحياة الخاصة ركيزة أساسية في بناء ثقة الأفراد في البيئة الرقمية، وضمان استخدام آمن للتكنولوجيا، بما يحمي كرامة الإنسان ويصون حرياته في ظل عالم مترابط ومعقد.

خـــاتمـــة

خاتمة:

لقد تبيّن من خلال هذا البحث أن الأمن المعلوماتي لم يعد مجرد آلية تقنية لحماية نظم المعلومات، بل أصبح عنصرًا حيويًا لحماية الحقوق الأساسية،وعلى رأسها الحق في الخصوصية. وقد أظهرت الدراسة أن حماية الحياة الخاصة في البيئة الرقمية لا يمكن أن تُفهم أو تُعزز بمعزل عن الإطار التقني،القانوني، والسياسي الذي يحكم الفضاء الرقمي. فمع تزايد الاعتماد على التكنولوجيا وتراكم البيانات الشخصية، تصاعدت التهديدات التي تستهدف الأفراد والدول، مما جعل من الأمن المعلوماتي ضرورة إستراتيجية لا تحتمل التأجيل.

كشفت المعالجة النظرية أن العلاقة بين الأمن المعلوماتي والأمن السيبراني علاقة تكاملية، حيث يوفر كل منهما بُعدًا مكمّلاً في منظومة الحماية الشاملة، كما أن دراسة الأطر التشريعية، سواء على المستوى الدولي أوالعربي، أظهرت وجود تفاوت كبير في نجاعة النصوص القانونية وتطبيقها، حيث

تعاني العديد من الدول العربية من فجوات قانونية، غياب التخصص القضائي،وضعف في ثقافة الأمن الرقمي على المستوى المجتمعي والمؤسساتي.

وقد أكدت النتائج أن الحماية الفعالة للحياة الخاصة في البيئة الرقمية تتطلب تكاملًا بين الآليات التقنية، كالتشفير وإدارة الوصول والذكاء الاصطناعي، والسياسات القانونية، مثل قوانين حماية البيانات والتزامات المسؤولين عن معالجتها. كما أن التحديات لا تقتصر على الإمكانيات التقنية والتشريعية، بل تمتد إلى الإشكاليات المرتبطة بالسيادة الرقمية، والرقابة العابرة للحدود، والمصالح الاقتصادية الكبرى للشركات التقنية العالمية.

وانطلاقا من التحليل، يُقترح ما يلي:

- ضرورة تحديث التشريعات العربية لتتوافق مع المعايير الدولية، مثل اللائحة العامة لحماية البيانات في الاتحاد الأوروبي (GDPR).

- إنشاء هيئات مستقلة لحماية البيانات الشخصية تتمتع بصلاحيات رقابية وتنفيذية حقيقية.

- دمج الثقافة الرقمية في المناهج التعليمية وبرامج التكوين المهني، بهدف رفع وعي المستخدمين بحقوقهم الرقمية.

- تعزيز التعاون الإقليمي العربي في مجال الأمن السيبراني وتبادل الخبرات والممارسات الفضلى.

- إن الرهانات المستقبلية المرتبطة بالذكاء الاصطناعي، وتحليل البيانات الضخمة، وتكنولوجيا التعرّف الحيوي، تفرض مراجعة مستمرة للمفاهيم القانونية، وتطوير آليات الحماية بما يواكب المتغيرات المتسارعة.

- فالخصوصية أصبحت حجر الزاوية في بناء الثقة في البيئة الرقمية، ومن دون حمايتها سيفقد الأفراد سيطرتهم على هوياتهم الرقمية.

وفي الختام، يمكن القول إن حماية الحياة الخاصة لم تعد ترفًا قانونيًا أو أخلاقيا، بل أصبحت أحد مقومات الأمن القومي والكرامة الإنسانية في العصر الرقمي، وإن إرساء توازن فعلي بين متطلبات الأمن وحماية الحقوق يستوجب إرادة سياسية، ووعيًا مجتمعيًا، وابتكارًا تشريعيًا يضع الإنسان في صلب التحول الرقمي.

قائمة المراجع

❖ **قائمة المراجع:**

❖ **الكتب:**

1- إبراهيم أحمد الصعيدي : نظام التشغيل الإلكتروني للبيانات، مطبعة المعرفة، 1981.

2- أيمن إبراهيم العشماوي، المسئولية المدنية عن المعلومات دار النهضة العربية، القاهرة، 2004.

3- جمال مصالح عبد الحليم، الحماية الجنائية للحق في الخصوصية في مواجهة نظم المعلومات دار النهضة العربية 2016، مصر.

4- الجواد دلال، صادق أمن المعلومات دار البازوري العلمية للنشر والتوزيع 2000، عمان.

5- حرام فتيحة، نقلا عن عبد الفتاح بيوم الحجازي، النظام الحماية التجارة الالكترونية، الكتاب الأول، دون طبعة. دار الفكر الجامعي، 2002، مصر.

6- حسن شوقي، "الأمن المعلوماتي في عصر العولمة"، دار الفكر العربي، 2018.

7- حسن عبد الله حسن، "مقدمة في الأمن السيبراني"، دار النشر للجامعات، 2021.

8- خالد ممدوح إبراهيم، الجرائم المعلوماتية، الإسكندرية، دار الفكر الجامعي، الطبعة الأولى، 2019.

9- خالد ممدوح إبراهيم، أمن المعلومات الإلكترونية، الدار الجامعية، الإسكندرية، 2008.

10- سامي عبد العزيز، "أمن المعلومات: المبادئ والمفاهيم"، دار الصفاء للنشر والتوزيع، 2019.

11- سعيد الحربي، "إدارة أمن المعلومات: نظرة شاملة"، مركز دراسات الشرق الأوسط، 2019.

12- سيفون باية، الأنترنت والصحافة الإلكترونية، دراسة في طبيعة العلاقة والتأثير، ط1، الجزائر، دار الخلدونية، 2016.

13- الشاعر عبد الرحمان بن ابراهيم، مواقع التواصل الاجتماعي والسلوك الإنساني، دار صفاء للنشر والتوزيع، عمان الأردن، 2015.

14- الشوابكة محمد أمين، جرائم الحاسوب والانترنت الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2007.

15- عبد الرحمان شعبان عطيات، أمن الوثائق والمعلومات، ط1، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004.

16- عبد الرشيد مأمون ومحمد سامي عبد الصادق حقوق المؤلف والحقوق المجاورة في ضوء قانون حماية حقوق الملكية الفكرية الجديد رقم 82 لسنة 2002، الكتاب الأول، دار النهضة العربية، القاهرة، 2004.

17- عبد العال، يوسف، الجرائم الإلكترونية في القانون المقارن، دار النهضة العربية، القاهرة، 2020.

18- عبد الله أبو الروس، "تأمين نظم المعلومات"، مكتبة الأنجلو المصرية، 2017.

19- علي بهلوان، استخدام قاعدة البيانات ومنتج التطبيقات، القاهرة، دار الكتب العلمية للنشر والتوزيع، الطبعة الثانية، 2018.

20- علي عبد العزيز، "أساسيات الأمن المعلوماتي"، مكتبة الأنجلو المصرية، 2020.

21- عماد زكي، "أمن المعلومات وأمن الشبكات"، دار الكتب العلمية، 2015.

22- الغثير خالد بن سليمان، أمن المعلومات بلغة مسيرة تقديم محمد بن ابراهيم السويل، مكتبة الملك فهد الوطنية، ط1، الرياض، 2009.

23- القاضي علي كحلون، الجوانب القانونية لقنوات الاتصال الحديثة والتجارة الإلكترونية، دار إسهامات في أدبيات المؤسسة، تونس، 2002.

24- لورنس م أوليفاء، ترجمة محمد مراياتي، أمن تقنية المعلومات نصائح من خبراء المنظمة العربية للترجمة، ب س ن.

25- محمد سامي الشواء ثروة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، 1994.

26- محمد سعيد مرسي، "الأمن السيبراني في المؤسسات الحكومية"، دار الفكر الجامعي، 2021.

27- محمد فتحي، "الإدارة الإلكترونية والأمن المعلوماتي"، دار الفكر الجامعي، 2016.

28- محمد محمود المكاوي، الجوانب الأخلاقية والاجتماعية والمهنية للحماية من الجرائم المعلوماتية (جرائم الكمبيوتر والانترنت)، ط1، المكتبة العصرية للنشر والتوزيع، مصر، 2010.

29- محمود عبد المعطى خيال: التأمين على المعلومات، ط 1999، القاهرة.

30- مختارية بوزيدي، ماهية الجريمة الالكترونية، كتاب أعمال الملتقى الوطني حول آليات مكافحة الجرائم الالكترونية في التشريع الجزائري، 2017.

31- مدير محمد الجنبيهي ممدوح محمد الجنبيهي، أمن المعلومات الالكترونية الإسكندرية، دار الفكر 73 الجامعي، 2006.

32- نادية حسن، "الجرائم المعلوماتية وحماية الخصوصية"، دار الجامعة الجديدة، 2020.

33- يوسف عبد العال، "الجرائم الإلكترونية في القانون المقارن"، دار النهضة العربية، القاهرة، 2020.

❖ **مذكرات ودراسات:**

34- بودابست، اتفاقية مجلس أوروبا حول الجرائم السيبرانية، 2001.

35- الحسين محمد حسام لطفي، عقود خدمات المعلومات، دراسة في القانونين المصري والفرنسي القاهرة، 1994.

36- حكيمة جاب الله انعكاسات الجريمة السيرانية على البيئة الرقمية، دراسة في آليات واستراتيجيات مكافحتها، حوليات جامعة الجزائر 663 الجزائر المجد 35 العدد 03.

37- خليفة التواجد الغير مشروع في أنظمة المعلوماتية، أطروحة دكتوراه، كلية الحقوق جامعة ناجي مختارة عناية الجزائر، 2011.

38- أيمن عبد الله فكري، جرائم نظم المعلومات - دراسة مقارنة - دار الجامعة الجديدة للنشر، الإسكندرية 2007.

39- صغير يوسف الجريمة المرتكبة عبر الانترنيت مذكرة ماجستير في القانون الدولي للأعمال، جامعة مولود معمري تيزي وزو، 2013/2014.

40- طالب أحسن مبارك، جرائم الاحتيال والعوامل الاجتماعية والنفسية المهيئة لها، جامعة نايف العربية للعلوم الأمنية، 2007.

41- عبد الحكيم الحناوي، الأمن السيبراني والجرائم المعلوماتية، منشورات الحلبي الحقوقية، بيروت، 2021.

42- عبد الرحمان حملاوي " دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية ورقة بحث مقدمة في الملتقى الوطني الجريمة المعلوماتية بين الوقاية والمكافحة ، جامعة محمد خيضر، بسكرة 2015.

43- عبد الرحمان شارع العتيبي، دور الأمن السيبراني في تعزيز الأمن الإنساني، مذكرة ماجستير، جامعة نايف المعلوم الأمنية: كلية العلوم الاستراتيجية، قسم الأمن الإنساني، 2015.

22- عبد الفتاح بيومي حجازي مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي: دراسة قانونية متعمقة في القانون المعلوماتي، الإسكندرية، دار الفكر الجامعي، 2020.

45- علاء الدين فرحان من الردعه النووي إلى الردع السيبراني دراسة لمدى تحقيق مبدأ الردع في القضاء السيبراني، الجزائر، جامعة بسكرة مجلة الفكرة المجلد 16، العدد 1، 2021.

46- عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة الكترونيا الدراسة مقارنة، دار النهضة العربية، مصر، 2010.

47- فاروق خلف، الآليات القاونية لمكافحة الجريمة المعلوماتية، ورقة بحث مقدمة في الملتقى الوطني - الجريمة المعلوماتية بين الوقاية والمكافحة، جامعة محمد خيضر، بسكرة، 2015.

48- فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية، رسالة لنيل درجة الدكتوراه في الحقوق جامعة عين شمس، كلية 35 الحقوق، مصر 2012.

49- محمد نصر الله، المسؤولية الجنائية لانتهاك الخصوصية المعلوماتية (دراسة مقارنة)، مركز الدراسات العربية والتوزيع، ط1، مصر، 2016.

50- المويشر، تركي بن عبد الرحمان، بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته، أطروحة دكتوراه في الفلسفة الأمنية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، السعودية، 2009.

51- وليد غسان سعيد جلعود، دور الحرب الإلكترونية في الصراع العربي الكبير، رسالة ماجستير، جامعة النجاح الوطنية، نابلس، 2013.

شفيق نوران، أثر التهديدات الإلكترونية على العلاقات الدولية – دراسة في أبعاد الأمن الالكتروني، ط1، المكتبي العربي للمعارف، القاهرة مصر، 2016

❖ **المواقع الإلكترونية:**

52- اللائحة العامة لحماية البيانات(GDPR) ، الاتحاد الأوروبي، الموقع الرسمي-https://gdpr : info.eu/ gdpr-info.eu، تاريخ الإطلاع: 2025/05/11، على الساعة: 10:30.

53- قانون أساسي عدد 63 لسنة 2004 مؤرخ في 27 يوليو 2004، تونس، الموقع الرسمي : https://legislation-securite.tn/ar/latest-laws/قانون-أساسي-عدد-63-لسنة-2004-مؤرخ-في-27-جويلية-2004/، تاريخ الإطلاع: 2025/05/10، على الساعة: 23:20د.

54- فهد عبد الله العبيد العازمي، مرجع سابق، ص 33، عمر ابوبكر بن يونس، أساسيات المعلومات، مقال منشور على الموقع.www.arablaw.org

55- عبد الكريم صالح المحسن، الاختراقات الالكترونية... قوة سياسية تتناسب مع الحروب الجديدة، متحصل عليه من http://all4syria.info/Archive/237537 ، بتاريخ: 2025/05/11، على الساعة: 22:39د.

56- الدرك الوطني "المعهد الوطني للأدلة الجنائية وعلم الإجرام"، متحصل عليه من : http://www.mdn.dz/cgn_site/index.php?L=ar#undefined، بتاريخ: 2025/05/11 على الساعة : 20:40د.

57- مبادئ الخصوصية لمنظمة التعاون الاقتصادي والتنمية، الموقع الرسمي : https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm، تاريخ الإطلاع: 2025/05/11، على الساعة: 18:00.

58- مجلة الناتو، « التهديدات الجديدة الأبعاد الالكترونية، http://www.nato.int/docu/review/AR/Threads Cyber/September/11/2006/ex-ind-htm.

59- الموقع الرسمي للبرنامج بروتن مايل تم الاطلاع عليه بتاريخ 10/06/2023 على الساعة 00:00 موجودة على الرابط التالي : https://play.google.com/store/apps/details?id=ch protonmalandroid ar&u=US

60- الموقع الرسمي للبرنامج سيدال تم الاطلاع على الموقع بتاريخ 02/06/2023 على الساعة 13:20 موجود على الرابط الثاني : : https//play.google.com/store/apps/details?id=ory thoughtcrime securesms &hl

61- الموقع الرسمي للبرنامج فينغر سيكريتي تم الاطلاع عليه بتاريخ 13/20230 على الساعة 02:05 موجود على الرابط التالي httpsFingersecurity.ar.uptodown.com/android : download

62- الموقع الرسمي للبرنامج ماي دانا ما تاجر تم الاطلاع على الموقع بتاريخ 28/05/2023 على الساعة 22:30 موجود على الرابط التالي : https://play.google.com/store/apps/details?id=com mobilia android.malm&hl=ar&al US.

❖ **المجلات:**

63- تغريدة صفاء، لبنى خميس مهدي، أثر السيبرانية في تطور القوة، مجلة حامور أبي للدراسات، بغداد د، مركز حمورابي للبحوث والدراسات الاستراتيجية، ع33-34، السنة 2020.

64- جابر، هدى، "التكييف القانوني للجرائم الإلكترونية"، مجلة الدراسات القانونية، عدد 12، 2021.

65- جابر، هدى، "تحديات الإثبات في الجرائم الإلكترونية"، مجلة العلوم القانونية والسياسية، جامعة باتنة، عدد 15، 2021.

66- حزام فتيحة حماية الأنظمة الرقمية بين الآليات الثانية وأجهزة الحماية لقراءة في أحكام المرسوم الرئاسي 20-05، مجلة الحقوق والعلوم الإنسانية الجزائر المجلد 13 العدد 03، 2020، ص 175، نقلا عن عبد الله بن عبد الله السند الأحكام الفقهية للتعاملات الالكترونية دار الفكر الجامعي، 2004، مصر.

67- حسين بن سليمان بن راشد الطيار، الأمن السيبراني في منظور مقاصد الشارع: دراسة تأصيلية المملكة العربية السعودية، جامعة الطائف، مجلة جامعة الطائف للعلوم الإنسانية، المجلد 6، العدد 21.

68- خالد منصور الخطيب، "التحديات المعاصرة في الأمن السيبراني"، المجلة الدولية لأبحاث المعلومات، 2021، العدد 10.

69- خلدون عمان سعيدة تطبيقات مفيدة لحماية الخصوصية الرقمية تؤمن تصفح الأنترنيت والتراسل ورسائل البريد الالكتروني، مقال منشور بتاريخ 12 جانفي 2021، تم الاطلاع عليه بتاريخ 01/06/2023 على الساعة 10:00 موجودة في الرابط التالي-https:my-data: manager.ar.uptodown.com/android.

70- صباح مهدي هادي الشمري، زيد محمد علي اسماعيل، الأمن السيبراني كمرتكز جديد في الاستراتيجية العراقية، العراق، مجلة قضايا سياسية، 2012، العدد 62، جامعة النهرين، كلية العلوم السياسية، 2020.

71- محمد فرحات، "التحقيق الجنائي في الجرائم المعلوماتية"، المجلة الجزائرية للقانون والاقتصاد، عدد 18، 2022.

72- نورة الصانع وآخرين، العلاقة بين الوعي بالأمن السيبراني والقيم الوطنية والأخلاقية والدينية التلاميذ المرحلتين الابتدائية والمتوسطة بمدينة الطائف، مجلة البحث العلمي في التربية، الطائف، 2020.

73- يوسف عبد الله سلامة، "الأمن المعلوماتي والأمن السيبراني: دراسة مقارنة"، المجلة العربية للأمن السيبراني، العدد 5، 2022.

74- هشام محمد خليل، الجوانب الإجرامية للجوانب المعلوماتية، مجلس الأمن والقانون، عدد 2، شرطة دبي، 2012.

المراجع بالفرنسية:

75- CATALA, Ebauche d'une théorie juridique de l'information D 1984.

76- ELISE Dragon, Etude sur le statut juridique de l'information, D. 1998, chron.

77- GALLOUX (J-C): Ébauche d'une définition juridique de l'information, D 1994, chron.

78- GDPR Regulation (EU) 2016/679, Official Journal of the European Union, L119, 4 May 2016.

79- Georgie penbey, the parkerian Hexad, cia model expanded.

80- Michael whitman and Hathord, Principles of information security, 5th Ed, usa, 2012.

81- Pierre Catala, les transformations de droit par informatique, Emergences du droit de l'informatique, 1983, P264.

82- Report Catherine A. Theohary, John W. Rollins, Op.cit.

83- Report Catherine A. Theohary, John W. Rollins. Cyberwarfare and Cyberterrorism: In Brief, [N.P], Congressional Research Service, March 27, 2015.

84- United Nations General Assembly, Resolution A/RES/68/167, The Right to Privacy in the Digital Age, 2013.

الفهرس

❖ **فهرس المحتويات:**

العنوان	الصفحة
شكر وعرفان	/
الإهداء	/
قائمة الجداول والأشكال	/
مقدمة	أ - د
الفصل الأول: الأمن المعلوماتي	
المبحث الأول: ماهية الأمن المعلوماتي	2
المطلب الأول: تعريف الأمن المعلوماتي وأهميته	2
الفرع الأول: مفهوم الأمن المعلوماتي	3
الفرع الثاني: أهمية الأمن المعلوماتي	11
المطلب الثاني: عناصر ووسائل الأمن المعلوماتي	12
الفرع الأول: عناصر الأمن المعلوماتي	12
الفرع الثاني: وسائل الأمن المعلوماتي	16
المبحث الثاني: دور الأمن السيبراني في دعم الأمن المعلوماتي	20
المطلب الأول: تعريف الأمن السيبراني وأهدافه	20
الفرع الأول: مفهوم الأمن السيبراني	20
الفرع الثاني: أهداف الأمن السيبراني	21
المطلب الثاني: العلاقة بين الأمن السيبراني والأمن المعلوماتي	24
الفرع الأول: الامن السيبراني والأمن المعلوماتي	24
الفرع الثاني: الترابط بين الأمن السيبراني والأمن المعلوماتي	25
الفصل الثاني: حماية الحياة الخاصة في ظل الأمن المعلوماتي	
المبحث الأول: خصوصية ومبادئ حماية الحياة الخاصة في ظل الأمن المعلوماتي	30
المطلب الأول: خصوصية الحماية القانونية للحق	30
الفرع الأول: مفهوم الحياة الخاصة والخصوصية	30
الفرع الثاني: وسائط الإختراق والجرائم الإلكترونية التي تهدد الخصوصية	31
الفرع الثالث: أشكال التعدي على خصوصية الفرد	35

المطلب الثاني: مبادئ الحماية القانونية للحق في الخصوصية	41
الفرع الأول: المبادئ الخاصة بضمان الأمن المعلوماتي للحق في الخصوصية	41
الفرع الثاني: مبادئ وأصناف الحماية الخاصة بضمان حقوق الأشخاص	43
الفرع الثالث: دور التطبيقات الإلكترونية والحماية الجزائية في حماية الخصوصية	48
المبحث الثاني: الإطار القانوني لحماية الحياة الخاصة في ظل الإطار القانوني والأمن المعلوماتي	49
المطلب الأول: التشريعات والتحديات الوطنية والدولية المنظمة لحماية البيانات الشخصية	49
الفرع الأول: التشريعات الوطنية والدولية المنظمة لحماية البيانات الشخصية	49
الفرع الثاني: تحديات تطبيق القوانين في مواجهة الجرائم الرقمية	52
المطلب الثاني: آليات تعزيز الأمن المعلوماتي لحماية الحياة الخاصة	55
الفرع الأول: الآليات الدولية والوطنية لضمان وتعزيز الأمن المعلوماتي	55
الفرع الثاني: حماية الخصوصية الرقمية القانونية	62
خاتمة	67
قائمة المراجع	/

❖ **قائمة الأشكال:**

الرقم	العنوان	الصفحة
01	مجالات أمن المعلومات	03
02	مثلث أمن المعلومات (The CIA Triad)	13
03	سداسي باركر للأمن المعلوماتي	14
04	أهداف الأمن السيبراني	22
05	أمن المعلومات والأمن السيبراني	24

- ملخص الدراسة:

يعد الأمن المعلوماتي منظومة من الإجراءات والتقنيات التي تهدف إلى حماية المعلومات من أي تهديد يمس سريتها وسلامتها وتوافرها، ويرتكز على عناصر أساسية مثل السرية والتكاملية والتوافر، لتحقيق بيئة معلوماتية آمنة تدعم الثقة والاستقرار من خلال أدوات تقنية كالتشفير، وسياسات إدارية فعالة، مدعوم بآليات الأمن السيبراني في حماية الحياة الخاصة، فهو فرع متخصص بحماية الأنظمة الرقمية والشبكات من الهجمات السيبرانية، ويُعتبر وسيلة عملية لتطبيق الأمن المعلوماتي في البيئات الرقمية، مما يعزز من حماية البيانات الإلكترونية.

في المقابل، أصبحت حماية الحياة الخاصة إحدى القضايا الأساسية في ظل تطور التكنولوجيا وتزايد التهديدات الرقمية، حيث أضحت البيانات الشخصية معرضة للاستغلال وسوء الاستخدام، مما يتطلب مبادئ واضحة لجمع ومعالجة البيانات، ضمن إطار قانوني يشمل التوازن بين الأمن المعلوماتي وحقوق الأفراد لضمان بيئة رقمية آمنة تحترم كرامة الإنسان وحرياته، من خلال تشريعات دقيقة، وتعاون دولي، ورقابة فعالة.

- الكلمات المفتاحية:

الأمن المعلوماتي، الأمن السيبراني، حماية الحياة الخاصة، الإطار القانوني، الخوصصة، البيئة الرقمية.

Study Summary:

Information security is a system of procedures and technologies aimed at protecting information from any threats that affect its confidentiality, integrity, and availability. It relies on fundamental elements such as confidentiality, integrity, and availability to achieve a secure information environment that supports trust and stability. This is accomplished through technical tools like encryption, effective administrative policies, and is supported by cyber security mechanisms for protecting privacy. Cyber security is a specialized branch focused on protecting digital systems and networks from cyber attacks and is considered a practical means of implementing information security in digital environments, thereby enhancing the protection of electronic data.

Conversely, the protection of privacy has become a fundamental issue amid technological advancements and increasing digital threats. Personal data is increasingly vulnerable to exploitation and misuse, necessitating clear principles for collecting and processing data within a legal framework that balances information security with individual rights. This balance aims to ensure a secure digital environment that respects human dignity and freedoms through precise legislation, international cooperation, and effective oversight.

Keywords:
Information security, cyber security, privacy protection, legal framework, privatization, digital environment.