

أمن المعلومات في ظل التحول الرقمي Information security in the digital age

حابت أمال

كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو (الجزائر)

habet_amel@yahoo.fr

تاريخ النشر:
2026/10/31

تاريخ القبول:
2026/09/27

تاريخ الارسال:
2026/04/21

الملخص:

تعتمد المجتمعات الحديثة بشكل متنامي على تكنولوجيا الاتصالات والمعلومات، غير أن هذا الاعتماد المطرد ترافقه مجموعة من المخاطر الناشئة والمحتملة التي تهدد الشبكات وأمن المعلومات والمجتمع المعلوماتي ككل، وهو ما جعل الأمن المعلوماتي يشكل جزءاً أساسياً من السياسة الأمنية للدول، فقد أصبح صناع القرار في الدول المتطورة كالولايات المتحدة الأمريكية، دول الاتحاد الأوروبي، روسيا، الصين وغيرها، يصنفون مسائل الأمن المعلوماتي كأولوية في سياسة الأمن الدفاعية الوطنية خاصة في ظل التوجه نحو الرقمنة في كافة الأنشطة الحياتية، وستتطرق في هذا العمل إلى الإطار المفاهيمي للأمن المعلوماتي وكيف كان وكيف أصبح؟.

الكلمات المفتاحية:

أمن- معلوماتي- سيبراني- فيروسات- تحول- رقمي.

Abstract:

Modern societies are increasingly dependent on information and communication technologies. However, this steady dependence is accompanied by a set of emerging and potential risks that threaten networks, information security, and the information society as a whole. This has made information security an essential part of the security policy of countries. Decision-makers in developed countries such as the United States of America, the countries of the European Union, Russia, China, and others, have classified information security issues as a priority in national defense security policy, especially in light of the trend towards digitization in all aspects of life. In this

work, we will address the conceptual framework of information security: how it was and how it has become.

key words:

Cyber -security - Information -Systems – Viruses- Transformation - digital.

مقدمة:

يعد الفضاء المعلوماتي إطاراً جديداً لعلاقات اجتماعية وسياسية وثقافية واقتصادية عابرة للقوميات والأماكن، بعد أن كانت محصورة في رقع جغرافية مكانية واحدة تحكمها قيم وقواعد محددة وواحدة، فبعد ظهور الانترنت ظهر شكل جديد من التفاعل الإنساني تشابكت فيه وتكاثرت المعاملات والصفقات، لدرجة أن بعض الشركات تفرض على المتعاملين معها اتخاذ أسلوب الاتصال الرقمي وترفض التعامل بالطرق الكلاسيكية، وهو منهج الحكومات أيضاً حيث تعتمد غالبية مؤسساتها اليوم على التعامل الإلكتروني.

بالمقابل، من سلبيات الفضاء المعلوماتي ضخامة حجم الاعتداءات التي تتم عبره، حيث يكفي أن نعلم أن الجرائم الإلكترونية بأنواعها المختلفة قد كلفت الاقتصاد العالمي أكثر من 10.5 تريليونات دولار العام الماضي (2025)¹، لذلك يعد الأمن المعلوماتي أحد أهم التحديات التي تواجه البشرية أفراداً ومؤسسات في زمن الثورة المعلوماتية .

يعتمد استقرار أي دولة على مفهوم الأمن في جميع مكوناتها، انطلاقاً من الإمكانيات العسكرية، مروراً بالحفاظ على استقرار النظام، وصولاً إلى حماية القيم الجوهرية لمجتمعاتها، وأمام الاعتداءات السيبرانية المتزايدة والتي دقت ناقوس الخطر وجدت الدول نفسها مجبرة من جهة: التنسيق فيما بينها من أجل الحفاظ على أمنها واستقرارها الاقتصادي والسياسي، من جهة أخرى وضع سياسة داخلية تقوم على تحقيق الأمن الوطني، بعد أن رفعت الإنترنت مستوى الأخطار التي تتعرض لها كل الأنظمة المعلوماتية للدول وللأفراد، والتي يمكن أن تتخذ أشكالاً غير متوقعة وتطال مجالات أساسية وحساسة وحيوية، وهوما التزم به غالبية دول العالم من خلال وضع قوانين نموذجية

¹ جاءت هذه الإحصائيات في بيان صادر عن اتحاد المصارف الإسلامية في 17-07-2025، لأكثر تفصيل

أطلع على الموقع:-<https://uabonline.org/international>

وعقد اتفاقات دولية وقوانين وطنية تجابه بها الخطر الرقمي الجديد وتحقق أمنا معلوماتيا.

ان التطور الذي يشهده العالم اليوم في أشكال الاعتداءات والمعتدين ووسائل الاعتداء تبعه تطور مطرد لفكرة الامن، وعليه، تطور مفهوم الأمن المعلوماتي يتطلب الربط بين مخاطر التحول التكنولوجي المتسارعة وبين مدى استجابة المنظومات التقنية والقانونية لهذا التحول.

انطلاقا من هذه المعطيات نتساءل عن مفهوم الامن المعلوماتي و هل بالفعل استطاع ان يواكب التطور الحاصل في ظل رهانات التحول الرقمي؟

تبعا لصيغة هذا الاشكال فان المنهج المناسب للدراسة هو المنهج الوصفي باعتباره الانسب لحصر مفهوم الامن المعلوماتي، ودراسة انتقاله من المفهوم الكلاسيكي لـ "أمن الأنظمة" الذي يركز على حماية الأجهزة إلى المفهوم الشامل لـ "الأمن السيبراني" الذي يمتد لحماية السيادة الرقمية والبيانات الضخمة والذكاء الاصطناعي.

يبرز جليا دور وأهمية أمن الأنظمة المعلوماتية في تحقيق الأمن الوطني والدولي، والتحول الرقمي جعل فكرة الامن المعلوماتي تتحول من مجرد اليات للدفاع عن الانظمة الى آليات اخرى تسعى للهجوم على الاعتداءات الاحتمالية مع ضمان استمراريتها حال الاعتداء عليها (مبحث أول) ولان التهديدات السيبرانية أصبحت احد التحديات الرئيسية التي يتحتم على الدول مواجهتها وجب عرض التحولات المعاصرة لأنماط الأمن المعلوماتي (مبحث ثان).

المبحث الأول: التحول من فكرة الدفاع الى فكرة الدفاع والهجوم في مفهوم الأمن المعلوماتي(الأمن الاستباقي)

يعتبر مفهوم الأمن المعلوماتي من أكثر المفاهيم المثيرة للاهتمام والدراسة، لدرجة أن هناك من يرى ضرورة وضع قانون مستقل له، على أن يعرف هذا القانون بأنه نظام قانوني مصمم للتعامل مع الإنترنت والحوسبة والفضاء الرقمي والقضايا القانونية ذات الصلة، بمعنى أن الوصف الملائم لقانون الأمن المعلوماتي هي: إيجاد قوانين ورقية لتنظيم وحماية العالم اللارقي.

من ناحية مفهومه، فقد تغير ليوالكب التحولات الرقمية الحاصلة في العالم من مفهوم تقليدي يعتمد على الدفاع(مطلب أول) الى مفهوم جديد يعتمد على الدفاع والهجوم والاستجابة والتعافي وحماية السيادة الرقمية (مطلب ثان).

المطلب الأول: المفهوم التقليدي للأمن المعلوماتي

في مفهوم الامن المعلوماتي كان التركيز ينصب على أمن المعلومات (Information Security)، أي حماية البيانات من الوصول غير المصرح، حيث سعى الامن المعلوماتي في بداياته لضمان سرية البيانات و سلامتها، و لتسليط الضوء على هذا المفهوم التقليدي للأمن المعلوماتي نبدأ أولاً بنشأته (فرع أول) ثم نستعرض مختلف التعاريف التي قيلت بشأنه (فرع ثان).

الفرع الأول: نشأة الامن المعلوماتي

تعود نشأة الأمن المعلوماتي إلى سبعينيات القرن الماضي، عندما صمم الباحث روبرت توماس برنامج كمبيوتر يسمى الزاحف (Creeper)، وهو برنامج قادر على التحرك عبر شبكة (ARPANET'S) تاركا خلفه مسار تحركاته، بعدها أنشأ مخترع البريد الإلكتروني راي توملينسون برنامجاً أسماه الحصاد (Reaper) والذي بدوره قام بحذف برنامج (Creeper)، وبالتالي أصبح برنامج (Reaper) بمثابة أول برنامج ذاتي النسخ لمكافحة الفيروسات الإلكترونية¹.

فترة الثمانينيات كان الفيروس الذي أوجده توماس موريس سببا في بداية مجال جديد في أمان الكمبيوتر، فقد دفع الكثيرين للبحث و تكثيف الجهود لإيجاد حلول لمكافحة تلك الفيروسات وإيجاد وسائل لمواجهة هجماتها المتواصلة.

شهدت سنة 1987 تصميم العديد من البرامج المقاومة للفيروسات، والتي أصبحت تُستخدم على مستوى واسع من قبل الكثير من مستخدمي الكمبيوتر، إذ تم إنتاج العديد منها، وكان أول برنامج لمكافحة الفيروسات هو (Ultimate Virus Killer)، ومع توفر الإنترنت خلال فترة التسعينات، ازدادت تهديدات أمان الشبكة بنحو كبير، الأمر الذي تطلب إنتاج برامج جدران حماية، وبرامج مكافحة الفيروسات.

تعد فترة 2000 هي المرحلة التي بدأت فيها المنظمات الإجرامية في تمويل الهجمات الإلكترونية بنحو كبير، وفي المقابل استمر أمن المعلومات في النمو بالتزامن مع نمو الإنترنت.

¹ لأكثر تفصيل أنظر: د. محمد أمين الرومي، جرائم الحاسب والإنترنت: الجريمة المعلوماتية في ضوء

القواعد القانونية والتقنية، دار المطبوعات الجامعية، الإسكندرية، مصر، 2019.

من أهم أنواع الفيروسات والبرامج الضارة¹ التي طالت الأجهزة الآلية وشبكة الانترنت ما يلي:

- برامج التجسس: صممت بهدف التجسس والتتبع وجمع البيانات عن المستخدم، وغالباً ما تتضمن هذه البرامج خاصية تعقب النشاطات، وجمع تفاصيل الضغط على لوحة المفاتيح وجمع البيانات، وفي محاولة للتغلب على الإجراءات الأمنية، تقوم برامج التجسس بتعديل إعدادات الأمان. وتجمع نفسها مع البرامج الشرعية.

- برامج الإعلانات المتسللة: بعض هذه البرامج تكون هدفها الدعاية الاعلانية فقط وبعضها يكون غطاء لبرامج التجسس.

- برنامج "روبو أو بوت"² صممت لتقوم بتنفيذ إجراء معين بشكل أوتوماتيكي ومعظم البوتات غير ضارة، إلا أن الاستخدام المتزايد لها يصيب أجهزة الحاسوب بالبوت التي تتم برمجتها لينتظر بهدوء الأوامر المقدمة من المهاجم.

- برامج طلب الفدية "Ransomware" هي برامج صممت من أجل تعطيل نظام الحاسوب و البيانات التي يحتويها وطلب فدية ولا يتم اصلاحه الا اذا تم الدفع.

¹ يمكن ان نذكر بعض أعراض البرامج الضارة الشائعة :

- البطء في سرعة الحاسوب

- توقف الحاسوب أو تعطله في أغلب الأحيان.

- البطء في سرعة تصفح مواقع الإنترنت داخل الشبكة.

- المشاكل الغامضة المتعلقة بالاتصال بالشبكة.

- تعديل الملفات

- حذف الملفات.

- تواجد الملفات أو البرامج أو الأيقونات على سطح المكتب غير المعروفة.

- تشغيل يحدث لعمليات غير معروف.

- إيقاف البرامج أو إعادة تشغيل نفسها.

- إرسال رسائل البريد الإلكتروني دون علم المستخدم أو موافقته. أنظر في ذلك: حسن طاهر داود،

الحاسب وامن المعلومات، معهد الإدارة العامة، السعودية، 2000، ص96 وما يليها.

² لأكثر تفصيل أنظر في ذلك: محمد علاء محمد، مقدمة للأمن السيبراني،

<https://www.kotobati.com/%D9%83%D8%AA%D8%A7>، تاريخ الاطلاع 2022-09-10، ص39

- برنامج استغلال الخوف "Scareware" هو برامج مصمم لإقناع المستخدم باتخاذ إجراء محدد بناء على الخوف، حيث يقوم بتكوين إطارات منبثقة تشبه نوافذ حوار تنقل رسائل مزورة تفيد بأن النظام في خطر و يحتاج إلى تنفيذ برنامج معين للعودة إلى التشغيل العادي، وإذا وافق المستخدم على البرنامج المذكور وتم تنفيذه، فسيتم إصابة نظامه .

- الفيروسات المتنقلة Worms هي شفرة خبيثة تقوم بتكرار نفسها من خلال استغلال الثغرات في الشبكات بشكل مستقل، وعادة ما تؤدي الفيروسات إلى إبطاء الشبكات، وبعد إصابة المضيف يمتلك الفيروس المتنقل القدرة على الانتشار بسرعة كبيرة على الشبكة¹.

الفرع الثاني: التعريف الكلاسيكي للأمن المعلوماتي

سنحاول عرض التعاريف التي قيلت بشأن أمن الانظمة المعلوماتية بدء بالتعريف اللغوي والاصطلاحي (أولا) ثم التعاريف القانونية (ثانيا).

أولاً: التعاريف اللغوية والاصطلاحية:

مصطلح الأمن المعلوماتي يتضمن شقين :

- شق الأمن: هو نقيض الخوف، أي بمعنى السلامة. والأمن مصدر الفعل أَمِنَ أَمْنًا وَأَمَانًا وَأَمَنَةً: أي اطمئنان النفس وسكون القلب وزوال الخوف، ويقال: أَمِنَ من الشر، أي سَلِمَ منه. وقد عرّفه قاموس بنغوين للعلاقات الدولية بأنه مصطلح يشير إلى غياب ما يهدد القيم النادرة .

الأمن نعني به شعور الفرد أو الجماعة بالطمأنينة، وإشاعة الثقة والمحبة بينهم، بعدم خيانة الأفراد لبعضهم البعض، وإزالة كل ما يهدد استقرارهم وعيشهم، وتلبية متطلباتهم الجسدية والنفسية لضمان قدرتهم على الاستمرار في الحياة بسلام وأمان.

اصطلاحاً: للأمن عدة زوايا يمكن ان نعرفه منها الا اننا سنعرفه من الزاوية الاجتماعية القانونية والزاوية التقنية.

الامن في المفهوم الاجتماعي والقانوني هو سيادة القانون وحماية الحقوق والحريات، بحيث يشعر الأفراد بأن أنفسهم وأموالهم وأعراضهم مصانة بموجب سلطة

¹ لأكثر تفصيل انظر في ذلك: محمد علاء محمد، مقدمة للأمن السيبراني، على الموقع:

<https://www.kotobati.com> ، تاريخ الاطلاع 10-09-2022، ص38.

شرعية تمنع الاعتداء وتجازي المعتدي .

الامن في السياق التقني هو التحصين التقني والإداري الذي يمنع الوصول غير المصرح به للبيانات، ويضمن بقاءها سليمة ومتاحة، ويحمي الأنظمة من التخريب أو التجسس¹.

- شق المعلوماتي: مصطلح المعلوماتية مشتق من كلمة معلومات² و مفردتها "معلومة"، و لغويا هي مشتقة من الجذر اللغوي الثلاثي ع ل م، والذي يدور معناه حول الإدراك، المعرفة، واليقين³.

اصطلاحا: المعلومات هي مجموعة من الحقائق أو البيانات التي خضعت للمعالجة أو النقل وصارت لها دلالة معرفية⁴.

تعرف المعلومات بصفة عامة أنها "مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح لأن تكون محلا للتبادل والاتصال أو للتفسير والتأويل أو للمعالجة سواء بواسطة الأفراد أو الأنظمة الإلكترونية، وهي تتميز بالمرونة بحيث يمكن تغييرها وتجزئتها وجمعها أو نقلها بوسائل وأشكال مختلفة"¹

¹ محمد منذر، مفهوم الأمن: دراسة في الأبعاد والمستويات، المؤسسة الجامعية للدراسات، بيروت، 2014، ص52.

² وقد عرف المشرع الأمريكي، المعلومات في قانون المعاملات التجارية الإلكترونية لعام 1999 في المادة 10/2 بأنها تشمل البيانات والكلمات والصور والأصوات والوسائل وبرامج الكمبيوتر والبرامج المضغوطة والموضوعة على الأقراص المرنة وقواعد البيانات أو ما شابه ذلك، انظر في ذلك: حامد قشقوش هدى، الحماية القانونية للتجارة الإلكترونية، دار النهضة العربية، مصر، 2000، ص84.

³ جاء في "لسان العرب" لابن منظور:

العلم هو نقيض الجهل، وعلم بالشيء أي عرفه وأدرك حقيقته. والمعلومات هي الأشياء التي استقر العلم بها وصارت واضحة للعقل.

⁴ ليس كل المعلومات خاضعة للحماية القانونية بل هناك شروط يجب توافرها فيها تتمثل في:

- أن يتوفر في المعلومة التحديد والابتكار أما الشيء الشائع فلا يتمتع بأي حماية قانونية.

- أن يتوفر في المعلومة السرية والاستثنائية وتكتسب المعلومة وصفها هذا إما بالنظر إلى طبيعتها أو إلى إرادة الشخص أو إلى الأمرين معا مثل الرقم السري، انظر في ذلك: محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، مصر، 2004، ص 40.

بالجمع بين المعنيين يمكن ان نعرف الامن المعلوماتي انه: مجموعة من الإجراءات والتدابير التقنية والإدارية التي تضمن حماية للحقائق والبيانات من المخاطر التي قد تعترضها، هذه الحماية تشمل سريتها (لا يراها إلا المخولون)، سلامتها (لا يتم تعديلها أو تخريبها)، وتوافرها (تكون متاحة عند الحاجة إليها).

ثانيا: التعاريف القانونية: الفقهية والتشريعية

انتقل في مفهوم الامن المعلوماتي من التركيز على الحماية والدفاع فقط الى اضافة عنصر جبر الاضرار، حيث قيل بشأن الأمن المعلوماتي عدة تعريفات أهمها:

أ- التعاريف المركزة على فكرة الدفاع:

عرف "ريتشارد كمرر" Kemmerr A Richard الأمن المعلوماتي أنه: عبارة عن وسائل دفاعية من شأنها كشف وإحباط المحاولات التي يقوم بها القرصنة.

كما جاء في التقرير الصادر عن الاتحاد الدولي للاتصالات، ان الامن المعلوماتي مجموعة من المهمات، مثل تجميع وسائل، وسياسات، وإجراءات أمنية، ومبادئ توجيهية، وتدريبات، وممارسات فضلى، وتقنيات يمكن استخدامها لحماية البيئة السيبرانية، وموجودات المؤسسات والمستخدمين².

عرفت هيئة الاتصالات وتقنية المعلومات الأمن المعلوماتي "هو حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة (عتاد) وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات، من أي اختراق أو تعطيل أو

¹ نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، لبنان، 2005، ص 28، يمكن ان نورد أيضا تعريف الأستاذ « Catala » "رسالة ما معبر عنها في شكل يجعلها قابلة للنقل أو الإبلاغ للغير" أنظر في ذلك: رشيدة بوكر، جرائم الإعتداء على نظم المعالجة الآلية في التشريع الجزائري و المقارن، منشورات الحلبي الحقوقية، لبنان 2012، ص 65، كما عرفت أيضا بأنها "النقل المجرد لوقائع معينة تم الحصول عليها من مصادر متعددة، أنظر في ذلك: خالد ممدوح ابراهيم، أمن الجريمة الالكترونية، الدار الجامعية، مصر، 2005، ص 27

² حنين جميل أبو حسين، الإطار القانوني لخدمات الأمن السيبراني، رسالة ماجستير في القانون الخاص،

تعديل أو دخول أو استخدام أو استغلال غير مشروع، ويشمل مفهوم الأمن السيبراني أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحو ذلك¹.

الملاحظ أن كل هذه التعاريف ركزت على أن الأمن المعلوماتي هو: وسيلة دفاعية ضد الهجمات وعمليات القرصنة على مختلف الحواسيب.

ب- التعاريف المضيفة لفكرة جبر الضرر:

حسب هذا الاتجاه فإن الأمن المعلوماتي هو عبارة عن مجموع الوسائل التقنية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتأمين حماية وسرية وخصوصية البيانات الشخصية ولحماية المواطنين.

عرف المعهد الوطني للمعايير والتقنية الأمريكي الأمن المعلوماتي بأنه: " الحماية من الأضرار واستعادة أنظمة الحاسب وأنظمة الاتصالات الإلكترونية وخدمات الاتصالات الإلكترونية والاتصالات السلكية والاتصالات الإلكترونية، بما في ذلك المعلومات الواردة فيها، لضمان توافرها وسلامتها والمصادقة والسرية وعدم الانتهاك"، يفهم من هذا النص أن الأمن المعلوماتي يهدف إلى حماية الأنظمة الحاسوبية من الوصول غير الشرعي لها، أو العبث بالمعلومات أثناء التخزين أو المعالجة، أما إذا حدث الاعتداء لا بد أن يعمل نظام الأمن المعلوماتي على استعادة الأنظمة لضمان توافرها وهذا ما يضيف للأمن المعلوماتي فكرة أنه يجب أن يعمل على جبر اضرار التي تسببت فيها الاعتداءات.

تأسيساً لما سبق، فإن التعريف الكلاسيكي للأمن المعلوماتي يركز على أنه نشاط يؤمن حماية الأنظمة المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن إمكانات الحد من الخسائر والأضرار، التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح إعادة الوضع إلى ما كان عليه، بأسرع وقت ممكن.

مما يعني أن الأمن المعلوماتي يتدخل بعد حدوث الاعتداء لردّه أو إيقافه كمرحلة أولى ثم جبر الاضرار واعادة الحالة الى اصلها كمرحلة ثانية، وهما وجهان دفاعيان للأمن المعلوماتي.

¹ إدريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، مجلة مصداقية، المجلد 1،

العدد 1، ديسمبر 2019، ص 103.

يمكن ان نشير هنا الى موقف المشرع الجزائري بشأن مفهوم الامن المعلوماتي والذي اصطلح عليه الامن السيبراني، ففي القانون رقم 04-18 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الالكترونية¹ في مادته 10/3 بأنه: مجموع الادوات والسياسات ومفاهيم الامن والاليات الامنية والمبادئ التوجيهية وطرق تسيير المخاطر والاعمال والتكوين والممارسات الجيدة والضمانات والتكنولوجيات التي يمكن استخدامها في حماية الاتصالات الالكترونية ضد اي حادث من شأنه المساس بتوفر وسلامة وسرية البيانات المخزنة او المعالجة او المرسلة.

ما يلاحظ على هذا التعريف انه تناول الشق المتعلق بالحماية من الاعتداءات فقط ولم يتضمن الشق الثاني من مفهوم الامن المعلوماتي والمتمثل في جبر الاضرار واعادة الحالة الى اصلها.

نشير أيضا أن المشرع الجزائري أصدر ترسنة من النصوص القانونية متشعبة تضمن أمن الانظمة المعلوماتية بشكل مباشر أو غير مباشر، بدء بقانون العقوبات² ، قانون الاجراءات الجزائية³، قانون رقم 04-09 المتعلق بالوقاية من جرائم تكنولوجيات الاعلام والاتصال ومكافحتها⁴، قانون رقم 05-18 المتعلق بالتجارة الالكترونية⁵ قانون رقم 07-18 المتعلق بحماية الاشخاص الطبيعيين في مجال معالجة البيانات ذات الطابع الشخصي⁶ المعدل والمتمم¹، القانون النقدي والمصرفي² الى جانب المرسوم الرئاسي رقم

¹ قانون رقم 04-18 مؤرخ في 10 ماي 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، الجريدة الرسمية عدد27 الصادرة في 13 ماي 2018.

² أمر رقم 66-156 مؤرخ في 8 جوان 1966، يتضمن قانون العقوبات ، معدل ومتمم بقانون 06-24 مؤرخ في 28 أفريل 2024، الجريدة الرسمية عدد30 الصادرة في 30 أفريل 2024.

³ قانون رقم 14-25 مؤرخ في 3 أوت 2025، يتضمن قانون الإجراءات الجزائية، الجريدة الرسمية عدد54 الصادرة في 13 أوت 2025.

⁴ قانون رقم 04-09 مؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من جرائم تكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية عدد47 الصادرة في 16 أوت 2009.

⁵ قانون رقم 05-18 مؤرخ في 10 ماي 2018، يتعلق بالتجارة الالكترونية، الجريدة الرسمية عدد28 الصادرة في 16 ماي 2018

⁶ قانون رقم 07-18 مؤرخ في 10 جويل 2018، يتعلق بحماية الاشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية عدد34 الصادرة في 10 جوان 2018.

20-05 المتعلق بوضع منظومة وطنية لأمن الانظمة المعلوماتية³ ، وقانون الثقة في المعاملات الالكترونية⁴ خاصة أمام اعتماد الجزائر على رقمنة جميع مصالحها وإنشاء محافظة سامية للرقمنة بموجب مرسوم رئاسي رقم 23-314⁵ المعدل بالمرسوم الرئاسي رقم 24-63⁶.

المطلب الثاني: المفهوم الحديث للأمن المعلوماتي

شهد مفهوم الأمن المعلوماتي تحولاً جذرياً، حيث انتقل من مجرد إجراءات تقنية لحماية أجهزة الحاسوب، إلى استراتيجية سيادية شاملة تمس أمن الدول والمجتمعات. بتفكيك هذه التحولات المعاصرة في مفهوم الأمن المعلوماتي نجد ان هذا التحول طال عدة جوانب للأمن المعلوماتي.

الفرع الأول: التحول من حيث النطاق: من "أمن المعلومات" إلى "الأمن السيبراني"

نتحدث اليوم عن الأمن السيبراني (Cybersecurity) وهو مفهوم أوسع عن الامن المعلوماتي فهو يشمل:

- حماية الأشخاص، والشبكات، والأنظمة، وحتى "السمعة الرقمية".

¹ قانون رقم 25-11 مؤرخ في 24 جويلية 2025، يعدل ويتم القانون رقم 18-07 مؤرخ في 10 جويلن 2018 والمتعلق بحماية الاشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية عدد48 الصادرة في 24 جويلية 2025.

² قانون رقم 23-09 مؤرخ في 21 جوان 2023، يتضمن القانون النقدي والمصرفي، الجريدة الرسمية عدد43 الصادرة في 27 جوان 2023

³ مرسوم رئاسي رقم 20-05 المؤرخ في 20 جانفي 2020، يتعلق بوضع منظومة وطنية لأمن الانظمة المعلوماتية، الجريدة الرسمية عدد4 الصادرة في 26 جانفي 2020.

⁴ قانون رقم 26-02 مؤرخ في 17 فيفري 2026، يحدد القواعد العامة المتعلقة بخدمات الثقة للمعاملات الالكترونية وبالتعريف الالكتروني، الجريدة الرسمية عدد14 الصادرة في 18 فيفري 2026.

⁵ مرسوم رئاسي رقم 23-314 مؤرخ في 6 سبتمبر 2023، يتضمن إنشاء محافظة سامية للرقمنة وتحديد مهامها وتنظيمها وسيورها، الجريدة الرسمية عدد59 الصادرة في 10 سبتمبر 2023

⁶ مرسوم رئاسي رقم 24-63 مؤرخ في 1 فيفري 2024، يعدل مرسوم رئاسي رقم 23-314 مؤرخ في 6 سبتمبر 2023، يتضمن إنشاء محافظة سامية للرقمنة وتحديد مهامها وتنظيمها وسيورها، الجريدة الرسمية عدد 8 الصادر في 4 فيفري 2042.

- تأمين الفضاء الذي يربط بين العالم الواقعي والعالم الافتراضي (مثل التحكم في سدود المياه أو محطات الكهرباء عبر الإنترنت...الخ).

مصطلح الأمن السيبراني مصطلح لاتيني الأصل (Cyber security) وكلمة سير معناها الأمن المعلوماتي فيصبح المقصود بالأمن السيبراني أمن الأمن المعلوماتي وهو تعبير أشمل وأعم من أمن المعلومات.

وإذا كنا قد عرفنا سابقا مفهوم الامن، فإن مصطلح السيبرانية والذي يعد الآن واحد من أكثر المصطلحات ترددا في معجم الأمن الدولي، تشير المقاربة الإيتيمولوجية¹ له إلى أنها لفظة يونانية الأصل مشتقة من كلمة "Cybernetes" بمعنى الشخص الذي يدير دفة السفينة أي التوجيه والسيطرة ، حيث تستخدم مجازاً للتحكم "governor". وتجدر الإشارة إلى أن العديد من المؤرخين يرجعون أصلها إلى عالم الرياضيات الأمريكي norbert Wiener 1894-1964 وذلك للتعبير عن التحكم الآلي، فهو الأب الروحي المؤسس للسيبرنتيقية من خلال مؤلفه الشهير: Cybernetics or control and communication in the Animal and the machine . وأشار في كتابه إلى أن السيبرنتيقية هي التحكم والتواصل عند الحيوان والآلة والإنسان والآلة مما أعطاها مفهومها الاصطلاحي الحديث وهو "علم القيادة والتحكم في الأحياء والآلات ودراسة آليات التواصل " ، ليستبدل مصطلح الآلة بعد الحرب العالمية الثانية بالحاسوب².

وعلى العموم، يمكن تعريف الأمن السيبراني أنه مجموعة من الوسائل التقنية والإدارية والقانونية التي تهدف إلى حماية الفضاء السيبراني (الشبكات، الأنظمة، البرمجيات، والبيانات) من الهجمات الرقمية (قائمة أو محتملة)، والوصول غير المصرح به، والتخريب، مع ضمان استمرارية الخدمات وسرية المعلومات وسلامتها".

الفرع الثاني: التحول نحو "المرونة السيبرانية (Cyber Resilience)"

تغيرت الفلسفة الأمنية من محاولة منع الهجوم أو الدفاع إلى مفهوم المرونة.

¹ نعي بالايتمولوجية علم اشتقاق الكلمات أو علم أصل الكلمات

² فارس قره، موسوعة العلوم السياسية على الموقع <https://political-encyclopedia.org/dictionary/>

نشر في: 2018-08-28

• **المفهوم القديم :** يهدف لحماية الأجهزة ببناء جدران حماية لمنع الدخول، إذن التركيز على منع الاختراق و توفير تقنيات للحد من الخسائر والمسؤول عن الامن هو مسؤول قسم التكنولوجيات لأي مؤسسة على اعتبار ان الامن المعلوماتي يقوم على حماية الخصوصية الفردية.

• **المفهوم الحديث :** يهدف لحماية الفضاء الرقمي الشامل من خلال الاعتراف بأن الاختراق قد يقع، لذلك لا بد من سرعة الاستجابة لتقليل الأضرار، واستعادة الأنظمة في أسرع وقت او التعافي، مع انتقال بيانات المؤسسات والدول من الخوادم المحلية إلى السحابة (Cloud)، وعليه الأمن السيبراني أصبح مسؤولية استراتيجية للدولة لأنه يسعى لحماية السيادة الرقمية الوطنية، مع ادخال الذكاء الاصطناعي في الدفاع والهجوم:

- الدفاع :استخدام خوارزميات تتنبأ بالهجوم قبل وقوعه من خلال تحليل سلوك الشبكة.

- الهجوم :ظهور الهجمات المؤتمتة التي تستخدم الذكاء الاصطناعي لتطوير فيروسات تغير شكلها باستمرار لتجاوز مضادات الفيروسات التقليدية، كما تقوم أيضا بتدمير أدوات وبرمجيات القرصنة، وهو ما يساعد في إحباط مخطط الهجمات نفسها، وتحديد هوية ومصدر الهجمة، بما يمكن من إطلاق هجمة إلكترونية مضادة فيما تعرف بـ "الاختراق العكسي (back-Hack)"

إن التوجه الجديد في تعريف الامن المعلوماتي أو الامن السيبراني كمفهوم حديث انتقل من مجرد مجموع الاجراءات التقنية لحماية البيانات الى مفهوم اكثر شمولية يركز على المرونة الرقمية¹ والثقة الرقمية ، كما انه انتقل من الاستجابة لرد الفعل- الطابع الدفاعي- الى الامن الاستباقي، حيث يعرف الامن السيبراني اليوم على انه منظومة ذكية قادرة على التنبؤ بالهجمات قبل وقوعها عبر تحليل السلوك باستخدام خوارزميات التعلم

¹ التوجه التقليدي كان يركز على بناء اسوار لمنع الاختراق اما التعريف الحديث يركز الامن المعلوماتي على قدرة النظام على الاستمرارية ومواصلة العمل اثناء التعرض للهجوم من جهة وعلى التعافي وسرعة العودة للحالة الطبيعية بعد الحادثة.

أمن المعلومات في ظل التحول الرقمي —————
الآلي بدلا من الاعتماد فقط على قواعد البيانات التقليدية للفيروسات¹ ومن ثمة التصدي لها مع ضمان استمرارية الانظمة وسرعة التعافي.

المبحث الثاني: أهداف الأمن المعلوماتي وأنماطه المستحدثة.

الأمن السيبراني يعد من أصعب وأعقد المفاهيم التي يتناولها التحليل العلمي، فهو مفهوم نسبي متغير ومركب وذو أبعاد متعددة² ومستويات مختلفة، ترتبط أساسا بطبيعة التغيرات التي لحقت مفهوم وطبيعة التهديد الذي أضى حقل تكنولوجيا المعلوماتية عرضة له، وللأمن المعلوماتي أهداف (مطلب أول) كم يصنف إلى عدة أنواع (مطلب ثان).

المطلب الأول: أهداف الأمن المعلوماتي

تظهر أهمية الأمن المعلوماتي في :

-يحافظ على حساسية وأمان المعلومات الخاصة بالمستخدمين ولاسيما التي قد تعرض الأشخاص للخطر أو الدول التي يقيمون فيها، وذلك لأن أي معلومة قد تكون هامشية أو غير مهمة بالنسبة لبعض الأفراد قد تكون هي حلقة الوصل الذي يحتاجها المخترق للقيام بعمله.

¹ Allison Cerra, Proactive cybersecurity :staying ahead of threats in the age of

AI,WILEY,USA,2025

² تتمثل أبعاد الأمن المعلوماتي في حماية البنى التحتية للدول حيث يتم استهدافها سواء كانت مدنية أو عسكرية بما يؤدي إلى شلل أنظمتها وتدمير أنظمة التشغيل الخاصة بها، والتأثير على تدفق المعلومات بما يؤدي إلى إرباك عمل البنية التحتية الحيوية، وينشأ عن مثل هذه الهجمات تعطيل العديد من مرافق الحياة في الدول وسيادة الفوضى ، مثل استهداف محطات الطاقة والوقود والخدمات المالية والمصرفية ونظم الاتصالات والمواصلات، ومن أبرز الأمثلة على ذلك تعرض أوكرانيا خلال شهر جوان 2017 لهجمة إلكترونية شملت محطات الطاقة، بالإضافة إلى المؤسسات المالية وأحد أكبر محطاتها أنظر في ذلك أميرة عبد العظيم محمد عبد الجواد، "المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام"، مجلة الشريعة والقانون، مجلد3، عدد 35، 2020، ص 431، و للأمن المعلوماتي أبعاد عسكرية، اقتصادية، اجتماعية وسياسية، أنظر في ذلك: إيهاب خليفة، مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي، العربي للنشر والتوزيع، القاهرة، 2019، ص115 وما يليها.

- يساعد الدول على الحفاظ على سرية معلوماتها من الاختراق من قبل الدول المعادية أو التعرض لهجمات إلكترونية تسبب الشلل أو الخسائر الفضائح لاقتصادها، وهو بدوره ما يمكن تصوره بكونه نوع من أنواع الحروب الحديثة في عصرنا الحالي.

- يساعد على تطور تقنية الخدمات السحابية وذلك لأن وجود جدار يحى خصوصية البيانات التي يتم تخزينها فيها يجعل المستخدمين أكثر ثقة في كفاءتها وأكثر استثمارا في إنفاق الأموال عليها بكل راحة¹.

- يساعد على منح مقدمو الخدمات ميزة تنافسية إضافية، بحيث يميل المستخدم إلى التعامل مع المواقع الآمنة ولاسيما التي يتطلب التعامل معها وجود بوابات دفع أو مشاركة بيانات حساسة أو معلومات شخصية.

- يساعد على حماية المستخدمين من الأنشطة الغير قانونية التي تحدث في عالم الويب المظلم والتي أغلبها ما يكون مهددا لحياة البشر أو يعرض متصفحه لخطر التعرض للمسائلة القانونية أيضا، ناهيك عن الناحية الأخلاقية كذلك.

لقد أصبح تأمين الفضاء المعلوماتي جزءا من استراتيجيات الأمن القومي لكل دول العالم ، إذ دفعت التهديدات المتزايدة لأمن هذا الفضاء للعمل على بذل الجهود الجماعية، مثل إنشاء هيئات لمواجهة الطوارئ المعلوماتية CERT"، أو استحداث قوانين مكافحة الجريمة الإلكترونية، وقد قامت بعض الدول بإنشاء قيادة عسكرية لحماية الفضاء المعلوماتي واستحداث وحدات للحرب الإلكترونية داخل الجيوش العسكرية والمشاركة في مناورات إلكترونية² ، ومن ناحية أخرى أطلقت منظمات حكومية وغير حكومية العديد من المبادرات، مثل الاتحاد الدولي للاتصالات، الذي أطلق مبادرة للأمن المعلوماتي، ومبادرة الاتحاد الأوروبي للأمن الإلكتروني، كما تبنت الولايات المتحدة الأمريكية "الاستراتيجية الدولية للفضاء الإلكتروني"، وهي أول وثيقة سياسية من هذا النوع تبين الرؤية الشاملة لمستقبل التعاون الدولي المتعلق بالفضاء المعلوماتي.

¹ د. خالد بن سليمان الغثر و د. محمد بن عبد الله القحطاني، أمن المعلومات، مكتبة الملك فهد الوطنية، الرياض، المملكة العربية السعودية، 2013.

² د. عادل عبد الصادق، الفضاء السيبراني: قضايا الصراع والتعاون في العلاقات الدولية، المركز العربي للبحوث والدراسات، القاهرة، 2020، ص232

المطلب الثاني: أنواع الأمن المعلوماتي:

ينقسم الأمن المعلوماتي إلى جيلين أساسيين؛ الجيل التقليدي الذي ركز على تأمين الأجهزة والبيانات الساكنة، والجيل الحديث (السيبراني) الذي يتعامل مع عالم مترابط، ذكي وبلا حدود.

الفرع الأول: أنواع الأمن المعلوماتي التقليدية

كانت تركز بشكل أساسي على مبدأ الحماية الفيزيائية والمنطقية المحدودة¹ داخل محيط المؤسسة:

- أمن الشبكات: (Network Security) تأمين الشبكات المحلية (LAN) باستخدام جدران الحماية (Firewalls) وأنظمة منع الاختراق التقليدية لمنع الدخول غير المصرح به².
- أمن التطبيقات: (Application Security) التركيز على سد الثغرات في البرمجيات أثناء تصميمها لمنع سرقة البيانات أو تعديلها.
- أمن البيانات: (Data Security) ويتمثل في تشفير البيانات المخزنة (Encryption) وضمان النسخ الاحتياطي الدوري. (Backup)
- الأمن الفيزيائي: (Physical Security) حماية مراكز البيانات والغرف التي تحتوي على الخوادم من السرقة، الحريق، أو الدخول المباشر للأشخاص غير المخولين.
- الأمن التشغيلي (Operational Security): يندرج تحت مظلة الأمن التشغيلي العمليات والقرارات المرتبطة بمعالجة أصول البيانات وحمايتها، بالإضافة إلى الأذونات التي يحتاج لها المستخدمون للوصول إلى الشبكة، والإجراءات الخاصة بكيفية ومكان تخزين البيانات أو مشاركتها.

¹ د. سمير حامد، الاستراتيجية الوطنية للأمن السيبراني كمدخل لتعزيز الأمن القومي، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة القاهرة، 2022، ص164.

² شريفة كلاع، الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني، مجلة الحقوق والعلوم الإنسانية، المجلد 15، العدد 1، 2022.

- الاسترداد بعد الكوارث واستمرارية الأعمال يهتم هذا النوع من الأمن بتحديد الكيفية المتبعة في استجابة المنظمة لحادث أمن سيراني أو أي حدث آخر يؤدي إلى فقدان العمليات أو البيانات، إذ تضع سياسات التعافي من الكوارث طرق استرداد المؤسسة لعملياتها ومعلوماتها بهدف استمرارية العمل.

الفرع الثاني: أنواع الأمن المعلوماتي الحديثة (السيرانية)

مع ظهور الحوسبة السحابية والذكاء الاصطناعي، ظهرت تخصصات أمنية جديدة لم تكن موجودة سابقاً¹:

- أمن الحوسبة السحابية: (Cloud Security)
 - يركز على حماية البيانات المخزنة في منصات خارجية (مثل Google Cloud أو AWS).
 - يتعامل مع تحدي "توزيع البيانات" عبر خوادم في دول مختلفة.
- أمن إنترنت الأشياء: (IoT Security) وذلك بتأمين الأجهزة الذكية (الكاميرات، أجهزة الاستشعار، الساعات الذكية)، فغالباً ما تكون ضعيفة أمنياً وتستخدم كـ "جسور" لاختراق الشبكات الكبرى.
- الأمن السيراني المعتمد على الذكاء الاصطناعي: (AI-Driven Security)
 - باستخدام خوارزميات "التعلم الآلي" للتنبؤ بالهجمات قبل وقوعها من خلال تحليل السلوك غير الطبيعي في الشبكة².
- أمن الهوية والوصول: (IAM - Identity and Access Management)
 - التحول من كلمة السر التقليدية إلى "المصادقة متعددة العوامل (MFA)" والبصمات البيومترية.
 - مبدأ "الثقة الصفرية: (Zero Trust)" يقتضي عدم الثقة بأي مستخدم حتى لو كان داخل الشبكة، وطلب التحقق باستمرار.

¹ د. خالد ممدوح إبراهيم، أمن المعلومات في ظل الحكومة الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2021.

² Ross Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 3rd Edition, Wiley, 2020.

- أمن العمليات: (Operational Security - OPSEC) و يتعلق بكيفية إدارة المخاطر واتخاذ القرارات الأمنية أثناء العمل اليومي، لمنع تسريب المعلومات الحساسة عبر الخطأ البشري.

- أمن الأجهزة المحمولة: (Mobile Security) من خلال تأمين الهواتف والأجهزة اللوحية التي أصبحت أداة العمل الأساسية، وحمايتها من التطبيقات الخبيثة وشبكات Wi-Fi العامة غير الآمنة.

الامن السيبراني يقوم على فكرة الأمن الاستباقي، هذا الاخير ليس مجرد جدران حماية بل هو منظومة وقائية ودفاعية في نفس الوقت تعتمد على ثلاث محاور رئيسية¹:

- الاستخبارات التهديدية Threat intelligence أو الهجوم السيبراني الإستباقي: من خلال جمع البيانات من الويب والمصادر المفتوحة للتنبؤ بالهجمات قبل وقوعها باستخدام مثلاً "الديدان البيضاء" وهي برامج قادرة على اكتشاف التطبيقات الضارة وتدميرها، كما تقوم أيضا بتدمير أدوات وبرمجيات القراصنة، وهو ما يساعد في إحباط مخطط الهجمات نفسها، وتحديد هوية ومصدر الهجمة، بما يمكن من إطلاق هجمة إلكترونية مضادة فيما يعرف بـ "الاختراق العكسي (back-Hack)"

- الكشف المبكر للهجمات في وقتها الحقيقي: او ما يسمى بالتحليل السلوكي باستخدام الذكاء الاصطناعي حيث تقوم الخورزميات بمراقبة السلوك الطبيعي للمستخدمين والانظمة وتنبيه المسؤولين عند وجود اي انحراف بسيط قد يشير الى محاولة اختراق ، ويتم ذلك من خلال استخدام حساسات على الشبكات والبرامج والتطبيقات، بالإضافة إلى توظيف المعلومات الاستخباراتية لرصد أي نشاط غير طبيعي قد يصنف على أنه هجمات سيبرانية، وبداية مواجهتها واحتواءها قبل أن تبدأ نشاطها في النظم المستهدفة.

-تكتيكات الخداع Deception technology وهو ما يتحقق عن طريق إخفاء هويات الأهداف الاستراتيجية على الأنترنت وتضليل الخصم أثناء محاولة الوصول إليها أو اختراقها، من خلال أدوات التمويه والخداع وتغيير ملامح الأهداف ، بما يساعد على تضليل الخصم وتشيت الانتباه عن الهدف الرئيسي خاصة بالنسبة للمؤسسات الضخمة

¹ Allison Cerra, op.cit, p45

الاقتصادية والدول كاستخدام المصائد الرقمية لإلهاء المهاجمين وكشف أساليبهم قبل وصولهم للبيانات الحقيقية¹.

خاتمة:

لم يعد الانتقال من النظم التقليدية الى البيئة السحابية والفضاء الافتراضي خيارا ترفيميا بل اصبح ضرورة للبقاء والمنافسة، هذا الانفتاح الرقمي الواسع ادى الى نشوء مساحات شاسعة من الضعف التقني مما جعل المعلومات عرضة لاعتداءات مختلفة، من هنا برز للوجود مفهوم امن المعلومات كضامن لاستمرارية هذا التحول مع حماية الخصوصية والسيادة الرقمية.

ولقد تعرضنا في هذا البحث الى تأثير التحول الرقمي على مفهوم الامن المعلوماتي حيث نقله من مجرد وسيلة للدفاع وحماية خصوصية فردية الى نظام شامل وقائي وردعي ومهاجم في ذات الوقت مسؤولة عنه الدول، ويمكن ان نلخص أهم نتائج البحث في النقاط التالية:

- تلازم الأمن والتحول: الأمن المعلوماتي هو "صمام الأمان" للتحول الرقمي، فبقدر ما يكون هذا الصمام متينا وحديثا، بقدر ما تكون مسيرة الرقمنة آمنة ومستدامة.
- الركائز الأساسية للأمن المعلوماتي ثلاثة وتدعى (الثالوث الأمني) وهي:
 - السرية: ضمان أن المعلومات لا يطلع عليها إلا الأشخاص المخولون بذلك فقط.
 - السلامة أو التكامل: التأكد من أن البيانات لم يتم تعديلها أو العبث بها أثناء تخزينها أو نقلها.
 - التوفر: ضمان بقاء المعلومات والأنظمة متاحة للمستخدمين عند الحاجة إليها، وحمايتها من الهجمات.

¹ أحمد عادل الخفاجي، التحول الرقمي وأثره على مبادئ أمن المعلومات: دراسة تحليلية، المجلة العربية للمعلوماتية الأمنية، جامعة نايف العربية للعلوم الأمنية، العدد 05، 2021.

- التحول نحو الاستباقية: انتقلت الاستراتيجية الوطنية من مرحلة "رد الفعل" بعد وقوع الهجوم إلى مرحلة "الدفاع الاستباقي" من خلال تفعيل دور الهيئات السيادية ومراكز الاستجابة للطوارئ (CERT)
- بناء على التطورات العالمية في مجال الأمن المعلوماتي والتحول الرقمي، يمكن صياغة مجموعة من التوصيات الاستراتيجية والتقنية التي تهدف إلى بناء بيئة رقمية صلبة ومستدامة.
- تبني نموذج الثقة الصفري: وهذا ما يدفع بالدول إلى سن تشريعات تضمن الثقة في المعاملات الرقمية.
- الاستثمار في المرونة السيبرانية و عدم الاكتفاء بأنظمة الوقاية، بل التركيز على وضع خطط لاستمرارية الأعمال وضمان القدرة على التعافي السريع من الكوارث الرقمية وتطوير أنظمة التنبؤ بالاعتداءات.
- توطين البيانات الحساسة: تخزين البيانات الاستراتيجية في مراكز بيانات محلية أو سحابة خاصة لضمان السيادة عليها من جهة وحفظ نسخ عنها إذا ما تم الاعتداء عليها من جهة أخرى .
- تفعيل المصادقة متعددة العوامل: جعل استخدام أكثر من وسيلة للتحقق معياراً إجبارياً (مثل كلمة السر + رمز على الهاتف) .
- التحديث التلقائي والترقيع الفوري: وضع بروتوكولات صارمة لتحديث البرمجيات والأنظمة فور صدور التحديثات الأمنية لسد الثغرات التي يستغلها المهاجمون.
- هندسة الوعي الأمني: تحويل الأمن المعلوماتي من "مسؤولية قسم التقنية" إلى "ثقافة مؤسسية" من خلال تدريبات دورية للموظفين على اكتشاف هجمات الهندسة الاجتماعية والاصطياد الإلكتروني.
- دمج الذكاء الاصطناعي في الدفاع: استخدام تقنيات تعلم الآلة لتحليل كميات ضخمة من البيانات واكتشاف الأنماط المشبوهة التي قد تعجز الأنظمة التقليدية عن رصدها.
- الأمن منذ التصميم: إلزام المطورين بدمج المعايير الأمنية في المراحل الأولى لبناء أي نظام أو تطبيق، بدلاً من إضافتها كطبقة حماية لاحقة.

في الاخير نقول أن أمن المعلومات ليس "مشروعاً" له تاريخ انتهاء، بل هو عملية مستمرة تتطلب التحديث الدائم لمواكبة المهاجمين الذين يطورون أدواتهم بصفة يومية دائمة ومستمرة.

قائمة المصادر والمراجع

المصادر:

قانون رقم 04-18 مؤرخ في 10 ماي 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، الجريدة الرسمية عدد 27 الصادرة في 13 ماي 2018.

المراجع:

باللغة العربية:

الكتب:

- إيهاب خليفة، مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي، العربي للنشر والتوزيع، القاهرة، 2019.
- حامد قشقوش هدى، الحماية القانونية للتجارة الإلكترونية، دار النهضة العربية، مصر، 2000.
- حسن طاهر داود، الحاسب وأمن المعلومات، معهد الإدارة العامة، السعودية، 2000.
- خالد بن سليمان الغنبر و د. محمد بن عبد الله القحطاني، أمن المعلومات، مكتبة الملك فهد الوطنية، الرياض، المملكة العربية السعودية، 2013.
- خالد ممدوح ابراهيم، أمن الجريمة الالكترونية، الدار الجامعية، مصر، 2005.
- رشيدة بوكر، جرائم الإعتداء على نظم المعالجة الآلية في التشريع الجزائري و المقارن، منشورات الحلبي الحقوقية، لبنان، 2012.
- عادل عبد الصادق، الفضاء السيبراني: قضايا الصراع والتعاون في العلاقات الدولية، المركز العربي للبحوث والدراسات، القاهرة، 2020.
- د/ محمد أمين الرومي، جرائم الحاسب والإنترنت: الجريمة المعلوماتية في ضوء القواعد القانونية والتقنية، دار المطبوعات الجامعية، الإسكندرية، مصر، 2019.
- محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، مصر، 2004.
- د. محمد منذر، مفهوم الأمن: دراسة في الأبعاد والمستويات، المؤسسة الجامعية للدراسات، بيروت، 2014.

- محمود محمد أبو فروة، الخدمات البنكية الالكترونية عبر الانترنت، دار الثقافة، الأردن، 2009.

- نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، لبنان، 2005.

الرسائل والمذكرات:

-حنين جميل أبو حسين، الإطار القانوني لخدمات الأمن السيبراني، رسالة ماجستير في القانون الخاص ، جامعة الشرق الأوسط، الأردن، 2021.

- سمير حامد، الاستراتيجية الوطنية للأمن السيبراني كمدخل لتعزيز الأمن القومي، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة القاهرة، مصر، 2022.

المقالات العلمية:

-أحمد عادل الخفاجي، التحول الرقمي وأثره على مبادئ أمن المعلومات: دراسة تحليلية، المجلة العربية للمعلوماتية الأمنية، جامعة نايف العربية للعلوم الأمنية، العدد 05، 2021.

-إدريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري ، مجلة مصداقية، المجلد1، العدد1، ديسمبر2019.

-أميرة عبد العظيم محمد عبد الجواد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، مجلد3، عدد 35، 2020 .

-شريفة كلاع، الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني، مجلة الحقوق والعلوم الإنسانية، المجلد15، العدد1، 2022.

-محمد علاء محمد، مقدمة للأمن السيبراني، على الموقع:
<https://www.kotobati.com/> ، تاريخ الاطلاع 2022-09-10.

الوثائق:

- بيان صادر عن اتحاد المصارف الاسلامية في 17-07-2025 ، على الموقع:
<https://uabonline.org/international-> تاريخ الاطلاع:2026-04-12.

باللغة الانجليزية:

-Allison Cerra, Proactive cybersecurity:staying ahead of threats in the age of AI,WILEY,USA, 2025

- Ross Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd Edition, Wiley, 2020.