الحماية الدستورية للأمن السيبراني ودوره في حماية الحق في الخصوصية المعلوماتية

إعداد

الدكتور / عادل السيد محمد علي

مدرس القانون

المعهد العالي للعلوم الإدارية بجناكليس – البحيرة

بريد إلكتروني: adel.esaied@gmail.com

ملخص البحث:

مسألة حماية البيانات الشخصية أصبحت مدرجة فى سلم أولويات الدول عامة، حيث تحظى باهتمامات كبيرة، وتوجب عليها مواكبة دائمة للتطورات المتصلة بمعالجتها ورصدًا معمقًا لآثار هذه العملية. ففي كل يوم تتزايد كمية البيانات الشخصية التي تعالج، ويخلق المزيد من وحدات التخزين، وتبتكر تقنيات وأساليب لجمعها وحفظها واستثمارها.

ونظرًا لارتفاع الهجمات الإلكترونية على هذه البيانات والمعلومات فإن الدول والمؤسسات والشركات تجد نفسها مضطرة لحماية بياناتها ومعلوماتها، بل أصبحت الهجمات والاختراقات السيبرانية تمثل تهديدًا حقيقيًا للأمن القومي للدول.

لذلك، أصبح حماية أمن الفضاء السيبراني من قبل آليات الأمن السيبراني يدخل ضمن أولويات السياسة الخارجية للعديد من الدول وضمن استراتيجيات الأمن القومي لديها، ودفعت التهديدات المتزايدة لأمن الفضاء السيبراني العديد من الدول للعمل على بذل جهود مضنية في استحداث قوانين لمكافحة الجريمة السيبرانية.

وتكمن أهمية البحث في الوقوف على وسائل وآليات الأمن السيبراني في التصدي لاختراق وانتهاك الخصوصية المعلوماتية للأفراد. **وقد استخدمت في البحث** المنهج الوصفي التحليلي، وكذلك المنهج الاستقرائي.

وهديًا على ما تقدم، جاء هذا البحث بعنوان: "**الحماية الدستورية للأمن السيبراني ودوره في حماية الحق في الخصوصية المعلوماتية**"، وتناولته من خلال مقدمة، ومبحثين، وخاتمة.

أما المبحث الأول تناولت فيه: مفهوم الأمن السيبراني ومخاطره وأهدافه وأبعاده، ومفهوم الحق في الخصوصية المعلوماتية وصور الاعتداء عليها.

والمبحث الثاني فقد ذكرت فيه: الحماية الدستورية للخصوصية المعلوماتية والأمن السيبراني، دور الأمن السيبراني في حماية الخصوصية المعلوماتية.

ثم اختتمت بحثي بما توصلت إليه من نتائج وتوصيات.

الكلمات المفتاحية:

الحماية الدستورية- الأمن السيبراني- الخصوصية- الخصوصية المعلوماتية.

Abstract:

The issue of the protection of personal data has become a top priority for countries in general, with great concerns, and must keep abreast of developments related to their processing and in-depth monitoring of the implications of this process. Every day the amount of personal data processed increases, creates more storage units, and creates techniques and methods for collecting, preserving and investing them.

Given the rise in cyber-attacks on such data and information, states, institutions and companies find themselves obliged to protect their data and information, and even cyber-attacks and hacks have become a real threat to countries' national security.

Protecting cyber security by cyber security has therefore become a priority of many States' foreign policy and national security strategies, and growing threats to cyber security have prompted many States to make strenuous efforts to develop laws to combat cybercrime.

The importance of research is to identify the means and mechanisms of cyber security in addressing the infringement and

violation of individuals' information privacy. The analytical descriptive approach, as well as the inductive approach, have been used in research.

This research, entitled "Constitutional Protection of Cyber security and its Role in Protecting the Right to Information Privacy", was designed to provide an introduction, researchers and conclusion.

The first examined the concept of cyber security and its risks, objectives and dimensions, and the concept of the right to information privacy and images of abuse.

The second research mentioned: the constitutional protection of information privacy and cyber security, the role of cyber security in protecting information privacy.

I then concluded my research with my findings and recommendations.

Keywords:

Constitutional Protection – Cyber security – Privacy – Information Privacy.

مقدمة

أحدثت تكنولوجيا المعلومات والاتصالات ثورة هائلة في جميع مناحي الحياة، وزادت هيمنة تكنولوجيا المعلومات والاتصالات على نسق الحياة العامة، وصاحب ظهور الحاسب الآلي والتوسع في استخدام شبكة الإنترنت في مجالات الحياة المختلفة ظهور بعض الآثار السلبية والمخاطر المترتبة على هذا التوسع الكبير؛ إذ كلما زاد الاعتماد على هذه التقنيات في التنمية زادت المخاطر الخاصة بحماية المعلومات والبيانات الشخصية للأفراد.

فمسألة حماية البيانات الشخصية باتت مدرجة في سلم أولويات الدول عامة، حيث تحظى باهتمامات كبيرة، وتوجب عليها مواكبة دائمة للتطورات المتصلة بمعالجتها ورصدًا معمقًا لآثار هذه العملية. ففي كل يوم تتزايد كمية البيانات الشخصية التي تعالج، ويخلق المزيد من وحدات التخزين، وتبتكر تقنيات وأساليب لجمعها وحفظها واستثمارها.

ومما لا ريب فيه، أن جزءًا هامًا منها لا يتعدى كونها بيانات عادية لا ضير من جمعها، لكن الأكيد أن تقنيات المعالجة الحديثة التي يمكن أن تعالجها إلى جانب معلومات أخرى تجعلها جد معبرة، وبالتالي كاشفة ومهددة للحق في الخصوصية.

فالأدوات والبرامج والتطبيقات وشبكات التواصل الاجتماعي، والحوسبة السحابية أصبحت جزءًا أساسيًا من الحياة اليومية لكل مواطن، وأداة لتسهيل عمل الأفراد والأشخاص المعنوية في القطاعين العام والخاص، وحولت تفاصيل الحياة اليومية لكل شخص طبيعي إلى مصدر معلومات، ذي قيمة يعتمد عليها في الاقتصاد الرقمي والخدمات الإلكترونية وتطوير عمل الهيئات دون استثناء. ونظرًا لارتفاع هذه الهجمات الإلكترونية فإن الدول والمؤسسات والشركات تجد نفسها مضطرة لحماية بياناتها ومعلوماتها، بل أصبحت الهجمات والاختراقات السيبرانية تمثل تهديدًا حقيقيًا للأمن القومي للدول؛ لصعوبة اكتشاف تلك الجرائم وإثباتها، وهو الأمر الذي يتطلب معه تضافر الجهود الداخلية والدولية في التصدي لمثل هذه الجرائم.

لذلك، أصبح حماية أمن الفضاء السيبراني يدخل ضمن أولويات السياسة الخارجية للعديد من الدول وضمن استراتيجيات الأمن القومي لديها، ودفعت التهديدات المتزايدة لأمن الفضاء السيبراني العديد من الدول للعمل على بذل جهود مضنية في استحداث قوانين لمكافحة الجريمة السيبرانية، وإنشاء قيادة عسكرية لحماية الفضاء الإلكتروني، وإنشاء هيئات لمواجهة الطوارئ المعلوماتية، واستحداث وحدات للحرب السيبرانية داخل الجيوش العسكرية.

فإن حماية الخصوصية المعلوماتية وحماية أمن الفضاء المعلوماتي أحد حقوق الإنسان الأساسية، وهذه الحقوق مثلها مثل بقية الحقوق تحتاج إلى الحماية، فكان لا بد من تكريس هذه الحقوق دستوريًا ضمن النصوص الدستورية أسوة ببقية حقوق الإنسان، إذ إن الدساتير الديمقراطية تحرص على إيراد هذه الحقوق ضمن نصوصها؛ نظرًا لأهميتها– سواء بنص صريح أم ضمني؛ وذلك لارتباط الحقوق بالحياة الشخصية للفرد؛ لذا أصبح لازمًا وضع حماية دستورية للبيانات والمعلومات الشخصية، من خلال تكريس هذا الحق دستوريًا. وهذا ما فطن إليه المشرع الدستوري بحمايته للحق في الخصوصية المعلوماتية وحماية أمن الفضاء المعلوماتي.

ونظرًا لانتشار المعاملات الإلكترونية اليومية ومشاركة الأفراد لبياناتهم الشخصية مع جهات أخرى– سواء أكانت جهات خاصة أم عامة، أصبح من السهل الاعتداء على تلك البيانات التي يقدمها الفرد سواء لإكمال المعاملات، أو الاشتراك في المواقع الإلكترونية؛ مما يعرض خصوصية حياتهم إلى الانتهاك والاعتداء من قبل الغير، فكان لا بد من تحرك الدول والأفراد من أجل الحفاظ على النتائج والمكتسبات التي تحققت من تطبيق تكنولوجيا المعلومات والاتصالات إلى البحث عن أساليب جديدة تدعم من الخطوط الدفاعية في مواجهة تلك الهجمات، وبحيث تعطي لها حصانة

قوية للوقاية منها، وتسمى تلك الأساليب بإجراءات أو ممارسات أو برامج الأمن السيبراني.

فالأمن السيبراني يُعد الإجراء الأمثل لحماية الأنظمة والشبكات والبرامج من الهجمات السيبرانية أو الإلكترونية الشرسة، حيث تلجأ الدول والمؤسسات والأفراد إلى هذه الممارسات للحفاظ على المعلومات الحساسة ومراكز البيانات والأنظمة المحوسبة الأخرى من المخترقين الذين يقومون بتغييرها أو حذفها أو تدميرها أو ابتزاز أصحابها بها.

ومن ثم، يحظى الأمن السيبراني بأهمية بالغة؛ نظرًا لما يقوم به من دور كبير في حماية الحق في الخصوصية المعلوماتية من الانتهاك أو الاختراق. وتعددت طرق وآليات الحماية التي منحها الأمن السيبراني لحماية الخصوصية المعلوماتية، فهناك الحماية القانونية أو التشريعية، والحماية التقنية، والحماية التنظيمية، والحماية التوعوية، وآليات حماية ذاتية من جانب الأفراد لخصوصيتهم تتمثل في التنظيم الأمثل لإعدادات الخصوصية.

أولًا: أهمية البحث

تكمن أهمية البحث في الوقوف على الحماية الدستورية للأمن السيبراني، وكذلك الحماية الدستورية للحق في الخصوصية المعلوماتية، ودور الأمن السيبراني في حماية الحق في الخصوصية المعلوماتية.

ثانيًا: إشكالية البحث

تتعاظم مشكلة البحث في الوقت الراهن في اختراق الخصوصية المعلوماتية في جميع دول العالم بشكل كبير، وما يترتب عليها من مشكلات اقتصادية واجتماعية وسياسية وتكنولوجية التي تهدد أمن المجتمع، فلا شيء آمن على شبكة الإنترنت، ومن ثم تتمحور مشكلة البحث في الإجابة على التساؤلات الآتية:

- ما معنى الأمن السيبراني والهجمات السيبرانية والخصوصية المعلوماتية؟
- هل حقق الدستور المصري الحماية الدستورية للأمن السيبراني وحماية الحق في الخصوصية المعلوماتية؟
- كيف ساهم الأمن السيبراني في معالجة جريمة انتهاك واختراق الخصوصية المعلوماتية؟

- كيف اهتمت التشريعات الوطنية بالأمن السيبراني في المؤسسات الحكومية والخاصة؟

ثالثًا: منهج البحث

تم استخدام المنهج الوصفي التحليلي، وكذلك المنهج الاستقرائي؛ لمعرفة الحماية الدستورية للحق في الخصوصية المعلوماتية، وكذلك الأمن السيبراني أو الحق في حماية أمن الفضاء المعلوماتي، وكذلك دور وآليات الأمن السيبراني في حماية الحق في الخصوصية المعلوماتية.

رابعًا: الدراسات السابقة

نظرًا لحداثة موضوع البحث فقد وجدت صعوبة كبيرة في إيجاد دراسات سابقة تتناول موضوع البحث بشكل تفصيلي، بل اكتفت هذه الدراسات بعرض أحد أجزاء الموضوع فقط؛ لذلك حاولت في هذا البحث تناول الحماية الدستورية للأمن السيبراني ودوره في حماية الحق في الخصوصية المعلوماتية بشكل أكثر تفصيلًا، نذكر من هذه الدراسات:

١. أميرة عبدالعظيم محمد عبدالجواد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، العدد ٣٥، مجلة الشريعة والقانون، ٢٠٢٠.

٢. أيمن مصطفى أحمد البقلي، حماية الخصوصية المعلوماتية لمستخدمي الإنترنت في مواجهة متطلبات التجارة الإلكترونية، المجلة القانونية، المجلد ٩، العدد ٤، جامعة القاهرة، كلية الحقوق، فرع الخرطوم، ٢٠٢١.

٣. إيناس ممدوح محمد سليمان، دور الأمن السيبراني في مواجهة الإرهاب الإلكتروني، المجلد ٦٤، العدد ٢، مجلة العلوم القانونية والاقتصادية، كلية الحقوق، جامعة عين سمش، يناير ٢٠٢٢.

٤. رؤى سعد القرني، الحماية القانونية للحق في الخصوصية المعلوماتية: دراسة مقارنة، العدد السادس، مجلة كلية الدراسات الإسلامية والعربية للبنات بدمنهور، ٢٠٢١.

٥. عزت عبدالمحسن إبراهيم سلامة، الحق في الخصوصية الرقمية وتحديات عصر التقنية، العدد الأول، السنة ٦٢، مجلة العلوم الاقتصادية والقانونية، كلية الحقوق، جامعة عين شمس، يناير ٢٠٢٠.

٦. ماجدة عبدالشافي خالد منصور، الحماية الدستورية للأمن السيبراني وأثره على النظام العام، المجلد ٤، العدد ٥٧، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنوفية، مايو ٢٠٢٣.

خامسًا: خطة البحث

ينقسم هذا البحث إلى: مقدمة، ومبحثين، وخاتمة، وذلك على النحو الآتي:

- **أما المقدمة فقد اشتملت على:** أهمية البحث، إشكالية البحث، منهج البحث، الدراسات السابقة، خطة البحث.
- **المبحث الأول: مفهوم الأمن السيبراني والخصوصية المعلوماتية.**

<u>وفيه مطلبان:</u>

  - **المطلب الأول:** مفهوم الأمن السيبراني ومخاطره وأهدافه وأبعاده.
  - **المطلب الثاني:** مفهوم الخصوصية المعلوماتية وصور الاعتداء عليها.
- **المبحث الثاني: الإطار الدستوري للخصوصية المعلوماتية والأمن السيبراني ودوره في حماية الخصوصية المعلوماتية.**

<u>وفيه مطلبان:</u>

  - **المطلب الأول:** الحماية الدستورية للخصوصية المعلوماتية والأمن السيبراني.
  - **المطلب الثاني:** دور الأمن السيبراني في حماية الخصوصية المعلوماتية.
- **الخاتمة:** وتشمل: النتائج والتوصيات.
- **المراجع.**

المبحث الأول

مفهوم الأمن السيبراني والخصوصية المعلوماتية

وفيه مطلبان:

- **المطلب الأول:** مفهوم الأمن السيبراني ومخاطره وأهدافه وأبعاده.
- **المطلب الثاني:** مفهوم الخصوصية المعلوماتية وصور الاعتداء عليها.

المطلب الأول

مفهوم الأمن السيبراني ومخاطره وأهدافه وأبعاده

الفضاء السيبراني واحد من قطاع الخدمات التي تشكل قيمة مضافة ودعامة أساسية لأنشطة الحكومات والأفراد على السواء، إلا أن الوجوه المتعددة للأمن السيبراني ومضاعفاتها الخطيرة التي لا تقف عند حدود الإساءة إلى الأفراد والمؤسسات بل تتعداها إلى تعريض سلامة الدول والحكومات، تزيد من مهمة القائمين على الموضوع تعقيدًا وصعوبة، وتستدعي مقاربة شاملة ومتكاملة لجميع التحديات التي يطرحها الفضاء السيبراني، بحيث تأتي الردود والحلول المقترحة ناجعة وفاعلة

في تحقيق الأمن وبناء الثقة في الفضاء السيبراني، من أساسيات تسخير تقنيات المعلومات والاتصالات في مجالات التنمية خدمة للمجتمعات الإنسانية[١].

ومع تراجع مبادئ الأخلاق وضعف البيئة القانونية الحاكمة للمجال الافتراضي أصبحت معايير الأمن من أهم متطلبات المعاملات الإلكترونية، حيث ظهرت العديد من الآثار السلبية للاقتصاد الرقمي على بيئة الأعمال، خصوصًا فيما يتعلق بالأمن المعلوماتي، حيث ظهرت الجرائم الإلكترونية والغش التجاري وانتهاك الخصوصية وسرية المعلومات.

فضلًا عن ذلك، فإن المستثمرين في أي دولة في العالم إذا لم يجدوا من الأنظمة والقوانين ما يواجه الجرائم السيبرانية التي تقوض الصناعات المعلوماتية، وإذا لم يجدوا دعمًا من الدولة، وحضورًا لأجهزتها لتنفيذ تلك الأنظمة والقوانين، فإنهم يبدلوا واجهتهم للاستثمار في هذا المجال وتطويره في مكان آخر، وهو ما يؤثر بالسلب على الاقتصاد[٢].

---

[١] سماح عبدالصبور، الصراع السيبراني: طبيعة المفهوم وملامح الفاعلين، العدد ٢٠٨، المجلد ٥٢، مجلة السياسة الدولية، مؤسسة الأهرام، ٢٠١٧، ص ١٧.

[٢] كامل فتحي كامل خضر، سمر المداح، العلاقة بين الاقتصاد الرقمي وأمن المعلومات: دراسة تطبيقية على عينة من عملاء البنك الأهلي المصري، العدد ٣، المجلة العلمية للاقتصاد والتجارة، ٢٠٢٠، ص ١٣.

لذلك، لا بد من التوقف بداية عند مفهوم الأمن السيبراني وتمييزه عن بعض المصطلحات الأخرى المرتبطة به، والأخطار السيبرانية، وأهميته وأهدافه، وأخيرًا التطرق لأبعاد الأمن السيبراني وما يتعلق به من تحديات، وذلك في أربعة أفرع على النحو الآتي:

- **الفرع الأول: مفهوم الأمن السيبراني والمفاهيم المرتبطة به.**
- **الفرع الثاني: الأخطار السيبرانية.**
- **الفرع الثالث: أهمية وأهداف الأمن السيبراني.**
- **الفرع الرابع: أبعاد الأمن السيبراني.**

الفرع الأول

مفهوم الأمن السيبراني والمفاهيم المرتبطة به

ظهر الأمن السيبراني في ثمانينات القرن الماضي، ليعبر عن ممارسات دقيقة لحماية الشبكات والأجهزة والبيانات من التلف أو الضياع أو السرقة أو الوصول غير المصرح به للبيانات والمعلومات الشخصية، وبذلك فإن الأمن السيبراني يحمي التقنيات الرقمية ومستخدميها من المخاطر الرقمية أو الجرائم المعلوماتية أو الإلكترونية، من ثم، فقد أصبح الأمن السيبراني ركيزة أساسية في كل المنظمات

والمؤسسات بل وحتى الدول لمواجهة الحروب الإلكترونية والجرائم المعلوماتية، وسوف نتناول تعريف الأمن السيبراني في اللغة والاصطلاح، ثم بيان أنواعه وخصائصه، وأخيرًا تمييزه عن بعض المصطلحات الأخرى المرتبطة به، وذلك على النحو الآتي:

أولًا- تعريف الأمن السيبراني في اللغة والاصطلاح:

الأمن السيبراني مركب وصفي من كلمتين: الأمن والسيبراني، ويقتضي بيان معنى المركب توضيح ما تدل عليه أجزاؤه، وعليه سوف نقوم بتعريف الأمن، ثم السيبراني لنصل إلى معنى الأمن السيبراني.

١. تعريف الأمن لغةً واصطلاحًا:

الأمن لغةً: أمِنَ أمنًا، وأمانًا، وأمانة، وأمنًا، وإمنًا، وأمنةً: اطمأن ولم يخف، فهو آمن، وأمِنٌ، وأمين. يقال: لك الأمان، أي: قد آمنتك، وأمِنَ الشر: منه سلم، وأمن فلانًا على كذا: وثق به واطمأن، أو جعله أمينًا عليه. والأمان والأمانة بمعنى واحد، فالأمن ضد الخوف، والأمانة ضد الخيانة، والمأمن: الموضع الآمن، قال تعالى: ﴿**وَعَدَ اللَّهُ الَّذِينَ آمَنُوا مِنْكُمْ وَعَمِلُوا الصَّالِحَاتِ لَيَسْتَخْلِفَنَّهُم فِي الْأَرْضِ كَمَا اسْتَخْلَفَ**

الَّذِينَ مِنْ قَبْلِهِمْ وَلَيُمَكِّنَنَّ لَهُمْ دِينَهُمُ الَّذِي ارْتَضَى لَهُمْ وَلَيُبَدِّلَنَّهُمْ مِنْ بَعْدِ خَوْفِهِمْ أَمْناً﴾[١]، [٢].

والأمن اصطلاحًا: للعلماء محاولات كثيرة في تعريف الأمن، إلا أن تعريفاتهم متباينة في مفرداتها، وغير متفقة في مضامينها؛ فبعضهم عرف الأمن بأنه: الإجراءات والسياسات التي تتخذها الدولة في حدود طاقاتها للحفاظ على كيانها ومصالحها في الحاضر والمستقبل مع مراعاة المتغيرات الدولية[٣].

وعرفه بعض الفقه بأنه: الطمأنينة التي تنفي الخوف والفزع عن الإنسان، فردًا أو جماعة، في سائر ميادين العمران الدنيوي، بل وأيضًا في المعاد الأخروي فيما وراء هذه الحياة الدنيا[٤].

---

[١] سورة النور، جزء من الآية: ٥٥.

[٢] أبو الفضل جمال الدين بن منظور، لسان العرب، الطبعة الأولى، دار الكتب العلمية، لبنان، بيروت، ١٩٩٢، ج ٢، ص ١٤٠؛ مجمع اللغة العربية، المعجم الوسيط، الطبعة الرابعة، مكتبة الشروق الدولية، القاهرة، ٢٠٠٤، ص ٢٨.

[٣] أمين هويدي، الأمن العربي في مواجهة الأمن الإسرائيلي، دار الطليعة للطباعة والنشر، بيروت، لبنان، ١٩٧٥، ص٤٢.

[٤] محمد عمارة، الإسلام والأمن الاجتماعي، الطبعة الأولى، دار الشروق، القاهرة، ١٩٩٨، ص ١٢.

وعُرّف أيضًا بأنه: تلك الحالة من الاستقرار التي يجب أن تشمل المنطقة بعيدًا عن أي تهديد سواء من الداخل أم من الخارج[١].

ويمكن تعريف الأمن بأنه: مجموعة من الإجراءات والسياسات التي تتخذها الدولة لتحقيق حالة من الطمأنينة والاستقرار، ولتحقيق مصالح أفرادها، وحماية كيانها من الأخطار التي تتهددها داخليًا وخارجيًا.

ويتشكل مفهوم الأمن من مقومات أو دعامات ترتكز على تحقيق التنمية الاقتصادية وصون حقوق الإنسان وحرياته، والحكم الراشد والمساواة الاجتماعية وسيادة القانون.

ويضم مصطلح الأمن أربعة مستويات، هي:

أ- **أمن الفرد:** ضد أية أخطار تهدد حياته أو ممتلكاته أو أسرته.

ب-**أمن الوطن:** ضد أي أخطار داخلية أو خارجية للدولة، وهو ما يعبر عنه بالأمن الوطني.

[١] عفاف الباز، الترابط بين مفهوم الأمن القومي العربي والمصالح القومية العربية، القاهرة، ١٩٧٨، ص ٢٧.

ت–**الأمن القطري أو الجماعي:** وهي اتفاق عدة دول في إطار إقليم واحد على التخطيط لمواجهة التحديات التي تواجهها داخليًا وخارجيًا، وهو ما يعرف بالأمن القومي.

ث–**الأمن الدولي:** وهو الذي تتولاه المنظمات الدولية سواء منها الجمعية العامة للأمم المتحدة أم مجلس الأمن الدولي؛ نظرًا لدورهما في الحفاظ على الأمن والسلم الدوليين.

وبناءً على ما تقدم من تعاريف، يُقصد بالأمن بصفة عامة: العنصر الأساسي والركيزة الصلبة التي تقوم عليها المجتمعات، حيث تؤسس قوتها وتضمن سلامتها واستمرارها من خلال توافره فيها، فهو مصطلح ملازم لكل مجالات الحياة، وينقسم إلى: أمن اقتصادي[١]، وأمن فكري[٢]، وأمن بيئي[٣]، وأمن غذائي[٤]، وأمن

[١] يقصد **بالأمن الاقتصادي:** توفير البيئة المناسبة لنمو الأعمال التجارية وزيادة الاستثمار الوطني والأجنبي الذي يعتبر دعامة أساسية للتنمية.

[٢] يقصد **بالأمن الفكري:** حماية فكر المجتمع وعقائده من أن ينالها عدوان أو ينزل بها أذى.

[٣] **الأمن البيئي:** هو الذي يستوجب تحقيقه مشاركة أفراد المجتمع في حماية البيئة من خلال اتباع وسائل تضمن الحصول على بيئة نظيفة وخالية من مصادر التلوث.

[٤] **الأمن الغذائي:** هو الذي يقوم على فكرة العناية بالأطعمة والمنتجات الغذائية داخل المجتمع من أجل منع أية تأثيرات سلبية لتلك الأطعمة على صحة أفراد المجتمع.

شخصي[١]، وأمن علمي، وأمن معلوماتي، وأمن صحي، وأمن سياسي، ومن بين مجالاته في المجال القانوني ما يسمى: بالأمن السيبراني.

فالأمن العام مطلق يحقق طمأنينة النفوس، وتنتشر به الهمم وتنمو به الملكات والطاقات؛ لأن الخوف- وهو المناقض للأمن- يقبض الناس عن مصالحهم، ويحجزهم عن تصرفهم، ويكفهم عن أسباب المواد التي بها قوام أودهم، وانتظام جملتهم[٢].

٢. تعريف السيبراني لغة واصطلاحًا:

السيبراني لغةً: مشتقة من الكلمة اللاتينية سايبر (Cyber)، ومعناها تخيلي أو افتراضي، والسيبر كلمة يجري استخدامها لوصف الفضاء الذي يضم الشبكات العنكبوتية المحوسبة، ومنظومات الاتصال والمعلومات وأنظمة التحكم عن بعد. وتعني: كل ما يتعلق أو يرتبط بالحواسيب وتكنولوجيا المعلومات والواقع الافتراضي، ومنها اشتقت صفة السيبرانية والسيبراني Cybernetics وتعني: علم التحكم

[١] **الأمن الشخصي:** هو الذي يقوم على منع انتشار الجريمة المنظمة والتي أصبحت تستخدم أحدث وسائل التكنولوجيا الحديثة.

[٢] محمد عمارة، مرجع سابق، ص ١٥.

الأوتوماتيكي، أو علم الضبط، كما تعني أيضًا: القيادة أو التوجيه، والذي يعني: علم الاتصالات وأنظمة التحكم الآلي في كل من الآلات والأشياء الحية[١].

والسيبراني اصطلاحًا: تعددت التعاريف التي تناولت مصطلح السيبراني كل حسب الزاوية التي نظر إليها منها، إلا أنها اشتركت في مضمون واحد متقارب في المعنى، وهو استهداف المواقع الإلكترونية والبيانات والحسابات الشخصية، والحقوق والحريات الأساسية للأشخاص من خلال وسائل إلكترونية.

وكلمة سيبراني تطلق على كل ما يتعلق بالشبكات الإلكترونية الحاسوبية، وشبكة الإنترنت، والفضاء السيبراني يعني: الفضاء الإلكتروني (Cyberspace)، وهو يعني كل ما يتعلق بشبكات الحاسوب، والإنترنت، والتطبيقات المختلفة (كالوتسآب، والفيس بوك، وغيرها من مئات التطبيقات)، وكل الخدمات التي يقوم

---

[١] منير البعلبكي، المورد: قاموس إنجليزي عربي، دار العلم للملايين، بيروت، ٢٠٠٤، ص ٢٤٣؛ قاموس أكسفورد على الموقع الآتي: https://en.oxforddictionaries.com/definition/cyber؛ صالح بن علي بن عبدالرحمن الربيعة، الأمن الرقمي وحماية المستخدم من مخاطر الإنترنت، منشور على الموقع الآتي: https://edu.moe.gov.sa/jeddah.

بتنفيذها كتحويل الأموال عبر النت، والشراء أون لاين، وغيرها من آلاف الخدمات في جميع مجالات الحياة على مستوى العالم[١].

وقد عُرف مصطلح السيبراني بأنه: مجموعة من الممارسات التي ترمي إلى حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية أيًا كان نوعها، وهذه الممارسات متنوعة إلى تدابير احتياطية استباقية قبل وقوع الخلل، وعلاجية بعد وقوع الخلل[٢].

٣. تعريف الأمن السيبراني باعتباره مركبًا وصفيًا:

مفهوم الأمن السيبراني من المفاهيم التي لاقت اهتمامًا كبيرًا في الآونة الأخيرة؛ نظرًا لظهور تقنيات تكنولوجية جديدة، واستخدامها بشكل واقع في كافة المنشآت العامة والخاصة.

---

[١] منى عبدالله السمحان، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، العدد ١١١، مجلة كلية التربية، جامعة المنصورة، يوليو ٢٠٢٠، ص ٩.

[٢] حسين بن سليمان بن راشد الطيار، الأمن السيبراني من منظور مقاصد الشارع: دراسة تأصيلية، مجلة جامعة الطائف للعلوم الإنسانية، جامعة الطائف، المملكة العربية السعودية، المجلد ٦، العدد ٢١، ٢٠٢٠م، ص ٢٦٤، منشور على الموقع الآتي:

- https://search.emarefa.net/ar/detail/BIM-1280150.

وقد عرف الأمن السيبراني بأنه: مجموعة القواعد التي يضعها مسؤولو الأمن في أي مكان، والتي يجب أن يتقيد بها جميع الأشخاص الذين يمكنهم الوصول إليها، فهي قواعد وأصول ضبط الاتصال وانتقال المعلومات وتخزينها وحفظها، كما تشمل أمن المواقع وأمن الأنظمة الإلكترونية وعمليات استثمارها إضافة إلى أمن الاتصالات[١].

كما يعرف بأنه: التقنيات والإجراءات التي تهدف إلى حماية أجهزة الكمبيوتر والشبكات والبيانات من الدخول غير القانوني ونقاط الضعف والهجمات المنقولة عبر الإنترنت من قبل الجانحين[٢].

كما يعرف الأمن السيبراني بأنه: مزيج من العمليات والتقنيات تهدف إلى حماية البرامج والتطبيقات والشبكات وأجهزة الكمبيوتر والبيانات من الهجوم، ويشمل الأمن السيبراني: الأمن المادي للشبكات وأجهزة الحاسب الآلي، وأمن غير مادي يتعلق

---

[١] يونس مؤيد يونس، استراتيجية الولايات المتحدة الأمريكية للأمن السيبراني، العدد ٥٥، مجلة قضايا سياسية، كلية العلوم السياسية، جامعة النهرين، بغداد، ٢٠١٨، ص ١، منشور على الموقع الآتي:

- https://search.emarefa.net/ar/detail/BIM-910984.

[2] K. K. Panigrahi, Information Security and Cyber Law , published by tutorials point ,2015 ,p.1.

بالبرامج والمعلومات والبيانات من أي هجوم وأضرار متعمدة والتحكم في الوصول الصحيح للأجهزة والشبكات لحمايتها من الضرر[١].

وذهب بعض الفقه بأنه: عبارة عن وسائل دفاعية من شأنها كشف وإحباط المحاولات التي يقوم بها القراصنة[٢].

وعرفت وزارة الدفاع الأمريكية الأمن السيبراني بأنه: جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية والإلكترونية من مختلف الجرائم، والهجمات، والتخريب والتجسس والحوادث[٣].

وفي التقرير الصادر عن الاتحاد الدولي للاتصالات (ITU) حول اتجاهات الإصلاح في الاتصالات لعام ٢٠١٠-٢٠١١ عرف الأمن السيبراني بأنه: مجموعة الأدوات والسياسات والمفاهيم الأمنية والضمانات الأمنية والمبادئ التوجيهية ونُهُـــج

---

[١] مصطفى إبراهيم سلمان الشمري، الأمن السيبراني وأثره في الأمن الوطني العراقي، مجلة العلوم القانونية والسياسية، المجلد ١٠، ٢٠٢١، ص ١٥٧، منشور على الموقع الآتي:

- https://www.lawjur.uodiyala.edu.iq/index.php/jjps/issue/view/2 .

[2] Richard A. Kemmerer, Cyber security, University of California, Santa Barbara Department of Computer Science, 2003, p 3.

[٣] يوسف بوغرارة، الأمن السيبراني، الاستراتيجية الجزائرية للأمن السيبراني والدفاع في الفضاء السيبراني، المجلد الأول، العدد الثالث، مجلة الدراسات الإفريقية وحوض النيل، المركز الديمقراطي العربي، سبتمبر ٢٠١٨، ص ١٠٧، منشور على الموقع الآتي:

- https://democraticac.de/wp-content/uploads/2018/09.

إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات وسبل الضمان والتكنولوجيات التي يمكن استخدامها في حماية البيئة السيبرانية[١].

وبناءً على ما تقدم، فإن الأمن السيبراني أو المعلوماتي أو الرقمي أو الإلكتروني يعني اتخاذ التدابير اللازمة لحماية الفضاء السيبراني من الهجمات السيبرانية، وذلك من خلال مجموعة من الوسائل المستخدمة تقنيًا وقانونيًا وتنظيميًا وإداريًا في منع الوصول غير المشروع للمعلومات الإلكترونية ومنع استغلالها بطريقة غير قانونية، وبذلك فإنه يهدف إلى الحفاظ على استمرارية الأنظمة والمعلومات المتوفرة بها، وحماية خصوصيتها وسريتها من خلال اتباع التدابير والإجراءات اللازمة لحماية البيانات الشخصية واحترام الحقوق والحريات الأساسية للأفراد.

والأمن السيبراني لا يعترف بالحدود الجغرافية ومن الصعب الاكتفاء باتخاذ إجراءات على المستوى الوطني فقط دون توسيع رقعة التعاون إلى دول إقليمية أخرى.

ثانيًا– أنواع الأمن السيبراني:

١– أمن الشبكات:

أغلب الهجمات التي تحدث تكون عبر الشبكات الإلكترونية، لذلك تم وضع أنظمة أمنية تعمل كصمام أمان للشبكة، وتضمن تلك الأنظمة حلولًا فورية وتحكم

[١] منى عبدالله السمحان، مرجع سابق، ص ١٠.

كامل في عناصر البيانات والوصول للشبكة، حتى تمنع أي هجمات تحاول سرقة أو إتلاف تلك البيانات المخزنة على الخوادم الخاصة بها.

٢- الأمن السحابي:

نظرًا لكون التوجهات الغالبة الآن لمعظم المؤسسات حول العالم هي استخدامها لتكنولوجيا الذكاء الاصطناعي والسحابات التخزينية، أصبح من اللازم تأمين السحابة الرقمية بسبب احتوائها على كمية بيانات هائلة لهذه المؤسسات، وتقدم مجموعة من الشركات المتخصصة في هذا المجال خدمات لحل تلك الأزمة، مثل: Google Cloud و Microsoft Azure.

٣- أمن التطبيقات:

تطبيقات الويب مثل أي شيء آخر متصل مباشرة بشبكات الإنترنت، وبالتالي فمن المنطقي أنها تكون مهددة بالهجمات على أمنها السيبراني، وهذا النوع من الأمن السيبراني يساعد الشركات والمؤسسات باكتشاف البيانات الحساسة التي يجب حمايتها من الهجمات المتوقعة، من خلال برامج مضادات الفيروسات، وجدران الحماية، وعمليات تشفير المعلومات.

٤- أمن إنترنت الأشياء:

رغم أن استخدام أجهزة إنترنت الأشياء، مثل: الأجهزة الذكية وأدوات الذكاء الاصطناعي والمستشعرات الحساسة عبر شبكة عالمية واحدة، يوفر العديد من الفوائد الإنتاجية، إلا أنه يعرض المؤسسات للتهديدات الإلكترونية، يقوم أمن الإنترنت الأشياء بحمايتها من خلال اكتشاف الأجهزة المتصلة وتصنيفها حسب دورها التشغيلي بالإضافة لمدى الصلاحية الممنوحة للوصول إلى قاعدة البيانات، وعند استشعار أي حركة غير مألوفة، يقوم بالتحكم في أنشطة الشبكة ومراقبة أي عملية استغلال لهذه الأجهزة وقت التشغيل والتعامل معها.

٥- أمن المستخدم النهائي:

أمان النقاط النهائية تكون عبارة عن مجموعة من الممارسات التقنية تُستخدم في حماية أجهزة المستخدمين النهائيين من الهجمات السيبرانية التي يكون مصدرها البرامج الضارة وغير المرغوب فيها، مثل أجهزة الحاسوب المكتبي والمحمول، والهواتف المحمولة، التي يستخدمها الموظفون في الولوج لشبكات الشركة والوصول إلى الموارد المتعددة، لذلك تسعى المؤسسات إلى حماية هذه الأجهزة بهدف منع أي محاولة خارجية بالوصول إلى الشبكات وقواعد البيانات المخزنة على خوادم الشركة.

٦- أمن البنية التحتية:

يتم تعريف أمان البنية التحتية للمؤسسات بأنه إجراء أمني يقوم على أساس حماية البنية التحتية الحيوية للنظام والحد من نقاط الضعف في هذه الأنظمة من فساد وتخريب وإرهاب، مثل: اتصالات الشبكة أو مركز البيانات أو الخادم أو مركز تكنولوجيا المعلومات، ويتم وضع خطة طوارئ في حالة استهداف الأنظمة لدى الشركة من قبل مجرمي الإنترنت، وتشمل البنية التحتية الحيوية ما يأتي:

أ. أنظمة الإمداد بالطاقة ونقلها.

ب. إمدادات المياه.

ت. نظام التبريد.

ث. التدفئة ودوران الهواء.

٧- التعافي من حالات الكوارث المتعلقة بالهجمات الإلكترونية أو الأسباب الطبيعية:

التعافي من حالات الكوارث أو استمرارية العمل في ظروف التعافي من الهجمات الإلكترونية، هي عملية استئناف الأعمال بعد حدوث تخريب في قواعد البيانات،

واعتمادًا على حجم الشركة ونطاقها وأعمالها، يتم تعيين خطط مختلفة لمساعدة الموظفين على التواصل والاستمرار في أداء وظائفهم في حالة حدوث الهجوم.

٨- أمن المعلومات والبيانات:

أمن المعلومات هو عملية تصميم ونشر الأدوات الخاصة بحماية المعلومات الهامة من التدمير أو التعطيل أو التغيير، فهو العامل الحاسم في تأمين الأمن السيبراني، تم تصميمه خصيصًا بهدف الحفاظ على سرية وسلامة وتوافر بيانات العمل، وضمان أن التطبيقات والأنظمة المصرح لها فقط هي من يمكنها الوصول إلى معلومات معينة، كما أن له دور محوري حيث يراقب ويحقق في السلوك الضار المحتمل، محاولة منه لاحتواء التهديدات والاستجابة الفورية للحوادث مع الحفاظ على الأدلة للمقاضاة المحتملة.

٩- الأمان المالي:

يظن البعض أن الأمن السيبراني وأمن البيانات غير مرتبطين بالدورة المحاسبية، ولكن بسبب تهديدات القرصنة على البيانات المالية الخاصة بالشركة والتي يمكن أن تشتمل على أخطاء والخرق الغير مقصود للبيانات، تم إنشاء نظام الأمان المالي وإعطاء حلولًا مبتكرة في حالة تم الهجوم على قواعد البيانات من قبل مجرمي

الإنترنت، وحماية البيانات من التهديدات والانتهاكات المالية التي تهدد سبل العيش ونمو الأعمال والعلاقات مع العملاء وغير ذلك[١].

ثالثًا- خصائص الأمن السيبراني:

للأمن السيبراني مجموعة من الخصائص التي تميزه عن غيره من المجالات، أهمها:

١- الثقة وعدم الثقة:

يمتلك جدار الحماية الخاص بنظام الأمن السيبراني بما يشبه مرشح إلكتروني لنوع وطبيعة البرامج والتقنيات المسموح بتفعيلها، بحيث يسمح بمرور البرامج التي بالفعل تمتلك الثقة من المستخدم وكذلك المتجر الإلكتروني وتم التأكد من أمان استخدامها، ومنع البرامج الخبيثة من التطفل أو استغلال الثغرات.

يمكن ترجمة فلسفة أمن المعلومات في هذه النقطة كون الأمن السيبراني يتعامل مع كافة البرامج كونها برامج غير جديرة بالثقة، حتى يتم السماح لها من قبل

[١] بحث بعنوان: كل ما ترغب في معرفته عن الأمن السيبراني: مفهومه وخصائصه وأشهر أنواع التهديدات فيه، بتاريخ ٢٠٢٣/١/١، منشور على الموقع الآتي: https://www.e3melbusiness.com/blog/cyber-security.

المستخدم والتأكد من أمانها من خلال مصداقيتها في المتاجر الإلكترونية، فيسمح بمرور ما تم التأكد من سلامته، ويمنع المصادر المجهولة من اختراق النظام.

٢- الحماية من التهديدات الداخلية:

من أهم خصائص الأمن السيبراني هو حماية الجهاز من التهديدات الداخلية والتي قد تتم بناءً على قلة ثقافة المستخدم أو جهله بمجال أمن المعلومات، وفيه قد يقوم بالسماح ببرامج مجهولة المصدر أن يتم تفعيلها أو أن يقوم باستخدام أدوات تمس أمنه الشخصي أو حساسية مشاركة ما يملكه من معلومات، أو تحتوي إحدى الأدوات التي يقوم باستخدامها بفيروس خبيث لا يجب أن يحتوي نظامه عليه، حينها يقوم الأمن السيبراني بسرعة تنبيه الفرد أو المؤسسة بالخطر التي تواجهه ويقوم بمنع حدوث هذا الإجراء في أسرع وقت.

٣- الحماية من التهديدات الخارجية:

تمثل خاصية الحماية من التهديدات الخارجية أهم صفات الأمن السيبراني، حيث يتم فيها بناء جدار حماية قادر على تصفية المخاطر الخارجية التي يسفر عنها التعامل مع العالم الرقمي، بداية من مخاطر الرسائل الإلكترونية الخطرة أو الروابط

الخبيثة أو الفيروسات أو معالجة الضعف في النظام أو الثغرات التي قد يستغلها طرف ثالث في السيطرة والتحكم.

٤- الرؤية الشاملة:

تقوم الأدوات الخاصة بالأمن السيبراني على منح مستخدميها- أفراد أو شركات- رؤية شاملة على ما يحتويه أنظمتهم من نقاط قوة وضعف، بحيث يمكنهم معرفة الثغرات التكنولوجية والعمل على حلها بأسرع وقت، مع منحهم اقتراحات تخص الطريقة المثالية لمنع تكراره مرة أخرى.

٥- المراقبة المستمرة:

يقوم الأمن السيبراني على خاصية المراقبة المستمرة، حيث لا يقوم جدار الحماية الخاص به بالعمل لمرة واحدة أو في ساعات معينة، بل النظام يعمل طوال الوقت بهدف اكتشاف أي خلل بمجرد وجوده والعمل على سرعة إصلاحه ومنعه من إحداث أي ضرر والحفاظ على أمن المعلومات والأمن الخاص بالمستخدم لأطول فترة ممكنة.

٦- الامتثال للسياسات والقوانين:

الهدف من الأمن السيبراني في المقام الأول هو الحفاظ على سرية وخصوصية البيانات والمعلومات، بالإضافة إلى مكافحة الفيروسات الضارة بجميع أنواعها، ولكي يتم تحقيق هذا الهدف بفعالية لا يجب أن يتم استغلال الصلاحيات التي تُمنح لمحترفيه في سبيل اختراق القاعدة التي من أساسها تم إنشائه.

لذلك، تعد خاصية الامتثال للقوانين والسياسات التشريعية الخاصة بأمن المعلومات واحدة من أهم خصائص الأمن السيبراني، حيث لا يتاح لمصادر خارجية الاطلاع عما يتم مشاركته من معلومات وبيانات حساسة، أو إساءة استغلالها بأي صورة ممكنة، وتتنوع هذه القوانين طبقًا لنوع وطبيعة المجال الذي يتم فيه تطبيق الحماية السيبرانية.

٧- التنوع:

يجب أن يمتلك النظام الخاص بالأمن السيبراني حلولًا مجمعة تتعلق بالتعامل مع التهديدات السيبرانية، بحيث لا يكون النظام مفعل للحماية من نوع معين من

التهديدات والسماح بأخر، بل عليه أن يحلل ويكتشف ويتعامل ويمنع كل أنواع الهجمات الممكنة والتي تشكل تهديدًا على سلامة وأمن المعلومات[١].

ثالثًا- تمييز الأمن السيبراني عن بعض المصطلحات الأخرى المرتبطة به:

هناك العديد من المفاهيم والمصطلحات الأخرى المرتبطة بالأمن السيبراني، والتي من أهمها:

١. **أمن المعلومات:** يعرف أمن المعلومات بأنه: نظام حماية المعلومات الرقمية، ويمكن من خلاله تشفير البيانات، وتوفير الشبكات والبنية التحتية التي تحتوي على معلومات شخصية، ومعلومات مالية، وبيانات خاصة بالشركات، وتكون كلها محمية بشكل مكثّف ضد أي اختراقات[٢].

بالرغم من التشابه الكبير بين الأمن السيبراني وأمن المعلومات في أن كلاهما ضابط حماية ضد المعلومات والبيانات التي سرقت، إلا أن هناك نقاط اختلاف جوهرية بينهما في المعلومات غير الإلكترونية، فأمن المعلومات يهتم بأمن

---

[١] يراجع في ذلك: خالد ظاهر عبدالله جابر السهيل المطيري، دور التشريعات الجزائية في حماية الأمن السيبراني بدول مجلس التعاون الخليجي، العدد الثامن والثلاثون، مجلة البحوث الفقهية والقانونية، جامعة الأزهر، كلية الشريعة القانون بدمنهور، يوليو ٢٠٢٢، ص ١٠٠٦.

[٢] أميرة عبدالعظيم محمد عبدالجواد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، العدد ٣٥، ٢٠٢٠، ج ٣، ص ٣٨٨.

المعلومات الفيزيائية "الورقية"، بينما لا يهتم الأمن السيبراني بذلك، فالعلاقة بين أمن المعلومات والأمن السيبراني تتقاطع من حيث الاهتمام بأمن المعلومات الموجودة بالسايبر، ويختلفان فيما تبقى من الاهتمامات[١].

كما يختلفان أيضًا في وظيفة كل منهما، فيتعامل الأمن السيبراني مع التهديدات التي قد تكون موجودة أو غير موجودة في عالم الإنترنت مثل حماية حسابات الوسائط الاجتماعية الخاصة، والمعلومات الشخصية، وما إلى ذلك، بينما يتعامل أمن المعلومات بشكل أساسي مع أصول المعلومات ونزاهتها وسريتها وتوافرها[٢].

٢. **الفضاء السيبراني Cyberspace:** عرفته الوكالة الفرنسية لأمن أنظمة الإعلام (ANSSSI)– وهي وكالة حكومية مكلفة بالدفاع السيبراني الفرنسي– بأنه: فضاء التواصل المشكل من خلال ربط البنى العالمية لمعدات المعالجة الآلية للمعطيات الرقمية. فهو بيئة تفاعلية حديثة، تشمل عناصر مادية وغير مادية، مكوّن من مجموعة من الأجهزة الرقمية، وأنظمة الشبكات والبرمجيات،

---

[١] مصطفى الطيب، مدونة العلوم، أمن المعلومات، الفرق بين الأمن السيبراني وأمن المعلومات، بحث منشور على الموقع الآتي: **https://www.oolom.com.**

(٢) الفرق بين الأمن السيبراني وأمن المعلومات، بحث منشور على الموقع الآتي: **http://www.computersciencedegreehub.com.**

والمستخدمين سواء مشغلين أم مستعملين. كما أن هناك من عرف الفضاء السيبراني بوصفه الذراع الرابعة للجيوش الحديثة[١].

وبذلك فالفضاء السيبراني هو فضاء افتراضي يضم العديد من المجتمعات الموزعة على نحو غير متساوٍ باستخدام بيئة تقنية الإنترنت في المقام الأول، حيث يستفيد المواطنون والمؤسسات من تكنولوجيا المعلومات والاتصالات في تفاعلاتهم من الشبكة المترابطة من البنى التحتية لتكنولوجيا المعلومات، والتي تشمل الإنترنت وشبكات الاتصالات السلكية واللاسلكية والنظم الحاسوبية والمعالجات المدمجة وأجهزة التحكم[٢].

٣. **الجريمة السيبرانية:** مجموعة الأفعال والأعمال غير القانونية التي تتم عبر معدات أو أجهزة إلكترونية أو شبكة الإنترنت أو تبث عبرها محتوياتها، وهي ذلك النوع من الجرائم التي تتطلب الإلمام الخاص بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها. فهي الجريمة المتصلة باستخدام الكمبيوتر، أي تصرف غير قانوني، يرتكب باستخدام

---

[١] منى عبدالله السمحان، مرجع سابق، ص ١٠.

[٢] الأمن السيبراني منهج مرجعي عام، الدفاع الوطني: مكتب القائد، أكاديمية الدفاع الكندية، ب Forces Station 17000، كنجستون، B4 K7 K O7.

تقنيات المعلومات والاتصالات، بقصد السيطرة على نظام الدولة الإلكتروني[١].

٤. **الهجمات السيبرانية:** يمكن تعريفها بأنها: فعلًا يقوض من قدرات ووظائف شبكة الكمبيوتر لغرض قومي أو سياسي، من خلال استغلال نقطة ضعف معينة تمكن المهاجم من التلاعب بالنظام[٢].

٥. **الردع السيبراني:** يعرف بأنه: منع الأعمال الضارة ضد الأصول الوطنية في الفضاء والأصول التي تدعم العمليات الفضائية. يقوم الردع السيبراني على ثلاثة مرتكزات في مجال استراتيجية الدفاع، متمثلة في: مصداقية الدفاع، بتوافر أنظمة نسخ احتياطية، والقدرة على الانتقام؛ وذلك بتكبد المهاجم ضررًا أكثر من المدافع، والرغبة في الانتقام، فالقدرة على الانتقام لا تكفي وحدها[٣].

---

(1) Catota, Frankie E ؛Morgan1, M. Granger and Douglas C. Sicker ، Cybersecurity education in a developing nation :the Ecuadorian environment ،Journal of Cybersecurity, 00(0), 2019, 1–19 doi: 10.1093/cybsec/tyz001.

(2) Matthew C. Waxman, "Cyber-Attacks and the Use of Force, The Yale Journal of International،Back to the Future of Article 2 (4), Vol. 36,2011,p 423.

(٣) يوسف بوغرارة، مرجع سابق، ص ١٠٧.

الفرع الثاني

الأخطار السيبرانية

لقد أدى التوسع في استخدام الفضاء السيبراني إلى ظهور العديد من المخاطر التي تواجه المجتمع في مختلف المجالات، وقد حددت الاستراتيجية الوطنية للأمن السيبراني ٢٠١٧-٢٠٢١ أهم التحديات والأخطار التي قد تواجه الأمن السيبراني فيما يأتي:

أولًا- خطر اختراق وتخريب البنى التحتية للاتصالات وتكنولوجيا المعلومات:

ظهرت أنماطًا جديدة خطيرة للغاية من الهجمات السيبرانية تستهدف إعاقة الخدمات الحيوية، وكذلك نشر برمجيات خبيثة وفيروسات لتخريب أو تعطيل البنى التحتية للاتصالات وتكنولوجيا المعلومات ونظم التحكم الصناعية الحيوية وخاصة في المرافق الهامة (منشآت الطاقة النووية والبترول والغاز الطبيعي والكهرباء والطيران والنقل بأنواعه وقواعد البيانات والمعلومات القومية والخدمات الحكومية والرعاية الصحية والإسعاف العاجل وغيرها)، وذلك عبر عدة قنوات تشمل الشبكات اللاسلكية والذاكرة النقالة بالإضافة إلى القنوات الأخرى الشائعة (البريد الإلكتروني ومواقع الإنترنت والشبكات الاجتماعية وشبكات الاتصالات السلكية)، مما يؤثر

تأثيرًا ملموسًا على البنى التحتية لتلك المنشآت والمرافق وعلى الخدمات والأعمال المرتبطة بها، وقد ثبت عمليًا أنها ليست بمنأى عن التعرض للهجمات السيبرانية الشرسة حتى لو كانت غير متصلة بالإنترنت[١].

ثانيًا- خطر سرقة الهوية الرقمية والبيانات الخاصة:

تعد سرقة الهوية الرقمية من أخطر الجرائم التي تهدد مستخدمي الإنترنت ومستقبل الخدمات الإلكترونية، حيث قد تتعرض البيانات الشخصية للمستخدم إلى السرقة بهدف انتحال شخصيته والاستيلاء على ممتلكاته وأمواله أو للزج باسمه في تعاملات مشبوهة أو غير قانونية. وعادة ما يستعين سارق الهوية بمعلومات موجودة بالفعل على الإنترنت، وبخاصة على مواقع شبكات التواصل الاجتماعية والمهنية المفتوحة أو قواعد البيانات والمعلومات القومية والشبكات الخاصة بالخدمات الحكومية وخدمات الضمان الاجتماعي وشبكات الرعاية الصحية ومواقع التجارة الإلكترونية والأسواق الافتراضية وشبكات المدفوعات الإلكترونية والصرافات الآلية وبورصة الأوراق المالية، فضلًا على أنه قد تتعرض الأدوات والأنظمة المستخدمة في إجراء المعاملات الإلكترونية للسرقة أو التخريب؛ مما

[١] الاستراتيجية الوطنية للأمن السيبراني ٢٠١٧-٢٠٢١.

يشكل خطرًا كبيرًا على مصالح المستخدمين ومستقبل الخدمات الإلكترونية وقد تؤثر الهجمات الموسعة على القطاع المالي الوطني بوجه عام. كما قد تتعرض البيانات الخاصة بالمؤسسات العامة والشركات للسرقة مما يكبدها خسائر فادحة مادية وأدبية، فضلًا عن الإضرار بسمعتها وخسارتها لعملائها وأصولها الأدبية؛ مما قد يضر بالاقتصاد الوطني بوجه عام[١].

ثالثًا- خطر الإرهاب والحرب السيبرانية:

تزداد صعوبة توفير الأمن زيادة كبيرة في عالم بات يعتمد وبشكل متنامي على التكنولوجيا في كافة مناحي الحياة، وقد برهنت المجموعات الإرهابية على درايتها وسرعة تمكنها من التعامل مع تشكيلة عريضة من ابتكارات الاتصالات والتواصل الجديدة، من أبعد أركان الشبكة المظلمة إلى منصات التواصل الاجتماعي الشائعة المتاحة للجميع. وتسمح هذه الوسائل بالانتشار السريع للأفكار والتكتيكات والاستراتيجيات بوتيرة لم تكن ممكنة خلال العقود الماضية، ويضاف إلى ذلك استغلالها لنظم الرسائل المشفرة التي تعقد الجهود الرامية إلى تعقب الإرهابيين المشتبه فيهم، أو تحديد شركائهم وشبكاتهم واستراتيجياتهم[٢].

---

[١] الاستراتيجية الوطنية للأمن السيبراني ٢٠١٧-٢٠٢١.

[٢] سجان م. غوهيل، بيترك فوستر، المنهج المرجعي لمكافحة الإرهاب، الناتو، ٢٠٢٠، ص ٥.

انتشرت مؤخرًا نوعية خطيرة من الهجمات والجرائم السيبرانية تعتمد على تقنيات متقدمة كالحوسبة السحابية والذكاء الاصطناعي وإنترنت الأشياء، وأجهزة تنصت على شبكات الاتصال (السلكية واللاسلكية)، وبرمجيات لفك شفرة ولاختراق لأنظمة الشبكات والحاسبات وقواعد البيانات، وبرمجيات لتشفير العمليات المشبوهة، وبرمجيات خبيثة لاختراق أنظمة أمن الشبكات والحاسبات لتسخيرها في القيام بعمليات إجرامية وتعاملات مشبوهة دون علم أصحابها فيما يسمى بالشبكات الآلية، حيث يمكن أن تضم شبكة آلية واحدة عشرات أو مئات الآلاف أو ملايين من الحواسب أو الأجهزة المتصلة بالإنترنت (إنترنت الأشياء) التي يمكن استخدامها لشن هجمات متنوعة، مثل الهجمات الموزعة لإعاقة الخدمات على شبكات ومواقع مستهدفة لأغراض إجرامية كالتخريب والإرهاب والتهديد والترهيب والابتزاز. وفي حين أنه من المرجح أن تطوير الفيروسات المعقدة والشرسة يتم

يعتبر مفهوم إنترنت الأشياء IoT (Internet of Things) الجيل الجديد المتطور والمتنامي في شبكة الإنترنت والذي يزيد من قدرة الأشياء المادية والأدوات والأجهزة المختلفة التي تتميز بعنوان IP مخصص لها من الاتصال بشبكة الإنترنت وتنظيم عملية التفاهم بين الأشياء المادية المترابطة مع بعضها والمتصلة عبر بروتوكول الإنترنت. يمكّن إنترنت الأشياء الإنسان من التحكم بشكل فعل وسهل بالأشياء عن قرب وعن بعد، فيستطيع المستخدم مثلًا تشغيل محرك سيارته والتحكم فيها من جهازه الحاسوبي. يمكن الرجوع في ذلك إلى إنترنت الأشياء على الموقع الآتي: **https://ar.wikipedia.org/wiki/.**

على مستوى متقدم ويستلزم منظومة خبرات مركبة لا تتوافر إلا في الدول المتقدمة تقنيًا، وذلك لأغراض استراتيجية وحربية يمكن لتلك الدول استخدامها بدلًا من (أو إلى جانب) الهجمة العسكرية التقليدية فيما يسمي بالحروب السيبرانية، إلا أنه قد بدأ بالفعل نقل هذه الأنماط واستنساخها من قبل التنظيمات الإرهابية والتشكيلات العصابية الدولية للاستخدام في العمليات الإرهابية وفي الجرائم المنظمة وفي تهديد وتعطيل البنى التحتية للاتصالات والمعلومات، وبالتالي يتوقع العديد من الخبراء في مجال الأمن السيبراني تنامي انتشار الهجمات السيبرانية الشرسة في الفترة القادمة[١].

وأخيرًا، لكي يتمكن الأشخاص من الوقاية من الهجمات أو التهديدات السيبرانية أو كشفها يجب القيام بإعداد عدد من الإجراءات التقنية المتطورة التي تساعد في اكتشاف هذا النوع من الهجمات قبل الإضرار أو الوقوع ضحيتها.

[١] الاستراتيجية الوطنية للأمن السيبراني ٢٠١٧-٢٠٢١.

الفرع الثالث

أهمية وأهداف الأمن السيبراني

أولًا- أهمية الأمن السيبراني:

يشكل الأمن السيبراني جزءًا أساسيًا من أي سياسة أمنية وطنية، فيعتبر الأمن السيبراني من أولويات الدول للدفاع عن سياسة الوطن، خاصة ما يتعلق بالجانب الوقائي للبيانات والمعلومات، والاتصالات المختلفة، وتتمثل أهمية الأمن السيبراني فيما يأتي:

١. حماية أمن واقتصاد الوطن من مخاطر الهجمات السيبرانية.

٢. حماية الأفراد من انتهاكات الخصوصية والسرية ومختلف أنواع البيانات الحساسة والمهمة من تعرضها للسرقة أو الإتلاف.

٣. زيادة الوعي لدى كافة شرائح المجتمع بمهددات الأمن السيبراني.

٤. الحفاظ على المعلومات وسلامتها وتجانسها، وذلك بكف الأيادي من العبث بها وتحقيق وفرة البيانات وجاهزيتها عند الحاجة إليها[١].

[١] منى عبدالله السمحان، مرجع سابق، ص ١٢.

٥. حماية الأجهزة والشبكات ككّل من الاختراقات لتكون درعًا واقيًا للبيانات والمعلومات.

٦. استكشاف نقاط الضعف والثغرات في الأنظمة ومعالجتها.

٧. استخدام الأدوات الخاصة بالمصادر المفتوحة وتطويرها لتحقيق مبادئ الأمن السيبراني.

٨. توفير بيئة عمل آمنة خلال العمل عبر الشبكة العنكبوتية.

وتنبع أهمية الأمن السيبراني من ثلاثة محاور رئيسة، هي:

- **السرية:** أي التحكم في الوصول إلى البيانات وإتاحتها لمن يسمح لهم فقط.
- **السلامة:** الحفاظ على سلامة البيانات والمعلومات وحمايتها من الهجمات التخريبية أو السرقة.
- **الجاهزية:** جاهزية جميع الأنظمة والخدمات والمعلومات وإتاحتها حسب الطلب[١].

[١] ماجدة عبدالشافى خالد منصور، الحماية الدستورية للأمن السيبراني وأثره على النظام العام، المجلد ٤، العدد ٥٧، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنوفية، مايو ٢٠٢٣، ص ٣٨٠.

ثانيًا– أهداف الأمن السيبراني:

الهدف الأساسي وراء ظهور الأمن السيبراني هو ظهور ما يعرف بالهجمات الرقمية الخطرة أو الفيروسات المنيعة، وفيها يتم الهجوم على الأنظمة الرقمية الخاصة بالأفراد أو المنشأة والسيطرة على ما تمتلكه من بيانات حساسة، وخضوعها لعمليات الابتزاز والسرقة، وكذلك التخريب المتعمد للمعلومات.

وجراء الخسائر الفادحة التي تسببها هذه الهجمات، ظهر الأمن السيبراني، لا بهدف الدفاع أو الحماية فقط من الهجمات الحاسوبية الضارة، بل أيضًا من أجل القيام بالهجوم المتعمد والذي يتم فيه اكتشاف الثغرات الموجودة في النظام والعمل على إصلاحها فور اكتشافها. وتبرز أهم أهداف الأمن السيبراني فيما يأتي:

١. تعزيز حماية أنظمة التقنيات التشغيلية على كافة الأصعدة ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات وما تحويه من بيانات.
٢. التصدي لهجمات وحوادث أمن المعلومات التي تستهدف الأجهزة الحكومية ومؤسسات القطاع العام والخاص.
٣. تعزيز حماية سرية وخصوصية البيانات الشخصية للأفراد.
٤. توفير بيئة آمنة موثوقة للتعاملات في مجتمع المعلومات.

٥. صمود البنى التحتية الحساسة للهجمات الإلكترونية.

٦. توفير المتطلبات اللازمة للحد من المخاطر والجرائم الإلكترونية التي تستهدف المستخدمين.

٧. التخلص من نقاط الضعف في أنظمة الحاسب الآلي والأجهزة المحمولة باختلاف أنواعها.

٨. سد الثغرات في أنظمة أمن المعلومات.

٩. مقاومة البرمجيات الخبيثة، وما تستهدفه من إحداث أضرار بالغة للمستخدمين.

١٠. الحد من التجسس والتخريب الإلكتروني على مستوى الدولة والمواطنين.

١١. اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين على حدٍ سواء من المخاطر المحتملة في مجالات استخدام الإنترنت المختلفة.

١٢. تدريب الأفراد على آليات وإجراءات جديدة لمواجهة التحديات الخاصة باختراق أجهزتهم التقنية بقصد الضرر بمعلوماتهم الشخصية سواء بالإتلاف أم بقصد السرقة[١].

[١] يراجع في ذلك: منى عبدالله السمحان، مرجع سابق، ص ١٢.

بناءً على ما تقدم، فإن الأمن السيبراني يهدف إلى الوقاية أو منع وقوع الهجمات السيبرانية من الأساس، ومقاومتها حال وقوعها بهدف التقليل والحد من آثارها، ومن ثم، وضع إجراءات سريعة للتعافي والرجوع إلى الوضع الطبيعي، سواء أكان ذلك عن طريق وضع خطط أم تنفيذ إجراءات أم رسم سيناريوهات لمواجهة مثل هذه التحديات.

الفرع الرابع

أبعاد الأمن السيبراني

يرتبط الأمن السيبراني بمجالات مختلفة سياسية وعسكرية واقتصادية وقانونية واجتماعية؛ بهدف تحقيق منظومة أمن متكاملة تعمل على الحفاظ على الأمن القومي للدولة والحفاظ على الحقوق والحريات الشخصية للمواطنين من أي هجمات أو تهديدات سيبرانية محتملة، ويمكن توضيح ذلك من خلال الآتي:

أولًا- البعد العسكري:

تنشأ أهمية الأمن السيبراني في هذا البعد في الحد من خطورة الهجمات السيبرانية والاختراقات التي تؤدي إلى نشأة الحروب والصراعات المسلحة، كما أنه يساعد في عملية تبادل المؤسسات العسكرية المعلومات الهامة بشكل إلكتروني

افتراضي بدون اختراق هذا التواصل؛ مما ينعكس إيجابًا على تحقيق الأهداف العسكرية للدولة.

وقد تتحول هذه الميزة إلى نقطة ضعف إن لم تكن الشبكة الإلكترونية المستخدمة في ذلك مؤمنة جيدًا من أي اختراق خارجي قد يتسبب في شن هجمات سيبرانية مضادة على شبكات القوات المسحلة وأجهزة الاستخبارات، ومن ثم، تدمير قواعد البيانات العسكرية، وتعطيل قدرة الدولة على النشر السريع لقدراتها وقواتها، أو قطع أنظمة الاتصال بين الوحدات العسكرية وتعطيل شبكات الكمبيوتر، كما يمكن أن يتم شل أنظمة الدفاع الجوي أو التوجيه الإلكتروني للخصم فضلًا عن إمكانية فقدان السيطرة على وحدات القيادة والتوجيه، بالإضافة إلى فقدان العدو قدرته على التحكم أو الاتصال بالأقمار الصناعية[١].

[١] محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي والإنترنت، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، المنعقد خلال الفترة من ١-٣ مايو ٢٠٠٠، بكلية الشريعة والقانون بدولة الإمارات العربية المتحدة، ص ٣٩، منشور على الموقع الآتي:

- https://library.dji.ae/libero/WebOpac.cls?VERSION.

ثانيًا– البعد السياسي:

هناك صراع سيبراني تحركه دوافع سياسية ويأخذ شكلًا عسكريًا ويتم فيه استخدام قدرات هجومية ودفاعية عبر الفضاء الإلكتروني؛ وذلك بهدف إفساد النظم المعلوماتية والشبكات والبنية التحتية وبما يتضمن استخدام أسلحة وأدوات إلكترونية من قبل فاعلين داخل المجتمع المعلوماتي أو من خلال التعاون ما بين قوى أخرى لتحقيق أهداف سياسية[١].

كما يشكل الأمن السيبراني دورًا هامًا في الحياة السياسية، حيث يتعاظم هذا الدور في ظل اعتماد المواطنين على مواقع التواصل الاجتماعي في تحقيق أهداف سياسية، كتنظيم حملات انتخابية أو تظاهرات افتراضية، وحركات احتجاجية إلكترونية[٢].

---

(1) Myriam Dunn, Information Age Conflicts, A Study of the, Center،Information Revolution and a Changing Operating Environment, ETH Zurich،for Security Studies (CSS, Issue No 64 ,2002, p14.

(٢) هلالي عبداللاه أحمد، اتفاقية بودابست لمكافحة الجرائم الإلكترونية (معلقًا عليها)، الطبعة الأولى، دار النهضة العربية، القاهرة، ٢٠٠٧، ص ١٢٩.

ثالثًا- البعد الاجتماعي:

يرتبط البعد الاجتماعي أيضًا بالمجالات العلمية، والثقافية، والخدمية، حيث يسمح التطور التكنولوجي بالوصول إلى مناطق بعيدة وإلى فئات محددة، ككبار السن، والمرضى، وغيرهم من ذوي الاحتياجات الخاصة. بالإضافة إلى الدور الذي يمكن أن يؤديه في تبادل المعلومات في أوقات الأزمات الإنسانية والكوارث، ولا تقف الأبعاد الاجتماعية عند حدود توفير اطمئنان المواطن إلى حياته اليومية، والاستفادة من طاقات تقنيات المعلومات والاتصالات، في تطوير نشاطاته المختلفة، بل تتعداها إلى صيانة القيم الجوهرية في المجتمع كالانتماء، وغيرها من المعتقدات[١].

رابعًا- البعد الاقتصادي:

يرتبط الأمن السيبراني ارتباطًا وثيقًا بالحفاظ على المصالح الاقتصادية لكل الدول، فالترابط وثيق بين الاقتصاد والمعرفة، فأغلب الدول تعتمد في تعزيز اقتصادها وازدهاره على إنتاج وتداول المعرفة والمعلومات على كافة المستويات، بالإضافة لاستخدام علوم الحاسب الآلي في تطوير الصناعات وتحريك الاقتصادات، وأصبحت

[١] عبدالرحمن عاطف أبوزيد، الأمن السيبراني في الوطن العربي: دراسة حالة المملكة العربية السعودية، العدد ٤٨، المركز العربي للبحوث والدراسات، ٢٠١٩، ص ٥، منشور على الموقع الآتي: http://www.acrseg.org/41356.

المعاملات المالية والاقتصادية محوسبة، وباتت شبكات البنوك والبورصة وشركات الأسواق المالية مرتبطة ببعضها البعض بنظم وشبكات إلكترونية، فأصبح الإنترنت هو أساس المعاملات المالية والاقتصادية وبات يشكل محورًا رئيسيًا للتطور الاقتصادي في القرن الحادي والعشرين، وهو ما أثار الحديث عن أهمية تحقيق الأمن السيبراني في المجال الاقتصادي[١].

ونتيجة لدخول العالم عصر المال الإلكتروني، بعد إطلاق خدمات المحافظ الإلكترونية، وتزايد استثمارات المصارف والمؤسسات المالية في مجال المال الرقمي، وتنافس الشركات على إصدار تطبيقات تسمح بآليات دفع آمنة، ويحفظ المال في المحفظة الإلكترونية؛ كان من الضروري على الدول وضع تشريعات خاصة بحماية هذا المال، وتشريعات للحد من بعض الجرائم الاقتصادية والمالية الخطرة، والعابرة للحدود، كتبييض الأموال، والتهرب من الضريبة؛ مما يبرر الدور الخطير للأمن السيبراني في حماية الاقتصاد.

[١] عبدالفتاح بيومي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، المحلة الكبرى، ٢٠٠٧، ص ١٩٨.

خامسًا- البعد القانوني:

تعد العلاقة بين القانون والتكنولوجيا علاقة تبادلية، فالتطورات التكنولوجية المختلفة تفترض مواكبة التشريعات القانونية لها من خلال وضع أطر وتشريعات للأعمال القانونية وغير القانونية منها، ولكن بصورة عامة تفتقد الجريمة السيبرانية حاليًا للأطر القانونية الصارمة للتعامل معها، ولعل هذا يعود حاليًا لعوامل مثل طبيعة الجريمة الإلكترونية ذاتها، وصعوبة تحديد هوية مرتكبي تلك الجرائم، ومرونة التعريفات المرتبطة بتكنولوجيا المعلومات، إلى جانب كون الجرائم السيبرانية غير مقيدة بحدود الدول؛ الأمر الذي يقتضي تفعيل التعاون الدولي المشترك لمكافحتها[١].

ولعل من أبرز الممارسات القانونية في مجال الأمن السيبراني هو ضمان بعض الحقوق، كحق النفاذ إلى الشبكة العالمية للمعلومات، وأيضًا توسعت بعض المفاهيم لتشمل أساليب الممارسة الجديدة باستخدام تقنيات المعلومات والاتصالات، كالحق في إنشاء المدونات الإلكترونية، والحق في إنشاء التجمعات.

ويوجد إطار تشريعي في مجال الأمن السيبراني المصري وإن كان ضعيفًا قبل صدور قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨، وقانون حماية

[١] هلالي عبداللاه أحمد، مرجع سابق، ص ١٣٥.

البيانات الشخصي رقم ١٥١ لسنة ٢٠٢٠، إلا أنه كان موجودًا متمثًلا في قانون الاتصالات رقم ١٠ لسنة ٢٠٠٣، وقانون التوقيع الإلكتروني رقم ١٥ لسنة ٢٠٠٤، وقانون حماية المستهلك رقم ١٨١ لسنة ٢٠١٨، والقرار الجمهوري رقم ٢٧٦ لسنة ٢٠١٤ بشأن انضمام مصر للاتفاقية العربية لمكافحة الجرائم التقنية، ثم جاء قانون مكافحة جرائم تقنية المعلومات ٢٠١٨ لتشهد مصر حراكًا قويًا في مجال أمن المعلومات على الإنترنت، وأيضًا الحق في حماية ملكية البرامج المعلوماتية.

المطلب الثاني

مفهوم الخصوصية المعلوماتية وصور الاعتداء عليها

لا ريب أن الحق في الخصوصية أو حرمة الحياة الخاصة تعد من الحقوق الدستورية الأساسية الملازمة للشخص الطبيعي بصفته الإنسانية كأصل عام، فهي تعد أساس بنيان كل مجتمع سليم، ويعتبر من الحقوق السابقة عن وجود الدولة ذاتها.

لذا، تحرص المجتمعات خاصة الديمقراطية منها على كفالة هذا الحق، وتعتبره حقًا مستقلًا بذاته، ولا تكتفي بسن القوانين لحمايته بل تسعى إلى ترسيخه في الأذهان، وذلك بغرس القيم النبيلة التي تلعب دورًا كبيرًا وفعالًا في منع المتطفلين والمجرمين من التدخل في خصوصيات الآخرين وكشف أسرارهم، ولقد حظي هذا الحق باهتمام كبير سواء من جانب الهيئات والمنظمات الدولية أم من جانب الدساتير أم من النظم القانونية.

ومع تزايد التقنيات الحديثة وتطورها المستمر زادت المخاطر على الخصوصية، وزاد التخوف من الانتهاكات والاعتداءات المحتملة، بسبب المقدرة الهائلة لنظم المعالجة الإلكترونية في الوصول إلى المعلومات والبيانات الشخصية المتعلقة بالأفراد، واستغلالها في غير الأغراض التي تجمع من أجلها؛ مما أثار تخوفات شديدة على حماية البيانات التي تتصل بالأفراد وحياتهم الخاصة.

وتغير الواقع التكنولوجي منذ الثمانينيات، فيما يتعلق بالجهات التي تملك وتسيطر على نظم الحاسوب؛ بسبب إطلاق الحواسيب الشخصية وانتشارها، وظهور شبكات المعلومات كنتيجة للاندماج بين تكنولوجيا المعلومات والاتصالات؛ لتصبح المعالجة الآلية للمعلومات المتعلقة بالأفراد تتم من قبل هيئات عامة وخاصة ولأغراض مختلفة، بل تحولت هذه المعلومات إلى سلعة يتم جمعها وتداولها دون علم أصحابها، بهدف توجيه الدعاية أو لقياس المؤشرات الاقتصادية، أو مراقبة الأفراد ورصد مختلف سلوكاتهم لأغراض أمنية، ما أكد أن الحياة الخاصة للأفراد إلى جانب باقي الحقوق والحريات بحاجة للحماية في عصر المعلومات[١].

وسنتناول فيما يأتي تعريف الخصوصية المعلوماتية، ثم بيان أوجه الاعتداء عليها، وذلك في فرعين على النحو الآتي:

- **الفرع الأول: مفهوم الخصوصية المعلوماتية.**
- **الفرع الثاني: صور الاعتداء على الحق في الخصوصية المعلوماتية.**

[١] علي عبود جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة: دراسة مقارنة، الطبعة الأولى، منشورات زين الحقوقية، بيروت، ٢٠١٣، ص ٤٠٨-٤٠٩.

الفرع الأول

مفهوم الخصوصية المعلوماتية

أولًا: تعريف الخصوصية المعلوماتية في اللغة والاصطلاح

١-تعريف الخصوصية لغة واصطلاحًا:

الخصوصية لغةً: تعني حالة الخصوص، والخصوص نقيض العموم، ويقال خصه بالشيء يخصه خصًا وخصوصًا وخصوصية، وخاصة الشيء: ما يختص به دون غيره، أي: ينفرد به، ويقال: اختص فلان بالأمر وتختص له، ويقال: فلان يخص فلان، أي: خاص به وله به خصية، والخاصة ما تخصه لنفسك، ومن مرادفات الخصوصية في اللغة العربية الانزواء والانعزال والعزلة والتوحد والتفرد والوحدة والانطواء[١].

ويقال: هذا الموضوع له خصوصية: له أهمية تميزه عن غيره، وهي تعني ما يتعلق بشخص أو بمجموعة أو بشيء محدد دون سواه، رسائل خصوصية: سرية، وخصوصيات الشخص: شؤونه الخاصة به[٢].

---

[١] ابن منظور، تهذيب لسان العرب، الطبعة الأولى، دار الكتب العلمية، لبنان، ١٩٩٣، ص٢٩٠.

[٢] أحمد مختار عمر، معجم اللغة العربية المعاصرة، الطبعة الأولى، عالم الكتب، القاهرة، ٢٠٠٨، ص ٦٥٢.

الخصوصية اصطلاحًا: كما هي معروفة بهذا المصطلح في النظام القانوني الأنجلو أمريكي privacy، والحياة الخاصة vie privée في النظام القانوني اللاتيني، فإن أغلب التشريعات اتجهت إلى عدم إيراد تعريف للخصوصية واكتفت بوضع نصوص تكفل حمايته وتعدد صور الاعتداء عليه، غير أن الفقه تصدى لهذه المهمة.

انعقد الإجماع على صعوبة التوصل إلى تعريف جامع مانع للحق في الحياة الخاصة أو الخصوصية أو السرية الشخصية كما يسميها البعض، ولهذا نجد أن هناك تعاريف متعددة ومتباينة تم وضعها للخصوصية، نستعرض منها ما يأتي:

ذهب جانب من الفقه بأن الخصوصية هي: حق من طبيعة مادية يرتبط بالشخصية الإنسانية التي لها عليه سلطة تقديرية كاملة[١].

وعُرفت الخصوصية بأنها: عبارة عن منظومة متكاملة ومتناسقة من الخصائص، لها سمات مادية وروحية، وهي أسلوب حياة، ومجموعة أخلاقيات، وتتمثل في النظرة إلى العالم ورؤية الذات والآخر، وقد أصبح الحق في الحياة

[١] عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الإنترنت: الأحكام الموضوعية والجوانب الإجرائية، دار النهضة العربية، القاهرة، ٢٠٠٤، ص ٥٩٤؛ حسام الدين الأهواني، الحق في احترام الحياة الخاصة: دراسة مقارنة، دار النهضة العربية، القاهرة، ١٩٧٨، ص ٤٨٠؛ ممدوح خليل بحر، حماية الحياة الخاصة في القانون الجنائي، دار النهضة العربية، القاهرة، ١٩٨٣، ص ٦٥٦؛ حسني الجندي، ضمانات حرمة الحياة الخاصة في الإسلام، دار النهضة العربية، القاهرة، ١٩٩٣، ص ٦٢١.

الخاصة أو الخصوصية من الحقوق التابعة للإنسان والموازية لكل الحقوق الأخرى الشخصية، رغم أن هذا الحق في الدول والمجتمعات التي تعتمد على معايير الإنسان تعتبره من أهم الحقوق وأقدسها[١].

وذهب جانب من الفقه بأنها: ادعاء الأفراد ليقرروا بأنفسهم متى وإلى أي مدى يتم إبلاغهم بالمعلومات عنهم، ومن خلال القول بأن المواطنين يحتفظون بالسيطرة على كيفية استخدام بياناتهم الشخصية[٢].

وذهب جانب آخر من الفقه بأنها: حق الفرد في أن يختار سلوكه الشخصي وتصرفاته في الحياة عندما يشارك في الحياة الاجتماعية مع الآخرين. ثم حدد ثلاث مجموعات رئيسية لهذا الحق، وهي:

- حرية التعبير عن الأفكار والاهتمامات الشخصية.
- حرية أن يكون لديه أولاد يربيهم وينشئهم.

---

[١] محمد فليح النمر، حماية خصوصية مستخدمي مواقع التواصل الاجتماعي على ضوء التشريعات في مملكة البحرين، مركز جيل البحث العلمي، كتاب أعمال المؤتمر الدولي المحكم حول الخصوصية في مجتمع المعلوماتية، العام السابع، العدد ٢٦، طرابلس، لبنان، يوليو ٢٠١٩، منشور على الموقع الآتي: https://jilrc.com/archives/1107 .

[٢] عائشة كريكط، حق الخصوصية لمستخدم الفضاء الرقمي: المخاطر والتحديات، المجلد ١٨، العدد ٢، مجلة الحقيقة للعلوم الاجتماعية والإنسانية، جامعة أحمد دراية، الجزائر، ٢٠١٩، ص ٢٥٧، منشور على الموقع الآتي: https://search.emarefa.net/ar/detail/BIM.

- حق الفرد في الكرامة وتحريره من القسر والقهر.
- حق الأفراد في تحديد متى وكيف وإلى أي مدى تصل المعلومات عنهم للآخرين، أو فهو حق الأفراد أو الجماعات أو المؤسسات في أن يقرروا بأنفسهم زمن وكيفية ومدى نقل المعلومات عن أنفسهم إلى الآخرين، والخصوصية منظور إليها من علاقة الفرد بالمشاركة الاجتماعية، هي انسحاب الفرد الطوعي والمؤقت من المجتمع العام عبر وسائل مادية أو نفسية[١].

ويقصد بالخصوصية أيضًا بأنها: حق الفرد مستخدم التقنيات الحديثة في أن يقرر بنفسه متى، وكيف، وإلى أي مدى يمكن أن تصل معلوماته وبياناته الشخصية الخاصة به إلى الآخرين من المستخدمين أو القائمين على هذه المواقع[٢].

---

[١] صالح جواد كاظم، التكنولوجيا الحديثة والسرية الشخصية، دار الشؤون الثقافية العامة، بغداد، ١٩٩١، ص ١٣٦، منشور على الموقع الآتي: https://alexalaw.ahlamontada.com/t3911-topic؛ محمد سامي الشوا، الغش المعلوماتي كظاهرة إجرامية مستحدثة، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، ١٩٩٣، ص ١٧٠.

[٢] تومي فضيلة، أيديولوجيا الشبكات الاجتماعية وخصوصية المستخدم بين الانتهاك والاختراق، العدد ٣٠، مجلة العلوم الإنسانية والاجتماعية، جامعة قاصدي مرباح ورقلة، الجزائر، سبتمبر ٢٠١٧، ص ٤٤، منشور على موقع دار المنظومة:

وهديًا على ما تقدم من تعاريف، فإنه يمكن القول أن هناك صعوبة في وضع تعريف جامع مانع للحق في الخصوصية؛ نظرًا لارتباط مفهوم هذا الحق بالتقاليد والثقافات والقيم الدينية والنظم السياسية، وهي محددات تختلف من مجتمع إلى آخر، الأمر الذي يصعب معه صياغة تعريف جامع مانع لهذا الحق بطريقة محددة.

لذلك، فإن الاتجاه العام في وقفتنا الحاضر يرى- وبحق- ضرورة عدم الانشغال بوضع تعريف للحق في الخصوصية، بحيث يترك الأمر للفقه والقضاء لتحديد ما يدخل في نطاق هذا الحق، بحسب ظروف المجتمع وتطوره وأفكاره ومعتقداته، ذلك أن وضع مثل هذا التعريف من شأنه تقييد هذا الحق، والإضرار بتطوره، بالنظر إلى أن مفهومه يعد من المفاهيم النسبية التي تختلف باختلاف الزمان والمكان والأشخاص[١].

ويمكن تقسيم الخصوصية إلى أربعة أنواع فيما يلي:

أ- **خصوصية جسدية:** وهي التي تتعلق بالحماية الجسدية للأفراد تجاه أية إجراءات ماسة بالنواحي المادية لأجسامهم كفحص المخدرات أو الجينات.

- https://search.mandumah.com/Record/843529.

[١] حسام الدين الأهواني، مرجع سابق، ص ٤٦٤؛ محمود عبدالرحمن محمد، نطاق الحق في الحياة الخاصة: دراسة مقارنة في القانون الوضعي (الأمريكي- الفرنسي- المصري) والشريعة الإسلامية، دار النهضة العربية، القاهرة، ١٩٩٤، ص ١٣١ وما بعدها؛ ممدوح خليل بحر، مرجع سابق، ص ٢٠٧ وما بعدها.

ب–**خصوصية الاتصالات والمراسلات:** وهي التي تتعلق بحق الأفراد في الحفاظ على سرية اتصالاتهم ومراسلاتهم وبريدهم الإلكتروني وغيرها من الاتصالات.

ت–**خصوصية مكانية:** وهي التي تتعلق بحرمة المسكن، والقواعد الإجرائية المنظمة للتفتيش الحاصل في الأماكن الخاصة والعامة.

ث–**خصوصية معلوماتية:** وهي التي تتمثل بالقواعد المنظمة لجميع إدارات البيانات الخاصة الموجودة على الأجهزة الإلكترونية أو على شبكة الإنترنت. ف"البيانات الخاصة"، "الخصوصية المعلوماتية"، "والمعلومات الاسمية"، جميعها مصطلحات تشير إلى حق الشخص في أن يتحكم بالمعلومات التي تخصه، فهذه المعلومات يطلق عليها "خاصة" كونها تتعلق بالشخص الطبيعي الذي تتصل به هذه المعلومات[١].

[١] يراجع في ذلك: يونس عرب، قانون الكمبيوتر، موسوعة القانون وتقنية المعلومات، اتحاد المصارف العربية، ٢٠٠١، ص ٢٠٣ وما بعدها.

٢- تعريف المعلوماتية لغة واصطلاحًا:

المعلوماتيـة لغـةً: مصـدر صـناعي مـن معلومـات، وهـي: مجموعـة التقنيـات المتعلقــة بالمعلومــات ونقلهــا وخاصــة معالجتهــا الآليــة والعقليــة بحســب العلــم الإلكتروني[١].

المعلوماتيـة اصطلاحًا: عند تعريف المعلوماتية تعريفًا اصطلاحيًا دقيقًا قد نجد صعوبة في تحديد معنى محدد للمعلومات في ظل استخدامها في عدد من المجالات المختلفة على الرغم من ملاحظة خصائصها وتأثيراتها في جميع مناحي الحياة.

وتعرف المعلوماتية بأنها: علم المعالجة العقلية للمعلومات باستخدام آلات تعمل ذاتيًا. ونجد أن هذا التعريف هو الراجح لدى الفقه لتضمنه جميع المعلومات التي يتم تجميعها بمعرفة الإنسان والتي تتمتع بالتجديد والابتكار والسرية والاستئثار، والمجمعة عن طريق شبكات المعلومات والمعالجة آليًا وفقًا لأنظمة المعلومات[٢].

---

[١] أحمد مختار عمر، مرجع سابق، ص ١٥٤٤-١٥٤٥.

[٢] سوير سفيان، جرائم المعلوماتية، رسالة مقدمة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، جامعة تلمسان، الجزائر، ٢٠١١، ص ١١، منشور على الموقع الآتي:

- https://www.elmizaine.com/2019/02/pdf_996.html.

وأشار القانون الفرنسي الصادر في ٢٩ يوليو ١٩٨٢ الخاص بالاتصالات السمعية والبصرية إلى تعريف عام للمعلومة، حيث وصفها بأنها: صوت أو صور أو وثائق أو بيانات أو رسائل من أي نوع[١].

لقد أصبح مصطلح المعلوماتية مرتبط ارتباطًا وثيقًا بالعديد من المجالات المختلفة في المجتمعات البشرية، الأمر الذي أدى إلى تطورها بشكل كبير، على اعتبار أنها اعتمدت على توفير كل الطرق المناسبة لاستخدام الأجهزة الإلكترونية الحديثة، وخصوصًا أجهزة الكمبيوتر التي صارت جزءًا لا تكاد تخلو منه الحياة اليومية، بوجودها في أغلب الأماكن من مدارس ومنازل ومنشآت العمل وغيرها، لذا، صار للمعلوماتية تأثيرًا كبيرًا على حياة الأفراد، وكل فرد يستفيد من أدواتها ووسائلها بالطرق والآليات التي تتوافق مع المجالات التي يستخدمها فيها.

٣- تعريف الخصوصية المعلوماتية باعتبارها مركبًا وصفيًا:

تعرف الخصوصية المعلوماتية على أنها: حق الفرد على بياناته الشخصية أو البيانات ذات الطبيعة الشخصية مما يسمح بمواجهة الاعتداءات الواقعة عليها، وتنظيم الحق على البيانات الشخصية وسيطرة صاحبها عليه[١].

[١] سوير سفيان، مرجع سابق، ص ١٠.

كما تعرف أيضًا بأنها: أحقية الفرد في أن يقرر بنفسه متى وكيف وإلى أي مدى يمكن أن تصل المعلومات الخاصة به إلى الآخرين، وهذه الخصوصية هي التي تضمن القواعد التي تحكم جمع وإدارة البيانات الخاصة، والتي تتميز عن غيره من الأفراد، كمعلومات بطاقة التعريف، أو المعلومات المالية، أو السجلات الطبية، أو الرسائل والمكالمات الهاتفية، ويدخل ضمن ذلك ما يتبادل بين الأشخاص عبر منصات التواصل الاجتماعي (مقاطع فيديوهات، صور، رسائل...)، وهي المحل الذي يتصل عادة بمفهوم حماية المعلومات[٢].

كما عرفت بأنها: حق الشخص في أن يتحكم بالمعلومات التي تخصه[٣].

وهي أيضًا: وصف لحماية البيانات الشخصية للفرد، والتي يتم نشرها وتداولها من خلال وسائط رقمية، وتتمثل البيانات الشخصية في البريد الإلكتروني والحسابات

---

[١] أيمن عبدالله فكري، جرائم نظم المعلومات: دراسة مقارنة، رسالة دكتوراة، كلية الحقوق، جامعة المنصورة، ٢٠٠٥-٢٠٠٦، ص٤٧٠-٤٧١.

[٢] محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة، الإسكندرية، ٢٠٠٩، ص ٣٢٨.

[٣] عائشة بن قارة مصطفى، الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية، المجلد ٢، العدد ٦، مجلة البحوث القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الطاهر مولاي بسعيدة، الجزائر، ٢٠١٦، ص ٢٧٤، منشور على الموقع الآتي:

- https://journals.ajsrp.com/index.php/ajsrp/article/view/1469/1407.

البنكية والصور الشخصية معلومات عن العمل والمسكن، وكل البيانات التي نستخدمها في تفاعلنا على الإنترنت أثناء استخدامنا للحاسب الآلي أو التليفون المحمول أو أي من وسائل الاتصال الرقمي بالشبكة العنكبوتية[١].

وعلى الرغم من اختلاف التعاريف المتعلقة بحماية الخصوصية المعلوماتية بين هؤلاء الفقهاء إلا أن النقاط المشتركة بينهم تتمثل في السعي وراء الحد من السلطة الممنوحة للحكومات أو الأفراد خاصة فيما يتعلق بعملية الاطلاع على البيانات الشخصية للأفراد واستعمالها بغض النظر عن الأسباب، مع تسليط الضوء على النقص التشريعي حول حماية الأفراد من الانتهاك الشخصي الإلكتروني ومن مخاطر التقنية بشكل عام.

ثانيًا: الموضوعات التي تدخل في نطاق الخصوصية المعلوماتية

أثار موضوع الحق في الخصوصية المعلوماتية جدلًا واسعًا؛ نتيجة لازدياد طلب المعلومات بشكل ملحوظ في كافة المجتمعات، فحماية خصوصية المعلومات وسريتها

[١] عاطف كريم، الخصوصية الرقمية بين الانتهاك والغياب التشريعي، مركز دعم لتقنية المعلومات، القاهرة، ٢٨ أكتوبر ٢٠١٣، ص ٢٠.

ضد تسربها من الحاسب الآلي، والشبكات، وخدمات المعلومات الإلكترونية أصبحت تشكل موضوع الساعة والغاية الأساسية لمعظم الدول[١].

ونتناول فيما يأتي بعضًا من هذه الموضوعات التي يعمد إلى إدراجها ضمن بند الخصوصية المعلوماتية، وبالتالي تمتعها بالحق في الضمان والحماية:

١. **البيانات الشخصية:** هي تلك البيانات التي من شأنها تحديد شخصية الشخص الطبيعي تحت أي شكل كان، وسواء أجريت المعالجة الإلكترونية بواسطة شخص طبيعي أم معنوي، أم هي تلك البيانات المؤلفة من المعلومات التي تخص الفرد، ويمكن أن يعرف بواسطة المعلومات عند اتصالها بمعلومات أخرى في حيازة مستخدم هذه المعلومات، وعليه، فإن البيانات أو المعلومات الفردية تدخل ضمن نطاقها العديد من المسميات كالاسم، الجنسية، الديانة، السكن، وصولًا إلى البصمة[٢].

---

[١] فريد كيت، ترجمة: محمد محمود شهاب، الخصوصية في عصر المعلومات، الطبعة الأولى، مركز الأهرام للترجمة والنشر، القاهرة، ١٩٧٩، ص ١٤٥ وما بعدها.

[2] Christopher J. Millard, Legal Protection of Computer Programs and Data, Sweet and Maxwell Limited, London, The Cars Well Company Limited Toronto, 1985, P.184.

وقد أضاف قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ في الفقرة الثانية من المادة الثانية على سبيل المثال هذا المبدأ بضرورة المحافظة على سرية البيانات التي تم حفظها وتخزينها، وعدم إفشائها أو الإفصاح عنها بغير أمر مسبب من إحدى الجهات القضائية المختصة، وما ذلك إلا تأكيدًا على أهمية وخصوصية البيانات الشخصية للفرد والحرص من قبل التشريعات على عدم المساس بها.

٢. **البيانات المالية:** هي البيانات التي تحتوي على دخل الفرد المادي وإنفاقاته وديونه في حال وجودها، وبمعنى آخر سمعته المالية ووضعه المادي في مختلف المجالات، أي أنها تضم الرصيد الشخصي للفرد والتزاماته، إذ تسعى معظم المصارف على التحري بدقة عن طالب الائتمان وتكون على قناعة كاملة بضرورة تمتع هذه المعلومات بالسرية التامة وعدم جواز نقلها إلى الغير سواء أفرادًا أم مصارف[١].

[١] يراجع في ذلك: عمرو أحمد حسبو، حماية الحريات في مواجهة نظم المعلومات، دار النهضة العربية، القاهرة، ٢٠٠٠، ص ١٢٠؛ محمد عبدالمحسن المقاطع، حماية الحياة الخاصة للأفراد وضماناتها في مواجهة استخدام الحاسب الآلي، ذات السلاسل للطباعة والنشر، الكويت، ص ٧٩؛ رافع خضر صالح، الحق في الحياة الخاصة وضماناته في مواجهة استخدام الكمبيوتر، رسالة ماجستير، كلية الحقوق، جامعة بغداد، ١٩٩٣، ص ٧٤، منشور على الموقع الآتي:

٣. **البيانات الاجتماعية:** هي المتعلقة بسيرة الفرد الاجتماعية والعائلية والأوساط التي يتعامل معها والطلاق في حال حصوله، فالأمور الشخصية تعد من كيان الشخص نفسه؛ لذا، يجب حمايتها، وأن الفقه شدد على ضرورة الاهتمام بالخصوصية بوصفها مبدأ عام يؤسس على حماية الكرامة الإنسانية[١].

٤. **البيانات الصحية:** هي كل ما يتعلق بالشخص من الناحية الصحية، فمعلوم أن الفرد لا يقبل أن تُكشف حالته الصحية أمام الجميع حتى ولو كانوا من أقرب الأقربين، وأن إفشاء مثل هذه البيانات أو المعلومات الصحية يعد إفشاءً لسر المهنة بالنسبة للطبيب أو للعامل في الحقل الطبي من ممرضين وممرضات، ومن ثم، لا يسمح لأي منهم إطلاع غيرهم على هذه المعلومات انطلاقًا من أهميتها وخصوصيتها على الصعيد الشخصي[٢].

- https://colaw.uobaghdad.edu.iq/?page_id=19816.

[١] نعيم مغبغب، مخاطر المعلوماتية والإنترنت، منشورات الحلبي الحقوقية، بيروت، ١٩٩٨، ص ١٨٦؛ علي أحمد عبدالزعبي، حق الخصوصية في القانون الجنائي: دراسة مقارنة، المؤسسة الحديثة للكتاب، لبنان، ٢٠٠٦، ص ٣٣٧.

[٢] محمد رياض الخاني، المبادئ الأخلاقية التي يجب أن يتحلى بها الطبيب في ممارسته لمهنته الطبية: دراسة مقارنة، العدد ٢، مجلة الشريعة والقانون، جامعة الإمارات العربية المتحدة، ١٩٨٨، ص ١٥٤، منشور على الموقع الآتي:

- https://scholarworks.uaeu.ac.ae/sharia_and_law/vol1988/iss2/6/.

٥. **المعلومات القضائية:** هي المعلومات المتعلقة بالقضايا المطروحة أمام القضاء، والمعلومات القضائية المتعلقة بالحياة الخاصة للأفراد أو المعلومات والبيانات الشخصية تعتبر من المعلومات الشخصية التي لا يجوز الاطلاع عليها بأي شكل من الأشكال سواء أثناء نظر الدعوى أم بعد الفصل فيها.

وبناءً على ما تقدم، فالحق في الخصوصية المعلوماتية يتعلق بالعديد من الموضوعات الشخصية لكل فرد، فالمساس بها أو اقتحامها يؤدي إلى الشعور بالغبن، ولكن لا يخفى قدرة العديد من الأشخاص في انتهاك هذه الخصوصية سواء فيما يتعلق بالنواحي المادية والاجتماعية أم حتى الصحية. كل ذلك وإن كان يدل على شيء فإنه يدل على التدخل غير المبرر من قبل العديد من الأشخاص سواء بالشكل المباشر أم غير المباشر والتي يلزم حمايتها قانونا.

الفرع الثاني

صور الاعتداء على الحق في الخصوصية المعلوماتية

أحدثت التطورات الهائلة في مجال تكنولوجيا المعلومات والاتصالات التي يشهدها العالم ثورة حقيقية في جميع مناحي الحياة، وقد أصبحت من أهم وسائل التعامل اليومي بين المؤسسات والأفراد بمختلف الطبقات، ولا ريب أن هذه التطورات

تقدم العديد من المزايا للخصوصية تسهيلًا لحياة الناس، إلا أنها في المقابل تحمل في طياتها العديد من المخاطر إذا ما تصورنا الحجم الهائل من المواد الإلكترونية المتعلقة بالحياة الخاصة للناس والمخزنة ضمن هده التقنيات.

إن وضع نظام لحماية الخصوصية في عصر المعطيات الرقمية عليه أن يراعي طبيعة التهديدات الخاصة التي تتعرض لها الخصوصية في نطاق استخدام التقنيات الجديدة، فتقنية المعلومات- خاصة الإنترنت- تخلق سلسلة من التحديات الجديدة في مواجهة خطط حماية الخصوصية، فالإنترنت زاد من كمية المعطيات المجمعة والمعالجة والمنشأة، كما أنها أتاحت عولمة المعلومات والاتصالات، وبالتالي فقدان المركزية وآليات السيطرة والتحكم[1].

إلا أن هذا التطور الكبير أسهم في ظهور الكثير من الاعتداءات والجرائم التي عرفت بالجرائم الإلكترونية؛ نتيجة إساءة استخدام المعلومات والبيانات المتعلقة بالأفراد، إذ يصعب حصر صور الاعتداءات على الخصوصية؛ وذلك لكونها تتطور

[1] يونس عرب، المخاطر التي تتهدد الخصوصية وخصوصية المعلومات في العصر الرقمي، بحث منشور على الموقع الآتي:
http://ww25.arablaw.org/Download/Privacy_Risks_Article.doc.

نتيجة تطور تكنولوجيا المعلومات باستمرار، إلا أننا يمكن أن نشير إلى أبرز الانتهاكات التي قد تطال حق الأفراد في حرمة حياتهم الخاصة فيما يأتي:

أولًا– الإفشاء غير المشروع للبيانات والمعلومات الإلكترونية:

عرفت المادة الأولى من قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ البيانات والمعلومات الإلكترونية بأنها: كل ما يمكن إنشاؤه أو تخزينه، أو معالجته أو تخليقه، أو نقله، أو مشاركته، أو نسخه بواسطة تقنية المعلومات؛ كالأرقام والأكواد والشفرات والحروف والرموز والإشارات والصور والأصوات، وما في حكمها[١].

وتبرز خطورة وسائل تقنية المعلومات الحديثة على حرمة الحياة الخاصة عند جمع وتخزين البيانات الاسمية وتشغيلها، وعند استخراج هذه المعلومات من ذاكرة النظام وإيصالها إلى الغير أيًا كانت هيئة حكومية أو غير حكومية أم شخصًا طبيعيًا، ومن ثم، تقع جريمة التخزين غير المشروع للبيانات الشخصية، متى تم ذلك دون رضاء صاحبها أو لاستخدامها لأغراض غير المخصصة لها[٢].

---

[١] الجريدة الرسمية، العدد ٢٨ مكرر (هـ)، في ١٥ يولية سنة ٢٠٢٠.

[٢] نائل عبدالرحمن صالح، واقع جرائم الحاسوب في التشريع الجزائي الأردني، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت المنعقد في كلية الشريعة والقانون، جامعة الإمارات العربية

وتتحقق هذه الجريمة على رأي في الفقه الجنائي حتى وإن كانت الحكومات هي من قامت بأفعال التخزين للبيانات الشخصية ما دامت هذه الأفعال قد حصلت دون سند في القانون أو في غير الحالات التي يصرح بها القانون أو دون أمر قضائي[١]، إلا أن التخزين يعد مشروعًا متى تم وفقًا للقانون أو أنه من مقتضيات الصالح العام، كما هو الحال في الدول التي تطبق أعمال الحكومات الإلكترونية بموجب قوانين نافذة[٢].

وتعد أكثر البيانات عرضة للإفشاء غير المشروع هي الخاصة بتعاملات البنوك الإلكترونية، وهذا ما ثبت من خلال قضية بنك (جزل تشافت) السويسري التي حاول خلالها عملاء فرنسيون تابعون لإدارة خدمات الرقابة على التعاملات التجارية والمالية فك شفرة بيانات شخصية لمواطنين فرنسيين تحمل حسابات لدى البنك، وذلك للاستعانة بها في أعمال البحث والتقاضي التي تجرى بشأن التهرب الضريبي[٣].

المتحدة، ٢٠٠٠، ص ١٠، منشور على الموقع الآتي:

- https://library.dji.ae/libero/WebOpac.cls?VERSION.

[١] آدم بديع آدم حسين، الحق في حرمة الحياة الخاصة ومدى الحماية التي يكفلها القانون الجنائي، دار النهضة العربية، القاهرة، ٢٠١١، ص ٥٠.

[٢] أحمد عوض بلال، قاعدة استبعاد الأدلة المتحصل عليها بطرق غير مشروعة، الطبعة الأولى، دار النهضة العربية، القاهرة، ٢٠١٠، ص ٩٢.

[٣] هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة،

ثانيًا– المعالجة غير القانونية للبيانات والمعلومات الإلكترونية:

تعد البيانات الشخصية هي قوام الحق في الخصوصية؛ فهي تمثل في مجموعها المعطيات والمعلومات الخاصة بالفرد والتي تكتسب صفة السرية، وعملية المعالجة غير المشروعة لجملة البيانات هي أبرز صور انتهاك تلك السرية من خلال مخالفة القائمين على عملية المعالجة للشروط والأساليب القانونية المنصوص عليها داخليًا كعدم منح التراخيص اللازمة من الجهات المختصة أو إلغائه أو انتهاء مدته، وهذا يشكل في جوهره اعتداء على حق الدولة في الرقابة على تداول ونقل البيانات الممنوحة للأشخاص المعنوية المصرح لها بذلك قانونًا[١].

وبهذا، تنشأ مخاطر تحول دون مهمة القائمين على تلك الرقابة في التكفل بعدم الاعتداء على الحياة الخاصة، ومن ثم، تغييب دور الدولة في ضبط مجال الرقابة على البيانات وحمايتها من شتى أنواع الجرائم الإلكترونية[٢].

أسيوط، ١٩٩٤، ص ١٩٥.

[١] محمد عزت عبدالعظيم، الجرائم المعلوماتية الماسة بالحياة الخاصة، الطبعة الأولى، دار النهضة العربية، القاهرة، ٢٠١٦، ص ٩٢.

[2] Jean–Jacques Hyest, la fraude informatique vue par le nouveau code pénale, exertises des systèmes de linformation Fvrier, 1992, P. 147.

كذلك إن فكرة المعالجة غير المشروعة للبيانات الشخصية تقوم على مسألة الاعتداء على حق الأفراد في الاستئثار بمعالجة البيانات الشخصية، الأمر الذي يعد ضروريًا في التفرقة بين البيانات القابلة لمعالجتها من قبل الغير وتلك غير القابلة لذلك[١].

ثالثًا- تجاوز الغرض أو الغاية من المعالجة الإلكترونية:

تقع جريمة تجاوز الغرض أو الغاية من المعالجة الإلكترونية بوقوع النشاط المادي المحقق للانحراف عن الغرض أو الغاية من المعالجة الإلكترونية للبيانات الشخصية، ويراد بالغرض أو الغاية موضوع المعالجة الإلكترونية الهدف الذي يتوخى القائم بالمعالجة الإلكترونية تحقيقه، وهو المبرر الوحيد لمعالجة البيانات الشخصية الإلكترونية، وتفترض هذه الجريمة الحصول على البيانات بصورة مشروعة[٢].

---

[١] يونس عرب، الخصوصية وأمن المعلومات في الأعمال اللاسلكية بواسطة الهاتف الخلوي، ورقة عمل مقدمة إلى منتدى العمل الإلكتروني بواسطة الهاتف الخلوي، اتحاد المصارف العربية، عمَّان، الأردن، ٢٠٠٢، ص ٥١٩، منشور على الموقع الآتي:

- https://books.google.com.eg/books?.

[2] Ulrich sieber Les crimes informatiques et dautres crimes dans la domaine de la technologieinformatique، Revue Internationale de droit penal, 1993 ,p53.

ويعد النشاط المادي لهذه الجريمة متحققًا إذا استغل الجاني البيانات الشخصية في الكشف عن مصادر ثروة صاحب البيانات الشخصية أو معرفة مركزه المالي أو شأن له صلة بحياته الخاصة[١].

رابعًا- التجسس الإلكتروني:

لقد أثبتت التجربة العملية أن خطورة استخدام شبكة الإنترنت تكمن أساسًا في ضعف الوسائل المستخدمة في حماية انتقال البيانات عبر الشبكة، بالإضافة إلى صعوبة الوصول إلى الأشخاص القائمين بالاعتداء؛ مما أدى إلى ظهور التجسس الإلكتروني كأخطر صور الاعتداءات التي تحدث في إطار التعاملات الإلكترونية، وهذا لارتباطه بشكل مباشر باغتصاب سرية المحادثات الشخصية والمراسلات والتعاملات التي تتم عبر شبكة الإنترنت في كل المستويات.

ولقد عرف التجسس الإلكتروني في مجال المحادثات الشخصية بأنه: عملية التنصت أو التقاط البيانات التي تنتقل بين جهازين عن بعد عبر شبكة الإنترنت، أو

[١] بولين أنطونيوس أيوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٩، ص ٤٢١.

بترجمة الانبعاثات الكهرومغناطيسية الصادرة من الحاسب إلى بيانات، وذلك باستخدام أي وسيلة من الوسائل التقنية[١].

والتجسس الإلكتروني الذي يصدر خارج إطار القانون والممارس من قبل سلطات الدولة يعد من الأساليب المحرمة دوليًا وداخليًا لانتهاكه حقوق وحريات الأفراد، وذلك في حالة ثبوت فعل التجسس بدون إذن من المحكمة المختصة، ويدخل في إطار التعسف في استعمال حق الدولة في المساس بحقوق الأفراد تحت مظلة الأمن القومي[٢].

بالإضافة إلى أن خطورة التجسس الإلكتروني أضحت تأخذ صورة أوسع مما كانت عليه سابقا خاصة في ظل العولمة والتقنيات الحديثة، بحيث لم تعد تقتصر على السلطات أو دوائر المخابرات، بل قد أصبحت وسائل التجسس متاحة إلى الأفراد العاديين خاصة في الدول المتقدمة على عكس الدول العربية التي ما زالت حركة

---

[١] المادة الثالثة من اتفاقية بودابست لسنة ٢٠٠١، المتعلقة بمكافحة الإجرام المعلوماتي.

[٢] خدوجة الدهبي، حق الخصوصية في مواجهة الاعتداءات الإلكترونية: دراسة مقارنة، المجلد الأول، العدد الثامن، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف بالمسيلة، الجزائر، ٢٠١٧، ص ١٤٢، منشور على الموقع الآتي:

- http://dspace.univ-msila.dz:8080/xmlui/bitstream/handle/.

تسويق أجهزة التجسس من الأمور المستصعبة، والتي لا يمكن تداولها بشكل حر ويسير [١].

وقد تعددت الوسائل المتبعة في التجسس الإلكتروني تبعًا لاختلاف ثقافة مستخدمي هذه الوسائل، من أبرزها: اتباع تقنية اعتراض الاتصال الشبكي التي تقوم على الاعتماد على برامج لتنفيذها، فيتم التخلي من قبل أحد الأشخاص الخارج عن الاتصالات الشبكية المقامة عبر الإنترنت كتبادل النصوص أو الأحاديث الصوتية، فيتم التقاط البيانات أو الصور أو التنصت على الأحاديث الصوتية، واعتراض المحادثات المقامة بالصوت والصورة عن طريق الكاميرات أثناء الاتصال[٢].

خامسًا– الإرهاب السيبراني:

يعرف الإرهابيون السيبرانيون بأنهم: أولئك الأشخاص الذين يهددون ويرغمون فردًا أو منظمة أو حكومة من خلال مهاجمتهم عبر شبكة الإنترنت؛ بهدف بث الأفكار المتطرفة، سواء كانت سياسية أم دينية أم عنصرية للسيطرة على وجدان

[١] نديم عبده، أمن الكمبيوتر: الفيروسات والقرصنة المعلوماتية وانعكاساتها على الأمن القومي، دار الفكر للأبحاث والدراسات، الطبعة الأولى، بيروت، ١٩٩١، ص ٨٦.

[٢] محمد عزت عبدالعظيم، مرجع سابق، ص ١٠١.

الأفراد، وإفساء عقائدهم، وإذكاء تمردهم، واستغلال معاناتهم في تحقيق مآرب خاصة تتعارض مع مصالح المجتمع[١].

وتتعدد أعمال الإرهاب المرتكبة في الفضاء السيبراني؛ فقد يكون بسيطًا عبر بث معلومات الإنترنت حول تفجيرات ينتظر وقوعها في المستقبل، وقد يكون خطيرًا مثل سرقة المعلومات والبيانات العسكرية أو التلاعب بها، وتعد هذه من أخطر الهجمات، ويتم من خلالها نقل كميات هائلة من المعلومات عبر شبكات المعلومات بصورة يومية، وتتميز كثير من هذه المعلومات بكونها على درجة كبيرة من الأهمية. وعلى الرغم من استخدام أجهزة تشفير تتولى تشفير الوسائل والمعلومات المهمة عند إرسالها وفك شفرتها عند استقبالها، إلا أن الاستيلاء على المعلومات التي يتم نقلها عبر شبكات المعلومات قد أصبح يشكل خرقًا كبيرًا يهدد أمن وسلامة هذه المعلومات[٢].

يعد هذا النوع من التهديدات من أخطر نماذج الإرهاب ومن أبرز السيناريوهات المحتملة التي تواجه المجتمع وتبدأ في مراحلها الأولى باختراق المنظومة الأمنية المتعلقة بالأسلحة الاستراتيجية ونظم الدفاع الجوي والصواريخ النووية، وقد تقوم

---

[١] حسنين المحمدي بوادي، الإرهاب الدولي بين التجريم والمكافحة، دار الفكر العربي، القاهرة، ٢٠٠٦، ص ٥٤.

[٢] أميرة عبدالعظيم محمد عبدالجواد، مرجع سابق، ص ٤٣٢.

الجماعات الإرهابية بفك الشفرات السرية للتحكم في تشغيل منصات إطلاق الصواريخ الاستراتيجية؛ مما يؤدي إلى خسائر فادحة، ويقلل من قدرات الدولة العسكرية وحماية أراضيها ومنشآتها الحيوية ومواطنيها.

ويرجع السبب في شن تلك الهجمات؛ لما تتميز به الحرب السيبرانية من خصائص تؤثر على البنية التحتية للمنشآت الحيوية، نتيجة اعتماد منشآت الطاقة والكهرباء على النظم المتقدمة في المعلومات، ولا يلقى هذا النمط الجديد من الصراع تنديدًا دوليًا مثل الهجوم التقليدي، وتتميز تلك الهجمات أنها سريعة الانتشار ورخيصة التكلفة وعدم معلومية مصدر الهجوم؛ مما يؤدي إلى ارتباك الخصم، وقد تتم تلك الهجمات عبر الشبكات عابرة الحدود الدولية[١].

ومن أبرز نماذج الإرهاب السيبراني أيضًا تحريض الجماعات الإرهابية على ارتكاب أعمال إرهابية تتعلق بالعنف. ومن أبرز القضايا في هذا الشأن: قضية الولايات المتحدة الأمريكية ضد "إيمرسون وينفيلد بيغولي"، فقد تم اتهام طالب أمريكي في الثانية والعشرين من عمره، بالضلوع في نشر معلومات على شبكة الإنترنت متعلقة بصنع القنابل والتحريض على ارتكاب أعمال عنف وجرائم أخرى، وكان

[١] ماجدة عبدالشافي الهادي منصور، مرجع سابق، ص ٣٦٧.

إيمرسون يعرف باسم مستعار: "أسد الله الشيشاني"، وله دور نشط في المنتدى الجهادي المعروف دوليًا والمسمى باللغة الإنجليزية: "شبكة أنصار المجاهدين"، وقد شارك في إدارته وعبر عن وجهة نظره المتطرفة، وقام بتشجيع الزائرين على ارتكاب أعمال إرهابية ضد الولايات المتحدة الأمريكية، ونشر أشرطة تحتوي على فيديوهات تبث كيفية تعلم صنع المتفجرات، وقد وجهت إليه المحكمة المحلية الأمريكية للدائرة الشرقية بولاية فرجينيا في ١٤ يولية عام ٢٠١١ عدة تهم منها: النشر على المنتدى الإلكتروني عبارات تدعو إلى الإرهاب[١].

سادسًا- اختراق الحاسبات الآلية والبريد الإلكتروني:

ذهب البعض من الفقه إلى تعريف جريمة الاختراق بأنها: عملية دخول غير مصرح بها إلى حاسب الآخر عن طريق استخدام برامج متطورة تحت تقنية وخبرة عاليين[٢].

---

[١] مكتب الأمم المتحدة المعني بالمخدرات والجريمة، استخدام الإنترنت في أغراض إرهابية، بالتعاون مع فرقة العمل التابعة للأمم المتحدة المعنية بتنفيذ تدابير مكافحة الإرهاب، نيويورك، عام ٢٠١٣، ص ٤٠، منشور على الموقع الآتي:

- https://www.unodc.org/romena/ar/about-unodc-romena.html.

[٢] عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت: الأحكام الموضوعية والجوانب الإجرائية، دار النهضة العربية، القاهرة، ٢٠٠٤، ص ٣٣١.

وبهذا، نجد أن عمليات الاختراق لا تقل خطورة عن النماذج السابقة على اعتبار أن الحاسب الشخصي أضحى يمثل أهم الوسائل المتاحة للاتصالات الحديثة بين الأفراد، وأضحى يعتمد عليه كليًا كآلية للمراسلات والمعاملات التي تصدر في إطار التعاملات الإلكترونية، وبهذا، فإن فكرة اختراق الحاسب الشخصي تقوم على أساس الاعتداء على خصوصية وسرية المعاملات وتسخيرها واستغلالها في شتى الأغراض غير المشروعة التي تلحق بالفرد عدة خسائر على المستوى المادي والمعنوي، وهذا ما عبر عنه في السنوات الأخيرة من خلال ما يعرف بالاختراق الأسود أو مخترقي القبعة السوداء، وهي مجموعة من المجرمين الإلكترونيين الذين اعتمدوا أسلوب اختراق الحاسبات الشخصية للأفراد بالدخول لأنظمة المعلومات وقواعد البيانات بصورة غير مشروعة وتعديل وتحريف وإتلاف البيانات بغرض الاستفادة المادية أو إحداث الضرر المعنوي للضحية، وقد تخل هذه التصرفات في غالب الأحيان في إطار العداءات الشخصية أو السياسية أو الدينية أو القيام بتلك الأفعال لحساب جهات منافسة أو معادية[١].

[١] محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، ١٩٩٤، ص ٥٦.

ويعد البريد الإلكتروني من أهم الوسائل الحديثة في إطار المعاملات الإلكترونية التي تقدمها شبكة الإنترنت التي تدخل في إطار تسهيل الاتصال الإلكتروني عن طريق تبادل الرسائل الفورية، وبهذا، يعد اختراق البريد الإلكتروني من أهم المخاطر التي تواجه حق الخصوصية وتعرض الفرد إلى انتهاك سرية المعاملات والمراسلات التي تدخل في شتى المجالات، وبهذا، فإن المقرر وفق القواعد العامة تكريس ضمانات لحماية سرية المراسلات في حدود وضوابط معينة بغض النظر عن الأساليب المستخدمة سواء كانت تقليدية أم حديثة[١].

سابعًا- الانتهاكات المالية:

تلك المعلومات المتعلقة ببطاقات الائتمان وسرقة أموال البنوك وسرقة كلمة السر أو الاستيلاء عليها، من خلال الحصول على معلومات الضحايا البنكية، أو انتحال شخصية مسؤول حكومي أو أشخاص آخرين من المؤسسات المالية، ومن يقدم على كسر هذا الباب والدخول فيه يكون قد ارتكب جريمة يعاقب عليها القانون، فعندما يوجد للنظام المعلوماتي كلمة سر فهذا يعني أنه يجب ألا يتخطى هذا الباب أحد؛ لذلك حرصت كثير من الشركات في الآونة الأخيرة على حماية عملائها من اختراق

[١] عمر محمد أبو بكر يونس، مرجع سابق، ٣٣٩.

الخصوصية والسرية بأنظمة حماية متطورة، ومن خلال التوعية بهذه الأساليب التي يقع فيها ضحاياها.

ثامنًا– المواد الإباحية:

وهي واحدة من أشهر أنواع الجرائم الإلكترونية، وفيها يتم اختراق المعلومات الشخصية للأفراد وانتحال شخصيات وهمية عبر البريد الإلكتروني ومواقع التواصل الاجتماعي، وإسقاط الضحايا لأسباب مختلفة منها: الأسباب الجنسية.

وتصنف المواقع ومقاطع الفيديو والصور الإباحية ضمن هذه الفئة، وهي الفئة التي وصفتها جامعة كارنيجي ميلون الأمريكية، عبر دراسة واسعة باعتبارها رعب جديد يتهدد هذا العصر، خاصة مع استغلال الأطفال جنسيًا، والمساهمة في نشر الشذوذ، وصولًا إلى إسقاط الضحايا وابتزازهم جنسيًا، وكل ذلك يبدأ من خلال التقرب منهم والسيطرة على معلومات شخصية عنهم تقود إلى تهديدهم وابتزازهم[١].

بناءً على ما تقدم، فإن التأثيرات السلبية الناجمة عن سوء استخدام تكنولوجيا المعلومات والاتصالات على الحق في الخصوصية من قبل الكثير من الشركات والأفراد والحكومات، أصبحت تمثل خطرًا كبيرًا على بعض أوجه حقوق الإنسان

[١] رؤى سعد القرني، الحماية القانونية للحق في الخصوصية المعلوماتية: دراسة مقارنة، العدد السادس، مجلة كلية الدراسات الإسلامية والعربية للبنات بدمنهور، ٢٠٢١، ص ١٠٤٩.

الأساسية وحرياته العامة، وفي ظل هدا الواقع بدأ الانتقال من حماية الحياة الخاصة إلى الاهتمام أكثر بحماية المعطيات الشخصية، وهو الجزء المعنوي من الحياة الخاصة؛ لذلك تعمل الدول والحكومات على فرض خطط وقوانين وأنظمة تحارب بها هذه الجرائم، مع فرض عقوبات قاسية على مرتكبيها، وهو أمر تبدو الدول العربية في حاجة ماسة إلى المضي قدمًا في تحقيقه، خاصة أن ضحايا الجرائم الإلكترونية في الدول العربية ما زالوا في تزايد مستمر.

المبحث الثاني

الإطار الدستوري للخصوصية المعلوماتية والأمن السيبراني ودوره في حماية الخصوصية المعلوماتية

وفيه مطلبان:

- **المطلب الأول:** الحماية الدستورية للخصوصية المعلوماتية والأمن السيبراني.
- **المطلب الثاني:** دور الأمن السيبراني في حماية الخصوصية المعلوماتية.

المطلب الأول

الحماية الدستورية للخصوصية المعلوماتية والأمن السيبراني

إن حماية الخصوصية المعلوماتية حق من حقوق الإنسان الأساسية، وهذا الحق مثله مثل بقية الحقوق يحتاج إلى الحماية، فلا بد من تكريس الحق دستوريًا ضمن النصوص الدستورية أسوة ببقية حقوق الإنسان، إذ أن الدساتير الديمقراطية تحرص على إيراد الحق ضمن نصوصها؛ نظرًا لأهمية الحق سواء بنص صريح أم ضمني؛ وذلك لارتباط الحق بالحياة الشخصية للفرد، ففي ظل التطور التكنولوجي الذي يمر به العالم وانتشار المعاملات الإلكترونية اليومية ومشاركة الأفراد لبياناتهم الشخصية مع جهات أخرى؛ سواء أكانت جهات خاصة أم عامة أصبح من السهل الاعتداء على

تلك البيانات التي يقدمها الفرد سواء لإكمال المعاملات، أو الاشتراك في المواقع الإلكترونية؛ مما يعرض خصوصية حياتهم إلى الانتهاك والاعتداء من قبل الغير، لذا أصبح لازمًا وضع حماية دستورية للبيانات والمعلومات الشخصية، من خلال تكريس هذا الحق دستوريًا.

كما جاء الدستور المصري الحالي الصادر عام ٢٠١٤ بنصوص تنظم الأمن السيبراني؛ نظرًا لأهميته ولما يلعبه الأمن السيبراني من دورٍ كبيرٍ في حماية الأمن القومي والاقتصاد الوطني وحماية المعلومات والبيانات من الاعتداء عليها.

فالأمن السيبراني يعد جزءًا أساسيًا من أمن الدول، يرتبط بالمسائل المتعلقة بحماية المعلومات على جميع أنظمة الحوسبة والشبكات الإلكترونية، لعظم أهمية الأمن السيبراني وحاجة الناس إليه ولارتباطه بواقعنا المعاصر؛ بات حماية الفضاء السيبراني ضرورة لا غنى عنها؛ لأن الحرب السيبرانية حرب عابرة للقارات، وهي أخطر الحروب، وتزداد خطورتها كلما زاد التقدم في المجال المعلوماتي، وبذلك أصبح الأمن السيبراني ضرورة لحماية القطاعات الحيوية للدولة.

وسوف يتضمن هذا المطلب الحماية الدستورية للحق في الخصوصية المعلوماتية، والحماية الدستورية للأمن السيبراني، وذلك في فرعين على النحو الآتي:

- **الفرع الأول: الحماية الدستورية للحق في الخصوصية المعلوماتية.**
- **الفرع الثاني: الحماية الدستورية للأمن السيبراني.**

الفرع الأول

الحماية الدستورية للحق في الخصوصية المعلوماتية

في ظل ازدياد تطور التكنولوجيا الحديثة زادت مخاطرها على الحق في الخصوصية، وأضحى الفرد مقيدًا في تعاملاته من خلال رصد البيانات الشخصية وتخزينها ومعالجتها بواسطة مختلف الوسائط المعلوماتية كتقنيات المراقبة أو التجسس أو الابتزاز أو القرصنة أو المساس بالمعطيات الخاصة بالأفراد، وهي جميعها تمثل تهديدًا مباشرًا على حياتهم الخاصة وحرياتهم الفردية بصورتها المستحدثة والمتمثلة في بنك المعلومات لا سيما إذا أُستغلت لغايات خارجة عن إرادة أصحابها ودون علمهم.

فالحياة الرقمية يترتب عليها العديد من المشكلات؛ وذلك بسبب اتساع شبكة الإنترنت، فالتقنيات التي تتحكم في مجموع التعاملات الإلكترونية تعتمد على شبكة الإنترنت، وهذه الأخيرة ليست بمنأى عن ولوج أي متطفل أو معتدي يستغل شتى الاتصالات التي تترك أثرًا حتى دون علم مُستخدم الشبكة، فتدفق المعلومات والاتصالات عبر الحدود دون أي اعتبار لحدود جغرافية أو سياسية، بحيث يعمل

الأفراد على تبادل المعطيات الخاصة بهم لجهات مختلفة داخلية وخارجية، وهو ما يثير مخاطر إساءة استخدام هذه البيانات[١].

والطبيعة الافتراضية لقنوات التعامل الإلكتروني التي تفتقد إلى المادية تجعل من الشخص وهو بصدد استخدام شبكة الإنترنت يتوقع قدرًا من الخفية في نشاطاته أكثر مما هو عليه الحال في العالم الواقعي، بينما الواقع يثبت عكس ذلك على اعتبار أن التعاملات الإلكترونية تترك آثارًا ودلالات على شكل سجلات رقمية حول الموقع المزار والأمور التي بحث عنها والمواد التي قام بتنزيلها والوسائل التي أرسلها والخدمات والبضائع التي قام بشرائها؛ مما يجعله عرضة للقرصنة ثم الاستغلال غير المشروع لها[٢].

والمتغيرات التي أدت إلى زيادة الشعور بأهمية الخصوصية لدى مستخدمي الاتصالات، وكذلك مستخدمي شبكات التواصل الاجتماعي، كوسيلة للحشد والتأييد في الفاعليات السياسية، بالإضافة إلى التزايد المستمر في عدد الفيروسات والبرمجيات

---

[١] جميل عبدالباقي الصغير، الإنترنت والقانون الجنائي، دار النهضة العربية، القاهرة، ٢٠٠٠، ص٤٠.

[٢] عمر محمد أبو بكر، الجرائم الناشئة عن استخدام الإنترنت: الأحكام الموضوعية والجوانب الإجرائية، دار النهضة العربية، القاهرة، ٢٠٠٤، ص ٣٩٨.

الخبيثة؛ مما شكل خطرًا على المعلومات الخاصة بالأفراد، وتعد الرقابة على الإنترنت أحد انتهاكات الخصوصية التي يمكن أن تقوم بها الحكومات لفرض سيطرتها على مجتمع مفتوح لا يمكن السيطرة عليه[١].

لهذا كله؛ كان لا بد من توفير ضمانات دستورية لحماية واحترام حقوق الإنسان في الخصوصية المعلوماتية، فهذه الحماية تعطي درجة كبيرة من الفعالية، وذلك من خلال إحاطتها بالضمانات اللازمة لذلك، وتعد الحماية أو التكريس الدستوري للحقوق والحريات من أهم الضمانات الكفيلة باحترامها، إلا أنه وعلى رغم أهمية وقدسية الحق في الخصوصية، فإنه نادرًا ما تضمنت الدساتير الوطنية نصًا يشير صراحة إلى هذا الحق.

ويقصد بالتنظيم الصريح للحق تكريسه بنصٍ يرد في الوثيقة الدستورية من قبل المشرع الدستوري، سواء عند إقرار الدستور أم بتعديل لاحق للنصوص الدستورية، إلا أنه بالبحث في دستور مصر الحالي الصادر عام ٢٠١٤ لم نجد أنه نص صراحة على حماية الخصوصية المعلوماتية، برغم أنه حق معترف به من قبل الأمم المتحدة

[١] محمد الطاهر، الحريات الرقمية: المفاهيم الأساسية، مؤسسة حرية الفكر والتعبير، القاهرة، ٢٠١٣، ص ٦.

بموجب الإعلانات والاتفاقيات الدولية؛ لذا يلزم النص صراحة على هذا الحق في الدستور حماية للحفاظ على خصوصية وسرية البيانات والمعلومات الشخصية للأفراد.

وعلى الرغم من عدم النص صراحة على حماية الخصوصية المعلوماتية في الدستور إلا أنه ورد ضمنا مع الحق الأصلي؛ إذ أن الحق الضمني يشتق من الحق الأصلي الذي هو مرتبط به ويشكل جزءًا منه، فأغلب الحقوق الأساسية أصبحت تشتق منها حقوقًا ضمنية وردت بصورة غير صريحة بسبب التغييرات التي تطرأ في مجال حقوق الإنسان؛ وبسبب التطورات الاجتماعية والثقافية والتكنولوجية التي تطرأ على المجتمع التي تؤثر على استحداث حقوق وحريات الإنسان.

ولما أن حماية البيانات والمعلومات الشخصية جزء من حماية الحق في الخصوصية، وهي ركن من أركانها، وأن كلا الحقين يرتبطان بالهدف ذاته وهو حماية خصوصية الأفراد، لذا، فإن ورود الحق في الخصوصية في الدستور بنص صريح يرافقه الاعتراف ضمنا بالحق في حماية الخصوصية المعلوماتية. ومن خلال البحث نجد أن الدستور المصري تناول الحق في حماية الخصوصية المعلوماتية بصورة ضمنية، حيث تناول الحق في الخصوصية وحرمة الحياة الخاصة، وهذا لا يقدح في كون النصوص الدستورية أساسًا قانونيًا لتلك الحماية، فليس من وظيفة الدستور

تفصيل الحقوق والحريات جميعها، وإنما تُمنح للمشرع وضع التنظيم القانوني لمعالجة تلك الضمانة.

فقد حرص المشرع الدستوري في دستور مصر الحالي الصادر عام ٢٠١٤ على التأكيد على حماية البيانات والمعلومات الشخصية، فقد نص في المادة (٦٨) على أنه: المعلومات والبيانات والإحصاءات والوثائق الرسمية ملك للشعب، والإفصاح عنها من مصادرها المختلفة، حق تكفله الدولة لكل مواطن، وتلتزم الدولة بتوفيرها وإتاحتها للمواطنين بشفافية، وينظم القانون ضوابط الحصول عليها وإتاحتها وسريتها، وقواعد إيداعها وحفظها، والتظلم من رفض إعطائها، كما يحدد عقوبة حجب المعلومات أو إعطاء معلومات مغلوطة عمدًا.

وتلتزم مؤسسات الدولة بإيداع الوثائق الرسمية بعد الانتهاء من فترة العمل بها بدار الوثائق القومية، وحمايتها وتأمينها من الضياع أو التلف، وترميمها ورقمنتها، بجميع الوسائل والأدوات الحديثة، وفقًا للقانون.

وبذلك، فالتخزين يعد مشروعًا متى تم وفقًا للقانون أو أنه من مقتضيات الصالح العام، كما هو الحال في الدول التي تطبق أعمال الحكومات الإلكترونية بموجب قوانين نافذة، إلا أنه تبرز خطورة وسائل تقنية المعلومات الحديثة على حرمة الحياة

الخاصة عند جمع وتخزين البيانات الاسمية وتشغيلها وعند استخراج هذه المعلومات من ذاكرة النظام وإيصالها إلى الغير، أيًا كانت هيئة حكومية أو غير حكومية، أم شخصًا طبيعيًا، ومن ثم، تقع جريمة التخزين غير المشروع للبيانات الشخصية، متى تم ذلك دون رضاء صاحبها، أو لاستخدامها لأغراض غير المخصصة لها، أو في غير الحالات التي يصرح بها القانون أو دون أمر قضائي[١].

ولا ريب أن تبني الدستور لقضايا حماية البيانات والمعلومات الشخصية يعطي لهذه البيانات والمعلومات قدسية خاصة. وذلك بالنظر إلى ما تحظى به هذه الوثائق من مكانة متميزة في البناء القانوني للدولة، وعادة ما تتصور أحكامها وقواعدها غيرها من القواعد القانونية الأدنى مرتبة، ويتعين أن تبنى جميع أعمال وتصرفات السلطات العامة والأفراد في دائرة هذه القواعد التزامًا بمبدأ سمو الدستور وعلوه، بحيث لا يجوز للقاعدة العادية أن تصدر بالمخالفة لأحكام الدستور نصًا وروحًا[٢].

---

[١] يراجع في ذلك: أحمد عوض بلال، مرجع سابق، ص ٩٢؛ نائل عبدالرحمن صالح، مرجع سابق، ص ١٠.

[٢] عادل عمر شريف، قضاء الدستورية: القضاء الدستوري في مصر، رسالة دكتوراة، كلية الحقوق، جامعة عين شمس، ١٩٨٨، ص ١٤٥.

وقد حرص المشرع الدستوري على شمول الحياة الخاصة والمراسلات الإلكترونية بالحماية، فقد نصت المادة (٥٧) على أنه: للحياة الخاصة حرمة، وهي مصونة لا تمس.

وللمراسلات البريدية، والبرقية، والإلكترونية، والمحادثات الهاتفية، وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة، ولا تجوز مصادرتها، أو الاطلاع عليها، أو رقابتها إلا بأمر قضائي مسبب، ولمدة محددة، وفي الأحوال التي يبينها القانون.

كما تلتزم الدولة بحماية حق المواطنين في استخدام وسائل الاتصال العامة بكافة أشكالها، ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها، بشكل تعسفي، وينظم القانون ذلك.

وبذلك، فللخصوصية المعلوماتية حرمة لا يجوز لأي شخص الاعتداء عليها أو انتهاكها أيًا كان شخص أو سلطة القائم على هذه المعلومات، كما أن الرسائل– أيا كان نوعها– ترجمة مادية لأفكار شخصية أو مسائل خاصة لا يجوز لغير مصدريها ومن توجه إليهم الاطلاع عليها، وإلا كان في ذلك انتهاك لحرمة المراسلات، واحترام هذه الحرمة يفترض ليس فقط تحريم الاطلاع على مضمون الرسالة، وإنما كذلك منع إعدامها أو إخفائها أو إعلام الغير حتى بمجرد وجودها.

وحسنًا ما فعله المشرع الدستوري حين لم يقصر الحماية على المراسلات البريدية والبرقية والإلكترونية والمحادثات التليفونية، وإنما أضاف: "وغيرها من وسائل الاتصال"؛ وذلك تحسبًا لما يمكن أن يظهر من وسائل الاتصال الجديدة التي لم تكن معروفة عند صدور الدستور، وهو ما حدث بالفعل وعلى نطاق واسع على مستوى العالم بأسره بالنسبة للبريد الإلكتروني، والمحادثات الصوتية عبر الإنترنت Voiced Chat، وقد اقتضت جدية حماية الاتصالات الإلكترونية قيام سلطات الأمن باستحداث إدارات متخصصة مزودة بالفنيين المعنيين والأجهزة اللازمة لمواجهة نوعية جديدة من الجرائم الذكية أو الإلكترونية التي تقع من خلال شبكة المعلومات العالمية والتي وصلت إلى حد التجسس الإلكتروني على وزارة الدفاع الأمريكية، واقتحام مواقعها الحصينة السرية.

ويتضح من صياغة نص المادة (٥٧) من الدستور، وجود ارتباط وثيق بين حرية الاتصال والحق في خصوصية المُستخدمين، إلا أن النص فيما يتعلق بحماية الحياة الخاصة كان قاطعًا، دون ذكر لاستثناءات أو الحاجة إلى الإحالة إلى القانون لوضع تفصيلات تنظيمية، وهو ما لا يسمح للمُشرع البرلماني بالتدخل لوضع ضوابط

تشريعية يُمكن من خلالها وضع قيود على هذا الحق، وأن صلاحية المُشرع البرلماني تقف عند حد وضع نصوص قانونية تُراعي حماية الحياة الخاصة.

ولم يتضمن نص المادة ما يسمح بالخروج عن هذه القاعدة، إلا في حالة تنفيذ الأوامر القضائية، والتي أيضًا خضعت لضوابط زمنية ومُبررات يجب أن تكون واضحة، بالإضافة إلى ذلك، فقد تضمنت الفقرة الثانية من نص المادة (٥٧) من الدستور عبارات قد تسمح للمُشرع البرلماني بالنص على ضوابط تتعلق بتنظيم عملية تعطيل أو وقف وسائل الاتصال، ولم تضع سوى قيد واحد على المُشرع البرلماني، وهي ألا يكون وقف أو تعطيل الاتصالات بشكل تعسفي.

ويرد على حرمة المراسلات عدة استثناءات تستند على مبررات منطقية، وتتعلق هذه الاستثناءات إما بالمسائل الجنائية بقصد كشف الجرائم وبعد استئذان النيابة العامة، وإما بنزلاء مستشفيات الأمراض العقلية بهدف علاجهم من أمراضهم، وإما بالمسائل الجمركية لمكافحة التهريب، وإما بحالة الطوارئ نزولًا على مقتضيات الضرورة.

كما نصت المادة (٥٨) من الدستور على أنه: للمنازل حرمة، وفيما عدا حالات الخطر، أو الاستغاثة لا يجوز دخولها، ولا تفتيشها، ولا مراقبتها أو التنصت عليها إلا

بأمر قضائي مسبب، يحدد المكان، والتوقيت، والغرض منه، وذلك كله في الأحوال المبينة في القانون، وبالكيفية التي ينص عليها، ويجب تنبيه من في المنازل عند دخولها أو تفتيشها، واطلاعهم على الأمر الصادر في هذا الشأن.

فحرمة المسكن حق لكل إنسان؛ لأن السكن مستقر أسرار الشخص ومحل حياته الخاصة مع عائلته، وبه يستريح وينعم بالحق في الهدوء والاستقرار والأمن؛ لذلك فالدستور يعطي حرمة للمسكن، بحيث لا يجوز لأحد الدخول فيه والاطلاع على خصوصيته إلا بإذن صاحبه ورضاه؛ لأنه اعتداء على الشخص ذاته، وبالتالي يمنع الاعتداء على حرمة مسكنه؛ لأنها جزء من الحرية الشخصية.

فدخول المساكن بدون إذن من أصحابها أمر محظور، إلا أنه يستثنى من ذلك حالتان:

أ-حالة ما إذا حدثت استغاثة من داخل المسكن لحدوث هدم، أو حريق، أو هجوم لصوص، عليهم أو ما شابه ذلك. فهنا يجوز لكل شخص أن يدخل المسكن دون استئذان للمساعدة في إنقاذ من بالداخل، فهذه حالة ضرورة، والضرورات تبيح المحظورات.

ب-دخول المسكن لمطاردة مجرم، أو للحصول على أدلة جريمة وقعت، ويفوت

تحصليها بالاستئذان، ذلك أن إقامة الحدود، وتطهير المجتمع من الجرائم أمر واجب، والحدود لا تقام إلا بثبوت جرائمها، وإذا توقف ذلك الإثبات على دخول المنازل فيجب؛ لأن ما لا يتم الواجب إلا به فهو واجب[١].

كما نصت المادة (٥٤) من الدستور على أنه: الحرية الشخصية حق طبيعي، وهي مصونة لا تُمس، وفيما عدا حالة التلبس، لا يجوز القبض على أحد، أو تفتيشه، أو حبسه، أو تقييد حريته بأي قيد إلا بأمر قضائي مسبب يستلزمه التحقيق.

ولما كانت الحق في الخصوصية من الحريات الشخصية فهي حق طبيعي للإنسان، ولها حرمتها ولا تمس، فلا يجوز القبض على الإنسان أو الاطلاع على بياناته أو تفتيشه أو حبسه أو تقييد حريته إلا في حالتين فقط، هما: حالة التلبس، وبالتالي أي قبض على أي شخص ليس في حالة تلبس يعتبر باطلًا، ويلحق به أي دليل مستمد من هذا القبض يعد دليلًا باطلًا لا يعول عليه، ويضحي كذلك القبض بناءً على عدم وجود تلك الحالة مدعاة بضرورة الإفراج الفوري، والحالة الثانية: أن يكون بأمر قضائي مسبب، والأمر بغير تسبيب لا قيمة له، وأن يكون محددًا زمنيًا

[١] محمد أحمد الصالح، حقوق الإنسان في القرآن والسنة، الطبعة الأولى، مكتبة الملك فهد الوطنية، الرياض، ٢٠٠٨، ص ١٨٤.

ومحددًا بالشخص أو بالمكان على نحو واضح ومفصل[١].

وقد حرص الدستور على حماية الحقوق والحريات الملازمة أو اللصيقة بشخص الإنسان والحقوق والحريات الشخصية، فقد نصت المادة (٩٢) على أنه: الحقوق والحريات اللصيقة بشخص المواطن لا تقبل تعطيلًا ولا انتقاصًا. ولا يجوز لأي قانون ينظم ممارسة الحقوق والحريات أن يقيدها بما يمس أصلها وجوهرها.

ونصت المادة (٩٩) على أنه: كل اعتداء على الحرية الشخصية أو حرمة الحياة الخاصة للمواطنين، وغيرها من الحقوق والحريات العامة التي يكفلها الدستور والقانون، جريمة لا تسقط الدعوى الجنائية ولا المدنية الناشئة عنها بالتقادم، وللمضرور إقامة الدعوى الجنائية بالطريق المباشر. وتكفل الدولة تعويضًا عادلًا لمن وقع عليه الاعتداء، وللمجلس القومي لحقوق الإنسان إبلاغ النيابة العامة عن أي انتهاك لهذه الحقوق، وله أن يتدخل في الدعوى المدنية منضمًا إلى المضرور بناءً على طلبه، وذلك كله على الوجه المبين بالقانون.

فالحق في الخصوصية المعلوماتية من حقوق الإنسان الملازمة لشخصيته؛ وبالتالي لا تقبل أي تعطيل أو انتقاص منها، ولا يجوز لأي قانون أن يقيدها أو يمس

[١] يراجع في ذلك: المادة ٣٠ من القانون رقم ١٥٠ لسنة ١٩٥٠ بشأن إصدار قانون الإجراءات الجنائية.

أصلها أو جوهرها، وأي اعتداء عليها جريمة لا تسقط بالتقادم، ولا تسقط الدعوى الجنائية ولا المدنية الناشئة عنها، وللمضرور الذي وقع له اعتداء على حياته الخاصة أن يُقيم الدعوى الجنائية بالطريق المباشر، ضد الشخص أو الجهة التي وقع انتهاك الحق في الخصوصية بسببها، كما تكفل له الدولة تعويضًا عادلًا من جراء انتهاك هذا الحق، كما يجوز للمجلس القومي لحقوق الإنسان إبلاغ النيابة العامة عن أي انتهاك لهذه الحقوق، وله أن يتدخل في الدعوى المدنية منضمًّا إلى المضرور بناءً على طلبه.

وهذا ما أكدت عليه وأرست مبادئه المحكمة الدستورية العليا، حيث قضت بأنه: إن ثمة مناطق من الحياة الخاصة لكل فرد تمثل أغوارًا لا يجوز النفاذ إليها وينبغي دومًا– ولاعتبار مشروع– ألا يقتحمها أحد ضمانًا لسريتها، وصونا لحرمتها، ودفعًا لمحاولة التلصص عليها أو اختلاس بعض جوانبها، وبوجه خاص من خلال الوسائل العلمية الحديثة التي بلغ تطورها حدًا مذهلًا، وكان لتنامي قدراتها على الاختراق أثرًا بعيدًا على الناس جميعهم حتى في أدق شؤونهم، وما يتصل بملامح حياتهم، بل وبياناتهم الشخصية التي غدا الاطلاع عليها وتجميعها نهبًا لأعينها ولآذانها. وكثيرًا ما لحق النفاذ إليها الحرج أو الضرر بأصحابها. وهذه المناطق من خواص الحياة

ودخائلها، تصون مصلحتين قد تبدوان منفصلتين، إلا أنهما تتكاملان، ذلك أنهما تتعلقان بوجه عام بنطاق المسائل الشخصية التي ينبغي كتمانها، وكذلك نطاق استقلال كل فرد ببعض قراراته الهامة التي تكون- بالنظر إلى خصائصها وآثارها- أكثر اتصالًا بمصيره وتأثيرًا في أوضاع الحياة التي اختار أنماطها. وتبلور هذه المناطق جميعها- التي يلوذ الفرد بها، مطمئنًا لحرمتها ليهجع إليها بعيدًا عن أشكال الرقابة وأدواتها- الحق في أن تكون للحياة الخاصة تخومها بما يرعى الروابط الحميمة في نطاقها. ولئن كانت بعض الوثائق الدستورية لا تقرر هذا الحق بنص صريح فيها، إلا أن البعض يعتبره من أشمل الحقوق وأوسعها، وهو كذلك أعمقها اتصالًا بالقيم التي تدعو إليها الأمم المتحضرة.

ولم يكن غريبًا في إطار هذا الفهم- وعلى ضوء تلك الأهمية- أن يستخلص القضاء في بعض الدول ذلك الحق من عدد من النصوص الدستورية التي ترشح مضموناتها لوجوده، وذلك من خلال ربطها ببعض وقوفًا على أبعاد العلاقة التي تضمها، فالدستور الأمريكي لا يتناول الحق في الخصوصية بنص صريح. ولكن القضاء فسر بعض النصوص التي ينتظمها هذا الدستور بأن لها ظلالًا Penumbras لا تخطئها العين، وتنبثق منها مناطق من الحياة الخاصة تعد من

فيضها Emanations، وتؤكدها كذلك بعض الحقوق التي كفلها ذلك الدستور، من بينها حقهم في تأمين أشخاصهم وأوراقهم ودورهم ومتعلقاتهم في مواجهة القبض والتفتيش غير المبرر، وحق المتهمين في ألا يكونوا شهودًا على أنفسهم توقيًا لإدلائهم بما يدينهم. وكذلك ما نص عليه الدستور الأمريكي من أن التعداد الوارد فيه لحقوق بذواتها، لا يجوز أن يفسر بمعنى استبعاد أو تقليص غيرها من الحقوق التي احتجزها المواطنون لأنفسهم.

وحيث إن دستور جمهورية مصر العربية قد نص على أن لحياة المواطنين الخاصة حرمة يحميها القانون، ثم فرع عن هذا الحق الحق في صون الرسائل البريدية والبرقية والهاتفية والإلكترونية.. وغيرها من وسائل الاتصال تقديرًا لحرمتها، فلا يصادرها أحد أو ينفذ إليها من خلال الاطلاع عليها إلا بأمر قضائي، يكون مسببًا ومحدودًا بمدة معينة وفقًا لأحكام القانون، إلا أن هذا الدستور لا يعرض البتة للحق في الزواج، ولا للحقوق التي تتفرع عنها كالحق في اختيار الزوج، بيد أن إغفال النص على هذه الحقوق لا يعني إنكارها، ذلك أن الحق في الخصوصية يشملها بالضرورة باعتباره مكملًا للحرية الشخصية التي يجب أن يكون نهجها متواصلًا Rational Continumm ليوائم مضمونها الآفاق الجديدة التي تفرضها القيم التي أرستها

الجماعة وارتضتها ضوابط لحركتها، وذلك انطلاقًا من حقيقة أن النصوص الدستورية لا يجوز فهمها على ضوء حقبة جاوزها الزمن، بل يتعين أن يكون نسيجها قابلًا للتطور، كافلًا ما يفترض فيه من اتساق مع حقائق العصر The Supposed Tune of Times. وحيث إن الشريعة الإسلامية في مبادئها الكلية تؤكد الحق في الحياة الخاصة بنهيها عن التلصص على الناس وتعقبهم في عوراتهم، يقول الله تعالى: "ولا تجسسوا"[١].

وأكدت المحكمة الدستورية العليا على تلك المبادئ الدستورية في حكم آخر لاحق عليه، حيث قضت بأنه: وحيث إن الدستور الحالى بعد أن نص فى الفقرة الأولى من المادة (٥٧) منه على أن للحياة الخاصـــــة حرمة، وهى مصونة لا تمس، فرَّع عن هذا الحق- وبنص الفقرة الثانية من هذه المادة- الحق في صون المراسلات البريدية والبرقية والإلكترونية والمحادثات الهاتفية، وغيرها من وسائل الاتصال تقديرًا لحرمتها، كما كفل سريتها، بحيث لا يجوز مصادرتها أو الاطلاع عليها أو رقابتها إلا بأمر قضائي مسبب ولمدة محددة، وفي الأحوال التي يبينها القانون، وفي هذا الإطار

[١] القضية رقم ٢٣ لسنة ١٦ ق دستورية عليا، جلسة ١٨ مارس ١٩٩٥، منشور على موقع المحكمة الدستورية العليا:

- https://www.sccourt.gov.eg/SCC/faces/RuleViewer.jspx.

أخضع تقرير المراقبة أو التسجيل وتحديد مدتها لمجموعة من الضوابط الحاكمة لها، التي تضمن جديتها وفاعليتها في صون الحقوق والحريات التي كفلها الدستور، فاشترط أن يصدر بها أمر مسبب من قاضي التحقيق– أو عضو النيابة العامة الذي لا تقل درجته عن رئيس نيابة– بناءً على ما تكشف له من التحريات والتحقيقات من دلائل على جدية الاتهام، والذي يصلح ويكفي سببًا لإصدار الأمر، للمدة التي يقدرها، والتي لا تزيد على ثلاثين يومًا، وإن أجاز تجديدها لمدة أو مدد أخرى مماثلة، إلا أنه أحاط تحديد تلك المدة وتجديدها بضمانات تكفل عدم تأبيدها، وعدم مساسها بالحرية الشخصية أو تجاوزها تخوم الحياة الخاصة، والتى كفلها الدستور في المادتين (٥٤، ٥٧) منه، إلا لضرورة تقتضيها مصلحة التحقيق باعتبارها أحد أوجه المصلحة العامة، وغايتها إظهار الحقيقة في جناية أو جنحة معاقب عليها بالحبس لمدة لا تزيد على ثلاثة أشهر، وفي الحدود التي يستوجبها ذلك، حتى لا تتخذ هذه الإجراءات مع خطورتها سبيلًا للتغول على حقوق الأفراد وحرياتهم، وفي جرائم قليلة الأهمية، وتحديدًا لنطاق هذا الحكم تطلب المشرع أن تكون هذه الإجراءات ذات فائدة في إظهار الحقيقة، كما عين موضوعها في مراقبة المحادثات السلكية أو اللاسلكية، أو إجراء تسجيلات لأحاديث جرت في مكان خاص، منظورًا في ذلك إلى أن

ضبط الأحاديث الشخصية عن طريق تسجيلها يعتبر – كما أبانت المذكرة الإيضاحية للقانون رقم ٣٧ لسنة ١٩٧٢ المشار إليه– نوعًا من التفتيش، ومن ثم، فإنه يجب أن يخضع لأحكام التفتيش، هذا فضلًا عن خضوع الأمر بالمراقبة أو التسجيل لسلطة محكمة الموضوع، ليبقى دائمًا ضمان عدم تأبيد مدتها أو تجاوزها الحدود المعقولة التي تقتضيها ضرورات التحقيق، وإظهار الحقيقة، شرطًا لمشروعيتها وتوافقها مع أحكام الدستور، ومصدره نص الدستور ذاته في المادة (٥٧) منه، واشتراطه أن يكون فرض الرقابة لمدة محددة، والمادة (٩٥) من قانون الإجراءات الجنائية المشار إليها، والتي اشترطت أن تكون المراقبة والتسجيل ذات فائدة في ظهور الحقيقة، والذي يعد قيدًا على السلطة مصدرة الأمر، وخاضعًا في الوقت ذاته لرقابة محكمة الموضوع، وتقديرها للدليل الناشئ عنه، في إطار حريتها في تكوين عقيدتها مما تطمئن إليه من أدلة وعناصر الدعوى التي تطرح عليها، لتقول هي وحدها كلمتها فيها، ليكون مرد الأمر دائمًا إلى ما استخلصته هي من وقائـــــع الدعوى، وحصلته من أوراقها، غير مقيدة في ذلك بوجهة نظر النيابة العامة أو الدفاع أو أي جهة أخرى بشأنها، إضافة إلى حق المتهم فى تفنيد هذا الدليل ودحضه، بما كفله له نص المادة (٩٨) من الدستور، من الحق في الدفاع أصالة أو بالوكالة، باعتباره أحد ضمانات المحاكمة

المنصفة العادلة التي كفلها الدستور للمتهم بمقتضى نص المادة (٩٦) منه، ليضحى التنظيم الذي أتى به النص في حدود النطاق المتقدم غير مصادم لنصوص المواد (٥٤، ٥٧، ٩٨) من الدستور[١].

ووفقًا لما تقدم، تعد الخصوصية من الحقوق الدستورية الأساسية الملازمة للشخص الطبيعي بصفته الإنسانية كأصل عام، فهي تعد أساس بنيان كل مجتمع سليم، وهي تعتبر من الحقوق السابقة على وجود الدولة ذاتها؛ لذلك، تحرص المجتمعات– خاصة الديمقراطية– على كفالة هذا الحق، وتعتبره حقًا مستقلًا قائمًا بذاته، ولا تكتفي بسن القوانين لحمايته، بل تسعى إلى ترسيخه في الأذهان؛ وذلك بغرس القيم النبيلة التي تلعب دورًا كبيرًا وفعالًا في منع المتطفلين من التدخل في خصوصيات الآخرين وكشف أسرارهم، ولقد حظي هذا الحق باهتمام كبير سواء من جانب الهيئات والمنظمات الدولية أم من جانب الدساتير أم النظم القانونية، وخاصة مع تزايد التقنيات الحديثة وتطورها المستمر زادت المخاطر على الخصوصية، لا سيما

[١] القضية رقم ٢٠٧ لسنة ٣٢ قضائية دستورية، جلسة الأول من ديسمبر ٢٠١٨، منشور على موقع المحكمة الدستورية العليا:

- https://www.sccourt.gov.eg/SCC/faces/RuleViewer.jspx.

مع بداية خضوع المعطيات الشخصية لنظام تحكم مركزي للإدارة العامة؛ مما أثار تخوفات شديدة على حماية البيانات التي تتصل بالأفراد وحياتهم الخاصة[١].

فحماية البيانات والمعلومات الشخصية أصبحت أمرًا حتميًا في ظل اتجاه الدولة نحو التحول الرقمي، واحتمالية تعرض هذه البيانات الشخصية للاعتداء عليها خاصة عند تبادل هذه البيانات والمعلومات بين إدارات المرافق العامة للدولة، وضد أفعال وتصرفات موظفي الإدارة العامة؛ ولذلك فتوفير إطار دستوري للتعاملات الإلكترونية يوفر الثقة والأمان والطمأنينة في نفوس الأفراد؛ لما يكفله من حماية الحياة الخاصة في مجال المعاملات الإدارية الإلكترونية.

الفرع الثاني

الحماية الدستورية للأمن السيبراني

عندما بدأت أجهزة الحاسب بمختلف أنواعها والأجهزة المحمولة Mobile Phones باحتواء معلومات مهمة، بدأ القلق على أمن هذه المعلومات والأجهزة التي تعالجها وتخزنها وتنقلها، فتم التفكير في حماية هذه الأجهزة وحماية المعلومات الموجودة بها، وعندما ارتبطت أجهزة الحاسب بشبكة الإنترنت واعتمد الناس على

[١] هشام فريد رستم، الخصوصية في عصر المعلومات، مركز الأهرام للترجمة والنشر، القاهرة، ١٩٩٩، ص ١٢٣.

الإنترنت في أعمالهم وتنمية تجارتهم، واستخدموها في التعليم والتواصل الاجتماعى Social Media، وإنهاء إجراءاتهم الحكومية، واستخدموا هذه الأجهزة في مهام عديدة ومتنوعة، أصبحت معلوماتهم الحساسة والبالغة الأهمية معرضة للخطر والاختراق والاستيلاء؛ فنشأ مجال أمن المعلومات Information Security، وبات من أهم العلوم في عصر التكنولوجيا للحفاظ على هذه الثروة المعلوماتية المهمة لكل جهة سواء أكانت حكومية أم خاصة بعد اعتمادها بشكل متنامي على حلول تقنية المعلومات information technology في تسيير أعمالها وذلك لتحقيق أهداف المنظمة أو المؤسسة[١].

وعندما نتحدث عن أمن المعلومات فلا بد أن يشمل الحديث الأمن السيبرانيCyber Security؛ لأن الأمن السيبراني يهتم بأمن كل ما هو موجود في الفضاء السيبراني أو في الفضاء المعلوماتي بما في ذلك أمن المعلومات، بينما يهتم مجال أمن المعلومات بالحفاظ على المعلومات الإلكترونية، حتى لو كانت على الإنترنت؛ وبذلك، يشمل الأمن السيبراني أمن المعلومات على أجهزة وشبكات

[١] عدنان مصطفى البار، خالد علي المرحبي، أمن المعلومات والأمن السيبراني، ٢٠١٨، ص ١، بحث منشور على الموقع الآتي:

- file:///C:/Users/facebook/Downloads/Article-of-this-week-DrAdnan-ALBAR-and-MrKhalid-Al-Marhabi-Jan-2018-1.pdf.

الحاسب الآلي، بما في ذلك العمليات والآليات التي يتم من خلالها حماية معدات الحاسب الآلي والمعلومات والخدمات من أي تدخل غير مقصود أو غير مصرح به أو تغيير أو إتلاف قد يحدث. لقد أصبح الأمن السيبراني ركيزة أساسية في كل المنظمات والمؤسسات الحكومية والخاصة، بل حتى الدول لمواجهة الحروب الإلكترونية، كما أصبح الأمن السيبراني يشكل جزءًا أساسيًا من أي سياسة أمنية وطنية؛ حتى بات معلومًا أن الدول أصبحوا يصنفون الأمن السيبراني كأولوية في سياساتهم الدفاعية الوطنية.

فمع انفجار الثورة المعلوماتية ودخول العصر الرقمي- خاصة في القرن الحادي والعشرين- وما نتج عنه من تداعيات عديدة؛ بسبب ظهور التهديدات والجرائم السيبرانية التي أصبحت تشكّل تحديًا كبيرًا للأمن القومي وكذلك الدولي، لدرجة أن العديد من الباحثين اعتبر الفضاء السيبراني بمثابة المجال الخامس في الحروب بعد البر والبحر والجو والفضاء، وهو ما استدعى ضرورة وجود ضمانات أمنية ضمن هذه البيئة الرقمية، تبلورت بشكل أساسي في ظهور الأمن السيبراني cyber security

كبعد جديد ضمن أجندة حقل الدراسات الأمنية، وقد اكتسب اهتمامات العديد من الباحثين في هذا المجال[١].

فالأمن السيبراني يهدف إلى تعزيز حماية جميع ما يتعلق بالدولة والأفراد لحماية هذه الأنظمة الإلكترونية، وأنظمة تقنية المعلومات، وأنظمة التقنيات التشغيلية، وجميع مكوناتها المحيطة بالمجتمع من أجهزة وبرمجيات ومعدات وجميع ما يؤثر على تقديم هذه الخدمات، وما تحويه من بيانات، فأصبحت هذه أيضًا من أهم الأولويات المهمة والحيوية لجميع دول العالم للحفاظ على بيانات مواطنيهم وحفظ ممتلكاتهم وبياناتهم الإلكترونية عن طريق:

- حماية شبكة المعلومات والاتصالات، والتي تلعب دورًا كبيرًا في تدفق خط سير البيانات بين المواطنين والدولة، ومن طرف إلى طرف آخر، والتي إذا تعرضت إلى تخريب أو تدمير أو اختراق حتمًا قد يؤثر ويقطع هذه الاتصالات ويتوقف سير العمل وتتوقف الخدمات.
- حماية شبكة المعلومات من أي هجوم؛ وذلك بمعرفة أحدث التقنيات الموجودة في هذا المجال، ومن أهمها: كشف أهداف رسائل العدو والتعرف على طبيعة

[١] منى عبدالله السمحان، مرجع سابق، ص ٤.

هذا المهاجم، وماذا يريد، من خلال معرفة أساليبه المستخدمة والأساليب المختلفة؛ لكي يتم العمل على إيقاف هذا الهجوم بأسلوب علمي وتقني مُحكم يمنع هذا الهجوم[١].

ونتيجة لذلك شهدت مصر حراكًا قويًا في مجال أمن المعلومات والشبكات، وذلك تزامنًا مع الاهتمام الدولي المتزايد بشأن أمن المعلومات، في ظل ما تشهده بعض دول المنطقة من اختراقات أمنية للبنية التحتية والشبكات والمعلومات نتيجة التطورات التكنولوجية المتسارعة. وإدراكًا منها لخطورة هذه التهديدات، فقد أولت الدولة المصرية اهتمامًا بالغًا بهذا المجال وسارعت باتخاذ العديد من التدابير والإجراءات لتنظيم الفضاء المعلوماتي وحماية البيانات وذلك على كافة المستويات؛ حتى تصبح قادرة على التصدي للتحديات والمخاطر العالمية الناجمة عن هذه التهديدات، على النحو الذي يدعم جهود الدولة في بناء مصر الرقمية، والتي يتم من خلالها رقمنة الخدمات الحكومية وتبني المعاملات الرقمية.

وكانت أولى هذه التدابير والإجراءات التي اتخذتها الدولة المصرية إضافة نص جديد إلى دستور ٢٠١٤ لحماية أمن المعلومات والفضاء المعلوماتي، فقد نصت

[١] ماجدة عبدالشافي خالد منصور، مرجع سابق، ص ٣٨٦.

المادة (٣١) من الدستور على أنه: أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه، على النحو الذي ينظمه القانون.

فقد حرصت مصر على حماية أمن فضائها المعلوماتي لسهولة التحول نحو الاقتصاد القائم على المعرفة والابتكار، والذي تشكل الاتصالات وتقنية المعلومات أحد عناصره، وركنًا أساسيًا من أركانه، وتعتبر أحد أهم الأهداف الاستراتيجية التي ركزت عليها الدولة المصرية ضمن خطط التنمية الاقتصادية التي تسعى لتحقيقها في الفترة المقبلة، والتي تتطلب توجيه الاستثمارات إلى قطاع تقنية المعلومات والاتصالات بهدف رفع كفاءة الأداء الوظيفي للإدارة العامة.

وفيما يتعلق بتأثير تكنولوجيا المعلومات والاتصالات على الاقتصاد الوطني، فمن الملاحظ أن حماية أمن المعلومات والاتصالات قد أصبح مفتاح الإنتاجية والمنافسة والإنجاز الاقتصادي ومجالًا وعاملًا بالغًا لتأثيره في النماء والتطوير والتفاعل الحي مع العالم المعاصر بسبب ما تقدمه من إفرازات في التعليم والثقافة والمعرفة[١].

[1] عبدالرزاق تومي، تكنولوجيا المعلومات ودورها في التنمية الوطنية: دراسات استراتيجية، –

وهذا ما حرص المشرع الدستوري على النص عليه في صلب الدستور، فقد نصت المادة (٢٨) على أنه: الأنشطة الاقتصادية الإنتاجية والخدمية والمعلوماتية مقومات أساسية للاقتصاد الوطني، وتلتزم الدولة بحمايتها، وزيادة تنافسيتها، وتوفير المناخ الجاذب للاستثمار، وتعمل على زيادة الإنتاج، وتشجيع التصدير، وتنظيم الاستيراد.

والحقيقة التي لا يراودها أدنى شك أن الأمن السيبراني يرتبط أشد الارتباط بالأمن القومي؛ فالتحديث الدائم للنظم التشريعية والإجراءات الوقائية والعمل على مكافحة الجريمة وتطوير التنمية البشرية والسياسية لجميع أفراد المجتمع لغاية مثلى، وهي دعم أطياف وألوان المجتمع كافة وانخراطهم في الحياة السياسية؛ يحافظ بلا شك على الدولة وشعبها وإقليمها، وهي غاية الأمن المعلوماتي والأمن القومي. ونتيجة لذلك تركز جميع البلدان المتقدمة بشكل خاص على إنشاء وتطوير البنية التحتية

العدد ١٥، مركز البصيرة للبحوث والاستفسارات والخدمات التعليمية، الجزائر، ٢٠١١، ص ٢٢، منشور على الموقع الآتي:
https://www.asjp.cerist.dz/en/downArticle/250/7/15/114650

والأنظمة المعلوماتية المختلفة لضمان مستوى عالٍ من الأمن القومي، ولارتباط أمن المعلومات ارتباطًا وثيقًا بالأمن القومي ومكوناته المختلفة[١].

فمصالح الدولة في مجال المعلومات تتكون من التنمية المستدامة والمتوازنة للبنية التحتية المعلوماتية للبلد، وخلق الظروف المواتية لإعمال الحقوق الدستورية للمواطنين من حيث المعلومات، وحماية موارد معلومات الدولة من الوصول غير القانوني، وضمان أمن المعلومات وأنظمة الاتصالات في الدولة[٢].

وانطلاقًا وتأكيدًا لما جاء في الدستور، فقد اتخذت الدولة المصرية مجموعة من التدابير اللازمة لحماية الأمن السيبراني والأمن المعلوماتي؛ فقد أصدرت وزارة الاتصالات العديد من القرارات التنظيمية الخاصة بتكنولوجيا المعلومات والاتصالات؛ بهدف حماية المعلومات والاتصالات، وما زال هناك العديد من الدراسات القانونية

(1) Rasim M. Alguliyev , Yadigar N. Imamverdiyev Rasim Sh. Mahmudov and Ramiz M. Aliguliyev, about Information security as a national security component, published on 20 Jul 2020, published by Journal A Global Perspective, from P3. to P4.

(2) Rasim M .Alguliyev، Yadigar N. Imamverdiyev Rasim Sh. Mahmudov and Ramiz M .Aliguliyev, about Information security as a national security component, published on 20 Jul 2020, published by Journal A Global Perspective, from P.4 to P5).

والجهود التشريعية التي تُبذل من أجل تأمين المعاملات الإلكترونية المختلفة من جميع جوانبها القانونية والجنائية[١].

ونشأ بموجب قرار مجلس الوزراء رقم ٢٢٥٩ لسنة ٢٠١٤ مجلسًا أعلى للأمن السيبراني التابع لرئاسة مجلس الوزراء، برئاسة وزير الاتصالات وتكنولوجيا المعلومات؛ لتكون مهمته تأمين البني التحتية للاتصالات والمعلومات بشكل متكامل لتوفير البيئة الآمنة لمختلف القطاعات لتقديم الخدمات الإلكترونية المتكاملة، وذلك في إطار جهود الدولة لدعم الأمن القومي وتنمية المجتمع المصري[٢].

---

[١] من بين هذه الجهود والمحاولات التشريعية الأخرى ما يلي: قرار وزير الاتصالات ١٠٧ لسنة ٢٠٠٥ بشأن مكتب حماية برامج الحاسب الآلي وقواعد البيانات، قرار وزير الاتصالات ١٢٨ لسنة ٢٠٠٦ بشأن اختصاص الجهاز القومي لتنظيم الاتصالات بنظر المنازعات المتصلة بالاتصالات، وإنشاء إدارة تُسمى "إدارة فض المنازعات" بالجهاز، قرار وزير الاتصالات ١٠٨ لسنة ٢٠٠٥ بشأن تحديد الخدمات والأعمال الخاضعة لرسم تنمية صناعة تكنولوجيا المعلومات والاتصالات.

[٢] نشر هذا القرار بالجريدة الرسمية في ديسمبر ٢٠١٤، العدد الخمسون مكرر (أ)، بتاريخ ٢٠١٤/١٢/١٥. ونص في على أنه: ينشأ مجلس أعلى لأمن البنية التحتية للاتصالات وتكنولوجيا المعلومات، يتبع رئاسة مجلس الوزراء، ويسمى المجلس الأعلى للأمن السيبراني، ويشكل برئاسة وزير الاتصالات وتكنولوجيا المعلومات وعضوية ممثلي وزارات: :الدفاع، والخارجية، والداخلية، والبترول، والثروة المعدنية، والكهرباء والطاقة المتجددة، والصحة والسكان، والموارد المائية والري، والتموين والتجارة الداخلية، والاتصالات وتكنولوجيا المعلومات، وجهاز المخابرات العامة، والبنك المركزي المصري، وعدد ٣ من ذوي الخبرة في الجهات البحثية والقطاع الخاص يرشحهم المجلس، ويصدر بتعيينهم قرار من وزير الاتصالات وتكنولوجيا المعلومات.

ونشرت الجريدة الرسمية قرارًا للمهندس شريف إسماعيل– رئيس مجلس الوزراء السابق– بشأن الأمن السيبراني، في عددها رقم ١٧ مكرر (ب) بتاريخ ٢ مايو٢٠١٧، وتنص المادة الأولى للقرار على التزام كافة الجهات الحكومية بكافة مستوياتها وشركات قطاع الأعمال العام بتنفيذ قرارات وتوصيات المجلس الأعلى للأمن السيبراني، فيما يتعلق بتأمين البنية التحتية الحرجة للاتصالات وتكنولوجيا المعلومات الخاصة بها، واتخاذ كافة الإجراءات الفنية والإدارية لمواجهة الأخطار والهجمات السيبرانية وتنفيذ الاستراتيجية الوطنية للأمن السيبراني. وقد نصت المادة الثانية للقرار على أن يتولى وزير الاتصالات وتكنولوجيا المعلومات وضع وتحديد قواعد وإجراءات تأمين البنية المعلوماتية الحرجة لقطاعات الدولة، ومتابعة تنفيذ قرارات وتوصيات المجلس الأعلى للأمن السيبراني وتطبيق أحكام هذا القرار.

ثم صدر القانون رقم ١٧٥ لسنة ٢٠١٨ الصادر بشأن مكافحة جرائم تقنية المعلومات، ولائحته التنفيذية رقم ١٦٩٩ لسنة ٢٠٢٠[١].

ونصت المادة (٣٤) من هذا القانون على أنه: إذا وقعت أي جريمة من الجرائم المنصوص عليها في هذا القانون بغرض الإخلال بالنظام العام أو تعريض سلامة

[١] الجريدة الرسمية، العدد ٣٢ مكرر (ج) في ١٤ أغسطس سنة ٢٠١٨.

المجتمع وأمنه للخطر، أو الإضرار بالأمن القومي للبلاد أو بمركزها الاقتصادي أو منع أو عرقلة ممارسة السلطات العامة لأعمالها، أو تعطيل أحكام الدستور أو القوانين أو اللوائح، أو الإضرار بالوحدة الوطنية والسلام الاجتماعي، تكون العقوبة السجن المشدد.

وصدر قرار وزير الجهاز المركزي للتنظيم والإدارة رقم ٨٧ لسنة ٢٠١٩ بشأن التقسيم التنظيمي لنُظم المعلومات والتحول الرقمي بوحدات الجهاز الإداري للدولة[١].

ونص في مادته الخامسة على أنه: يختص التقسيم التنظيمي الفرعي للبنية الأساسية وتأمين المعلومات بالآتي: ... ٥. توفير التأمين السيبراني لنظم معلومات الوحدة ضد المخاطر المحتملة سواء بشرية أم طبيعية، ووضع الضوابط اللازمة لذلك.

وكان آخر هذه التطورات التشريعية وأهمها القانون رقم ١٥١ لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية المعالجة إلكترونيًا جزئيًا أو كليًا لدى أي حائز أو متحكم أو معالج لها، وذلك بالنسبة للأشخاص الطبيعيين[٢].

---

[١] منشور بالوقائع المصرية، العدد رقم ٢٠٨ تابع، في ١٨ من سبتمبر ٢٠١٩.

[٢] الجريدة الرسمية، العدد ٢٨ مكرر (هـ)، في ١٥ يوليه سنة ٢٠٢٠.

ثم أصدر رئيس الجمهورية قرارًا بقانون ١٥٠ لسنة ٢٠٢١ بتعديل بعض أحكام قانون العقوبات الذي نص في مادته الأولى على أنه: يُستبدل بنص المادة ٨٠ (أ) من قانون العقوبات، النص الآتي:

مع عدم الإخلال بأي عقوبة أشد يَنص عليها أي قانون آخر، يُعاقب بالحبس مدة لا تقل عن ستة أشهر ولا تزيد على خمس سنوات وبغرامة لا تقل عن خمسة آلاف جنيه ولا تجاوز خمسين ألف جنيه:

١- كل من حصل بأي وسيلة غير مشروعة على سر من أسرار الدفاع عن البلاد، ولم يقصد تسليمه أو إفشاءه لدولة أجنبية، أو لأحد ممن يعملون لمصلحتها.

٢- كل من أذاع بأي طريقة سرًا من أسرار الدفاع عن البلاد.

٣- كل من نظم أو استعمل أي وسيلة من وسائل التراسل بقصد الحصول على سر من أسرار الدفاع عن البلاد أو تسليمه أو إذاعته.

٤- كل من قام بجمع الاستبيانات أو الإحصاءات أو إجراء الدراسات لأي معلومات أو بيانات تتعلق بالقوات المسلحة أو مهامها أو أفرادها الحاليين أو السابقين بسبب وظيفتهم دون تصريح كتابي من وزارة الدفاع.

فإذا وقعت الجريمة في زمن الحرب، أو باستعمال وسيلة من وسائل الخداع أو الغش أو التخفي أو إخفاء الشخصية أو الجنسية أو المهنة أو الصفة، أو بإحدى وسائل تقنية المعلومات، أو كان الجاني من ضباط القوات المسلحة أو أحد أفرادها أو من العاملين المدنيين لديها كانت العقوبة السجن.

ويُعاقب بالعقوبات نفسها على الشروع في ارتكاب هذه الجرائم[١].

ثم صدر قرار رئيس جمهورية مصر العربية رقم ٢٣٢ لسنة ٢٠٢١ بإنشاء مجمع الإصدارات المؤمنة والذكية، الذي نص في مادته الأولي على بعض التعريفات منها: تعريف النظام البيومتري بأنه: نظام معلوماتي يَكفُل تَمييز كل فرد عن الآخر عن طريق الخصائص الحيوية التي يتم التزام الجهات كافة بتطبيقها، على أن يتم توحيد وسائل وتقنيات إدخالها لبيانات على مستوى الدولة ومؤسساتها المختلفة.

البيانات البيومترية: البيانات التي تحدد هوية الفرد بما يكفل تمييزه عن الآخرين ويضمن عدم تكرارها[٢].

---

[١] القانون رقم ١٥٠ لسنة ٢٠٢١ بتعديل بعض أحكام قانون العقوبات، والمنشور بالجريدة الرسمية العدد رقم ٤٦ مكرر، في ٢٠ من نوفمبر ٢٠٢١.

[٢] قرار رئيس الجمهورية رقم ٢٣٢ لسنة ٢٠٢١، الجريدة الرسمية، العدد ٢٢ (مكرر)، في يونيه سنة ٢٠٢١، بإنشاء مجمع الإصدارات المؤمنة والذكية.

أما على الجانب العربي وبتاريخ ١٩/٩/٢٠١٤؛ فقد أصدر السيد رئيس الجمهورية القرار رقم ٢٧٧ لسنة ٢٠١٤، بشأن الموافقة على انضمام مصر إلى الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية الموقعة في القاهرة بتاريخ ٢١/١٢/٢٠١٠.

ثم أصدر وزير الخارجية المصري قرارًا بالموافقة على الاتفاقية العربية لمكافحة جرائم المعلومات، وتهدف هذه الاتفاقية إلى تعزيز التعاون بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات لدرء أخطار هذه الجرائم؛ حفاظًا على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها[١].

كما قامت مصر باقامة وعقد معرض ومؤتمر أمن المعلومات والأمن السيبراني CAISEC" "22 على مدار يومي ١٣ و ١٤ يونيه ٢٠٢٢ تحت عنوان: "الأمن السيبراني وقت الأزمات" برعاية ودعم من وزارات مختلفة، كما شاركت شركات عملاقة في هذا المؤتمر.

ناقش المؤتمر مجموعة من القضايا الأكثر أهمية من خلال لقاءات وجلسات تفاعلية بين المؤسسات الحكومية والشركات المصرية والعالمية الرائدة في أمن

[١] قرار وزير الخارجية رقم ٤٥ لسنة ٢٠١٤، بشأن الموافقة على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، والمنشور بالجريدة الرسمية بالعدد رقم ٤٦ لسنة ٢٠١٤، بتاريخ ٢٠١٤/١١/١٣.

المعلومات، حيث ناقش المؤتمر خلال جلساته ملف الجيل الخامس من الحروب وهو الحرب السيبرانية في محاضرة متخصصة لأول مرة يلقيها ممثل عن القوات المسلحة المصرية، كما ناقش المؤتمر الأمن السيبراني والمرونة الإلكترونية، وكذا جلسة عن الأمن السيبراني والخدمات المصرفية المفتوحة والرقمية.

كما تتضمن المؤتمر جلسة للتباحث فيما يخص حماية الأصول العينية باستخدام خطط الأمن السيبراني، بالإضافة إلى جلسة أخرى لمناقشة بناء وتأمين أنظمة البنية التحتية الحيوية، وأخرى فتحت ملف الحاجة إلى تشييد مركز عمليات الأمن، وعلى مدار يومين من التباحث المشترك بين مؤسسات وشركات القطاعين العام والخاص يناقش المؤتمر أيضًا تحليل الأمن السيبرانى والحلول السحابية وكيفية إدارة مخاطر سلسلة التوريد للأمن السيبراني.

كما انعقدت على هامش المؤتمر معرض أمن المعلومات والأمن السيبراني"CAISEC 22"، لاستعراض أحدث ما توصلت إليها الشركات المصرية والعالمية في مجالات حماية البيانات والأمن السيبراني وما تقدمه من خدمات مستحدثة لمختلف القطاعات.

ومن خلال قراءة التشريعات الحاكمة لمنظومة تكنولوجيا المعلومات والاتصالات، يؤخذ على هذه التشريعات عدد من الملاحظات، أهمها: عملية إعدادها التي جاءت بشكل منفرد من قبل السلطات، دون إشراك أصحاب المصلحة المعنيين، أو منظمات المجتمع المدني العاملة في المجال، مرورًا بدورانها حول الأمن القومي وحماية المصالح العليا للبلاد، بديلًا من حماية حقوق المستخدمين.

كما تشترك هذه القوانين في استخدام مصطلحات مبهمة وفضفاضة، وما يتبع ذلك من اتساع السلطات التقديرية للسلطات الحكومية، وبالتالي إساءة استعمال القانون؛ ينتج عن ذلك كله ازدياد ممارسات الرقابة على الإنترنت ومراقبة المستخدمين، والتضييق على الإعلام الرقمي، كما تسمح تلك القوانين بمحاكمة مستخدمي الإنترنت لأسباب تتعلق بالتعبير عن الرأي؛ مما ساهم في تدهور حرية الإنترنت في مصر.

ولذا، يجب على الدولة المصرية مراجعة التشريعات التي سُنت مراجعة تشريعية جادة، على أن تخضع الصلاحيات الاستثنائية التي توجد ضرورة للإبقاء عليها لرقابة القضاء؛ وذلك لضمان عدم إساءة استعمال السلطة من قبل الجهات التي تتمتع بهذه الصلاحيات. كذلك يجب على السلطات وضع قيود واضحة على سلطات الضبط في التوقيف والتفتيش وفحص أجهزة الاتصال الخاصة بالأفراد لضمان ألا تتحول عمليات

إنفاذ القانون إلى مسرح لانتهاك خصوصية الأفراد، وعلى أن تكون الإجراءات الماسة بخصوصية الأفراد في حدود الأذون القضائية التي ترخصها.

بالإضافة إلى ذلك، يجب على المشرع إلزام الجهات المخول لها بالتدخل في خصوصية الأفراد وحياتهم خاصة، في ظروف محددة، بإبلاغ الأشخاص المستهدفين بخضوعهم للمراقبة لتمكينهم من المطالبة بالتعويض في حال تجاوز هذه المراقبة للحدود التي يرسمها الدستور والقانون. أيضًا يجب على السلطات توفير آليات مبسطة للتعويض عن انتهاكات الحق في الخصوصية التي تقوم بها الحكومة أو الشركات، وإزالة كافة العقبات التي تعوق إثبات هذه الممارسات أو تطيل أمد الانتصاف لضحايا هذه الانتهاكات[١].

المطلب الثاني

دور الأمن السيبراني في حماية الخصوصية المعلوماتية

انتشرت نوعية خطيرة من الهجمات والجرائم السيبرانية التي تعتمد علي تقنيات متقدمة، كالحوسبة السحابية والذكاء الاصطناعي وبرمجيات لفك الشفرة ولاختراق أنظمة الشبكات والحاسبات وقواعد البيانات، وبرمجيات لتشفير

[١] الحق في الخصوصية في القوانين المصرية: معوقات تشريعية وخطوات لم تكتمل، ٢١ يونيه ٢٠٢١، بحث منشور على الموقع الآتي: https://masaar.net/ar.

العمليات المشبوهة، وبرمجيات خبيثة لاختراق أنظمة أمن الشبكات والحاسبات لتسخيرها في القيام بعمليات إجرامية وتعاملات مشبوهة دون علم أصحابها[١].

لذا، كانت الحاجة ملحة وضرورية لنشر دعائم الأمن السيبراني وتأمين سلامة الممارسات الإلكترونية، فحماية أمن الفضاء السيبراني أمر اهتمت به الدول في كل أنحاء العالم؛ لارتباط أمن المعلومات ارتباطًا قويًا بالأمن القومي في معظم دول العالم، ذلك أن الاعتداء على البنى التحتية المهمة ومنها الاتصالات والأنظمة الإلكترونية يمكن أن يؤثر على كل الدول في منطقة جغرافية معينة، المؤثر بدوره المباشر على مصالح الدولة المعنية بالفضاء المعلوماتي، والتي تشكل بنيتها التحتية للاتصالات والمعلومات جزءًا من تركيبة البنية التحتية للفضاء السيبراني.

لذلك، اتخذت الدول مجموعة من الإجراءات على الصعيدين المحلي والدولي لحماية الخصوصية ومواجهة تقنية المعلومات ضد جميع أشكال الجرائم السيبرانية، وهذه الإجراءات تنطوي على عدد من الاعتبارات للتخفيف من المخاطر والتهديدات السيبرانية، فيما يتم التشجيع على إمكانية الوصول والانفتاح عبر مختلف أنواع الشبكات والأجهزة المترابطة.

[١] الاستراتيجية الوطنية للأمن السيبراني في مصر ٢٠١٧-٢٠٢١.

وسوف يتضمن هذا المطلب الركائز والمتطلبات الأساسية التي يقوم عليها الأمن السيبراني، والآليات والتدابير التي يتخذها الأمن السيبراني في حماية الخصوصية المعلوماتية، باعتباره أحد الضمانات الهامة والضرورية في حماية الخصوصية المعلوماتية، وذلك في ثلاثة أفرع فيما يلي:

- **الفرع الأول:** متطلبات تحقيق الأمن السيبراني.
- **الفرع الثاني:** الأمن السيبراني ضمانة هامة لحماية الخصوصية المعلوماتية.
- **الفرع الثالث:** آليات الأمن السيبراني في حماية الخصوصية المعلوماتية.

الفرع الأول

متطلبات تحقيق الأمن السيبراني

الأمن السيبراني هدف يمكن الوصول إليه، ولكن لا بد من توفير وتهيئة العديد من المتطلبات لتطبيق هذا الهدف على أرض الواقع، وهناك بعض المتطلبات اللازمة لتحقيق الأمن السيبراني على المستوى القومي حددتها الاستراتيجية الوطنية للأمن السيبراني في مصر ٢٠١٧-٢٠٢١، مع إضافة بعض المتطلبات التي نراها لازمة وضرورية لترسيخ وتحقيق الأمن السيبراني، وهذه المتطلبات هي:

أولًا– الدعم السياسي والمؤسسي الاستراتيجي والتنفيذي: ويشمل ذلك الوعي بخطورة التهديدات السيبرانية، وضرورة التعامل معها كأولوية وبأعلى قدر من الجدية، مع الاهتمام بالاستعداد المسبق بما يشمل الخطط الاستراتيجية والتنفيذية وخطط الطوارئ وآليات التنسيق العرضي، وإعداد الكوادر والتجهيزات التقنية واللوجستية.

ثانيًا– الإطار التشريعي: وضع الإطار التشريعي الملائم لأمن الفضاء السيبراني ومكافحة الجرائم السيبرانية، وحماية الخصوصية وحماية الهوية الرقمية وأمن المعلومات، وذلك بمشاركة من الأطراف المعنيين، وذوي الخبرة في القطاع الخاص ومؤسسات المجتمع المدني، مع الاسترشاد بالخبرات والتجارب والبرامج الدولية ذات الصلة، مع إعداد وتدريب المتخصين في إنفاذ القانون في الجهات القضائية والشرطية.

ثالثًا– الإطار التنظيمي والتنفيذي: وضع الإطار التنظيمي وإنشاء منظومة وطنية لحماية أمن الفضاء السيبراني، وتأمين البنى التحتية للاتصالات وتكنولوجيا المعلومات، ونظم وقواعد البيانات والمعلومات القومية، وبوابات الخدمات الحكومية والمواقع الحكومية على الإنترنت، وذلك بإعداد وتفعيل ما يعرف بفرق الاستعداد

والاستجابة لطوارئ الحاسبات والشبكات، في القطاعات الحيوية على المستوى الوطني، انطلاقًا من التجربة الرائدة في قطاع الاتصالات وتكنولوجيا المعلومات. تكون هذه الفرق مسؤولة عن أعمال المتابعة الأمنية لشبكات الاتصالات والمعلومات الوطنية والحواسب المتصلة بها، وعن التعامل مع أية أخطار سيبرانية تهددها أو هجمات سيبرانية توجه إليها، وعن التوعية والإعداد لمواجهتها.

رابعًا- البحث العلمي والتطوير وتنمية صناعة الأمن السيبراني: تشجيع ودعم وتنمية البحث العلمي والتطوير ودعم التعاون بين الجهات البحثية والشركات الوطنية، خاصة في مجال تحليل البرمجيات الخبيثة المتقدمة، ومجال تحليل الأدلة الرقمية، وفي مجال حماية وتأمين نظم التحكم الصناعية، ومجال تطوير أجهزة وأنظمة تأمين النظم والشبكات، ومجال التشفير والتوقيع الإلكتروني، ومجال حماية البنى التحتية للاتصالات وتكنولوجيا المعلومات، ومجال تأمين الحواسب السحابية وحماية قواعد البيانات الكبرى ومجال تقنيات الذكاء الاصطناعي وإنترنت الأشياء.

خامسًا- تنمية الكوادر البشرية والخبرات اللازمة لتفعيل منظومة الأمن السيبراني في مختلف القطاعات، بالتعاون والشراكة مع القطاع الخاص والجامعات ومؤسسات المجتمع المدني.

فلا بد من وضع سياسة رشيدة تستند على تدريب المختصين، مع توحيد الجهود في مواجهة الهجمات للحد من مخاطرها على المجتمع، ونشر ثقافة الأمن السيبراني، والتخذير من عدم فتح أي روابط أو تحميل ملفات مجهولة المصدر أو تبادل الأرقام السرية وغيرها.

سادسًا– التعاون مع الدول الصديقة والمنظمات الدولية والإقليمية ذات الصلة: ويشمل تبادل الخبرات وتنسيق المواقف في مجال أمن الفضاء السيبراني ومكافحة الجرائم السيبرانية، حيث إن تلك الجرائم لا تعترف بالحدود الجغرافية أو السياسية.

سابعًا– التوعية المجتمعية: وضع وتنفيذ خطط وحملات للتوعية المجتمعية بالفرص والمزايا التي تقدمها الخدمات الإلكترونية المؤمنة للأفراد والمؤسسات، وبأهمية الأمن السيبراني لحماية تلك الخدمات من المخاطر والتحديات التي قد تواجهها، فضلًا عن حماية الخصوصية وإطلاق برامج حماية الأطفال والنشء على الإنترنت.

إن تغير معايير النجاح والتميز في إطار الأمن السيبراني واختلاف قياسه يتطلب إعداد:

- برامج إعلامية خاصة بالأمن السيبراني، تستهدف كافة فئات المجتمع لتعرفه وتوعيه بكل الجوانب التي يحتويه الأمن السيبراني من ميزات وأخطار.
- إعداد برامج ودورات تدريبية لقطاعات الأعمال الحكومية والخاصة، لتمكينها من إعداد إطارات للتعامل في مجال الأمن السيبراني.
- إعداد إطارات تقنية متخصصة في البنية المعلوماتية ونظم العمل على شبكات الإنترنت.
- تطوير مؤسسات التعليم المتخصص في المجالات المرتبطة الأمن السيبراني، وذلك بالقيام بفتح فروع في الكليات لتدريس الأمن السيبراني، كتخصص قائم ذاته.

ثامنًا- تأمين البنية التحتية الحيوية: تتألف البنية التحتية الحيوية للأمن السيبراني من عناصر مادية، مثل: المرافق والمباني، وعناصر افتراضية، مثل: الأنظمة والبيانات والشبكات، وتأمين الأنظمة والبيانات؛ لدعم الثقة في التعاملات الإلكترونية بوجه عام وفي الخدمات الحكومية الإلكترونية بوجه خاص.

تاسعًا- تحديد المخاطر السيبرانية: ومواطن الضعف التي تحيط بالشباب والأطفال في الفضاء السيبراني.

ما تقوم به الشبكات في المجتمع الافتراضي يشكل قناعة الشباب وأفكاره وتعتبر من أكبر مغريات الشباب، وأكثرها خطورة، بل وباتت هي القوة المهيمنة على اهتمامات الناس عمومًا، والشباب على وجه خاص. فلقوى الشر والضلال وجود قوي ومؤثر عبر شبكات الإنترنت، عندما أدركوا مدى تأثيراتها البالغة على وعي وفكر شبابنا وأطفالنا مستفيدين من ميزتها في سرعة انتقال المعلومات المشبوهة والمغلوطة؛ نظرًا لاعتماد المؤسسات بشكل كبير على أنظمة المعلومات للقيام بالعملية الإنتاجية، تزيد احتمالية حدوث الخطر، مما يعني أن جميع المنظمات معرضة لخطر الهجوم السيبراني، وبالتالي يدور تقييم مخاطر الأمن السيبراني حول تحديد المخاطر وإدارتها والتحكم فيها.

وتعد إدارة المخاطر جزءًا لا يتجزأ من أي استراتيجية على مستوى المنظمة. وتُستخدم تقييمات المخاطر السيبرانية لتحديد وتصنيف المخاطر التي تتعرض لها العمليات والأصول التنظيمية الناتجة عن استخدام أنظمة المعلومات.

فالغرض الأساسي من تقييم المخاطر السيبرانية هو تقديم ملخص تنفيذي لمساعدة صانعي القرار وفهم قيمة المعلومات التي تحاول حمايتها، لذلك، يجب توفير الوقت والموارد لتحسين الأمن، أو تحديد التهديدات المحتملة، أو توفير نموذج أو

تجنب مشكلة توقف التطبيقات، ويجب أن نتكرر مع ظهور تهديدات جديدة، وإدخال أنشطة جديدة[١].

عاشرًا- تفعيل الشراكة بين القطاع الخاص والحكومة: ويتم ذلك بمشاركة القطاع الخاص في إعداد القواعد والنظم والتدابير والإجراءات اللازمة للأمن السيبراني، بالإضافة إلى توفير وإتاحة المراكز التكنولوجية ومراكز المعلومات اللازمة لدعم المؤسسات الصغيرة والمتوسطة الحجم.

بذلك، يمكننا رفع مستوى الأمان باتخاذ أسباب الوقاية من المخاطر السيبرانية، فهو مهم للغاية، ويجب أن تعمل كل الجهات المعنية بالفضاء السيبراني على توفير جميع الإمكانات التي من شأنها توفير أكبر قدر ممكن من الحماية.

إن مواجهة الأخطار والجرائم السيبرانية تحتاج إيمانًا صادقًا وجهدًا دؤوبًا وشراكة مجتمعية موسعة تشمل الجهات الحكومية والقطاع الخاص والمؤسسات البحثية والتعليمية ومنظمات الأعمال والمجتمع المدني؛ لتعظيم الاستفادة من الفرص

---

[١] بحث بعنوان: مخاطر الأمن السيبراني، كيفية تقييم المخاطر السيبرانية والتعامل معها؟: المخاطر الأمنية والامتثال، منشور على الموقع الآتي:
https://bakkah.com/ar/knowledge-center/how-to-perform-a-.cyber-risk-assessment

المتميزة التي تتيحها تقنيات الاتصالات والمعلومات الحديثة في شتى مجالات التنمية الاقتصادية والاجتماعية والثقافية، مع حماية مجتمعنا من مخاطر وأضرار الجرائم والهجمات السيبرانية[١].

الفرع الثاني

الأمن السيبراني ضمانة هامة لحماية الخصوصية المعلوماتية

إن التطورات الحديثة في تقنية المعلومات والاتصالات أحدثت تغيرات مستمرة ومضطردة في أساليب العمل والميادين كافة، إذ أصبحت عملية انتقال المعلومات عبر الشبكات المحلية والدولية وأجهزة الحاسب من الأمور الروتينية في عصرنا الحالي وإحدى علامات العصر المميزة التي لا يمكن الاستغناء عنها؛ لتأثيرها الواضح في تسهيل متطلبات الحياة العصرية، من خلال تقليل حجم الأعمال وتطوير أساليب تخزين وتوفير المعلومات، حيث إن انتشار أنظمة المعلومات المحوسبة أدى إلى أن تكون عرضة للاختراق؛ لذلك أصبحت هذه التقنية سلاحًا ذو حدين تحرص المنظمات على اقتنائه وتوفير سبل الحماية له[٢].

---

[١] الاستراتيجة الوطنية الوطنية للأمن السيبراني في مصر ٢٠١٧-٢٠٢١.

[٢] نبيل علي، الثقافة العربية وعصر المعلومات، عالم المعرفة، المجلس الوطني للثقافة والفنون والآداب، الكويت، ٢٠٠١، ص ١٢٠.

فقد نقلت نظم الكمبيوتر والإنترنت النشاط الاجتماعي والتجاري والسياسي والثقافي والاقتصادي من العالم المادي إلى البيئة الإلكترونية؛ وعليه فلا بد من مرافقة هذا التطور توجه واسع بشأن حماية خصوصية الأفراد، فقد يترك التصفح والتجول عبر الإنترنت على سبيل المثال لدى الموقع الذي تم زيارته كمية من المعلومات، كاسم المستخدم وعنوانه وأرقام الهاتف والفاكس وعنوان البريد الإلكتروني، بالإضافة إلى بعض المعلومات الاجتماعية كالسن والجنس والحالة الاجتماعية ومحل الإقامة والدخل الشهري، وأحيانًا بعض الاهتمامات الشخصية، أما مواقع البيع والشراء على الإنترنت والمواقع التي يتم فيها دفع، فإنها تتطلب رقم بطاقة الاعتماد ونوعها وتاريخ انتهائها[١].

ولعل الحديث عن الخصوصية في العصر الرقمي قد اكتسب أهمية قصوى مؤخرًا خاصة بعد تسريب بيانات ملايين المستخدمين لموقع فيسبوك والمعروفة إعلاميًا بفضيحة "كامبدرج أناليتيكا"[٢]، والتي مثل بسببها مؤسس فيسبوك لجلسة

---

[١] عبدالفتاح مراد، شرح جرائم الكمبيوتر والإنترنت، شركة البهاء للبرامجيات والكمبيوتر والنشر الإلكتروني، الإسكندرية، بدون سنة نشر، ص ٣٤.

[٢] فضيحة بيانات فيسبوك أناليتيكا هي فضيحة سياسية كبري تفجرت في أوائل عام ٢٠١٨ عندما تم الكشف عن أن شركة كامبريدج أناليتيكا قد جمعت "بيانات شخصية" حول ملايين الأشخاص على موقع فيسبوك من دون موافقتهم قبل أن تستخدمها لأغراض "الدعاية السياسية"، وقد وصفت

استماع أمام مجلس الشيوخ الأمريكي وأبدى ندمه واعتذاره عما شاع عبر موقع فيسبوك من أخبار كاذبة واستشراء لخطاب الكراهية[١].

لذلك، أصبحت خصوصية البيانات والمعلومات إحدى حقول البحث متزايدة الأهمية في عصرنا الحالي– عصر تقنية المعلومات، خاصة في إدارة بيانات المؤسسات والإدارات الحكومية، وكذلك الشركات الخاصة التجارية والخدمية والصحية، تلك التي تقوم بتخزين مئات الآلاف أو الملايين من سجلات العملاء أو المواطنين، والتي تتضمن بياناتهم الشخصية واهتماماتهم والأنشطة التي قاموا بها وميولهم، مع الإمكانية الجبارة في تحليل هذه البيانات ومقارنتها وسهولة نقلها بين القارات في ثوانٍ معدودة، وبتصاعد عدد المخترقين (Hackers) وسارقي الهويات (Theft Identity)، فعمليات اختراق خصوصية البيانات تقوم بالتأثير على حياتنا الخاصة وأعمالنا بشكل لم نكن لنتخيله من قبل[٢].

الفضيحة من قبل الكثيرين على أنها لحظة فاصلة في الفهم العام للبيانات الشخصية، كما أدت إلى حدوث هبوط كبير في سعر أسهم شركة فيس بوك العالمية، فيما دعا آخرون إلى تنظيم أكثر صرامة لاستخدام شركات التكنولوجيا للبيانات الشخصية.

[1] Corinne Cath ,Governing artificial intelligence : ethical ,legal and technical opportunities and challenges, 2018 ،available at : **http://dx.doi.org/10.1098/rsta.2018.0080.**

[٢] منى تركي الموسوي، جان سيريل فضل الله، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات

فقد أثرت تقنية المعلومات على الحق في الخصوصية على نحو أظهر إمكان المساس بهذا الحق؛ مما استدعي وجوب وضع إطار تشريعي ملائم لأمن الفضاء السيبراني ومكافحة الجرائم السيبرانية وحماية الخصوصية، ووضع إطار تنظيمي وإنشاء منظومة وطنية لحماية أمن الفضاء السيبراني، وتأمين البنى التحتية للاتصالات وتكنولوجيا المعلومات، ونظم وقواعد البيانات والمعلومات القومية وبوابات الخدمات الحكومية والمواقع الحكومية على الإنترنت.

فموضوع الأمن السيبراني يرتبط ارتباطًا وثيقًا بأمن الحاسوب، فلا يوجد الأمن السيبراني إذا لم يراعى أمن الحاسوب، وفي ظل التطورات المتسارعة في العالم والتي أثرت على الإمكانات التقنية المتقدمة المتاحة والرامية إلى خرق منظومات الحاسوب بهدف السرقة أو تخريب المعلومات أو تدمير أجهزة الحاسوب؛ كان لا بد من التفكير الجدي لتحديد الإجراءات الدفاعية والوقائية وحسب الإمكانات المتوفرة لحمايتها من

الحديثة عليها، مجلة كلية بغداد للعلوم الاقتصادية الجامعة، ٢٠١٣، ص ٣٢٣، منشور على الموقع الآتي: https://www.iasj.net/iasj/article/72783.

أي اختراق أو تخريب، وكان على إدارة المنظمات أن تتحمل مسؤولية ضمان خلق أجواء أمنية للمعلومات تضمن الحفاظ عليها[١].

ومن أهم عوامل تحقيق الأمن السيبراني: السرية والسلامة بالنسبة للبيانات وغيرها من المعلومات المتعلقة بالمستخدم. والمقصود بالسرية هنا: الموثوقية، وتعني: التأكد من أن المعلومات لا تُكشف ولا يُطلع عليها من قبل أشخاص غير مخولين بذلك. والمقصود بالسلامة: ضمان عناصر أمن المعلومات كلها أو بعضها يعتمد على المعلومات محل الحماية واستخدامها وعلى الخدمات المتصلة بها، فليس كل المعلومات تتطلب السرية وضمان عدم الإفشاء، وليس كل المعلومات بذات الأهمية من حيث الوصول لها أو ضمان عدم العبث بها[٢].

بيد أن الأمن السيبراني هو أحد وسائل وضمانات حماية الخصوصية المعلوماتية؛ إذ هو استراتيجية وسياسة ذات طبيعة تقنية تتصل بتأمين الدخول إلى البيانات أو معالجتها أو نقلها إلكترونيًا، ويذاع استخدام الأمن السيبراني والأمن

---

[١] منى تركي الموسوي، جان سيريل فضل الله، مرجع سابق، ص ٣٢٣.

[٢] أحمد أنور بدر، مجتمع المعلومات الكوني ومشكلات الخصوصية وأمن المعلومات وحق التأليف، المجلد ٣، العدد ٢، مكتبة الملك فهد الوطنية، الرياض، السعودية، ١٩٩٨، ص ٧٥، منشور على الموقع الآتي: http://ecat.kfnl.gov.sa:88/ipac20/ipac.jsp?session.

المعلوماتي من قبل المؤسسات وبنوك المعلومات أكثر منه من قبل الأفراد، وتهدف سياسة الأمن السيبراني إلى الآتي:

أولًا: تعريف المستخدمين والإداريين بالتزاماتهم وواجباتهم لحماية نظم الكمبيوتر والشبكات، كذلك حماية المعلومات والبيانات الشخصية وغير الشخصية في مراحل إدخالها ومعالجتها وتخزينها ونقلها وإعادة استراجعها.

ثانيًا: وضع آليات وتدابير لمكافحة تسريب المعلومات أو الدخول غير الآمن لها من خلال البرامج الإلكترونية التي تدعم تلك الحماية للبيانات الشخصية.

ثالثًا: وضع استراتيجية لخصوصية البيانات الشخصية، وعدم تعرضها لخطر الإفشاء، بالإضافة إلى سلامة المحتوى، والتي يقصد بها أن البيانات محل الحماية بيانات صحيحة لم يتم تعديلها أو العبث بها أو لم يتم إتلاف محتوى المعلومات عن طريق التدخل غير المشروع أو غير القانوني لمعالجة البيانات الشخصية[١].

---

[١] يراجع في ذلك: رفعت شميس العراقي، الأمن المعلوماتي بين القرصنة والإرهاب الإلكتروني، شبكة موسوعة دهشة، ٢٠٠٧، ص ٥٨؛ يونس عرب، موسوعة القانون وتقنية المعلومات، قانون الكمبيوتر، الطبعة الأولى، منشورات اتحاد المصارف العربية، ٢٠٠١، ص ٢٨١-٢٨٢؛ جبريل حسن محمد العريشي، أمن الملعومات، جامعة الملك سعود، الرياض، ٢٠٠٢، ص ٦٣؛ عايض المري، الحق في الخصوصية في العصر الرقمي، مقال منشور على الموقع الآتي:
.http://www.dralmarri.com/show.asp?field=res_a&id=205

ومن المنظور القانوني، فإن الأمن السيبراني هو محل دراسات وتدابير حماية سرية وسلامة المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة، وهو هدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها (جرائم الكمبيوتر والإنترنت)[1].

جدير بالذكر أن الأمن السيبراني لا يتحقق إلا من خلال توفير الحماية المتكاملة لقطاعي المعلومات والكمبيوتر، ويتخذ الأمن السيبراني عدة أنماط متعددة، منها: أولًا: الحماية المادية، وتشمل كافة الوسائل التي تمنع الوصول إلى نظم المعلومات وقواعدها كالإقفال والحواجز والغرف المحصنة. ثانيًا: الحماية الشخصية، وهي تلك التي تتعلق بالموظفين العاملين على النظام التقني المعني، من حيث التعريف بوسائل التعريف الخاصة بكل منهم وتحقيق التدريب والتأهيل للمتعاملين بوسائل الأمن إلى جانب الوعي بمسائل مخاطر الاعتداء على المعلومات. ثالثًا: الحماية الإدارية، والمقصود منها سيطرة جهة الإدارة على إدارة نظم المعلومات وقواعدها، مثل: التحكم بالبرمجيات الخارجية والأجنبية عن المنشأة ومسائل الإشراف والرقابة والمتابعة.

(1) John wiley& sons, Inc. Handbook of information security, 2006, volume.2, p.60.

وأخيرًا: الحماية المعرفية، كالسيطرة على إعادة إنتاج المعلومات وعلى عملية إتلاف مصادر المعلومات الحساسة والخاصة[١].

ووفقًا لما تقدم، فإن مخاطر الفضاء السيبراني أصبحت تشكل خطرًا كبيرًا في ظل انعدام الرقابة المهنية على الخصوصية المعلوماتية، كعمليات الابتزاز من قبل المخترقين وسارقي الهويات من خلال طلب المال أو تنازلات تؤدي إلى إغراق الضحية، ولمحاربة كل أشكال الجريمة الإلكترونية من الابتزاز والفدية والتجسس والهجوم.. وغيرها؛ لذا يجب تطبيق سياسة الأمن السيبراني وأنظمة الحماية البرمجية والمادية؛ لتحديد الإجراءات الدفاعية والوقائية لحمايتها من أي اختراق أو تخريب، ومقاومتها حال وقوعها بهدف التقليل والحد من آثارها.

الفرع الثالث

آليات الأمن السيبراني في حماية الخصوصية المعلوماتية

نظرًا لما يحاط بالخصوصية المعلوماتية من تحديات ومخاطر في الفضاء السيبراني، فإن الأمر يتطلب وجود مجموعة من الضوابط والآليات اللازمة لحمايتها، واتخاذ التدابير والإجراءات اللازمة للحفاظ على البيانات والمعلومات والاتصالات

[١] منى تركي الموسوي، جان سيريل فضل الله، مرجع سابق، ص ٣٠٦؛ يونس عرب، موسوعة القانون وتقنية المعلومات، مرجع سابق، ص ٢٨٤.

والمراسلات في المجتمع الرقمي، من حيث جمعها وتخزينها وتحليلها ونقلها ومعالجتها، وتوضيح الغرض من جمع البيانات، وتحديد الجهات التي يحق لها ذلك، ومدة حفظها، وإقرار مبدأ المسؤولية عند التجاوز في جمع البيانات أو تخزينها أو تحليلها أو معالجتها ونقلها، وكذلك إقرار مسؤولية بنوك المعلومات عن أي تجاوزات تؤثر على حرمة الحياة الخاصة، وخصوصًا مع تزايد قيمة البيانات من الناحية التجارية والأدبية، وخطورة ما يترتب على انتهاك الخصوصية من آثار سلبية، في ظل الإصرار على جمع المعلومات دون الحصول على إذن أو موافقة حقيقية من أصحابها ودون وجود اهتمام بحمايتهم[١].

وتلتزم الدولة بحماية أفرادها من مخاطر وتحديات الفضاء السيبراني؛ لأن انتهاك الخصوصية لا يهدد أفراد الدولة بل يمتد آثاره إلى الإضرار بالدولة نفسها، وتتعدد آليات الأمن السيبراني في حماية الخصوصية المعلوماتية في الفضاء السيبراني من حماية قانونية أو تشريعية، وحماية تقنية، وحماية تنظيمية، وحماية توعوية، وآليات حماية ذاتية من جانب الأفراد لخصوصيتهم تتمثل في التنظيم الأمثل لإعدادات الخصوصية، ونوضح ذلك فيما يأتي:

[١] يسري عبدالله عبدالباري عبدالمطلب، الحماية المدنية للخصوصية المعلوماتية، رسالة دكتوراة، كلية الحقوق، جامعة عين شمس، ٢٠١٦، ص ١٤٧-١٤٨.

أولًا- الحماية القانونية:

الحماية القانونية للحق في الخصوصية المعلوماتية تتمثل في ضرورة وجود مجموعة من التدابير أو القواعد التي تنظم حماية البيانات والمعلومات في الفضاء المعلوماتي؛ لضمان الحصول عليها بطرق مشروعة، واستخدامها وفقًا للغرض المحدد من جمعها، وأن تتمتع بالسرية والخصوصية، ويتم حذفها بعد تحقيق الغرض من جمعها؛ ولذلك نحتاج إلى قانون موحد وشامل ليحقق التوازن بين الخصوصية ومحدداتها من الحق في التعبير عن الرأي والحق في الحصول على المعلومات، ومحدد الأمن السيبراني أو الأمن المعلوماتي، وسياسات الخصوصية وشروط الاستخدام، ومحدد المصلحة العامة.

وتتزايد الحاجة إلى القانون الموحد لحماية الخصوصية المعلوماتية في ظل التحديات والمخاطر التي تواجهها، ومن أصعب هذه التحديات: تحدي الأمية الرقمية، وتحدي التجسس والتصنت من قبل السلطات الحكومية، وتحدي المراقبة من قبل الأفراد، وصعوبة الرقابة على المحتوى الرقمي من قبل مقدمي الخدمات، وتحدي الربط بين نظم الاتصالات والمعلومات، وتحدي التشتت والتعدد في جمع وتخزين

ومعالجة البيانات، وتحدي التطور في البرامج والتطبيقات على الإنترنت، وتحدي صعوبة تحديد القانون واجب التطبيق، والمحكمة المختصة بنظر النزاع[١].

فعملية سن القوانين والقرارات ذات النزعة الصارمة تفيد بشكل كبير في حماية الأمن السيبراني حتى لا يعتقد مخترقو الأمن المعلومات أنهم بمنأى عن العقاب، ومن ثم، الإفلات من المسؤولية القانونية بالهروب والتخفي بارتكاب جرائمهم المخلة بالأمن المعلوماتي عبر شبكات الإنترنت.

لذلك يلزم وضع قانون موحد للأمن السيبراني وحماية الحق في الخصوصية، يتسع نطاقه لحماية كل عناصر الخصوصية لتشمل حماية البيانات والمعلومات والاتصالات والمراسلات في الفضاء المعلوماتي، ولمنع انتهاكها بواسطة شبكة الإنترنت، وضرورة حماية البيانات المخزنة والمعالجة آليا؛ فمسألة الأمن السيبراني أصبحت مسألة قانونية أكثر منها مسألة تقنية؛ لتعلقها بمجالات الخصوصية وأمن المعلومات، لذلك لا بد أن يكون للقانونيين دور في تصميم الإجراءات والتدريب وتقديرات المخاطر.

---

[١] عزت عبدالمحسن إبراهيم سلامة، الحق في الخصوصية الرقمية وتحديات عصر التقنية، العدد الأول، السنة ٦٢، مجلة العلوم الاقتصادية والقانونية، كلية الحقوق، جامعة عين شمس، يناير ٢٠٢٠، ص ١١٢٢.

ثانيًا- الحماية التقنية:

تتمثل الحماية التقنية أو التكنولوجية للأمن السيبراني في خضوع أنظمة تقنية الاتصالات والمعلومات للمعايير التي تحقق الحماية اللازمة لمنع التعدي على المعلومات واختراقها، والحماية من عمليات معالجة البيانات غير المرغوب فيها أو غير الضرورية، وتهدف الحماية التقنية إلى التقليل من الثغرات الموجودة في الأمن المعلوماتي للتقليل من انتهاك الخصوصية والقضاء على القرصنة، الذين يعملون على كسر الشبكة الخاصة وأنظمة التشغيل للتعرف على الثغرات واختراقها.

ويمكن للأمن السيبراني حماية الخصوصية المعلوماتية من الناحية التقنية من خلال العديد من الآليات أهمها: تقنيات التشفير، تقنيات التجهيل، البرامج المتخصصة ضد القرصنة، وجدران النار، وتتمثل هذه التقنيات فيما يأتي:

١- تقنية تشفير المعلومات المنقولة والمحفوظة:

تقنية التشفير هي تقنية أو عملية بمقتضاها يتم ترجمة معلومة مفهومة إلى معلومة غير مفهومة، عبر بروتوكولات سرية قابلة للانعكاس، أي يمكن إرجاعها إلى حالتها الأصلية، وتستخدم تقنية التشفير لتوفير أمن وسلامة وسرية المعلومات على شبكة الإنترنت، وتقنيات التشفير تعد في مقدمة الوسائل والأدوات المبتكرة في مجال

أمن وسلامة وسرية المعلومات والمعاملات على الإنترنت، ومن خلال هذه التقنية يتم حظر الوصول للمعلومات للغير[١].

والتشفير يعني الحفاظ على المعلومات أو الحقوق الرقمية في بيئة آمنة، والتشفير من أهم الوسائل في مجال تأمين الشبكات، فتشفير المعلومات يعني تغيير وتحوير صورتها بحيث يختفي معناها الحقيقي ولا يستطيع غير المرخص له الاطلاع عليها، فيحقق التشفير سرية البيانات ويضمن سلامتها وعدم الاعتداء عليها؛ لأن البيانات التي لا يمكن قراءتها لا يمكن تعديلها أو تزييفها[٢].

ويلزم لعملية التشفير توافر مفتاح خاص يستخدم لعملية التشفير ذاتها، ويكون مع المرسل الذي ينشئ الدليل الرقمي ولا يعرفه سواه، وهناك مفتاح عام يشتق من المفتاح الخاص ويستخدم لفك الشفرة ويكون مع المرسل إليه، ويتم إنشاء المفتاح العام والخاص عن طريق اللوغاريتمات[٣].

---

[١] عزت عبدالمحسن إبراهيم سلامة، مرجع سابق، ص ١١٤٩.

[٢] محمد لطفي عبدالرحي، الجرائم المعلوماتية: التحديات والحلول، كلية الملك فهد الأمنية، الرياض، ٢٠٠٧، ص ٤٤.

[٣] محمد محمد أبو زيد، دور التقدم البيولوجي في إثبات النسب، العدد الأول، مجلة الحقوق، جامعة الكويت، مجلس النشر العلمي، الكويت، مارس ١٩٩٦، ص ٢٨٦، منشور على موقع دار المنظومة:

- https://search.mandumah.com/Record/75093/Details.

وآخر ما أُستُحدث في مجال التشفير هو تقنية التشفير الكمي Quantum Cryptography، وهي تقنية تستخدم مبدأ من مبادئ علم الفيزياء الكمية في عملية نقل البيانات من موقع إلى آخر بأسلوب آمن ١٠٠%، ومثل ذلك يجعل من المستحيل على أي متنصت معرفة محتويات الرسالة المرسلة، إلا بتغير المحتوى [١].

٢- تقنية التجهيل:

تعتبر تقنية التجهيل تقنية متطورة تؤمن لمستخدمي الإنترنت الاتصال الآمن بصورة مستترة، وذلك باستخدام أجهزة وتطبيقات تجعل الشخص مخفي في الفضاء الإلكتروني مما يصعب الوصول إليه ويصعب اختراق خصوصيته، ولكن يعيب تقنية التجهيل إمكانية إساءة استعمالها والقيام بأنشطة غير مشروعة؛ نظرًا لصعوبة القيام بأعمال المراقبة، وتتم تقنية التجهيل من خلال استخدام تقنية تعدل من السمات المميزة للشخصية الرقمية لتكون مجهولة، وتقنية التجهيل هي وسيلة من وسائل الأمن التقني أو الإلكتروني والذي يقوم على تأمين البيانات والمعلومات التي تتداول عبر الشبكات الداخلية أو الخارجية، والتي يتم تخزينها من الاختراقات، وهو مصطلح أوسع من

---

[١] ليتيم فتيحة، ليتيم نادية، الأمن المعلوماتي للحكومة الإلكترونية وإرهاب القرصنة، العدد الثاني عشر، مجلة المفكر، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر، مارس ٢٠١٥، ص ٢٤٩، منشور على الموقع الآتي:

- https://www.asjp.cerist.dz/en/downArticle/131/10/1/51530.

الأمن المعلوماتي، ويقصد به حماية البيانات والمعلومات سواء أكانت على جهاز الكمبيوتر وحماية أنظمة الكمبيوتر من الوصول إليها بطريق غير مشروع، أم العبث بالمعلومات أثناء التخزين أو المعالجة أو النقل، ويهدف إلى الحماية ضد التعطيل[١].

ويهتم الأمن السيبراني بالوسائل الضرورية لاكتشاف وتوثيق ورصد كل التهديدات، ويهتم بمجالات كثيرة كالتشفير، والتخزين، والتأمين الفيزيائي، والمعايير الأمنية، وإدارة أمن المعلومات والمخاطر.. وغيرها، وتقوم الشركات المتخصصة في الأمن المعلوماتي في تطوير نظم الحماية وتقديم أحدث تطبيقات جدران الحماية، وبرامج مكافحة فيروسات الحاسوب، والبريد الإلكتروني التطفلي، وتطبيقات الحماية ضد محاولات اختراقات الأنظمة المعلوماتية[٢].

وتسمح تقنية التجهيل للمستخدم أن يتصل بنظم المعلومات بصورة مستترة أو مجهولة ولا يمكن اكتشاف وجوده حيث حذف جميع العناصر المعرفة له، ويصبح التجهيل مشروعًا إذا كان هدفه حماية الحياة الشخصية وبياناته الرقمية[٣].

---

[١] عزت عبدالمحسن إبراهيم سلامة، مرجع سابق، ص ١١٥٠-١١٥١.

[٢] عمر يونس، استراتيجيات وتقنيات الحماية من أنشطة الاعتداء على خصوصية المعلومات، بحث منشور على الموقع الآتي: https://www.bibliotdroit.com.

[٣] بارق منتظر عبدالوهاب لامي، جريمة انتهاك الخصوصية عبر الوسائل الإلكترونية في التشريع الأردني: دراسة مقارنة، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، ٢٠١٧، ص ٦٢

٣- البرامج المتخصصة ضد القرصنة:

ويوجد الكثير من البرامج المستخدمة لمنع القرصنة التي تعمل على الإيقاع بالقراصنة واكتشافهم كحصان طروادة، حيث يتم عمل مسح كامل لجميع الملفات الموجودة بجهاز المستخدم ومطابقتها مع الموجودة بقاعدة البيانات الأساسية، بالإضافة إلى برنامج ارتباطات الأمن المعلوماتي بالأمن القومي "طبق العسل"، الذي يهدف لخداع القراصنة عن طريق توجيه المخترق أو القرصان إلى نظام معلومات ليس ذي أهمية ومتصل بأجهزة الأمن والتنبيه[١].

٤- جدران النار:

الجدران النارية هي مجرد أدوات بسيطة تعمل كمنقذ لتعاملات الإنسان على شبكة الإنترنت، بكلمات أخرى كحراس على طرف الشبكة، وقد تم استخدام أولى الجدران النارية لتحقيق الأمن المعلوماتي في أوائل التسعينات، وعلى الرغم من أن جدران النار لا تعد علاجًا لجميع أمن المعلومات على شبكة الإنترنت، إلا أنها ضرروية لأي استراتيجية متبعة، فهي حاجز بين شبكتين؛ إذ تقوم برمجيات جدران

وما بعدها، منشورة على الموقع الآتي:

- https://meu.edu.jo/libraryTheses/59e6f01aef1f3_1.pdf.

[١] ليتيم فتيحة، ليتيم نادية، مرجع سابق، ص ٢٤٩.

النار بفحص رزم البيانات القادمة والخارجة، اعتمادًا على مجموعة القواعد التي يضعها المشرف على الشبكة للسماح لهذه الرزم، أو لحجبها ومنعها من الوصول إلى الشبكة الموثوقة الداخلية[١].

ثالثًا– الحماية التنظيمية:

تتمثل الحماية التنظيمية في مجموعة القواعد أو الأعراف المهنية التي تستخدم لحماية الخصوصية عند مزاولة نشاط معين على الإنترنت، حيث إن المحترفين داخل مهنة معينة يتبعون قواعد تحكم علاقاتهم المهنية وتنظمها، على سبيل المثال ما تقوم به غرفة التجارة الدولية، وكذلك لمجلس أوروبا دور متقدم في وضع نماذج للعقود تسهل نقل البيانات ومنها البيانات الخاصة مع ضمان الالتزام بقواعد الحماية[٢].

فالحماية التنظيمية تتمثل في مجموعة ضوابط تضعها الشركات أو يُتفق عليها بين الشركات المهنية التي تقدم خدمات الإنترنت، وهذه الشركات تهدف إلى تقديم مجموعة من القواعد التنظيمية لمواجهة مخاطر أو تحديات الفضاء المعلوماتي ولخلق

---

[١] جميل زكريا محمود، الجريمة المعلوماتية وأساليب التأمين، المؤتمر الدولي لأمن المعلومات الإلكترونية، معًا نحو تعامل رقمي آمن، سلطنة عمان، خلال الفترة من ١٨–٢٠/١٢/٢٠٠٥.

[٢] بولين أنطونيوس أيوب، مرجع سابق، ص ٢٦٨.

نوع من الثقة والطمأنينة في نفوس المواطنين داخل المجتمع الرقمي، ومن أهم هذه الآليات والوسائل التنظيمية ما يأتي:

١- آلية تأكيد القبول أو القبول الثاني:

في المجتمع الرقمي يتم التعبير عن الإرادة بالضغط على أيقونة القبول؛ ونظرًا لأن هذا الضغط قد يصدر بالخطأ، لذلك لا تكون الضغطة الواحدة للتعبير عن القبول كافية كضمانة لرضاء حقيقي يحافظ على الحقوق الرقمية، نظرًا لاحتمالية الخطأ أو عدم وجود الرضا الواعي؛ لأن الضاغط قد يكون شخصًا آخر خلاف صاحب الحق الرقمي[١].

لذلك كان لا بد من وجود قواعد تنظيمية أو مهنية داخل شركات التقنية تقوم على اعتماد القبول المتكرر أو قاعدة تأكيد القبول للحصول على رضاء حقيقي من المستخدم.

وتوجد وسائل وآليات كثيرة لتأكيد القبول وعدم الاكتفاء بالقبول الأول فقط، وقد يتم تأكيد القبول بتكرار الضغط على المفتاح المخصص للقبول أكثر من مرة، أو إرسال كود معين على رقم الهاتف أو الإيميل الإلكتروني أو إعادة إرساله مرة أخرى،

---

(1) Rapport de la Cnil, Voix, image et protection des donneés Documentation francaise, 1996,p.50.

أو بالضغط على رقم معين، أو بملء استمارة القبول وإرسالها، أو الإجابة على بعض الأسئلة، أو باستلام رسالة البيانات، أو بإرسال رقم كودي.

والهدف من تأكيد القبول التيقن من صدور القبول على وجه اليقين وارتباطه به، ومواجهة مخاطر التقنية والمتمثلة في اللمس الخاطئ للجهاز الرقمي، والقيمة القانونية لهذا التأكيد، تتمثل في أن القبول لن يتم إلا بصدور التأكيد، وهنا يعني أن هذا التأكيد هو القبول بعينه[١].

كما يمكن تزويد النظام المعلوماتي بتقنية تمنع إرسال القبول من مجرد اللمس أو الضغط، بل ينبغي التأكد أكثر من مرة، أو بث رسالة تفيد القبول خلال مدة محددة، والضغط لتأكيد عملية القبول؛ لأن التأكيد يعني أن المستخدم على علم كافٍ بعملية القبول، لذلك يلزم أن يكون التأكيد مؤكدًا.

٢- التوثيق المعتمد للشخصية الرقمية:

تهدف آلية التوثيق المعتمد للشخصية الرقمية إلى ضمان عدم وجود شخصيات وهمية داخل المجتمع الرقمي، ويوجد الموثق الإلكتروني للتأكد من البيانات الشخصية وضمان دقتها فضلًا عن تقديم خدمة التصديق على البيانات، ويصدر التوقيع

[١] أسامة أبو الحسن مجاهد، حماية المصنفات على شبكة الإنترنت، دار النهضة العربية، القاهرة، ٢٠١٠، ص ٨٥ وما بعدها.

وشهادات التصديق الإلكتروني من مصادر محددة مختصة، يتم اعتمادها من هيئة تنمية وصناعة تكنولوجيا المعلومات، ويشترط لاعتماد هذه الجهات أن تستوفي الضوابط الفنية والقانونية، ومنها أن يكون لجهة التصديق وكيل بمصر، وأن يرخص له بإصدار شهادات تصديق، وأن يكون مرخصًا لها بإصدار شهادات في بلدها، وأن تكون من ضمن الجهات التي وافقت عليها بموجب اتفاقية دولية[١].

ووفقًا للمادة الحادية والعشرون من قانون التوقيع الإلكتروني المصري رقم ١٥ لسنة ٢٠٠٤ فإن بيانات التوقيع الإلكتروني والبيانات المحملة على أي وسيط إلكتروني وأي معلومات أخرى تقدم إلى الجهة المرخصة لها بإصدار شهادات التصديق الإلكتروني تكون سرية، ولا يجوز لمن قدمت إليه، أو اتصل بها بحكم عمله إفشاؤها للغير، أو استخدامها في غير الغرض الذي قدمت من أجله[٢].

لذلك لا بد من تأمين المعلومات والتعاملات الإلكترونية من خلال سلطة مختصة معتمدة لطمأنة مستخدم التقنية الإلكترونية من مستهلكين ومتعاقدين حتى يتم

---

[١] إبراهيم الدسوقي أبو الليل، الجوانب القانونية للتعاملات الإلكترونية، لجنة التأليف والتعريب والنشر، جامعة الكويت، الكويت، ٢٠٠٣، ص ١٣٤.

[٢] الجريدة الرسمية، العدد ١٧ تابع (د)، في ٢٢ أبريل ٢٠٠٤.

الوثوق بالتقنية وبهذه المواقع؛ لأن شركات الاعتماد لا تمنح شعارها إلا بعد استيفاء عدد من الضوابط والشروط الفنية والقانونية.

وتتولى الجهة المعتمدة عمليات التسوية المالية، وقد تتولى فك الشفرة الخاصة ببطاقة الائتمان الإلكترونية وتسجيل البيانات الشخصية من أسماء وأرقام صاحب البطاقة والبطاقة نفسها، وتوفير إجراءات معقولة لتأمين المعلومات الخاصة مثل استخدام كلمة السر أو التشفير أو الكود أو التكنولوجيا المماثلة[١].

ويتم تحديد هوية الأشخاص في المجتمع الرقمي وحقوقهم الرقمية عن طريق مجموعة من الضمانات من أهمها: التوقيع الإلكتروني وكلمات السر، ولكن يلزم أن تكون كلمة السر معقدة وديناميكية، والبطاقات الذكية وشهادة التصديق الإلكتروني الصادرة من جهة التصديق الإلكتروني، ومن الوسائط الأخرى التي يمكن أن تحدد هوية الشخص تسجيل المعلومات ببصمات العين، والوجوه، والأصوات، وقزحية وشبكية العين، والتوقيع اليدوي.

[١] عبدالرحمن محمد عبدالمحسن الصفتي، دور الشرطة في التأمين التقني للعقود الإلكترونية، رسالة دكتوراة، كلية الحقوق، جامعة عين شمس، ٢٠١٧، ص ٢٨-٢٩.

رابعًا- الحماية الذاتية:

حماية المستخدم لبياناته ومعلوماته يكون من خلال التحكم في إعدادات الخصوصية واستخدام إجراءات وأدوات جديدة لحمايتها مثل استخدام المتصفح الخفي الذي يمكن أن يخفي هوسية المستخدم، ويتولى التنظيم الذاتي للخصوصية المستخدم نفسه حيث يجب أن يرفض المستخدمين الذين لا يلتزمون بمدونات السلوك على الإنترنت، ويحظر أو يقيد الوصول لهم عبر البرامج المعلوماتية للتصفية، ويمكن للمستخدم في المجتمع الرقمي أن يحدد نطاق النشر والمشاركة والتعليق من قبل الأشخاص، فيمكنه النشر للعامة وفتح المجال للمشاركة والتعليق، ويمكنه حذف أو إخفاء ما ينشره، والكثير من المستخدمين يتجاهل ضبط الخصوصية، ويتجاهل اتخاذ التدابير اللازمة عليها ومراجعتها وعدم إفشاء الرقم السري للحساب لأي شخص[١].

ويراعى جعل النشر قاصرًا على الأصدقاء المقربين أو الموثوق فيهم، فضلًا على ضرورة إخفاء أو قفل البيانات الشخصية كإخفاء الموقع والوظيفة والحالة الاجتماعية

(1) Social media and online video privacy, Seminar lesson plan and class activities, A Consumer Action Publication, www.consumer-action.org, p 5-7.

والصورة الشخصية، كما يمكن إخفاء بعض البيانات كإخفاء الأصدقاء أو من يمكنه الاتصال بك أو التواصل معك، ومنع أي شخص من الاطلاع عليهم أو معرفتهم.

وضبط إعدادات الخصوصية إن كان يحمي من انتهاك الخصوصية من جانب الأشخاص العاديين إلا أنه قد لا يوفر الخصوصية الكافية للمحتوى المنشور من صور ثابتة أو فيديوهات أو منشورات أو مؤلفات، والسبب يرجع إلى أن شروط الاستخدام أو سياسات الاستفادة من الخدمة قد تحتمل اللبس، وتعطي الحق لمقدمي الخدمة أو متعهدي الإيواء في الاستفادة من المحتوى الرقمي الذي يشمله الحساب أو الموقع استنادًا إلى سياسة الخصوصية أو شروط الاستخدام[١].

وتتطلب حماية الخصوصية المعلوماتية الاهتمام بسلامة الجهاز الشخصي والمعلومات المدونة عليه، وذلك بالتحكم في نظام المشاركة المحلية في النظام، فتعتبر هذه الملفات أكبر مصدر للتهديد الأمني؛ لأنها تسمح لأي شخص على الإنترنت بالدخول على الجهاز ومشاركة الملفات والمعلومات الموجودة على الجهاز، كما يجب عدم تحميل ملفات أو برنامج من مصادر غير معروفة أو موثوق فيها، كما يلزم ألا

(1)Nicola Rabson, Social media and the law: A handbook for UK companies ،January 2014, http://www.linklaters.com/pdfs/mkt/london/TMT-Social-MediaReport., p 10.

نمكن الآخرين من الاطلاع على الجهاز الشخصي أو الرقم السري، وتجنب فتح الملفات والرسائل الإلكترونية الغريبة أو الآتية من مصادر غير معروفة، كما يلزم عدم حفظ اسم المستخدم وكلمة السر؛ لأن تخزينها يسهل من التعرف عليها.

وقد ألزمت الدول- في الآونة الأخيرة- الشركات والمؤسسات التجارية والمهنية بوضع تنظيم ذاتي أو نظام قانوني لحماية البيانات والمعلومات الشخصية للمواطنين، وفرض حماية كبيرة على البيانات؛ لأنها تكون على دراية بالمعلومات المخزنة وكيفية حمايتها بالوسائل التقنية أو غيرها، وكذلك وضع حد عادل ومتوازن للاستخدام والنقل والإفصاح عن البيانات بالقدر الذي لا يعيق عمل تلك الجهات.

خامسًا- الحماية التوعوية:

لكي يتم اعتماد سياسات الأمن السيبراني يلزم تجنب أخطار القراصنة والمحترفين في استهدافهم المستمر للمعلومات الاستراتيجية في الدولة والمعلومات الشخصية للأفراد؛ لذلك يجب توعية الجمهور والمواطنين داخل إقليم الدولة، ومن الضروري أن تقوم الدولة بحملة توعية عامة حول أمن البلاد من جانب الأمن السيبراني أو الأمن المعلوماتي بداية من رأس الدولة وصولًا إلى موظفيها وجمهور المواطنين حيث تشرح لهم المخاطر الأمنية وكيفية تفاديها، وما الإجراءات التي قامت وتقوم بها الدولة في

هذا المجال، بالإضافة إلى إمكانية عقد ندوات تدريبية وتثقيفية وإصدار نشرات إعلامية وتوعوية بهذا الخصوص.

فتلعب وسائل الإعلام دورًا مهمًا في إدراك الأشياء على ما هي عليه دون أن يشوبها أهواء أو مصالح أو تحيز، فهي تتنافى مع الكذب والخداع، ومرجو منها أن تقوم بإبراز الحقيقة وتمييزها عن الوهم، ومن ثم، يجب التحقق والتثبت دائمًا والتدقيق على المعلومات، والتحري والدقة في اختيار المصدر الذي يتم التعامل معه، كما ينبغي على محترفي وسائط الأخبار تعزيز الأخلاق المهنية، وحجب القول الفاحش البذيء الذي يروج للفاحشة والمنكر، بحيث يتم التعدي على معتقدات الناس وأخلاقياتهم ويشجع على تفشي الرذيلة بينهم أو يعكر صفو أمنهم، كذلك المادة الإعلامية لا يجوز للحصول عليها سلوك السبل والوسائل المُجَرّمة، فلا تنصت ولا تجسس ولا هتك للحرمات الشخصية.

الخاتمة

أولًا: النتائج

١. الأمن السيبراني يعني اتخاذ التدابير اللازمة لحماية الفضاء السيبراني من الهجمات السيبرانية، وذلك من خلال مجموعة من الوسائل المستخدمة قانونيًا وتقنيًا وتنظيميًا وإداريًا وتوعويًا في منع الوصول غير المشروع للبيانات والمعلومات الإلكترونية ومنع استغلالها بطريقة غير قانونية.

٢. أحدثت التطورات الهائلة في مجال تكنولوجيا المعلومات والاتصالات ثورة حقيقية في جميع مناحي الحياة، وقد أصبحت من أهم وسائل التعامل اليومي بين المؤسسات والأفراد بمختلف الطبقات، ولا ريب أن هذه التطورات تقدم العديد من المزايا للخصوصية تسهيلًا لحياة الناس، إلا أنها في المقابل تحمل في طياتها العديد من المخاطر والتهديدات التي تواجه المجتمع في مختلف المجالات، منها: خطر سرقة الهوية الرقمية والبيانات الخاصة؛ لذلك كانت الحاجة ماسة وضرورية لتبني الدول للأمن السيبراني لحماية القطاعات الحيوية للدولة والحفاظ على الخصوصية المعلوماتية.

٣. يشكل الأمن السيبراني جزءًا أساسيًا من أي سياسة أمنية وطنية، فيعتبر الأمن السيبراني من أولويات الدول للدفاع عن سياسة الوطن، فهو يهدف إلى الوقاية أو منع وقوع الهجمات السيبرانية من الأساس، ومقاومتها حال وقوعها بهدف التقليل والحد من آثارها، ومن ثم، وضع إجراءات سريعة للتعافي والرجوع إلى الوضع الطبيعي، سواء أكان ذلك عن طريق وضع خطط أم تنفيذ إجراءات أم رسم سيناريوهات لمواجهة مثل هذه التحديات.

٤. تعد حماية الحق في الخصوصية من الحقوق الدستورية الأساسية الملازمة للشخص الطبيعي بصفته الإنسانية كأصل عام، فهي تعد أساس بنيان كل مجتمع سليم، وهي تعتبر من الحقوق السابقة على وجود الدولة ذاتها؛ لذلك، تحرص المجتمعات على كفالة هذا الحق، وتعتبره حقًا مستقلًا قائمًا بذاته، ولا تكتفي بسن القوانين لحمايته، بل تسعى إلى ترسيخه في الأذهان؛ وذلك بغرس القيم النبيلة التي تلعب دورًا كبيرًا وفعالًا في منع المتطفلين من التدخل في خصوصيات الآخرين وكشف أسرارهم.

٥. لم يشر الدستور المصري على الحق في الخصوصية المعلوماتية بشكل مباشر، ولكن تناول هذا الحق ضمن حرمة الحياة الخاصة، وهذا لا يقدح في عدم

النص على الخصوصية المعلوماتية صراحة، فأغلب الحقوق الأساسية أصبحت تشتق منها حقوقًا ضمنية وردت بصورة غير صريحة بسبب التغيرات التي تطرأ في مجال حقوق الإنسان؛ وبسبب التطورات الاجتماعية والثقافية والتكنولوجية التي تطرأ على المجتمع التي تؤثر على استحداث حقوق وحريات الإنسان.

٦. حرصت مصر على حماية أمن فضائها المعلوماتي دستوريًا لسهولة التحول نحو الاقتصاد القائم على المعرفة والابتكار، والذي تشكل الاتصالات وتقنية المعلومات أحد عناصره، وركنًا أساسيًا من أركانه، وتعتبر أحد أهم الأهداف الاستراتيجية التي ركزت عليها الدولة المصرية ضمن خطط التنمية الاقتصادية التي تسعى لتحقيقها في الفترة المقبلة، والتي تتطلب توجيه الاستثمارات إلى قطاع تقنية المعلومات والاتصالات.

٧. اتخذت الدول مجموعة من الإجراءات على الصعيدين المحلي والدولي لحماية أفرادها من مخاطر وتحديات الفضاء السيبراني؛ لأن انتهاك الخصوصية لا يهدد أفراد الدولة بل يمتد آثاره إلى الإضرار بالدولة نفسها. وتعددت آليات الأمن السيبراني في حماية الخصوصية المعلوماتية في الفضاء السيبراني من حماية قانونية أو تشريعية، وحماية تقنية، وحماية تنظيمية، وحماية توعوية،

وآليات حماية ذاتية من جانب الأفراد لخصوصيتهم تتمثل في التنظيم الأمثل لإعدادات الخصوصية.

٨. اتخذت مصر خطوات فاعلة في مجال حماية الأمن السيبراني والأمن المعلوماتي من المخاطر والتهديدات السيبرانية والجرائم الإلكترونية، مثل: أطر تشريعية وتنظيمية وتقنية وذاتية وتوعوية جيدة، مثل: إنشاء استراتيجية وطنية قوية أنشأها المجلس الأعلى للأمن السيبراني الذي خضع لوزارة الاتصالات، ومن قبل وجود غرفة صناعة تكنولوجيا المعلومات والاتصالات

٩. بالرغم من أهمية دور البحث والتطوير في تحقيق التقدم التكنولوجي والتعزيز من التوطين في مجالات الفضاء المعلوماتي، إلا أن الدول العربية والإسلامية لم تولِ اهتمامًا كافيًا لهذا القطاع الحيوي الذي يمكن أن يسهم بشكل كبير في تطوير مجتمعات غنية بالثقافة والمعرفة التكنولوجية. ويظهر ذلك من خلال ضعف المؤشرات فيما يتعلق بالاستثمار في مجالات البحث والتطوير، وندرة الكفاءات والمختصين والطلاب والعلماء في الميادين التكنولوجية والتطبيقية.

ثانيًا: التوصيات

١. لا بد من تكاتف الجهود الداخلية والدولية لحماية أسرار البيانات والمعلومات الشخصية، وإدراج الجرائم السيبرانية في إطار معاهدات تسليم المجرمين، ويجب أن تباشر الدعاوى الخاصة بتلك الجرائم في العديد من الدول، وأن تراعى أحكام الإدانة الصادرة عن إحداها، وبخاصة في مجال تشديد العقوبة المنطوق بها في دول أخرى بالنسبة لمعتادي مثل هذا النوع من الإجرام، وإنشاء منظمات دولية وإقليمية، وإبرام اتفاقيات ثنائية وجماعية تكون متخصصة مهمتها الأساسية التنسيق بشأن مواجهة الجرائم السيبرانية واحتوائها ومحاولة التخفيف منها.

٢. ضرورة قيام الدولة على الصعيدين الحكومي والخاص بتبني تنظيم ذاتي لحماية الخصوصية أو تكليف القطاعات المتخصصة في الدولة بوضع تنظيم ذاتي داخلها لحماية البيانات الشخصية للمواطنين، وفرض الحماية القصوى على البيانات التي تضر بالدولة.

٣. يلزم وضع قانون موحد للأمن السيبراني وحماية الحق في الخصوصية المعلوماتية، يتسع نطاقه لحماية كل عناصر الخصوصية، لتشمل حماية

البيانات والمعلومات والاتصالات والمراسلات في الفضاء المعلوماتي، ولمنع انتهاكها بواسطة شبكة الإنترنت؛ فمسألة الأمن السيبراني أصبحت مسألة قانونية أكثر منها مسألة تقنية؛ لتعلقها بمجالات الخصوصية وأمن المعلومات، لذلك لا بد أن يكون للقانونيين دور في تصميم الإجراءات والتدريب وتقديرات المخاطر.

٤. ضرورة تشكيل محكمة مختصة بالجرائم السيبرانية على غرار إنشاء المحاكم الاقتصادية المتخصصة؛ نظرًا لصعوبة القضايا المتعلقة بها، وحاجتها إلى المزيد من المعطيات الخاصة قد لا تتوافر للقضاء العادي. كما أنه من الضروري إنشاء نيابة متخصصة للتحقيق ومواجهة وضبط أنواع الجرائم السيبرانية، وتصميم نظام أمني قوي يختص في متابعة وتطوير طرق الحماية من الهجمات السيبرانية. كما ينبغي تغليظ العقوبات المقررة لجرائم التعدي على الخصوصية المعلوماتية للأفراد خاصة في ظل انتصار أجهزة التنصت والتجسس التي صغرت حجمها وكثرت مصائبها.

٥. ضرورة التنسيق بين الدول من خلال منظمة الأمم المتحدة لإصدار قانون دولي شامل لتحصين الخصوصية المعلوماتية للأفراد ضد القرصنة

الإلكترونية، إن مثل هذا القانون يعزز ثقة الجمهور في المعاملات الإلكترونية، ومن ثم، دعم الاقتصاد القائم على المعرفة في عالمنا المعاصر.

٦. بالنظر لأهمية وخطورة الجرائم الماسة بحرمة الحياة الخاصة التي تقع عبر وسائل تقنية المعلومات الحديثة ولخصوصية بعض صورها وبغية تسهيل الإجراءات نقترح عدم الاكتفاء بتشريع قانون موضوعي، وإنما يجب تشريع قانون إجرائي ينسجم مع الطبيعة الخاصة للجرائم موضوع البحث على أن يتضمن القانون إجراءات تفتيش وسائل تقنية المعلومات الحديثة وأنظمتها وضبط محتوياتها ومراقبة المعلومات أثناء عملية انتقالها بالإضافة الى إجراءات التحقيق والمحاكمة في هذه الجرائم.

٧. يجب على الحكومة ممثلة في وزارة الاتصالات وتكنولوجيا المعلومات إصدار دليل إرشادي لاستخدام شبكة الإنترنت عمومًا وشبكات التواصل الاجتماعي خصوصًا، بحيث يعمم هذا الدليل على الجهات الحكومية والمؤسسات الخاصة ويتاح عبر وسائل الإعلام بسبل الاستخدام الأمثل لهذه الشبكات، وتجنب المخاطر الناجمة عنها ومن أبرزها بطبيعة الحال مخاطر انتهاك خصوصية المستخدمين.

٨. ضرورة إدراج مجال الفضاء السيبراني والأمن السيبراني ضمن المواد العلمية لكليات الحقوق والشرطة والكليات العسكرية؛ لضمان فهم سليم لأمن

المعلومات وخطورة تعرضه للانتهاك، وارتباطه بالأمن القومي وسياسات الدولة، والإشراف على صياغة الكوادر المعلوماتية الوطنية، بما يعني إنشاء وتطوير البنية التحتية والأنظمة المعلوماتية المختلفة؛ لضمان مستوى عالٍ من الأمن القومي.

قائمة المراجع

أولًا: القرآن الكريم.

ثانيًا: المعاجم

١. أبو الفضل جمال الدين بن منظور، تهذيب لسان العرب، الطبعة الأولى، دار الكتب العلمية، لبنان، ١٩٩٣م.

٢. أبو الفضل جمال الدين بن منظور، لسان العرب، الطبعة الأولى، دار الكتب العلمية، لبنان، ١٩٩٢م.

٣. أحمد مختار عمر، معجم اللغة العربية المعاصرة، الطبعة الأولى، عالم الكتب، القاهرة، ٢٠٠٨م.

٤. مجمع اللغة العربية، المعجم الوسيط، الطبعة الرابعة، مكتبة الشروق الدولية، القاهرة، ٢٠٠٤م.

٥. منير البعلبكي، المورد: قاموس إنجليزي عربي، دار العلم للملايين، بيروت، ٢٠٠٤م.

ثالثًا: المراجع العامة

١. عبدالفتاح بيومي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، المحلة الكبرى، ٢٠٠٧م.

٢. عبدالفتاح مراد، شرح جرائم الكمبيوتر والإنترنت، شركة البهاء للبرامجيات والكمبيوتر والنشر الإلكتروني، الإسكندرية، بدون سنة نشر.

٣. نبيل علي، الثقافة العربية وعصر المعلومات، عالم المعرفة، المجلس الوطني للثقافة والفنون والآداب، الكويت، ٢٠٠١م.

٤. يونس عرب، قانون الكمبيوتر، موسوعة القانون وتقنية المعلومات، الطبعة الأولى، منشورات اتحاد المصارف العربية، ٢٠٠١م.

رابعًا: المراجع المتخصصة

١. إبراهيم الدسوقي أبو الليل، الجوانب القانونية للتعاملات الإلكترونية، لجنة التأليف والتعريب والنشر، جامعة الكويت، الكويت، ٢٠٠٣م.

٥. أحمد عوض بلال، قاعدة استبعاد الأدلة المتحصل عليها بطرق غير مشروعة، الطبعة الأولى، دار النهضة العربية، القاهرة، ٢٠١٠م.

٢. آدم بديع آدم حسين، الحق في حرمة الحياة الخاصة ومدى الحماية التي يكفلها القانون الجنائي، دار النهضة العربية، القاهرة، ٢٠١١م.

٦. أسامة أبو الحسن مجاهد، حماية المصنفات على شبكة الإنترنت، دار النهضة العربية، القاهرة، ٢٠١٠م.

٣. أمين هويدي، الأمن العربي في مواجهة الأمن الإسرائيلي، دار الطليعة للطباعة والنشر، بيروت، لبنان، ١٩٧٥م.

٤. بارق منتظر عبدالوهاب لامي، جريمة انتهاك الخصوصية عبر الوسائل الإلكترونية في التشريع الأردني: دراسة مقارنة، كلية الحقوق، جامعة الشرق الأوسط، ٢٠١٧م.

٥. بولين أنطونيوس أيوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٩م.

٦. جبريل حسن محمد العريشي، أمن المعلومات، جامعة الملك سعود، الرياض، ٢٠٠٢م.

٧. جميل عبدالباقي الصغير، الإنترنت والقانون الجنائي، دار النهضة العربية، القاهرة، ٢٠٠٠م.

٨. حسام الدين الأهواني، الحق في احترام الحياة الخاصة: دراسة مقارنة، دار النهضة العربية، القاهرة، ١٩٧٨م.

٩. حسني الجندي، ضمانات حرمة الحياة الخاصة في الإسلام، دار النهضة العربية، القاهرة، ١٩٩٣م.

٧. حسنين المحمدي بوادي، الإرهاب الدولي بين التجريم والمكافحة، دار الفكر العربي، القاهرة، ٢٠٠٦م.

١٠. رفعت شميس العراقي، الأمن المعلوماتي بين القرصنة والإرهاب الإلكتروني، شبكة موسوعة دهشة، ٢٠٠٧م.

٨. سجان م. غوهيل، بيترك فوستر، المنهج المرجعي لمكافحة الإرهاب، الناتو، ٢٠٢٠م.

١١. سماح عبدالصبور، الصراع السيبراني: طبيعة المفهوم وملامح الفاعلين، مجلة السياسة الدولية، مؤسسة الأهرام، ٢٠١٧م.

١٢. صالح جواد كاظم، التكنولوجيا الحديثة والسرية الشخصية، دار الشؤون الثقافية العامة، بغداد، ١٩٩١م.

١٣. علي أحمد عبدالزعبي، حق الخصوصية في القانون الجنائي: دراسة مقارنة، المؤسسة الحديثة للكتاب، لبنان، ٢٠٠٦م.

١٤. علي جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة: دراسة مقارنة، منشورات زين الحقوقية، بيروت، ٢٠١٣م.

١٥. عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت:

الأحكام الموضوعية والجوانب الإجرائية، دار النهضة العربية، القاهرة، ٢٠٠٤م.

١٦. عمرو أحمد حسبو، حماية الحريات في مواجهة نظم المعلومات، دار النهضة العربية، القاهرة، ٢٠٠٠م.

١٧. فريد كيت، ترجمة: محمد محمود شهاب، الخصوصية في عصر المعلومات، الطبعة الأولى، مركز الأهرام للترجمة والنشر، القاهرة، ١٩٧٩م.

١٨. محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة، الإسكندرية، ٢٠٠٩م.

١٩. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، ١٩٩٤م.

٢٠. محمد عبدالمحسن المقاطع، حماية الحياة الخاصة للأفراد وضماناتها في مواجهة استخدام الحاسب الآلي، ذات السلاسل للطباعة والنشر، الكويت، ١٩٩٢م.

٢١. محمد عزت عبدالعظيم، الجرائم المعلوماتية الماسة بالحياة الخاصة، الطبعة الأولى، دار النهضة العربية، القاهرة، ٢٠١٦م.

٢٢. محمد عمارة، الإسلام والأمن الاجتماعي، الطبعة الأولى، دار الشروق، القاهرة، ١٩٩٨م.

٢٣. محمد لطفي عبدالرحي، الجرائم المعلوماتية: التحديات والحلول، كلية الملك فهد الأمنية، الرياض، ٢٠٠٧م.

٢٤. محمود عبدالرحمن محمد، نطاق الحق في الحياة الخاصة: دراسة مقارنة في القانون الوضعي (الأمريكي– الفرنسي– المصري) والشريعة الإسلامية، دار النهضة العربية، القاهرة، ١٩٩٤م.

٢٥. ممدوح خليل بحر، حماية الحياة الخاصة في القانون الجنائي، دار النهضة العربية، القاهرة، ١٩٨٣م.

٢٦. نديم عبده، أمن الكمبيوتر: الفيروسات والقرصنة المعلوماتية وانعكاساتها على الأمن القومي، الطبعة الأولى، دار الفكر للأبحاث والدراسات، بيروت، ١٩٩١م.

٢٧. نعيم مغبغب، مخاطر المعلوماتية والإنترنت، منشورات الحلبي الحقوقية، بيروت، ١٩٩٨م.

٢٨. هشام محمد فريد رستم، الخصوصية في عصر المعلومات، مركز الأهرام للترجمة والنشر، القاهرة، ١٩٩٩م.

٢٩. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، ١٩٩٤م.

٣٠. هلالي عبداللاه أحمد، اتفاقية بودابست لمكافحة الجرائم الإلكترونية (معلقًا عليها)، الطبعة الأولى، دار النهضة العربية، القاهرة، ٢٠٠٧م.

خامسًا: الرسائل العلمية

١. أيمن عبدالله فكري، جرائم نظم المعلومات: دراسة مقارنة، رسالة دكتوراة، كلية الحقوق، جامعة المنصورة، ٢٠٠٥-٢٠٠٦م.

٢. بارق منتظر عبدالوهاب لامي، جريمة انتهاك الخصوصية عبر الوسائل الإلكترونية في التشريع الأردني: دراسة مقارنة، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، ٢٠١٧م، منشورة على الموقع الآتي:

-https://meu.edu.jo/libraryTheses/59e6f01aef1f3_1.pdf.

٣. رافع رافع خضر صالح، الحق في الحياة الخاصة وضماناته في مواجهة استخدام الكمبيوتر، رسالة ماجستير، كلية الحقوق، جامعة بغداد، ١٩٩٣م،

منشورة على الموقع الآتي:

- https://colaw.uobaghdad.edu.iq/?page_id=19816.

٤. سوير سفيان، جرائم المعلوماتية، رسالة مقدمة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، جامعة تلمسان، الجزائر، ٢٠١١، منشورة على الموقع الآتي:

- https://www.elmizaine.com/2019/02/pdf_996.html.

٥. عادل عمر شريف، قضاء الدستورية: القضاء الدستوري في مصر، رسالة دكتوراة، كلية الحقوق، جامعة عين شمس، ١٩٨٨م.

٦. عبدالرحمن محمد عبدالمحسن الصفتي، دور الشرطة في التأمين التقني للعقود الإلكترونية، رسالة دكتوراة، كلية الحقوق، جامعة عين شمس، ٢٠١٧م.

٧. يسري عبدالله عبدالباري عبدالمطلب، الحماية المدنية للخصوصية المعلوماتية، رسالة دكتوراة، كلية الحقوق، جامعة عين شمس، ٢٠١٦م.

سادسًا: الدوريات والمؤتمرات

١. أحمد أنور بدر، مجتمع المعلومات الكوني ومشكلات الخصوصية وأمن المعلومات وحق التأليف، المجلد ٣، العدد ٢، مكتبة الملك فهد الوطنية،

الريـــاض، الســـعودية، ١٩٩٨، منشـــور علـــى الموقـــع الآتـــي:

.http://ecat.kfnl.gov.sa:88/ipac20/ipac.jsp?session

٢. أميرة عبدالعظيم محمد عبدالجواد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، العدد ٣٥، مجلة الشريعة والقانون، ٢٠٢٠.

٣. تومي فضيلة، أيديولوجيا الشبكات الاجتماعية وخصوصية المستخدم بين الانتهاك والاختراق، العدد ٣٠، مجلة العلوم الإنسانية والاجتماعية، جامعة قاصدي مرباح ورقلة، الجزائر، ٢٠١٧م، منشور على موقع دار المنظومة:

- https://search.mandumah.com/Record/843529.

٤. جميل زكريا محمود، الجريمة المعلوماتية وأساليب التأمين، المؤتمر الدولي لأمن المعلومات الإلكترونية، معًا نحو تعامل رقمي آمن، سلطنة عمان، ٢٠٠٥م.

٥. حسين بن سليمان بن راشد الطيار، الأمن السيبراني من منظور مقاصد الشارع: دراسة تأصيلية، المجلد ٦، العدد ٢١، مجلة جامعة الطائف للعلوم الإنسانية، جامعة الطائف، المملكة العربية السعودية، ٢٠٢٠م، منشور على الموقع الآتي:

- https://search.emarefa.net/ar/detail/BIM-1280150.

٦. خالد عبدالله السهيل المطيري، دور التشريعات الجزائية في حماية الأمن السيبراني بدول مجلس التعاون الخليجي، العدد الثامن والثلاثون، مجلة البحوث الفقهية والقانونية، جامعة الأزهر، كلية الشريعة القانون بدمنهور، يوليو ٢٠٢٢م.

٧. خدوجة الدهبي، حق الخصوصية في مواجهة الاعتداءات الإلكترونية: دراسة مقارنة، المجلد الأول، العدد الثامن، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف بالمسيلة، الجزائر، ٢٠١٧م، منشور على الموقع الآتي:

- http://dspace.univ-msila.dz:8080/xmlui/bitstream/handle/.

٨. رؤى سعد القرني، الحماية القانونية للحق في الخصوصية المعلوماتية: دراسة مقارنة، العدد السادس، مجلة كلية الدراسات الإسلامية والعربية للبنات بدمنهور، ٢٠٢١م.

٩. سماح عبدالصبور، الصراع السيبراني: طبيعة المفهوم وملامح الفاعلين، العدد ٢٠٨، المجلد ٥٢، مجلة السياسة الدولية، مؤسسة الأهرام، ٢٠١٧م.

١٠. صالح جواد كاظم، التكنولوجيا الحديثة والسرية الشخصية، دار الشؤون الثقافية العامة، بغداد، ١٩٩١م، منشور على الموقع الآتي:
.https://alexalaw.ahlamontada.com/t3911-topic

١١. عاطف كريم، الخصوصية الرقمية بين الانتهاك والغياب التشريعي، مركز دعم لتقنية المعلومات، القاهرة، ٢٨ أكتوبر ٢٠١٣م.

١٢. عائشة بن قارة مصطفى، الحق في الخصوصية المعلوماتية بين تحديات التقنية واقع الحماية، المجلد ٢، العدد ٦، مجلة البحوث القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الطاهر مولاي بسعيدة، الجزائر، ٢٠١٦م، منشور على الموقع الآتي:

- https://journals.ajsrp.com/index.

١٣. عائشة كريكط، حق الخصوصية لمستخدم الفضاء الرقمي: المخاطر والتحديات، المجلد ١٨، العدد ٢، مجلة الحقيقة للعلوم الاجتماعية والإنسانية، جامعة أحمد دراية، الجزائر، ٢٠١٩م، منشور على الموقع الآتي:
.https://search.emarefa.net/ar/detail/BIM

١٤. عبدالرحمن عاطف أبوزيد، الأمن السيبراني في الوطن العربي: دراسة حالة

المملكة العربية السعودية، العدد ٤٨، المركز العربي للبحوث والدراسات، ٢٠١٩م، منشور على الموقع الآتي: http://www.acrseg.org/41356.

١٥. عبدالرزاق تومي، تكنولوجيا المعلومات ودورها في التنمية الوطنية: دراسات استراتيجية، العدد ١٥، مركز البصيرة للبحوث والاستفسارات والخدمات التعليمية، الجزائر، ٢٠١١م، منشور على الموقع الآتي:

- https://www.asjp.cerist.dz/en/downArticle/250/7/15/114650.

١٦. عزت عبدالمحسن إبراهيم سلامة، الحق في الخصوصية الرقمية وتحديات عصر التقنية، العدد الأول، السنة ٦٢، مجلة العلوم الاقتصادية والقانونية، كلية الحقوق، جامعة عين شمس، يناير ٢٠٢٠م.

١٧. كامل فتحي كامل خضر، سمر المداح، العلاقة بين الاقتصاد الرقمي وأمن المعلومات: دراسة تطبيقية على عينة من عملاء البنك الأهلي المصري، العدد ٣، المجلة العلمية للاقتصاد والتجارة، ٢٠٢٠م.

١٨. كتاب أعمال المؤتمر الدولي، المحكم حول الخصوصية في مجتمع المعلوماتية، طرابلس، لبنان، يوليو ٢٠١٩م، منشور على الموقع الآتي:

- https://jilrc.com/wp-content/uploads/2019/07.

١٩. ليتيم فتيحة، ليتيم نادية، الأمن المعلوماتي للحكومة الإلكترونية وإرهاب القرصنة، العدد ١٢، مجلة المفكر، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر، مارس ٢٠١٥م، منشور على الموقع الآتي:

- https://www.asjp.cerist.dz/en/downArticle/131/10/1/51530

٢٠. ماجدة عبدالشافى خالد منصور، الحماية الدستورية للأمن السيبراني وأثره على النظام العام، المجلد ٤، العدد ٥٧، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنوفية، مايو ٢٠٢٣.

٢١. مجلس التعاون الخليجي، العدد ٣٨، مجلة البحوث الفقهية والقانونية، جامعة الأزهر، كلية الشريعة والقانون بدمنهور، ٢٠٢٢م.

٢٢. محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، بكلية الشريعة والقانون بدولة الإمارات العربية المتحدة، المنعقد خلال الفترة من ١-٣ مايو ٢٠٠٠م، منشور على الموقع الآتي:

- https://library.dji.ae/libero/WebOpac.cls?VERSION.

٢٣. محمد رياض الخاني، المبادئ الأخلاقية التي يجب أن يتحلى بها الطبيب في

ممارسته لمهنته الطبية: دراسة مقارنة، العدد ٢، مجلة الشريعة والقانون، جامعة الإمارات العربية المتحدة، ١٩٨٨م، منشور على الموقع الآتي:

- https://scholarworks.uaeu.ac.ae/sharia_and_law.

٢٤. محمد سامي الشوا، الغش المعلوماتي كظاهرة إجرامية مستحدثة، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، ١٩٩٣م.

٢٥. محمد فليح النمر، حماية خصوصية مستخدمي مواقع التواصل الاجتماعي على ضوء التشريعات في مملكة البحرين، مركز جيل البحث العلمي، كتاب أعمال المؤتمر الدولي المحكم حول الخصوصية في مجتمع المعلوماتية، العام السابع، العدد ٢٦، طرابلس، لبنان، يوليو ٢٠١٩م، منشور على الموقع الآتي:

-https://jilrc.com/archives/1107

٢٦. محمد محمد أبو زيد، دور التقدم البيولوجي في إثبات النسب، العدد الأول، مجلة الحقوق، جامعة الكويت، مجلس النشر العلمي، الكويت، مارس ١٩٩٦م، منشور على الموقع الآتي:

-https://search.mandumah.com/Record/75093/Details

٢٧. مصطفى إبراهيم سلمان الشمري، الأمن السيبراني وأثره في الأمن الوطني

العراقي، المجلد ١٠، مجلة العلوم القانونية والسياسية، ٢٠٢١م، منشور على الموقع الآتي:

- https://www.lawjur.uodiyala.edu.iq/index.php/jjps/issue/view.

٢٨. مكتب الأمم المتحدة المعني بالمخدرات والجريمة، استخدام الإنترنت في أغراض إرهابية، بالتعاون مع فرقة العمل التابعة للأمم المتحدة المعنية بتنفيذ تدابير مكافحة الإرهاب، نيويورك، عام ٢٠١٣م، منشور على الموقع الآتي:

- https://www.unodc.org/romena/ar/about-unodc-romena.html.

٢٩. منى تركي الموسوي، جان سيريل فضل الله، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها، مجلة كلية بغداد للعلوم الاقتصادية الجامعة، ٢٠١٣، منشور على الموقع الآتي: https://www.iasj.net/iasj/article/72783.

٣٠. منى عبدالله السمحان، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، العدد ١١١، مجلة كلية التربية، جامعة المنصورة، يوليو ٢٠٢٠م.

٣١. نائل عبدالرحمن صالح، واقع جرائم الحاسوب في التشريع الجزائي الأردني،

بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت المنعقد في كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ٢٠٠٠م، منشور على الموقع الآتي:

- https://library.dji.ae/libero/WebOpac.cls?VERSION.

٣٢. يوسف بوغرارة، الأمن السيبراني، الاستراتيجية الجزائرية للأمن السيبراني والدفاع في الفضاء السيبراني، المجلد الأول، العدد الثالث، مجلة الدراسات الإفريقية وحوض النيل، المركز الديمقراطي العربي، سبتمبر ٢٠١٨م، منشور على الموقع الآتي:

- https://democraticac.de/wp-content/uploads/2018/09.

٣٣. يونس عرب، الخصوصية وأمن المعلومات في الأعمال اللاسلكية بواسطة الهاتف الخلوي، ورقة عمل مقدمة إلى منتدى العمل الإلكتروني بواسطة الهاتف الخلوي، اتحاد المصارف العربية، عمَّان، الأردن، ٢٠٠٢م، منشور على الموقع الآتي:

- https://books.google.com.eg/books?.

٣٤. يونس مؤيد يونس، استراتيجية الولايات المتحدة الأمريكية للأمن السيبراني،

العدد ٥٥، مجلة قضايا سياسية، كلية العلوم السياسية، جامعة النهرين، بغداد، ٢٠١٨م، منشور على الموقع الآتي:

- https://search.emarefa.net/ar/detail/BIM-910984.

سابعًا: المراجع الأجنبية

1. Catota, Frankie E ؛Morgan1, M. Granger and Douglas C. Sicker, Cybersecurity education in a developing nation :the Ecuadorian environment, Journal of Cybersecurity, 00(0), 2019, 1–19 doi: 10.1093/cybsec/tyz001.
2. Christopher J. Millard, Legal Protection of Computer Programs and Data, Sweet and Maxwell Limited, London, The Cars Well Company Limited Toronto, 1985.
3. Corinne Cath ,Governing artificial intelligence : ethical ,legal and technical opportunities and challenges,

2018 ,available at : http://dx.doi.org/10.1098/rsta.2018.0080.

4.Jean-Jacques Hyest, la fraude informatique vue par le nouveau code pénale, exertises des systèmes de linformation Fvrier, 1992.

5.John wiley& sons, Inc. Handbook of information security, 2006, volume.2.

6.Matthew C. Waxman, "Cyber-Attacks and the Use of Force, The Yale Journal of International،Back to the Future of Article 2 (4), Vol. 36,2011.

7.Myriam Dunn, Information Age Conflicts, A Study of the, Center،Information Revolution and a Changing Operating Environment, ETH Zurich،for Security Studies (CSS, Issue No 64 ,2002.

8.Nicola Rabson, Social media and the law: A handbook for

UK companies, January 2014, http://www.linklaters.com/pdfs/mkt/london/TMT-Social-MediaReport.

9. Rasim M. Alguliyev , Yadigar N. Imamverdiyev Rasim Sh. Mahmudov and Ramiz M. Aliguliyev, about Information security as a national security component, published on 20 Jul 2020, published by Journal A Global Perspective.

10. Richard A. Kemmerer, Cyber security, University of California, Santa Barbara Department of Computer Science, 2003.

11. Social media and online video privacy, Seminar lesson plan and class activities, A Consumer Action Publication, www.consumer-action.org.

12. Ulrich sieber Les crimes informatiques et dautres crimes dans la domaine de la technologieinformatique, Revue Internationale de droit penal, 1993.

ثامنًا: المواقع الإلكترونية

١.الأمن الرقمي وحماية المستخدم من مخاطر الإنترنت، منشور على الموقع الآتي: https://edu.moe.gov.sa/jeddah.

٢.بحث بعنوان: كل ما ترغب في معرفته عن الأمن السيبراني: مفهومه وخصائصه وأشهر أنواع التهديدات فيه، بتاريخ ٢٠٢٣/١/١، منشور على الموقع الآتي: https://www.e3melbusiness.com/blog/cyber-security.

٣.بحث بعنوان: مخاطر الأمن السيبراني، كيفية تقييم المخاطر السيبرانية والتعامل معها؟: المخاطر الأمنية والامتثال، منشور على الموقع الآتي: https://bakkah.com/ar/knowledge-center/how-to-perform-a-.cyber-risk-assessment

٤.الحق في الخصوصية في القوانين المصرية: معوقات تشريعية وخطوات لم تكتمل، ٢١ يونيو ٢٠٢١ بحث منشور على الموقع الآتي: https://masaar.net/ar.

٥.عايض المري، الحق في الخصوصية في العصر الرقمي، مقال منشور على

الموقع الآتي:

http://www.dralmarri.com/show.asp?field=res_a&id=205

٦.عدنان مصطفى البار، خالد علي المرحبي، أمن المعلومات والأمن السيبراني، ٢٠١٨، بحث منشور على الموقع الآتي:

file:///C:/Users/facebook/Downloads/Article-of-this-week-DrAdnan-ALBAR-and-MrKhalid-Al-Marhabi-Jan-2018-1.pdf.

٧.عمر يونس، استراتيجيات وتقنيات الحماية من أنشطة الاعتداء على خصوصية المعلومات، بحث منشور على الموقع الآتي:

https://www.bibliotdroit.com.

٨.الفرق بين الأمن السيبراني وأمن المعلومات، بحث منشور على الموقع الآتي:

http://www.computersciencedegreehub.com.

٩.قاموس أكسفورد، منشور على الموقع الآتي:

https://en.oxforddictionaries.com/definition/cyber.

١٠.مصطفى الطيب، مدونة العلوم، أمن المعلومات، الفرق بين الأمن السيبراني

وأمن المعلومات، بحث منشور على الموقع الآتي:

.https://www.oolom.com

١١.يونس عرب، المخاطر التي تتهدد الخصوصية وخصوصية المعلومات في العصر الرقمي، بحث منشور على الموقع الآتي:

http://ww25.arablaw.org/Download/Privacy_Risks_Article.