ISSN: 2519 – 6138 (Print)
E-ISSN: 2663 – 8983(On Line)

TUJR
مجلة جامعة تكريت للحقوق
Tikrit University Journal for Rights

IRAQI Academic Scientific Journals
العراقية المجلات الاكاديمية العلمية

Tikrit University Journal for Rights
Journal Homepage : http://tujr.tu.edu.iq/index.php/t

كلية القانون
College of Law

The Evolution of the Administrative Control Function in the Face of Cybersecurity Issues

"A Comparative Analytical Study"

Assistant Professor .Dr. Ismail Fadel Halwas

College of Law, University of Fallujah, Fallujah, Iraq

dr.ismael.hellawss@uofallujah.edu.iq

Article info.

Article history:
- Received 22 March 2025
- Accepted 5 April 2025
-Available online 1 December 2025

Keywords:

Abstract: Technological advancements and their associated digital transformation processes, along with the emergence of artificial intelligence technologies, play the most significant and powerful role in shaping the reality we live in. Despite their countless benefits across all fields and sectors, they also have drawbacks that, in one way or another, undermine the morals, values, and principles of societies due to their misuse and the hostile nature of some entities or individuals..

تطور وظيفة الضبط الإداري في مواجهة قضايا الأمن السيبراني

"دراسة تحليلية مقارنة"

أ.م.د. إسماعيل فاضل حلواص

كلية القانون، جامعة الفلوجة، الفلوجة، العراق

dr.ismael.hellawss@uofallujah.edu.iq

معلومات البحث :

تواريخ البحث:
- الاستلام : ٢٢ / اذار/ ٢٠٢٥
- القبول : ٥ / نيسان/ ٢٠٢٥
- النشر المباشر: ١/كانون الاول/٢٠٢٥

الكلمات المفتاحية :

الخلاصة: وتلعب التطورات التكنولوجية وما ارتبط بها من عمليات التحول الرقمي، إضافة إلى ظهور تقنيات الذكاء الاصطناعي الدور الأهم والأقوى في تشكيل الواقع الذي نحياه، فرغم فوائدها التي لاحصر لها على في كافة المجالات والقطاعات المختلفة إلا أن لها من السلبيات ما ينال بشكل أو بآخر من الأخلاق وقيم ومبادئ المجتمعات نتيجة للاستخدامات السيئة لها والطابع العدائي لبعض الجهات أو الأشخاص.

المقدمة : في عصرٍ يتسم بالتقدم التكنولوجي الواسع، تواجه الحكومات صعوبات متلاحقة في مواجهة العديد من التحديات والمخاطر الأمنية، حيث تتعامل الهيئات والمؤسسات الحكومية على جميع مستوياتها وعبر الفضاء الإلكتروني مع كم هائل من البيانات والمعلومات، وهذه البيانات والمعلومات تشكل أهمية خاصة للدول والأفراد على حد سواء، مما يجعلها أهدافًا رئيسية للهجمات السيبرانية. فمن خلال اعتماد الجهات والمؤسسات الحكومية على كم متنوع من البيانات الضخمة يتم القيام بالعديد من المهام والمسئوليات. ومع الوقت توسعت وتشعبت العلاقات وتزايدت تبعا لهذا الانفتاح حدة المخاطر التي قد تنال من الجوانب الأمنية والسياسية والاقتصادية للدول[١].

وتلعب التطورات التكنولوجية وما ارتبط بها من عمليات التحول الرقمي، إضافة إلى ظهور تقنيات الذكاء الاصطناعي الدور الأهم والأقوى في تشكيل الواقع الذي نحياه، فرغم فوائدها التي لاحصر لها على في كافة المجالات والقطاعات المختلفة إلا أن لها من السلبيات ما ينال بشكل أو بآخر من

(1) يوسفي سفيان، وكلثوم مسعودي. الأمن الفكري وتحديات الأمن السيبراني - دراسة نظرية- ، مجلة الباحث، مج ١٦،ع ٢،٢٠٢٤، http://search.mandumah.com/Record/1516032ص ٦٥٥.

الأخلاق وقيم ومبادئ المجتمعات نتيجة للاستخدامات السيئة لها والطابع العدائي لبعض الجهات أو الأشخاص[١].

وقد أدى التكامل السريع للتكنولوجيا في مختلف جوانب الحياة، والتي تشمل الكثير من مجالات الأعمال للمؤسسات الخاصة، والحكومية، وكذلك الاستخدام الشخصي إلى ظهور فرص وتحديات غير مسبوقة[٢]. ومن أكثر التحديات إلحاحًا ذلك المشهد المتطور باستمرار للتهديدات السيبرانية، ومع تزايد تعقيد الهجمات السيبرانية وتكرارها، أصبحت ضرورة حماية مجالاتنا الرقمية أمرًا بالغ الأهمية [٣]. بل إننا لا نبالغ إذا قلنا أن التكنولوجيا الرقمية وما يرتبط بها من تحديات غيرت من المفاهيم التقليدية للقيادة والسيطرة سواء ما تعلق منها بالأعمال المدنية أو ما كان منها يخص المجالات العسكرية[٤].

ولمواجهة هذه التهديدات السيبرانية، يجب على الهيئات الحكومية تبني استراتيجيات جادة وقائمة على أسس علمية وتقنية حديثة تمنحها القدرة على مجابهة التحديات والمخاطر المختلفة الناتجة عن الاستخدام غير المشروع من قبل مرتكبي الهجمات السيبرانية.

أهمية البحث:

تكمن أهمية هذا البحث في التعرف على تطور وظيفة الضبط الإداري في ظل التنامي السريع لتكنولوجيا المعلومات والاتصال، ومدى الحاجة إلى وجود ضبط إداري إلكتروني قادر على مجابهة التحديات الأمنية المتمثلة في الهجمات السيبرانية[٥]. وذلك لأجل تحقيق غايات وأهداف الضبط الإداري في حماية النظام العام داخل الدولة بعناصره التقليدية والحديثة دون أن يتعدى ذلك الحقوق والحريات العامة [٦]. كما تبدو أهمية البحث أيضاً من منطلق أن الواقع الجديد المتمثل في سيطرة الفضاء الرقمي[٧]

---

[١] لمزيد من التفاصيل ينظر: د. صلاح الدين رجب فتح الباب صميدة. المواجهة التشريعية لمخاطر الذكاء الاصطناعي في ضوء المعايير الدولية، المحور الأول: دراسات في القضايا القانونية المستجدة بكافة مجالاتها، المؤتمر الدولي العلمي الثاني، القضايا القانونية المستجدة، مجلة كلية القانون ، جامعة سوران، أربيل، الفترة من ٢٢-٢١-٤-٢٠٢٤، المجلد ٧، العدد ١، ص٢٩٧-٣١٨.

[2] Alemayehu Tegegn, D. (2024). The role of science and technology in reconstructing human social history: effect of technology change on society. *Cogent Social Sciences*, *10*. https://doi.org/10.1080/23311886.2024.2356916

[3] Tzavara, V., Vassiliadis, S. Tracing the evolution of cyber resilience: a historical and conceptual review. Int. J. Inf. Secur.23, 1695–1719 (2024). https://doi.org/10.1007/s10207-023-00811-x

[4] Robert McLaughlin and Hitoshi Nasu .(2014). New Technologies and the Law of Armed Conflict, p.2. https://link.springer.com/book/10.1007/978-90-6704-933-7

[5]Araz Taeihagh, Governance of artificial intelligence, POLICY AND SOCIETY 2021, VOL. 40, NO. 2, p.138. https://doi.org/10.1080/14494035.2021.1928377

[٦] د. دعاء محمد ابراهيم بدران، التشريعات الممكنة للضبط الإداري والأمني لمكافحة الانحراف الفكري عبر منصات التواصل الاجتماعي، مجلة البحوث الفقهية والقانونية، كلية الشريعة والقانون بدمنهور، جامعة الأزهر، العدد ٤٠، يناير ٢٠٢٣، ص ٦٣٦.

على كافة مناحي الحياة يفترض وجود الإطار القانوني والتنظيمي الذي يسمح لسلطات الدولة من فرض سيادتها في الرقابة وضبط التصرفات غير المشروعة حماية لأمن واستقرار المجتمع.

وفي هذا الصدد تؤدي أنظمة الأمن السيبراني دوراً حيوياً لا غنى عنه في حماية البيانات والمعلومات سواء ما تعلق منها ببيانات الأفراد أو المؤسسات، وبصفة خاصة الهيئات والأجهزة التابعة للدولة، فالأمن السيبراني ولا شك يمثل جدار الحماية الأول لمواجهة عمليات القرصنة الإلكترونية التي تزايدت وتيرتها مع التقدم المذهل للتكنولوجيا وما تتسم به من ميزات ووظائف مختلفة ومتنوعة[١]. وهذا يتطلب أنشاء تحتية رقمية قوية مع أنظمة أمان فحسب بل ضرورة اتباع سياسة تضمن توفير العنصر البشري المدرب على استخدام أنظمة الأمن السيبراني والذي يمتلك كفاءة معينة[٢].

إشكالية البحث:

يعد أكبر التحديات التي تواجهها أنظمة الأمن السيبراني على كافة المستويات الوطنية والدولية هو ذلك الكم الهائل والمتنوع من البيانات الضخمة Big Data التي يزخر بها الفضاء الإلكتروني[٣]، للحد الذي جعل كافة العلماء على اختلاف تخصصاتهم يصفون تلك البيانات بالثورة التي غيرت العالم[٤]، بسبب حجمها وما تثيره من فوضى عند معالجتها وما يرتبط بذلك من إشكاليات تتعلق بإمكانية الاعتداء عليها والتلاعب بها، إضافة إلى أنها تشكل قيمة لأصحابها من أفراد ومؤسسات سواء خاصة أو حكومية. ومن جانب آخر تساعد البيانات الحكومات في المزيد من عمليات المراقبة، ومن الصعب في كثير من الأحيان الموازنة بين هذه المصالح والحق الأساسي للفرد في الخصوصية وحماية البيانات

---

(٧) لمزيد من التفاصيل ينظر: حسين أحمد مقداد عبد اللطيف، دور الضبط الإداري في الحد من مخاطر الفضاء الإلكتروني في مصر وفرنسا، مجلة العلوم القانونية والاقتصادية، العدد الأول، السنة الخامسة والستون، يناير ٢٠٣، ص ٦٣٩ وما بعدها.

(1) للمزيد ينظر: على آل مداوى، الأمن السيبراني: تعريفه - أهميته - أنواعه – استراتيجيات الوقاية من الهجمات السيبرانية، مجلة الدراسات الدولية، العدد٣٤، ٢٠٢٣، ص ١١٨.

https://0810gqbqu-1106-y-https-search-mandumah-com.mplbci.ekb.eg/Record/1454807

(2) Tom Kirkham, The critical role of administrative controls in cybersecurity, https://tomkirkham.com/the-critical-role-of-administrative-controls-in-cybersecurity/

(3) Rohit Kalakuntla, Anvesh Babu Vanamalaand Ranjith Reddy Kolipyaka, Cyber Security, HOLISTICA – Journal of Business and Public Administration,Volume 10 (2019): Issue 2, pp. 115-128. DOI: https://doi.org/10.2478/hjbpa-2019-0019

(4) Mayer-Schönberger, V., & Cukier, K. (2013). Big data: A revolution that will transform how we live, work, and think. Houghton Mifflin Harcourt.; Sk Tahsin Hossain, Tan Yigitcanlar, Kien Nguyen, Yue Xu, Cybersecurity in local governments: A systematic review and framework of key challenges, Urban Governance, Volume 5, Issue 1, 2025, Pages 1-19. https://doi.org/10.1016/j.ugj.2024.12.010.

الشخصية، فالناس لديهم سيطرة ضئيلة على بياناتهم الشخصية، كما قد يفتقرون إلى المعرفة بالبيانات الشخصية التي يتم جمعها[١].

وأحد أهم الأسئلة التي يطرحها البحث هو النظر في مدى الاستفادة من التقنيات الحديثة في توفير مزيد من الحماية للنظام العام من الانتهاكات الواقعة عبر الفضاء الرقمي، وذلك من خلال وضع استراتيجيات وخطط قائمة على دمج التكنولوجيا في أنظمة الأمن السيبراني للتخفيف من حدة الهجمات السيبرانية في الوقت الذي يُنظر فيه إلى التكنولوجيا ذاتها كأحد العوامل الرئيسية في تزايد هذه الهجمات[٢]. وهل تستطيع سلطات الضبط الإداري الإلكتروني تطوير وسائلها الأمنية الفنية والإدارية، وخاصة العنصر البشري المدرب على التعامل باحترافية مع التقنيات التكنولوجية للوقوف في وجه التهديدات الحديثة للهجمات السيبرانية؟

منهج البحث:

يعتمد هذا البحث على المنهج الوصفي، والمنهج التحليلي، مع التعرض للدور الذي تقوم به سلطات الضبط الإلكتروني ومدى تطور أدواته لمجابهة التحديات والمخاطر السيبرانية، كما سيتم الاستعانة بالمنهج المقارن للتعرف على المجهودات الدولية والوطنية في مجال الأمن السيبراني مع بيان التجارب الرائدة في هذا المجال الحيوي، مع التعرض لواقع الأمن السيبراني في العراق.

خطة البحث:

وفي سبيل الإلمام بموضوع البحث فسوف نقسمه إلى مبحثين على النحو التالي: المبحث الأول: الضبط الإداري مواجهة في تحديات العصر الرقمي. المبحث الثاني: التجارب الدولية والوطنية في مجال الأمن السيبراني.

---

(1) Elif Kiesow Cortez. (2020). Data Protection Around the World: An Introduction. Privacy Laws in Action, Pp. 1-6.

(2) Masike Malatji, Alaa Tolah. (2024): Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI, p.1-2. https://link.springer.com/article/10.1007/s43681-024-00427-4

المبحث الأول

الضبط الإداري في مواجه تحديات العصر الرقمي

تمهيد وتقسيم:

تعد البيئة الرقمية في العصر الحالي المصدر الحديث للمعلومات والمعارف المختلفة، حيث تعتمد عليها كافة المؤسسات العامة والخاصة وكذلك الأفراد لأداء المهام والأعمال المختلفة. فلا غرو أن التكنولوجيا الرقمية أصبحت من أهم موارد الاقتصاد العالمي[١]. والواقع أثبت أن الرقمنة باتت من السمات الأساسية للمجتمعات الحديثة، وأن المزيد من الأنشطة الاجتماعية والاقتصادية أصبحت موجودة عبر الفضاء الرقمي وهذه الأنشطة تعتمد على نماذج تفاعلية ذات تقنيات عالية تعمل على ربط الأشخاص والشركات والدول بالمعلومات، وإذ تشكل تلك المعلومات قيمة مادية ومعنوية ولذلك يتم الاعتراف بشكل متزايد بأهمية حمايتها والحفاظ عليها، ولذلك قامت معظم الدول بوضع وتحديث التشريعات التي تكفل حماية البيانات من خطر الاعتداء عليها[٢] واعتبرت ذلك واجباً قانونياً لا يقل في أهميته عن أي حق آخر يندرج تحت مظلة القانون[٣].

وغني عن البيان فإن التطور التكنولوجي ورغم ما يحققه من منافع جمة للمجتمعات، إلا أنه قد ارتبط به ظهور مجموعة من السلوكيات العدائية التي تزعزع استقرار النظام في المجتمع، وهذه الطائفة من السلوكيات باتت تعرف بالجرائم المعلوماتية [٤]. تلك الجرائم التي انتشرت بشكل كبير في السنوات الأخيرة بسبب طبيعتها العابرة للحدود، واعتمادها على تقنيات متطورة، والتي قد يصعب حتى على المتخصصين حماية أنفسهم منها، إضافة إلى أنه قد لا تتمكن سلطات الدولة في الكثير من الأحيان من اكتشاف تلك الجرائم أو تتبعها وضبط أدلتها أو ملاحقة مرتكبيها إذ أنها ترتكب من أي مكان[٥].

---

[١] محمد محمود مكاوي، البيئة الرقمية بين سلبيات الواقع وآمال المستقبل، مجلة المعلوماتية، العدد ٩، ٢٠٠٥، ص ٣٨-٤٩. http://search.mandumah.com/Record/28615

[2] Data Protection and Privacy Legislation Worldwide | UN Trade and Development (UNCTAD)

[٣] لمزيد من التفاصيل ينظر: وليد السيد سليم، ضمانات الخصوصية في الإنترنت، دار الجامعة الجديدة، ٢٠١٢، ص ٤ وما بعدها؛ د. عبد الفتاح المالحي، الإطار القانوني لحماية الحق في الخصوصية في عصر الرقمنة، مجلة الباحث للدراسات القانونية والقضائية، العدد ٥٦، يوليو ٢٠٢٣، ص ٣٨-٥٧؛

[٤] صلاح الدين رجب فتح الباب، أثر استخدام تقنيات الذكاء الاصطناعي على النظام العام، مصدر سابق، ص ٨٢ وما بعدها.

[٥] د. أميره محمد ابراهيم ساتي، الجريمة المعلوماتية في النظام السعودي، مجلة الأندلس للعلوم الإنسانية والاجتماعية، جامعة الأندلس للعلوم والتقنية، العدد ٧٥، يونيو ٢٠٢٣، ص ٩٢ وما بعدها.

ولذلك يتم النظر إلى السلوكيات غير المشروعة[١] عبر البيئة الرقمية على أنها تشكل تحدياً أمنياً بالغ الخطورة، وأن الهجمات السيبرانية المدعومة بالتقنيات الذكية تزيد المشهد الأمني تعقيداً، وتنال بشكل أو بآخر من الاستقرار المجتمعي. وهو ما يفرض على الدول اتخاذ نهج استباقي يركز على تحديث وتطوير القواعد القانونية لتتناسب مع التطورات المتسارعة في التكنولوجيا الرقمية[٢]، إضافة إلى ضرورة توفير الوسائل والأدوات الفنية القائمة على التكنولوجيا ذاتها، من أجل توفير مزيد من الحماية لأمن البيانات وبما يمنح الثقة للمستخدمين[٣]. ولأجل تحقيق تلك الحماية وبما أن الدولة تتحمل مسؤولية حفظ الأمن وإقرار النظام في المجتمع فإنها تسند تلك المهمة لهيئات الضبط الإداري.

وعلى هدى ما تقدم فسوف نتناول إيضاح الفكرة من خلال تقسيم هذا المبحث إلى مطلبين على النحو التالي: المطلب الأول: انعكاسات التطور التقني على وظيفة الضبط الإداري، المطلب الثاني: آليات الضبط الإداري في مواجهة التهديدات السيبرانية

المطلب الأول

انعكاسات التطور التقني على وظيفة الضبط الإداري

تتسم وظيفة الضبط الإداري بحسب الأصل بطابعها الوقائي الذي يمنع أي محاولات تستهدف الإخلال بالنظام العام قبل أن يحدث، إلا أن الأمر بالنسبة لمخاطر التقنيات الحديثة يجعل من الصعب على سلطات الضبط مواجهتها بالأساليب التقليدية، نظراً لأن أنشطة الأفراد التي تتم عبر تلك التقنيات الرقمية ليس لها وطن محدد فهي عابرة للحدود. فضلاً عن أنها تستهدف المجتمعات بكافة فئاتها العمرية ومستوياتها الثقافية، ولذلك فإنها تشكل خطورة غير اعتيادية على الجميع، ويجب على الدولة ومن خلال كافة الأجهزة المعنية وعلى رأسها سلطات الضبط الإداري أن تطوير أدواتها لتتناسب مع تلك المخاطر الإلكترونية. وعلى هذا الأساس ينعكس التطور التقني على وظيفة الضبط الإداري من عدة وجوه. وهو

---

(1) Isakov Abror Fakhriddinovich, Urozov Fakhridin Isakovich, Abduzhapporov Shahboz Muzaffar Ugli, Isokova Mukhlisa Fakhriddin kizi. (2024). ENHANCING CYBERSECURITY: PROTECTING DATA IN THE DIGITAL AGE, Innovations in Science and Technologies" ilmiy-elektron jurnal. Vo.1, No.1 pp.40-48.

(2) Kneuper, R. (2025). Technical and Organizational Implementation of Data Protection. In: Data Protection for Software Development and IT. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-70639-8_6

(3) Edwards, D.J. (2024). Data Protection. In: Critical Security Controls for Effective Cyber Defense. Apress, Berkeley, CA. pp. 57-96 https://doi.org/10.1007/979-8-8688-0506-6_3

ما سوف نتناوله من خلال فرعين الأول سيتناول تحديات حماية النظام العام في البيئة الرقمية أما الفرع الثاني سنتناول فيه ظهور الذكاء الاصطناعي وتزايد التحديات والمخاطر الأمنية

الفرع الأول: تحديات حماية النظام العام في البيئة الرقمية

يتكون النظام العام من عدة عناصر تشكل صمام الأمان لبقاء واستمرار أي مجتمع، ويلعب الرأي العام بخلفياته الثقافية والاجتماعية دوراً حيوياً في تشكيل خطوط الدفاع الأولى عن استقرار الأمن والحفاظ على النظام العام. بيد أن المفاهيم التقليدية للنظام العام والتي كانت تقتصر على عناصر محددة –الأمن العام والصحة العامة والسكينة العامة– قد اتسعت عن ذي قبل فشملت جوانب أخرى للمصلحة العامة، كالنظام العام الاقتصادي المعني بتحقيق الاستقرار الاقتصادي[١]، والنظام العام البيئي والحضري أو العمراني المتعلق بجمالية العمران، ثم شملت المفاهيم حماية الآداب العامة للحفاظ على قيم واخلاقيات المجتمع، كما ضمت كذلك صون الكرامة الإنسانية.

ولا شك أن تنظيم العلاقات داخل أي مجتمع ضرورة أولية من ضرورات الحياة الاجتماعية، ولن يتأتى الاستقرار إلا إذا وجدت السلطة التي تستطيع أن تلزم الأفراد باحترام القانون. ومن هنا كانت السلطة التنفيذية بما تملكه من امتيازات السلطة العامة هي القادرة على القيام بإلزام الأفراد باحترام القانون حماية للمصلحة العامة، وتقوم هيئات الضبط القضائي والإداري في الدولة بهذه المهمة[٢].

ولأن التطور سنة الحياة، فقد تطورت المجتمعات على مر الزمن، وأثرت العوامل السياسية والاقتصادية في كافة دول العالم على تشكيل المجتمعات. فمن جانب تغيرت العديد من النظم السياسية نتيجة للثورات وحركات التحرر وانتشار الأفكار والمبادئ الديمقراطية على يد الفلاسفة والمفكرين، وتبع ذلك تغير في طبيعة وشكل الحقوق والحريات العامة، وانتقلت الدول من مرحلة الدولة الحارسة إلى الدولة المنتجة، وترتب على ذلك زيادة في المجالات التي تشارك فيها الدولة[٣]، وقد أدى كل ذلك الى اتساع مدلول النظام العام وتطور عناصره وأملت الضرورات الاجتماعية على الحكومات ضرورة الموازنة بين المصلحة العامة والمصلحة الخاصة للأفراد، ولأجل تغليب مصلحة على أخرى كان على الدول أن تُسن

---

(1) Herscovici, A. (2023). Beyond Episteme: The Concept of Order. In: Value, Historicity, and Economic Epistemology. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-21157-7_8

(٢) د. أنور رسلان، وجيز القانون الإداري، ط ٣، بدون دار نشر، ٢٠٠٤، ص ٢٨١ وما بعدها.؛ د. ماجد راغب الحلو، القانون الإداري، دار الجامعة الجديدة، الأسكندرية، ٢٠٠٦، ص ٣٩٥.

(٣) محمد عبد العال السناري، مبادئ ونظريات القانون الإداري، دراسة مقارنة، ٢٠٠٤/٢٠٠٥، ص ١٩٥ وما بعدها.

التشريعات التي تنظم بها الأنشطة الفردية لأجل الصالح العام لجموع المواطنين، وأن تتولى السلطة التنفيذية مهمة حفظ النظام العام ولو باستخدام القوة لإلزام الأفراد على احترام القانون.

وقد غيرت تلك المعادلة من آليات عمل سلطات الضبط الإداري سواء من حيث نطاقه أو أهدافه أو الأساليب التي تعتمد عليها في أداء وظيفتها الضبطية. حيث توسعت المجالات التي تندرج ضمن نطاق عمل سلطات الضبط الإداري، فلم تقتصر على حماية النظام العام التقليدي المتمثل في حفظ الأمن العام والصحة العامة والسكينة العامة، بل شمل إلى جانب ذلك حماية النظام العام الاقتصادي والبيئي والأخلاقي. ومن جانب آخر تنوعت أساليب الضبط الإداري التي تنظم السلوك العام والنشاط الفردي من خلال إصدار القرارات التنظيمية (اللوائح) التي تضع قواعد عامة ومجردة للحفاظ على النظام العام، أو من خلال قرارات إدارية فردية تطبق على فرد محدد بذاته أو مجموعة أفراد محددين بذواتهم[١].

وقد أدى ظهور التكنولوجيا وبزوغ عصر الثورة المعلوماتية الى العديد من التغيرات في حياة الافراد والمجتمعات وكان لهذا التطور عدة مراحل مهمة يمكن أن نحدد بدايتها في ظهور الحاسوب والذي كان اه الأثر الفاعل في إعادة تشكيل الواقع الاجتماعي.

ففي بداية خمسينات القرن الماضي ظهر الحاسوب، حيث شهد عام ١٩٥٨ نقطة تحول في تطور تاريخ التكنولوجيا بتأسيس جمعية تاريخ التكنولوجيا (SHOT) ومجلتها "التكنولوجيا والثقافة(T&C)[٢]. وبمرور الوقت تطورت التكنولوجيا بشكل كبير ومتسارع، وتطورت معها تقنيات التخزين التي ساعدت على تخزين كم هائل من البيانات، وبالتزامن مع ذلك حدثت طفرات هائلة في مجال الاتصالات وانتشار شبكات الإنترنت الأمر الذي زاد من وتيرة التطور من حيث سرعة الحصول على المعلومات والمعارف المختلفة بمجرد الدخول على شبكات الإنترنت.

ومن المؤكد أن الثورة التكنولوجيا أحدثت تغيراً كبيراً في طريقة حياتنا سواء في بيئة الأعمال أو في محيط التفاعل الاجتماعي محلياً وعالمياً [٣]، وشمل ذلك التأثير مختلف شرائح المجتمع، وسرع من وتيرة

---

[١] مصلح محمود الصرايرة، القانون الإداري، الكتاب الأول، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، ٢٠١٢، ص ٣١٧.

[2] Neil J. Smelser, Paul B. Baltes, History of Technology, International Encyclopedia of the Social & Behavioral Sciences, Pergamon, 2001, Pages 6852-6857, https://doi.org/10.1016/B0-08-043076-7/02648-6. https://www.sciencedirect.com/science/article/pii/B0080430767026486

[3] Abou El Seoud, Mahinour. Exploring the Potential of E-Government in Reducing Corruption – Case of Egypt. 2024. American University in Cairo, Master's Thesis. AUC Knowledge Fountain.pp.8-12. https://fount.aucegypt.edu/etds/2207.

الابتكار والتنمية الاقتصادية[١]. كما اسهمت التكنولوجيا في تحسين جودة وأسلوب الحياة، وشمل ذلك مجالات الصناعة الزراعة، الرعاية الصحية، التعليم والتدريب، الأمن، وسجلات الهوية الوطنية وغيرها، كما أن الاستعانة بالتكنولوجيا الرقمية ترسخ من مفاهيم المساواة والعدالة الاجتماعية والسياسية [٢]. وبالتوازي مع تلك التحولات فإن التقنيات الرقمية ورغم ما تقدمه من مزايا ومنافع إلا أنه يرتبط بها العديد من المخاطر والأضرار التي قد تنال من السلم والاستقرار المجتمعي من خلال تهديد النظام العام[٣].

وبما أن العلاقات والروابط المجتمعية باتت متشابكة ومرتبطة ببعضها البعض، فهي ترتكز وبلا شك على عناصر متعددة، ورغم تنوعها واختلافها إلا أنها لا تخرج بأي حال عن الإطار القانوني والتنظيمي الذي تضعه الدولة، فالأمن والاستقرار لا ينفصل بسبب كون العلاقة خاصة أو عامة، إنما هو مفهوم شامل لا يتجزأ[٤]. ومن هذا المنطلق يشير البعض إلى ضرورة أن يشمل التنظيم القانوني كافة المسائل التي يثيرها التقدم التكنولوجي بسبب الآثار السلبية المرتبطة بالعديد من التقنيات الحديثة على أمن وسلامة المجتمعات، نتيجة للتغييرات الكبيرة التي شملت كافة مناحي الحياة الاجتماعية[٥]. ووصل التطور التكنولوجي الى مراحل لم يكن متوقعا بهذا الشكل الذي وصل اليه والذي يمكن ان لا يقف عند حدود يمكن صورها وهذا ما سنتناوله في الفرع التالي.

الفرع الثاني: الذكاء الاصطناعي وتزايد التحديات والمخاطر الأمنية

الذكاء الاصطناعي (AI) يمثل الصورة الحديثة للتهديدات التي أفرزتها التكنولوجيا، والتي تستدعي العمل على مواجهة ما قد ينتج عنه من مساوئ أخلاقية تلحق الضرر بأمن المجتمعات أو بالقيم الأخلاقية فيها، أو تنال من مقدرات الدول الاقتصادية لدرجة جعلت البعض ينظر إلى تلك الآثار السلبية ويصفها بالجانب المظلم للذكاء الاصطناعي[٦].

وبشأن تزايد الهجمات السيبرانية عن طريق استغلال التقنيات الذكية في التزييف أو الانتحال أو لشن هجمات إلكترونية، فإن البعض يرى أن تلك الأفعال من قبل المهاجمين تمثل استخداماً خبيثاً للذكاء

---

(1) Reza Montasari, Cyber Threats and National Security: The Use and Abuse of Artificial Intelligence, p.680.

(2) MarshMcLennan, Global cyber terrorism incidents on the rise,2021. https://www.mmc.com/insights/ publications/2018/nov/global cyber-terrorism-incidents-on-the-rise.html.

(3) GCHQ, Pioneering a new national security: the ethics of artificial intelligence, 2021. https://www. gchq.gov.uk/files/GCHQAIPaper.pdf .

(٤) صلاح الدين رجب فتح الباب صميده، المواجهة التشريعية لمخاطر الذكاء الاصطناعي في ضوء المعايير الدولية، مصدر سابق، ص ٣٠٤.

(5) Tai, M.C. (2020). The Impact of Artificial Intelligence on Human Society and Bioethics. Tzu Chi Medical Journal, 32(4), 339-343. http://doi:10.4103/tcmj.tcmj_71_20

(6) Reza Montasari, Cyber Threats and National Security: op. cit, p.685.

الاصطناعي[١]. كما قد يؤدي الاستغلال السيء للذكاء الاصطناعي إلى خلق المزيد من التعقيدات لدفاعات الشبكة من خلال تعطيل روبوت أو تحييده، أو لتقليد الأفراد الموثوق بهم، والتعرف عليهم ثم استخدام الروبوتات لتقليد سلوكياتهم ولغتهم. وفي المقابل تستطيع الجهات والعصابات الإجرامية ومن خلال الذكاء الاصطناعي من اكتشاف الثغرات الأمنية في الشبكات غير المحمية أو جدران الحماية غير المصححة بسرعة أكبر. وهذا من شأنه أن يضمن إمكانية تنفيذ الاعتداء في فترة زمنية قصيرة جدًا، وتتزايد خطورة الذكاء الاصطناعي عندما يستهدف الاعتداء الأمن القومي للدول[٢].

ويُعرف الذكاء الاصطناعي[٣] بأنه أحد الفروع البحثية لعلوم الكمبيوتر، والذي يهدف إلى إنشاء أنظمة ذكية تعتمد على الرقمنة لتقديم حلول للمشكلات بكفاءة[٤]، ويُعرف أيضاً بأنه ذلك العلم الذي يسعى نحو إنتاج آلة أو أنظمة ذكية لها قدرات شبيهة بقدرات العقل البشري[٥].

ففي الأونة الأخيرة أفرزت لنا التكنولوجيا نماذج وكيانات أخرى تتمتع بالقدرة على القيام بمهام حيوية ذات تأثير كبير في البيئات المختلفة. ويبدو أنها تعيد تشكيل المجتمعات بصور وأشكال مغايرة في العلاقات، سواء بين الأفراد وبعضهم البعض، أو بينهم وبين المؤسسات العامة. بل أن الأمر تعدى ذلك إلى التأثير على العلاقات بين الدول وبصفة خاصة بسبب التنافس القائم على امتلاك القوة التكنولوجية والتي سيكون لها تداعيات أمنية واقتصادية على مستقبل الدول السياسي والاجتماعي.

هذا وقد جاء بالقرار رقم ٢٠٦م ث/٤٢ الصادر عن منظمة اليونسكو التابعة للأمم المتحدة الخاص بإصدار توصية موجهة للدول الأعضاء وطبقاً للمادة ٤ من الميثاق المتعلق بالاتفاقيات الدولية، "أن

---

(1) Hoadley DS, Lucas NJ (2018) Artificial intelligence and national security. Congressional Research Service, Washington, DC.

(٢) صلاح الدين رجب فتح الباب، أثر استخدام تقنيات الذكاء الاصطناعي على النظام العام، مصدر سابق، ص ٨٣ وما بعدها.

(٣) الذكاء الصناعي artificial intelligence عبارة عن عملية محاكاة للوصول قدر الامكان الى الذكاء البشري، باستخدام الآلات، وأنظمة الحاسوب العملاقة... وتتم هذه العملية باستخدام علوم عدة مثل علم الحاسوب والرياضيات والهندسة والبيانات. لتقليد الوظائف تمامًا مثل الدماغ البشري. للمزيد ينظر:

-Haenlein. Siri, .in my Hand, who's the Fairest in the Land? On the Interpretations, Illustrations and Implications of Artificial Intelligence, Business Horizons. (1) 62.

- Goodfellow, Ian, Yoshua Bengio, and Aaron Courville. Deep learning. MIT press, 2016.

(4) Christian Djeffal, Artificial Intelligence and Public Governance: Normative Guidelines for Artificial Intelligence in Government and Public Administration, January 2020, pp.277-290. DOI: 10.1007/978-3-030-32361-5_12

(٥) عبد الحميد بسيوني: الذكاء الاصطناعي والوكيل الذكي، دار الكتب العلمية للنشر والتوزيع، القاهرة، بدون تاريخ نشر، ص١٩.

الذكاء الاصطناعي يندرج في عِداد القضايا الكبرى لعصر التكنولوجيات المتقاربة، إذ يعود بعواقب شديدة على البشر والثقافات والمجتمعات والبيئة. فقد يؤدي الذكاء الاصطناعي إلى تغيير معالم مستقبل التربية والتعليم والعلوم والثقافة والاتصال والإعلام والمعلومات، أيْ جميع المجالات التي تشملها المهمة المسندة إلى اليونسكو... وينبغي أن يقترن العمل في هذا المجال بالتفكر في المسائل الأخلاقية المتعلقة بالذكاء الاصطناعي لأن وسائل تكنولوجيا الذكاء الاصطناعي غير محايدة، بل متحيزة بحكم طبيعتها ..... ومنها أوجه التحيز المتعلقة بالاعتبارات القائمة على الجنس أو النوع. وبحث مسألة حماية خصوصيات الناس وبياناتهم الشخصية، واحتمالات ومخاطر ظهور أشكال جديدة للاستبعاد وعدم المساواة، ومسائل التوزيع العادل للمنافع والمخاطر، وكذلك المساءلة والمسؤولية، والعواقب على التوظيف وعلى مستقبل العمل، فضلًا عن العواقب الأمنية، واحتمالات ومخاطر الاستخدام المزدوج". ويهدف هذا القرار إلى وضع وثيقة تتضمن صياغة قانونية بشأن أخلاقيات الذكاء الاصطناعي، وتدعوا الوثيقة الدول الأعضاء إلى التعاون الدولي والتنسيق فيما بينها من أجل ذكاء اصطناعي قائم على القيم الإنسانية لمنفعة الأجيال الحاضرة والمقبلة[١].

والتجارب أثبتت أن استخدام الذكاء الاصطناعي في السنوات الأخيرة ورغم ما يقدمه من منافع في مجالات عديدة وعلى كافة المستويات، إلا أنه نتج عنه العديد من التحديات والمخاطر على الصعيد القانوني والأخلاقي والأمني[٢]. وليس من شك فإن النظام العام في أي دولة يهدف إلى حماية القيم الاجتماعية والأخلاقية من خلال التشريعات المنظمة للسلوك العام، والتي تتمثل في نهاية الأمر في عملية الضبط الإداري[٣].

---

(1) https://unesdoc.unesco.org/ark:/48223/pf0000369455_ara

[٢] محمد سعد أحمد، دور التأمين في مواجهة المخاطر الناشئة عن الذكاء الاصطناعي وتكنولوجيا المعلومات، دراسة تحليلية، مجلة مصر المعاصرة، الجمعية المصرية للاقتصاد السياسي والتشريع، القاهرة، العدد ٥٤٣، يونيو ٢٠٢١، ص ٤٥٩ وما بعدها.
https://espesl.journals.ekb.eg/article_229848_02c346ef848dc371ef1504401444927b.pdf

[٣] محمد جمال جبريل وآخرون، القانون الإداري، الجزء الثاني، النشاط الإداري، الإسراء للطباعة، القاهرة، ب. ت، ص٢١.

المطلب الثاني

آليات الضبط الإداري في مواجهة التهديدات السيبرانية

يهدف الضبط الإداري بوجه عام إلى الحفاظ على النظام العام من خلال اتخاذ تدابير إدارية وأمنية لمنع أي إخلال ينال من أمن واستقرار المجتمع، وتتسم تلك التدابير بطابعها الوقائي، أي أنها تطبق بشكل استباقي يمكن سلطات الضبط من توقي أي ضرر محتمل يقع نتيجة لأنشطة الأفراد، ويمس بشكل أو بآخر من النظام العام في كل أو بعض عناصره، ومع ذلك فإن التحولات الأخيرة التي لحقت بالمجتمعات نتيجة انتشار التكنولوجيا والقدرات الكبيرة في مجال الاتصالات غيرت من شكل وطبيعة العلاقات الاجتماعية، وتغيرت تبعاً لذلك المفاهيم الأمنية، فضلاً عن أن مفهوم النظام العام متغير من دولة إلى أخرى، وحيث أن الأفعال والسلوكيات المنحرفة التي تقع في البيئة الرقمية –كما سبق وأن أشرنا– ليس لها وطن محدد، فإن سيطرة سلطات الضبط عليها قد تواجه بصعوبات كثيرة، كما قد يختلف التعاطي من دولة لأخرى بحسب أنظمة كل دولة. من أجل توضيح الصورة بشكل أكبر والتعرف على كيفية تغلب سلطات الضبط الإداري على هذه الصعوبات، فإننا سوف نتناول هذا المطلب من خلال فرعين على النحو التالي:

الفرع الأول: طبيعة التهديدات السيبرانية

استطاعت عصابات الإنترنت استخدام التقنيات الحديثة واستغلال الثغرات الأمنية في المواقع الإلكترونية للهجوم على البينية التحتية الرقمية[١]، مما قد يشكل خطراً على المصلحة العامة بمفاهيمها الاقتصادية والسياسية والأمنية والأخلاقية. وقد أثارت كل تلك التحديات المخاوف من عدم قدرة سلطات الضبط على مواجهة ما قد ينجم عن الاستخدام غير المشروع للتكنولوجيا من مخاطر على أمن وسلامة المجتمعات. وبصفة خاصة ذلك الكم المتزايد من الهجمات السيبرانية.

---

[١] لمزيد من التفاصيل ينظر: طارق السيد محمود، تقنيات الذكاء االصطناعي ودورها فى تسهيل الإرهاب الإلكتروني ومكافحته، مجلة جامعة الزيتونة الأردنية للدراســــــات القانونية، المجلد الخامس، اصدار خاص، ٢٠٢٤، ص٢٨٥.

ومع تزايد استخدامات الفضاء الإلكتروني تبدو الحاجة ملحة إلى وضع استراتيجيات للسيطرة والتحكم لمواجهة ما يطلق عليه التهديدات السيبرانية. وبصفة خاصة ما يمكن أن يترتب على إساءة استخدام التكنولوجيا من مخاطر أمنية[١].

بيد أنه يجب التمييز بين كل من الجريمة السيبرانية والهجمات السيبرانية، فالجريمة السيبرانية هي: "أي فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلومات، يهدف الى الاعتداء على الأموال المادية أو المعنوية أو الاعتداء على خصوصية الأفراد"[٢]. أما الهجمات السيبرانية (Cyber Attacks): فهي عبارة عن هي محاولات خبيثة لاختراق أو تعطيل الأنظمة الرقمية، الشبكات، أو سرقة البيانات[٣]. وتتم بأساليب تقنية بحته لتعطيل الخدمة في قطاع أو أكثر من القطاعات الحساسة أو لاختراق الأنظمة. ومن أشهر أنواعها، هجمات الفدية ((Ransomware) ،هجمات التصيد ((Phishing) ،هجمات حجب الخدمة (DDoS). وعلى خلاف الجرائم السيبرانية التي قد يكون منفذوها أفراد أو منظمات إجرامية، فإن الهجمات السيبرانية قد تقع في الغالب من جماعات هاكرز، أو جهات دولية (حروب إلكترونية).

وتتنوع صور وأشكال الهجمات السيبرانية لغرض القيام بأنشطة خبيثة، مثل تطوير هجمات إلكترونية جديدة أو استغلال الثغرات الأمنية الموجودة[٤]. فقد تتمكن جماعات القرصنة والكتائب الإلكترونية ذات التوجهات المعادية للحكومات استغلال نقاط ضعف الشبكات واختراقها لإحداث اضطرابات أمنية، أو هجمات على البنى التحتية أو على السلم الاجتماعي أو للإضرار بالمقدرات الاقتصادية بما ينال من السيادة الوطنية والقوة الاقتصادية للدول.

والتهديدات السيبرانية التي يمكن أن تشكل خطراً على المصالح العليا للدولة عبر الفضاء الرقمي (سواء باستخدام التكنولوجيا عبر المنصات الرقمية أو وبدعم من التقنيات الذكية)، قد تتخذ صوراً وأشكالاً متعددة منها على سبيل المثال تزييف الحقائق، نشر الشائعات والدعاية المضللة للرأي العام، نشر الأخبار ومقاطع الفيديو المفبركة بهدف التأثير على الجبهة الداخلية الوطنية أو لضرب العلاقات بين

---

(١) وائل أحمد عبد الله صبرة، التحديات الأخلاقية التي تواجه العلم والتكنولوجيا في عصر البيانات الضخمة، مجلة كلية الآداب، جامعة سوهاج، العدد ٥٣، ٢٠١٩، ص ٦٠٠-٥٥٧. https://search.mandumah.com/Record/1035437

(٢) فارس محمد العمارات، ابراهيم الحمامصة، الأمن السيبراني المفهوم وتحديات العصر، دار الخليج للنشر والتوزيع، عمان، الأردن ، ٢٠٢٢، ص ٧٤.

(٣) للمزيد ينظر: محمد طه ابراهيم الفليح، الجريمة السيبرانية في النظام القانوني الأردني، مجلة الزرقاء للبحوث والدراسات الإنسانية، المجلد الرابع والعشرون، العدد الأول، ٢٠٢٤، ص ١١٦ وما بعدها.

(4) Masike Malatji, Alaa Tolah.op.cit.

الدول[١]. وقد يترتب على ذلك الخداع والتضليل تفاقم الأزمات داخل الدول، ومن الأحداث الشهيرة التي استخدمت فيها تقنيات الذكاء الاصطناعي الانتخابات الأمريكية ٢٠١٦م، واستفتاء Brexit في انجلترا، وغيرها من الأحداث السياسية[٢].

ويزداد الوضع تعقيداً مع ظهور أنواع مستحدثة من الجرائم الإلكترونية[٣]. والتي تتم عن طريق قيام المهاجمين باستغلال نقاط الضعف في المواقع الإلكترونية والتسلل إلى قواعد البيانات الخاصة بالأفراد والمؤسسات، وإزالة ومحو البيانات الشخصية، أو التلاعب بها[٤]. وهذا الأمر في حد ذاته يشكل خطراً كبيراً على أمن واستقرار داخل المجتمع[٥]. ويرى البعض[٦] أن الهجوم السيبراني قد يتخذ خمسة أنماط، وهي: التجسس السيبراني الذي ترعاه بعض الحكومات لجمع المعلومات بهدف شن الهجمات السيبرانية المستقبلية، الهجوم السيبراني الذي يهدف إلى زعزعة الاستقرار وبث الفوضى داخل الدول، الهجوم السيبراني لأجل تعطيل البنى التحتية وتسهيل الاعتداء المادي والمعنوي على الأفراد والمؤسسات، الهجوم السيبراني الذي يأتي تالياً للعدوان المادي، والهجوم السيبراني بهدف التدمير أو التعطيل على نطاق واسع كهدف نهائي والذي اصطلح على تسميته بالحرب السيبرانية.

كذلك أشارت العديد من التقارير إلى أن المهاجمين السيبرانيين يشكلون تهديدًا خطيرًا للتشغيل الآمن للشبكات[٧]. وقد تم الإبلاغ عن ستة وأربعين هجوماً سيبرانياً على قطاع الطاقة في عام ٢٠١٥،

---

(1) Julian Richards, Cyber-War: The Anatomy of the Global Security Threat, PALGRAVE MACMILLAN, 2014, P.3-6. DOI: 10.1057/9781137399625.0001

(٢) سعيد مفلح حمود الصويلح، الدور الإستشرافي للذكاء الاصطناعي في إدارة الأزمات الأمنية، مجلة الفكر الشرطي، المجلد ٣٢، العدد ١٢٧، اكتوبر ٢٠٢٣، ص ٤٧.

(٣) سلامة فضل الشامي، جرائم الاعتداء على الحق في الخصوصية في ضوء التطور التكنولوجي، رسالة ماجستير، أكاديمية الإدارة والسياسة للدراسات العليا وجامعة الأقصى بغزة، ٢٠١٨، ص ٤٢ وما بعدها.

(٤) يارا حافظ الجندي، البيانات الشخصية بين التهديد والحماية، دراسة فى ضوء أحكام القانون رقم ١٥١ لسنة ٢٠٢٠، مجلة الدراسات القانونية والاقتصادية، المجلد ٩، العدد ٤، كلية الحقوق، جامعة مدينة السادات، ديسمبر ٢٠٢٣، ص ٢٧٧٩ وما بعدها.

(5) Mahira, D. F., Rohmahwatin, D. S., & Suciningtyas, N. D. (2020). Strengthening Multistakeholder Integrated through Shared Responsibility in the face of Cyber Attacks Threat. Lex Scientia Law Review, 4(1), 59-69. https://doi.org/10.15294/lesrev.v4i1.38191

(6) Alibasic, A., Al Junaibi, R., Aung, Z., Woon, W. L., & Omar, M. A. (2017). Cybersecurity for smart cities: A brief review. In Data Analytics for Renewable Energy Integration: 4th ECML PKDD Workshop, DARE 2016, Riva del Garda, Italy, September 23, 2016, Revised Selected Papers 4 (pp. 22-30). Springer International Publishing. https://link.springer.com/chapter/10.1007/978-3-319-50947-1_3

(7) NCCIC and ICS-CERT, "NCCIC/ICS-CERT 2015 Year in Review," Apr. 19, 2016. [Online]. Available at: https://icscert.uscert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf

واستهدفت معظمها نظام تكنولوجيا المعلومات. وتشير وزارة الطاقة الأمريكية (DOE) إلى أن العدد الفعلي للهجمات السيبرانية أعلى من المبلغ عنه[١].

وتعد فئة الجرائم الناتجة عن الهجمات الإلكترونية من أخطر التحديات التي تواجهها الدول تشريعياً وقضائياً، وبصفة خاصة تلك التي تشكل اعتداء على البنية التحتية المسئولة عن أداء الخدمات العامة، أو تنال من المؤسسات المالية من شركات مالية وبنوك وغيرها[٢]. وذلك بسبب ما تحدثه من خسائر مادية ومعنوية تنال من المصالح الأساسية للدول، إضافة إلى الاعتداء على البيانات الخاصة بالأفراد، وقد لا تتمكن سلطات الضبط من مواجهة هذه الأفعال بالقدر الكافي، لأن من طبيعة هذه الجرائم أنها تتغير كل يوم نتيجة التطورات التكنولوجيا المتسارعة، وأن مرتكبيها يعملون بشكل منفرد أو من خلال عصابات عبر العديد من الدول، وهنا تتجلى أهمية الدور الذي يلعبه الأمن السيبراني كأحد الحلول التي يتم الاعتماد عليها في مواجهة الهجمات الإلكترونية والوقاية من مخاطرها، وهذا الدور يحتاج بلا شك إلى بيئة تشريعية قوية تَعضد من الحماية المرجوة منه.

الفرع الثاني: الضبط الإداري الإلكتروني وآليات تحقيق الأمن السيبراني:

لا جدال في أن التكنولوجيا غيرت من واقعنا الحالي بصورة كبيرة، والمجتمعات تواجه تحديات مختلفة ومتسارعة فلا يمر يوم إلا وتطل علينا التكنولوجيا بتطور جديد، يحمل ميزات أخرى تضاف إلى سابقتها، وفي ذات الوقت تلقي تلك التطورات بتحديات جسام على مكتسبات الدول الاجتماعية والاقتصادية، فمن جانب هناك الفرص التي يجب استغلالها لاستمرار عمليات التنمية في وقت تشتد فيه المنافسة بين الدول في المجال الرقمي، ومن جانب آخر لا يقل أهمية والذي يتمثل فيما تتعرض له المجتمعات من جملة من المخاطر التي تشكل تحديات لا يمكن الوقوف أمامها موقف الصمت والعجز، بل لا بد من مواجهتها والتغلب عليها، ومن هنا تبدو الحاجة للتطوير المستمر على كافة المستويات، وأن تستغل الدول نتاج التطور التقني لما يخدم مصالحها الاقتصادية والاجتماعية. ويمكن ملاحظة التطور الذي طال وسائل الضبط الاداري من خلال النقاط التالية.

---

(1) The U.S. Department of Energy, "Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector," Aug. 2016. [Online]. Available at: https://energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf

(٢) لمزيد من التفاصيل ينظر: خالد ظاهر عبد الله جابر السهيل، دور التشريعات الجزائية في حماية الأمن السيبراني بدول مجلس التعاون الخليجي، مجلة البحوث الفقهية والقانونية، جامعة الأزهر، كلية الشريعة والقانون، دمنهور، العدد ٣٨، يوليو ٢٠٢٢، ص ٩٧٥ وما بعدها. https-search-mandumah-com.mplbci.ekb.eg/Record/1302190.

أولاً: تطور مضمون وآليات الضبط الإداري:

أحد أهم هذه المجالات التي طورت الادارة وسائلها في مجال وظيفتها الضبطية هو المجال الضبطي القائم على الرقمنة ذاتها، وهو ما تجسد فعليًا من خلال الضبط الإداري الإلكتروني، والذي لا يختلف في مضمونه وأهدافه عن الضبط الإداري التقليدي إلا من حيث الوسائل والأدوات المستخدمة فيه، فهو بشكل عام يتفق مع الهدف الرئيس لوظيفة الضبط، وهو المحافظة على النظام العام، وذلك باتخاذ التدابير اللازمة والمتناسبة مع البيئة الرقمية، ووضع الضوابط والقيود التي تنظم نشاط الأفراد والجهات المختلفة على المنصات الرقمية لغايات حماية المصلحة العامة.

وانتقال سلطة الضبط الإداري من الواقع المادي إلى الواقع الرقمي أو الإلكتروني يأتي استجابة للتطورات التكنولوجية المتسارعة، ويتفق أيضاً مع ما نادى به الفقه القانوني وتبنته غالبية التشريعات في كافة دول العالم[١] من أن هناك ضرورة ملحة لتطوير البيئة التشريعية والإدارية حتى تكون قادرة على التعامل مع الواقع الجديد.

بيد أنه لا يمكن في ظل تلك التطورات أن نحدد لسلطات الضبط أدوات أو وسائل معينة تتعامل بها، لأن هذا التحديد وإن كان يصلح في نطاق السلطة المقيدة إلا أنه قد يعوق سلطات الضبط الإداري عن القيام بمهامها المنوطة بها في حماية وحفظ النظام العام، لذلك نؤيد ما نادى به البعض[٢] من ضرورة منح سلطات الضبط الإلكتروني قدراً من المرونة في الأدوات والوسائل التي تستعين بها، مع ضرورة الالتزام بالقواعد القانونية لمنع إي اعتداء على الحقوق والحريات الفردية.

ومع ذلك يمكن لسلطات الضبط الإداري الإلكتروني على سبيل المثال لا الحصر القيام باستخدام واحد أو أكثر من الوسائل الآتية[٣]:

١- **المراقبة الإلكترونية:** في إطار سعي سلطات الضبط الإلكتروني إلى الحفاظ على الأمن العام ومنع وقوع الجرائم الماسة بالنظام العام فإنها تقوم بالرقابة على المواقع والأنشطة الرقمية، من خلال تتبع عمليات الدخول والخروج من المواقع والمنصات الرقمية والتحقق من مدى مشروعيتها، وعدم استهدافها أمن المجتمع، كما تستهدف سلطات الضبط الإلكتروني من خلال عمليات المراقبة الإلكترونية حماية

---

[١] د.محمد عبد الله المنشاوي، جرائم الإنترنت في المجتمع السعودي، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، ٢٠٠٣، ص ٤٠.

[٢] صلاح الدين رجب فتح الباب، أثر استخدام تقنيات الذكاء الاصطناعي على النظام العام، مصدر سابق، ص ٩٩.

[٣] د.سامي حسن نجم الدين الحمداني، دور الضبط الإداري الالكتروني في مكافحة الشائعات المخلة بالأمن العام، بحث منشور في مجلة الحقوق، جامعة تكريت، العدد (١)، المجلد (٥)، الجزء (١)، السنة (٥)، ٢٠٢٠، ص٨٨-١١٨.

الفضاء الرقمي والبنية التحتية من أي تهديدات سيبرانية تستهدف الإخلال بالنظام العام. على أنه ينبغي أن تتم عملية المراقبة وفق الضوابط التشريعية وأن تخضع لرقابة القضاء لتحقيق التوازن بين حماية الحقوق والحريات كمصلحة خاصة، وحق المجتمع في الأمن ومنع الجريمة كمصلحة عامة، مع تغليب المصلحة العامة على المصالح الخاصة للأفراد عند التعارض بينهما.

٢- **الترخيص الإلكتروني:** يعتبر الترخيص الإلكتروني من أساليب الرقابة السابقة أو الوقائية، وهو بمثابة الإذن (الرخصة) يستطيع بموجبه المرخص له القيام بالنشاط وفق الشروط التي حددتها القوانين واللوائح. ويلاحظ أن سلطة الإدارة في مجال منح الإذن أو الترخيص مقيدة، إذ يجب على الإدارة منح الترخيص حال توافرت الشروط التي تطلبها القوانين واللوائح لممارسة نشاط معين، ويجب كذلك أن يكون رائد جهة الإدارة بشأن منح الترخيص أو رفضه هو ابتغاء المصلحة العامة ومبدأ المساواة بين الأفراد أمام القانون[١].

٣- **الحظر الإلكتروني:** الحظر الإلكتروني أو المنع هو إجراء تلجأ إليه سلطات الضبط الإداري لمنع الأنشطة غير المشروعة والتي يُحظر على الأفراد القيام بها حماية للنظام العام على وجه العموم والأمن العام على وجه الخصوص، ويعد الحظر وسيلة استثنائية إذ الأصل أن سلطات الضبط الإداري لا تلجأ إليه إلا في عند استحالة المحافظة على النظام العام بوسيلة أخرى، وذلك لأن الحظر المطلق والكلي للحريات غير مشروع لأنه يعتبر بمثابة إلغاء أو مصادرة للحريات العامة، ولذلك يأتي الحظر بصورة جزئية أو مؤقتة حتى لا يترتب عليه منع الحريات أو إلغاءها، فإذا ما تغولت جهة الإدارة على حريات الأفراد ووصلت بالإجراء إلى حد الحظر المطلق للحرية فإن القضاء يقف لها بالمرصاد ويقضي ببطلان الإجراءات التي اتخذتها جهة الإدارة[٢]. وفي المجال الرقمي يمكن للسلطات مراقبة الانحرافات الخطيرة ومواجهتها، وتحديد عمليات الدخول غير الطبيعية، وقد تتضمن بعض المواقع تطلب المصادقة لتمكين المستخدم من الوصول وغيرها من تدابير المتطورة والمتنوعة والمستجدة لحماية أمان الشبكات.

ثانياً: آليات تحقيق الأمن السيبراني:

يؤدي الأمن السيبراني دورًا حيويًا ومهمًا للغاية في حماية المعلومات والأنظمة الإلكترونية، من خلال توفير الحلول الرقمية لمواجهة المشكلات السيبرانية ولمنع الإخلال بالبيئة الرقمية أو شل حركتها أو

---

[١] د.محمد جمال جبريل، مصدر سابق ، ص ٤٢-٤٣.

[٢] د.محمد جمال جبريل، مصدر سابق ، ص ٤١.

تعطيل عملها[١]. وتعمل أنظمة الأمن السيبراني على التصدي للهجمات ومنعها من الوصول إلى البيانات أو محوها أو تعطيل عمل المؤسسات من خلال توفير الحماية للبنية التحتية للأنظمة الألكترونية ، وكذلك الوقاية من المحاولات التي تحاول الاحتيال على أموال الأفراد تهدد أمنهم وخصوصيتهم.

ويعد الأمن السيبراني جدار الحماية الأول للحفاظ على الخصوصية وضمان سرية البيانات في مواجهة عمليات القرصنة الإلكترونية التي تزايدت وتيرتها مع التقدم المذهل للتكنولوجيا وما صاحبها من ميزات ووظائف مختلفة ومتنوعة[٢].

أ- مفهوم الأمن السيبراني:

يعود مجال الأمن السيبراني بأصوله إلى سبعينيات وثمانينيات القرن الماضي حين أصبحت تكنولوجيا الحوسبة أكثر انتشارًا في الأعمال الخاصة والحكومية والاستخدام الشخصي. وبمرور الوقت، نضج هذا المجال، وتكيف مع التهديدات الناشئة والتقنيات المتطورة. وكان جوهر الأمن السيبراني دائمًا هو تأمين الأنظمة والبيانات الرقمية من الوصول غير المصرح به أو التلف أو التعطيل[٣]. ويستخدم مصطلح الأمن السيبراني للإشارة إلى التدابير التي تتخذها المؤسسات الحكومية لحماية الجمهور والمؤسسات نفسها من التهديدات في المجال "السيبراني"، والمعروف أيضًا باسم "الفضاء السيبراني".

ويقصد بالأمن السيبراني "عملية الدفاع عن أمن الشبكات والمعلومات والأجهزة والبرامج بطريقة تقنية تكنولوجية من خلال اتخاذ الإجراءات والتدابير والوسائل التكنولوجية الحديثة، بقصد الحماية من أي هجمات إلكترونية لضمان أمن وسلامة وتوافر المعلومات"[٤]. ويعرفه البعض أيضاً بأنه: "كافة الأنشطة والعمليات التي يتم بموجبها حماية أنظمة المعلومات والاتصالات والمعلومات الواردة فيها من التلف أو الاستخدام أو التعديل أو الاستغلال غير المصرح به أو الدفاع عنها ضد أي هجمات"[٥].

---

[١] علي آل مداوي، الأمن السيبراني، تعريفه-أهميته- أنواعه-استراتيجيات للوقاية من الهجمات السيبرانية، مجلة الدراسات الدولية العدد ٣٤، ١٤٤٥هـ/٢٠٢٣، ص١١٥
https://0810gqbqu-1106-y-https-search-mandumah-com.mplbci.ekb.eg/Record/1454807
وينظر أيضاً: منى الأشقر جبور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والفضائية، ٢٠١٢، ص ٢.
آل مداوى، الأمن السيبراني، مصدر سابق، ص ١١٨. [١] لمزيد من التفاصيل ينظر: على

[٣] لمزيد من التفاصيل ينظر: جيهان سعد محمد الخضري وآخرون، الأمن السيبراني والذكاء الاصطناعي في الجامعات السعودية" دراسة مقارنة"، مجلة تطوير الأداء الجامعي، المجلد ١٢، العدد ١، ٢٠٢٠، ص ٢٢٠.
https://jpud.journals.ekb.eg/article_170391_ac7fb65b42daa75c25cc7e0586fec704.pdf
[٤] إيمان محمد الشورة، الأمن السيبراني في البنوك الإسلامية الأردنية، كلية الشريعة، الجامعة الأردنية، ٢٠٢٠، ص ٣٣.
[5] Morten Bay, (2016). WHAT IS CYBERSECURITY? In search of an encompassing definition for the post-Snowden era, French Journal For Media Research pp. 4-9. https://www.researchgate.net/publication/308609163_WHAT_IS_CYBERSECURITY_In_search_of_an_encompassing_definition_for_the_post-Snowden_era

كما يستخدم الأمن السيبراني كمرادف لأمن تكنولوجيا المعلومات أو أمن المعلومات الإلكترونية[١]. وهو جانب أساسي من الواقع الرقمي الحديث، ويشمل مجموعة من التدابير التي تهدف إلى حماية المعلومات الحساسة والتخفيف من المخاطر التي تشكلها التهديدات الإلكترونية[٢].

ب- أهمية الأمن السيبراني:

أصبحت حماية الفضاء الرقمي من أكثر الصعوبات التي تواجهها الدول في الوقت الحالي، والأمن السيبراني هو السبيل لحماية هذا الفضاء الرقمي، للعمل على مواجهة الجرائم الإلكترونية والهجمات السيبرانية المتزايدة التي تتعرض لها الدول.

ومن الأسباب التي تجعل الأمن السيبراني مهمًا للغاية في العالم الرقمي يمكن نذكر بعضها هنا، وكما يلي:

١- الهجمات السيبرانية تتسبب في تكبيد المؤسسات العامة، والشركات خسائر مالية باهظة.
٢- بالإضافة إلى الخسائر المالية، قد يتسبب خرق البيانات في أضرار تنال من سمعة المؤسسات.
٣- تزايد الطابع العدائي والمدمر للهجمات السيبرانية، حيث يستخدم مجرمو الإنترنت طرقًا أكثر تطورًا لشن الهجمات السيبرانية.
٤- إن اللوائح التنظيمية الموضوعة لحماية البيانات تضع التزاماً على المؤسسات بحماية البيانات والمعلومات التي تحتفظ بها.

وهذه الأسباب المذكورة ليست هي الأسباب الوحيدة بل أن الواقع العملي يشير إلى أن التهديدات السيبرانية باتت تشكل خطراً حقيقياً ليس فقط على الجانب الاقتصادي والمالي للدول، بل على أمن وسلامة المجتمع من كافة الجوانب السياسية والأمنية والاخلاقية، وهو الأمر الذي استتبع أن يكون الأمن السيبراني جزءًا مهمًا من العمل للمؤسسات والأفراد على حد سواء، وينصب التركيز من قبل أجهزة الدولة وغيرها من المؤسسات المعنية على تطوير خطط الاستجابة المناسبة التي تقلل من الأضرار في حالة وقوع هجوم سيبراني.

ج- آلية عمل أنظمة الأمن السيبراني:

تعتمد آلية عمل أنظمة الأمن السيبراني على عدة محاور تعتبر بمثابة عوامل النجاح له في توفير الحماية للفضاء الرقمي وهي كما يلي:

---

(1) https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security
(2) https://www.dataguard.com/cyber-security/

١- **التشفير:** يعد التشفير أداة قوية لحماية المعلومات حال تعرضها للتهديدات من قبل المهاجمين الإلكترونيين[١]. وأسلوب التشفير عبارة عن عملية ترميز للرسائل بحيث لا يتمكن المبرمجون من قراءتها. وهو إجراء يتم من خلاله ترميز الرسالة وتحويلها إلى محتوى رقمي مشفر، وعادة يتم ذلك باستخدام "مفتاح تشفير" يوضح كيفية ترميز الرسالة. ويسهم التشفير في تقديم حماية أولية للبيانات والمعلومات[٢]. إضافة إلى إسباغ مزيد من الحماية عند نقل المعلومات.

٢- **السرية:** تعتبر السرية من أساسيات عمل الأمن السيبراني، وتتعلق السرية بمنع الكشف عن البيانات وإبقائها مخفية عن الأطراف غير المصرح لها. كما تهدف السرية إلى الحفاظ على هوية الأطراف المصرح لها في مشاركة البيانات والاحتفاظ بها. وتشمل التدابير القياسية لإثبات السرية تشفير البيانات، رموز الأمان، المصادقة الثنائية، والتحقق البيومتري.

٣- **النسخ الاحتياطي:** ويقصد بالنسخ الاحتياطي عمل نسخ متعددة من جميع الملفات المخزنة على الموقع حتى تتمكن الجهات من الرجوع إلى البيانات التي سبق تخزينها واسترجاعها سليمة كما كانت، وذلك في الحالات التي قد يترتب عليها حدوث تلف أو ضياع للبيانات المخزنة. ويتم عمل النسخ الاحتياطية في مكان رقمي آمن، فإذا واجه موقع الويب مشكلة في أي وقت، فيمكن استخدام نتائج ومخرجات النسخ الاحتياطي لإعادة الموقع إلى حالته السابقة[٣].

٤- **خوادم الويب:** يمثل أمان الويب أهمية كبيرة لضمان سلامة الأعمال والمعاملات التي تتم عبر أجهزة الكمبيوتر أثناء اتصالها بالإنترنت، فإذا تعرض موقع ويب للاختراق أو تمكن المهاجمون من التلاعب بالنظام أو البرامج، فقد يتم تعطيل موقع الويب الخاص بالمستخدم، وقد يتسبب ذلك في توقف أو تعطيل الشبكة بشكل كامل، مما يؤدي إلى توقف العمليات والمهام التي يقوم بها الأفراد والمؤسسات.

وحتى يتم تأمين مواقع الويب من الهجمات يتم الاستعانة بالعديد من الإجراءات التي تعرف باسم أمان الويب بهدف توفير الحماية للشبكات والخوادم وأنظمة الكمبيوتر من التلف أو سرقة البرامج أو الأجهزة أو

---

(1) Chih-Che Suna , Adam Hahna , Chen-Ching Liu,.(2018). Cyber Security of a Power Grid: State-of-the-Art, International Journal of Electrical Power & Energy Systems, Volume 99, July 2018, Pp. 45-56. https://doi.org/10.1016/j.ijepes.2017.12.020

(2) Sharma, R. (2012). Study of Latest Emerging Trends on Cyber Security and its challenges to Society. International Journal of Scientific & Engineering Research, 3(6).

(3) https://www.hostgator.com/help/article/how-to-generatedownload-a-full-backup

البيانات المخزنة، ويشمل ذلك حماية أنظمة الكمبيوتر من سوء التوجيه أو تعطيل الخدمات التي يتم تقديمها عبر المنصات المختلفة[١].

وأدوات أمان الويب صورة من صور الأمن السيبراني، بما في ذلك أمان السحابة وأمان تطبيقات الويب، والتي تدافع عن الخدمات السحابية والتطبيقات المستندة إلى الويب على التوالي. وقد مكنت تقنية حماية موقع الويب من تقديم حماية محسنة، مثل حماية الشبكة الخاصة الافتراضية (VPN)، والتي تندرج أيضًا تحت مظلة أمان الويب.

المبحث الثاني

التجارب الدولية والوطنية في مجال الأمن السيبراني

أدى التقدم في الإلكترونيات الدقيقة ولغات البرمجة، وظهور الإنترنت، إلى خلق فائض ضخم من المعلومات، حيث تجمع المليارات منها على الأجهزة وتعالج وتخزن بكميات هائلة[٢]. وأصبحت البيانات سوقًا رائجًا للتجارة الدولية، ولقد ترتب على ذلك ظهور العديد من المخاطر التي ضاعفت من مسؤوليات سلطات الضبط في مواجهة ما يفرضه التطور التقني من تحديات.

ولقد اتسمت السنوات الأخيرة بتزايد الهجمات الإلكترونية ضد البُنى التحتية الحيوية للدول ذات السيادة، والإدارات الحكومية، والمؤسسات الاقتصادية، سواءً كانت هجمات موجهة نحو السيطرة على البنية التحتية أو للتجسس وسرقة البيانات السرية، ولذلك أصبح الأمن السيبراني أحد التحديات المحورية التي تواجهها الحكومات اليوم، والتي تحتاج إلى نهج شامل وتحليلي لمنع الهجمات الإلكترونية وتحديدها والاستجابة لها بسرعة[٣].

---

[١] خوادم الويب تعد بوابة الولوج أمام المتصفحين عند قيامهم بعمليات البحث المختلفة على شبكة الانترنت، فخادم الويب web server هو برنامج مصمم للعمل على مشغل حاسوبي يسمح بالتجول على شبكة إنترنت باستخدام متصفح ويب لأجل رؤية المحتوى الرقمي، وما يرتبط به (صور، ملفات صوتية، ملفات مرئية)، وفي البداية كانت خوادم الويب محدودة ويتم التعامل عليها لنقل البيانات بين المستخدمين في نطاق محدد، ولكن بعد عام ٢٠٠٤ تغير الوضع كثيراً خاصة مع ظهور نظام ورد برس Word Press لإدارة المُحتوى، إضافة إلى شبكة فيسبوك الاجتماعية Facebook، وبالتالي ازدادت عدد الطلبات على الخوادم. للمزيد ينظر الموقع الإلكتروني التالي:
https://www.fortinet.com/resources/cyberglossary/what-is-web-security

[2] Herman P The military-technical revolution. Def Analysis 10(1):91–95. https://doi.org/10.1080/07430179408405608

[3] M. Martellini (ed.), Cyber Security Deterrence and IT Protection for Critical Infrastructures, SpringerBriefs in Computer Science, DOI: 10.1007/978-3-319-02279-6_1

ولإبراز المجهودات الدولية والوطنية في مجال الأمن السيبراني فإننا نرى تقسيم هذا المبحث إلى مطلبين نتناول في المطلب الأول الأمن السيبراني على المستوى الدولي، في حين نخصص الثاني للتعرف على تجارب بعض الدول العربية في مجال الأمن السيبراني، وذلك على النحو التالي:

المطلب الأول

الأمن السيبراني على المستوى الدولي

تسعى الكثير من الدول للحد من المخاطر التي قد تواجهها من الهجمات السيبرانية التي تستهدف الكم الهائل من المعلومات المهمة والتي قد تتعلق بالأمن القومي لتلك الدول أو تلك التي تستهدف البيانات للبنية التحتية والمعلومات الشخصية للأفراد، وسنتطرق الى بعض التجارب على المستوى الدولي لمواجهة تزايد الهجمات الالكترونية ضد البنى التحتية الحيوية لتلك الدول.

الفرع الأول : التجارب على مستوى القارة الاوربية

أولاً: الاتحاد الأوروبي:

يعد اعتماد الاتحاد الأوروبي لاستراتيجية الأمن السيبراني ترجمة للنهج القانوني لسياسة الاتحاد الأوروبي في هذا المجال وهي –في المقام الأول– أداء السوق الداخلية وفقًا للمادة ١١٤ من معاهدة الاتحاد الأوروبي بشأن توحيد القواعد الوطنية المتعلقة بإنشاء السوق الداخلية ووظيفتها[١].

وفي عام ٢٠٠١ اعتمد الاتحاد الأوروبي اتفاقية دولية خاصة بمكافحة الجرائم الإلكترونية والمعروفة باتفاقية بودابست رقم ١٨٥ لسنة ٢٠٠١[٢]، وفي عام ٢٠٠٥ قام الاتحاد الأوروبي بالتوسع في خطة عمل بشأن شبكة انترنت أكثر أماناً (safer internet plus) بهدف تعزيز الاستخدام الآمن

---

(1) Jed Odermatt, 'The European Union as a Cybersecurity Actor' in Steven Blockmans and Panos Koutrakos (eds), Research Handbook on EU Common Foreign and Security Policy (Edward Elgar Publishing 2018) 359. See also **Ana Paula Brandão and Isabel Camisão**, 'Playing the Market Card: The Commission's Strategy to Shape EU Cybersecurity Policy' (2022) 60 Journal of Common Market Studies 1335; Helena Carrapico and André Barrinha, 'The EU as a Coherent (Cyber)Security Actor?' (2017) 55 Journal of Common Market Studies 1254, 1259.

(٢) اتفاقية بوادبست ٢٠٠١ رقم ١٨٥ بشأن الجريمة الإلكترونية، والمعتمدة في ٢٠١١/١١/٢٣ مجموعة المعاهدات، مجلس أوربا. ينظر الرابط التالي:
https://rm.coe.int/budapest-convention-in-arabic/1680739173

لشبكات الانترنت وما يرتبط بها من تكنولوجيا حديثة، وبصفة خاصة لمواجهة الممارسات غير القانونية[١].

وتؤكد استراتيجية عام ٢٠١٣ على تبنيها نموذج حوكمة متعدد الأطراف، قائم على التعاون بين القطاعين العام والخاص، بهدف التصدي للتهديدات السيبرانية، إذ يعتبر أن أمن الشبكات وأنظمة المعلومات أحد جوانب الأمن الشامل في المفهوم الأوربي الذي يصب مباشرة في المصلحة العامة. وأن على الدول الأعضاء اتخاذ التدابير التكنولوجية لأجل تعزيز الخصوصية، والأمن السيبراني وضمان اتخاذ مشغلي الخدمات الأساسية التدابير المناسبة الفنية والتنظيمي [٢]، لإدارة المخاطر التي تهدد أمن الشبكة وأنظمة المعلومات التي يستخدمونها، مع تبني استراتيجية وطنية تلتزم بالمعايير الواردة بوثيقة التوجيه، وفي حالة وجود تشريعات خاصة بقطاعات محددة يتم تطبيق هذا التشريع طالما أنه يحتوي على متطلبات معادلة على الأقل لتلك الواردة في توجيه أنظمة المعلومات الوطنية[٣].

وإدراكا للمخاطر التي تتزايد وتيرتها مع التطورات المتسارعة التكنولوجيا، قامت دول الاتحاد الأوربي بوضع مجموعة من التوجيهات والتي تعتبر بمثابة أطر رئيسية لتشريعات الأمن السيبراني، ومن هذه التوجيهات الآتي:

١- **توجيه NIS:** وهذا التوجيه يهدف إلى ضمان المرونة الشاملة لمشغلي ومقدمي الخدمات الرقمية، وهو خطوة هامة وأساسية نحو الاعتراف بالتهديدات المتزايدة الناتجة عن الحوادث السيبرانية، وقد تم اعتماد هذ التوجيه في يوليو ٢٠١٦ ودخل حيز النفاذ في أغسطس ٢٠١٦. وتتمثل آليه عمل هذا التوجيه في التنسيق بين دول الاتحاد الأوروبي لمواجهة التحديات الأمنية في البيئات الرقمية من خلال التعاون بين الدول لتعزيز ممارسات إدارة المخاطر، مع منح التفويض لمشغلي الخدمات الأساسية في الإبلاغ عن التهديدات والهجمات التي تشكل حوادث سيبرانية.

---

(1) Kathryn C. Seigfried-Spellar, Gary R. Bertoline, and Marcus K. Rogers. (2011). Internet Child Pornography, U.S. Sentencing Guidelines, and the Role of Internet Service Providers, Digital Forensics and Cyber Crime,Third International ICST Conference, ICDF2C 2011, Dublin, Ireland, October 26-28, 2011, Springer, pp. 17-30. file:///C:/Users/vip/Downloads/978-3-642-35515-8.pdf

(2) Pier Giorgio Chiara, (2024). Towards a right to cybersecurity in EU law? The challenges ahead, Computer Law & Security Review, Volume 53, July 2024, 105961. Pp. 1-9. http://www.elsevier.com/locate/clsr

(٣) يراجع وثيقة مصدرية حول الإخطار بالحوادث لمشغلي الخدمات الأساسية، فبراير ٢٠١٨ : https://ec.europa.eu/digital-single-market/en/nis-cooperation-group

٢- توجيه **NIS 2**: وهذا التوجيه يهدف إلى تعزيز الأمن السيبراني في الاتحاد الأوروبي بين الدول الاعضاء من خلال مستويات عالية من التعاون المشترك للأمن السيبراني لأنظمة الشبكات والمعلومات في الشركات والمؤسسات عبر الاتحاد الأوروبي، وهذا التوجيه جاء لمعالجة أوجه القصور في توجيه NIS، حيث وسع توجيه **NIS 2** من نطاق القطاعات التي تندرج تحت حمايته، فالملحق الأول من التوجيه يشمل القطاعات الحساسة كالطاقة، إدارة تكنولوجيا المعلومات والاتصالات، والبنية التحتية الرقمية، والصرف الصحي، النقل، المصارف والخدمات المالية، الصحة والمياه نظم الإدارة العامة، والخدمات الفضائية، بينما تضمن الملحق الثاني من التوجيه مزودي الخدمة الرقميين، الخدمات البريدية والتوصيل، إدارة النفايات، تصنيع وإنتاج وتوزيع المواد الكيميائية، إنتاج ومعالجة وتوزيع الغذاء، والبحث، والتصنيع. كما يضع التزامات على القطاعات المذكورة أعلاه تتمثل فيما يلي[١]:

أ- **واجب الرعاية:** وهو إجراء تقييمي للمخاطر، وبناءً على هذا التقييم يجب اتخاذ التدابير اللازمة لضمان استمرار الخدمات قدر الإمكان وحماية المعلومات المستخدمة.

ب- **واجب الإبلاغ:** حيث يلزم الإبلاغ عن الحوادث إلى السلطة المختصة خلال ٢٤ ساعة إذا تعلق الأمر بالحوادث التي من المحتمل أن تعطل بشكل كبير تقديم الخدمات الأساسية. وفي حالة تعلق الأمر بحادث إلكتروني يجب الإبلاغ عن ذلك أيضًا إلى فريق الاستجابة لحوادث الأمن السيبراني (CSIRT). ويعتمد ما إذا كان الحادث خاضعًا لواجب الإبلاغ من عدمه على عدة عوامل، منها على سبيل المثال، عدد الأشخاص المتأثرين بالاضطراب، ومدة الاضطراب، والخسائر المالية المحتملة.

أما تشريعات الأمن السيبراني في الاتحاد الأوروبي فهي تتضمن مجموعة من القوانين والمبادرات التي تهدف إلى تعزيز الأمن السيبراني وحماية المعلومات في دول الاتحاد. وأبرز هذه التشريعات ما يلي[٢]:

- **قانون الأمن السيبراني للاتحاد الأوروبي:** صدر هذا القانون في مارس ٢٠١٩ وذلك بهدف إنشاء آلية لتطوير مخطط طوعي لإصدار الشهادات لمنتجات وعمليات وخدمات أمن تكنولوجيا المعلومات والاتصالات. ولم تقترح المفوضية الأوروبية بعد المجالات المحددة التي قد تستفيد من مخططات الشهادات، وقد أنشأت وكالة الأمن السيبراني التابعة للاتحاد الأوروبي مجموعات أصحاب

---

[١] راجع وثيقة مصدرية حول الإخطار بالحوادث لمشغلي الخدمات الأساسية، فبراير ٢٠١٨ :
https://ec.europa.eu/digital-single-market/en/nis-cooperation-group

[2] Pier Giorgio Chiara,Op.cit. Pp. 1-9.

مصلحة تختص بتقديم المساعدة اللازمة في إنشاء مخططات الشهادات، والتي تشمل مشاركة الصناعة في المنتجات الرقمية وفقًا للقانون[١].

- **قانون ترخيص التشغيل الرقمي(DORA)** : في يناير ٢٠٢٥، اتخذ الاتحاد الأوروبي خطوات فعالة لتعزيز الأمن السيبراني وبصفة خاصة في المجال المالي، من خلال تطبيق قواعد جديدة ضمن قانون المرونة التشغيلية الرقمية (DORA). وهذا القانون يفرض على المؤسسات المالية اتخاذ تدابير أكثر صرامة لضمان استمرار عملياتها الرقمية وتقليل المخاطر السيبرانية التي قد تتعرض لها.

- **مقترح قانون المرونة السيبرانية** [٢]: يفرض مشروع القانون مسؤوليات أكبر على الشركات المصنعة لضمان أمن منتجات الأجهزة والبرامج، وقد نشر هذا المقترح في ١٥ سبتمبر ٢٠٢٢، بهدف وضع قواعد قانونية لحماية الدول الأعضاء من الهجمات السيبرانية، وضمان مستويات عالية من الحماية للأجهزة والبرمجيات في السوق الأوروبية. ويتمثل جوهر القانون في فرض التزامات جديدة على الشركات المصنعة لتوفير تحديثات البرامج التي تعمل على إصلاح الثغرات الأمنية، وتقديم الدعم الأمني للمستهلكين من خلال تعزيز الشفافية بشأن المخاطر السيبرانية وأمن المنتجات. وهو جزء من إطار أوسع للأمن السيبراني يتضمن لوائح أخرى مثل قانون الأمن السيبراني للاتحاد الأوروبي وتوجيه NIS2. ومن شأن التشريع، لأول مرة، أن يطبق علامة CE على البرامج، وينشئ عمليات الموافقة على مجموعة واسعة من المنتجات والخدمات الرقمية المطلوبة للحصول على العلامة حتى تكون مؤهلة للبيع والاستخدام في سوق الاتحاد الأوروبي. يخضع القانون حاليًا للمفاوضات بين البرلمان الأوروبي والمجلس والمفوضية [٣].

ثانياً: فلندا:

تعتبر الاستراتيجية الوطنية للأمن السيبراني جزءاً من الأمن الشامل في مجتمع فنلندا الرقمي، إذ تستهدف ضمان ظروف عمل ملائمة للأمن الوطني، والدفاع الوطني، وأمن الإمدادات، ومجتمع الأعمال، والمجتمع المدني. وقد أكد التحول في الظروف الجيوسياسية على أهمية التعاون الوطني

---

(1) Dimitra Markopoulou, Vagelis Papakonstantinou, Paul de Hert, (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation, Computer Law & Security Review,Volume 35, Issue 6, November 2019, pp.1-11. http://www.sciencedirect.com/

(2) https://blog.uniqkey.eu/eu-cybersecurity-regulations/
https://www.kiteworks.com/risk-compliance-glossary/eu-cybersecurity-act/

(٣) للمزيد من التفاصيل حول الأمن السيبراني: راجع دليل التبادل التجاري لدول الاتحاد الأوروبي، متاح على الربط التالي:
https://www.trade.gov/country-commercial-guides/eu-cyber-security

والدولي في ضمان الأمن السيبراني، مع تزايد الحاجة إلى التعاون بين السلطات العامة ومجتمع الأعمال، ودعم مرونة المجتمع، والتصدي للأنشطة العدائية. حيث يتم النظر إلى الأمن السيبراني من منظور تقني، وليس كمسألة أمن وطني فقط. وتتعلق الاستراتيجية التي تتبناها فلندا بالتركيز على الأمن السيبراني الوطني كأولوية وطنية، من خلال تبني التدابير التي تمكن المجتمع الرقمي من الاستعداد للحوادث في الأنظمة الإلكترونية والشبكية، وتحديدها، ومكافحتها، والصمود في وجهها، والحد من تأثيراتها على الوظائف والخدمات الحيوية للمجتمع، وتقديم معالجات وحلول للتعافي منها، وضمان الظروف التشغيلية اللازمة للأمن الوطني والدفاع الوطني وأمن الإمدادات [١].

وتهدف الاستراتيجية الوطنية لأمن المعلومات إلى التركيز على ضمان التنافسية في سياق السوق الرقمية الموحدة للاتحاد الأوروبي، وتعزيز وحماية الخصوصية وغيرها من الحقوق الأساسية. كما تتناول الاستراتيجية المسائل التي تُزعزع الثقة، مثل حوادث الأمن الرقمي وانتهاكات الخصوصية واسعة النطاق في شبكات الاتصالات.

ويشمل أحد عناصر الاستراتيجية تنفيذ توجيه الاتحاد الأوروبي بشأن أمن الشبكات والمعلومات (NIS)، كما سيتم إجراء تقييم لتأثير التشريعات الوطنية على فرص المواطنين والشركات في استخدام الخدمات الرقمية ونماذج الأعمال بشكل آمن مع إدارة المخاطر المرتبطة بالتعامل مع البيانات [٢].

ووفقاً لمنصة Mix Mode التي تجري تحليلاً لمجموعة بيانات شاملة تضم مؤشرات مختلفة[٣]، حصلت فلندا على ترتيب متقدم في كافة المؤشرات، حيث حققت في مؤشر السلامة السيبرانية ٩٢.٨١ نقطة، حيث وصلت درجتها بمؤشر الأمن السيبراني الوطني إلى ٨٥.٧١ نقطة، وبمؤشر التعرض للأمن السيبراني إلى ٨٩ نقطة، ومؤشر الأمن السيبراني العالمي إلى ٩٥.٧٨ نقطة، ومؤشر المرونة السيبرانية إلى ٩٣.٦٤ نقطة.

ثالثاً: المملكة المتحدة:

وفقاً لإحصائيات الأمن السيبراني والهجمات الإلكترونية (CDR) في المملكة المتحدة لعام ٢٠٢٣، تعرضت أكثر من (٨٠٪) من المؤسسات البريطانية لهجمات في الفترة ما بين ٢٠٢١ – ٢٠٢٢. وفي

---

(1) For more: Finland's Cyber Security Strategy 2024–2035 . https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/165893/VNK_2024_13.pdf

(2) Information Security Strategy for Finland The World's Most Trusted Digital Business Environment, Ministry of Transport and Communications and the development group for business with information security. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/75353/92016_Information_Security_Strategy_for_Finland.pdf?sequence=1&isAllowed=y

(3) https://www.cnbcarabia.com/128373/2024/21/09

الفترة من فبراير ٢٠٢٢ – فبراير ٢٠٢٣ تأثرت نحو (٧٣٪) من مؤسسات المملكة المتحدة بهجمات برامج الفدية، خاصة وأن (٧٩٪) فقط من الشركات البريطانية تلجأ إلى استخدام تقنية الذكاء الاصطناعي والتعلم الآلي، ما دفع نحو (١٣٪) من الشركات والمؤسسات البريطانية لدفع الفدية لإنهاء الاختراق الإلكتروني الذي تعرضت له. وتسعى بريطانيا لتسخير إمكانياتها لمواجهة هذه المخاطر[١]، لذا يعمل أكثر من (٥٠) ألف موظف في مجال الأمن السيبراني، ما يمثل زيادة بنسبة (١٣٪) عن عام ٢٠٢٠، ويعمل حوالي (٦٤٪) من الموظفين بمؤسسات كبرى. أكدت الحكومة على التزامها بإنفاق (٢٢) مليار جنيه إسترليني على تطوير التقنيات الرقمية، وبلغت الأرباح من صناعة الأمن السيبراني نحو (١٠) مليارات جنيه إسترليني في الفترة ٢٠٢١– ٢٠٢٢.

كما أطلقت بريطانيا في ٢٦ يناير ٢٠٢٢ استراتيجيتها للأمن السيبراني، بهدف زيادة الحماية للشركات والخدمات العامة، وتعد هذه الخطوة استكمالا للاستراتيجية الإلكترونية الوطنية والمركز الوطني للأمن السيبراني" NCSC" الذي أطلق في ٢٠١٦ لضمان امتلاك مؤسسات الدولة وسائل دفاع عن نفسها في الفضاء الإلكتروني [٢]. تشتمل الاستراتيجية الجديدة على خمس ركائز:

- تعزيز النظام البيئي السيبراني في بريطانيا وتطوير مهارات الموظفين في هذا المجال.
- الحد من المخاطر الإلكترونية وتعميق الشراكة بين الحكومة والأوساط الأكاديمية.
- بناء بريطانيا الرقمية المرنة بتعظيم الفوائد التكنولوجية وجعل البريطانيين أكثر أماناً عبر الإنترنت.
- بناء القدرات في التقنيات الحيوية الإلكترونية وقيادة النظام العالمي في مسألة الأمن السيبراني.
- الكشف عن المهاجمين السيبرانيين وردعهم لتعزيز أمن المملكة المتحدة في الفضاء السيبراني.

وتستهدف بريطانيا من هذا الاستراتيجية أن تصبح قوة إلكترونية كبرى بحلول عام ٢٠٣٠، وتمكنت من إيقاف نحو (٤٣٪) من هجمات برامج الفدية الضارة قبل تشفير البيانات خلال ٢٠٢٢.

كما حظرت بريطانيا في ١٦ مارس ٢٠٢٣" تطبيق تيك توك" الصيني من الأجهزة والهواتف الحكومية لأسباب أمنية، وبالمثل اتخذ البرلمان البريطاني في ٢٣ مارس ٢٠٢٣ نفس الخطوة، مع حرمان نوابه من الوصول للتطبيق عبر شبكة الإنترنت الخاصة به، وأرجعت بريطانيا هذه الخطوة إلى أن الأمن السيبراني بات مهدداً بسبب الاختراقات من بعض الدول والشركات التي تعمل لحسابها.

---

[١] لمزيد من التفاصيل ينظر: د. محمد السعيد القزعة، د. طارق السيد، المواجهة الجنائية لاستخدام الويب المظلم في الاعتداء على البيانات الشخصية، مجلة جرش للبحوث والدراسات، المجلد٢٥، العدد٢(ب)، الأردن، ٢٠٢٥، ص ٤٥٩-٤٩٣.

[2] https://www.europarabct.com

ويعد المركز الوطني للأمن السيبراني" NCSC" الذي أنشئ مؤخراً حلقة وصل بين الشركات الكبيرة والصغيرة والمنظمات والوكالات الحكومية، إضافة إلى جهات الاستخبارات وإنفاذ القانون والأمن في المملكة المتحدة. ويعمل على تقوية القطاع الرقمي بالمملكة المتحدة، وردع المجرمين السيبرانيين. من خلال دعم معايير الأمن السيبراني وتحسين القدرات التكنولوجية للقطاعي العام والخاص، والتصدي للهجمات وتحديد هوية ومصدر وموقع الهجوم، وتقوية الأنظمة الرقمية الحساسة الخاصة والحكومية.

على الرغم من التحديات، تحافظ المملكة المتحدة على ترتيب جدير بالاحترام فيما يتعلق بالأمن السيبراني. فالنسبة لدرجة مؤشر السلامة السيبرانية حصلت على ٨٩.٧٥ نقطة. ويؤكد إطار الأمن السيبراني القوي على مرونتها في مواجهة التهديدات السيبرانية، وهو ما يؤكده مؤشر الأمن السيبراني الوطني الذي يبلغ ٨٩.٦١ نقطة، ومؤشر التعرض للأمن السيبراني الذي يبلغ ٧٩.٣ نقطة، ومؤشر الأمن السيبراني العالمي الذي يبلغ ٩٩.٥٤ نقطة، ومؤشر المرونة السيبرانية الذي يبلغ ٩٠.٤٠ نقطة [١].

الفرع الثاني: جهود الولايات المتحدة الأمريكية في الحماية السيبرانية .

وكمثال للجهود الفردية المتميزة على المستوى الدولي سنلقي الضوء على تجربة الولايات المتحدة الامريكية كمثال للعمل الفعال في المجال القانوني والأجرائي المبذول من الدول بمستوى يوازي المخاطر العديدة التي تواجهها الدول لحماية أمنها وبتطور يلاحق تزايد المخاطر التي تهدد النظام العام للدول.

تتصدر الولايات المتحدة الأمريكية قائمة الدول ضمن الترتيب العالمي الأولى، حيث تحل الأولى عالميًا في مؤشر الأمن السيبراني لعام ٢٠٢٥. وذلك من بمعدل استثمار ضخم في الأمن السيبراني من خلال وزارة الأمن الداخلي ووكالة الأمن السيبراني وأمن البنية التحتية (CISA). إضافة إلى شراكات قوية بين القطاعين العام والخاص، خاصة في مجالات الدفاع السيبراني وحماية البنية التحتية الحيوية. كما أنها تتبنى مجموعة من البرامج التعليمية المتقدمة في الجامعات مثل MIT وStanford لتخريج خبراء أمن معلومات.

وبحسب التقرير الرسمي الصادر عن مركز الدراسات الاستراتيجية في واشنطن CSIS بالتعاون مع شركة ما كافي لبرنامج الأمن المعلوماتي McAfee والذي تم نشره بداية عام ٢٠١٨م فإن الخسائر الناتجة عن النمو المتسارع للجرائم السيبرانية ارتفعت من ٤٥ مليار دولار عام ٢٠١٤ إلى نحو ٦٠٠

(1) https://www.cnbcarabia.com/128373/2024/21/09

مليار دولار عام ٢٠١٧ والرقم مرشح للزيادة، وترجع هذه الزيادة إلى الاستخدام المتطور للتقنيات الحديثة في تنفيذ الهجمات السيبرانية[١].

وتشريعات الأمن السيبراني في الولايات المتحدة الأمريكية تضمن مجموعة من القوانين الفيدرالية التي تهدف إلى حماية الأنظمة الرقمية، البيانات الحساسة، والبنية التحتية الحيوية من التهديدات السيبرانية، ومن أهم هذه التشريعات قانون نذكر:

- قانون حماية المعلومات الصحية HIPAA لعام ١٩٩٦م الذي يفرض معايير لحماية البيانات الصحية الإلكترونية ويلزم المؤسسات الصحية باتخاذ تدابير أمنية لمنع الوصول غير المصرح به.
- قانون حماية المعلومات المالية GLBA لعام ١٩٩٩م، وهذا القانون يلزم المؤسسات المالية بحماية المعلومات الشخصية للعملاء.
- قانون الأمن السيبراني الوطني CISA لعام ٢٠١٨م، وبموجب هذا القانون تم إنشاء وكالة الأمن السيبراني وأمن البنية التحتية (CISA)، حيث تعمل الوكالة على تنسيق الجهود الوطنية لحماية البنية التحتية الحيوية من الهجمات السيبرانية.
- قانون الأمن السيبراني الفيدرالي FISMA لعام ٢٠٠٢م، وقد فرض هذا القانون على الوكالات الفيدرالية تقييم وإدارة مخاطر الأمن السيبراني. مع عمل مراجعة دورية للأنظمة الأمنية وتوثيق الإجراءات.

بالإضافة إلى القوانين الفيدرالية، أصدرت ولايات عديدة قوانين تحظر القرصنة وغيرها من الجرائم الإلكترونية، بعضها أوسع نطاقًا من القوانين الفيدرالية. على سبيل المثال، تحظر ولاية نيويورك استخدام الحاسوب عن علم بقصد الوصول إلى مواد حاسوبية (التعدي على ممتلكات الحاسوب)، وذلك بموجب المادة ١٥٦/١٠من قانون العقوبات في نيويورك، مع فرض عقوبة السجن التي تصل لمدة أربع سنوات.

كما أن وزارة الدفاع البنتاجون قد عدلت من استراتيجيتها للفضاء السيبراني عام ٢٠١١م لتشمل إلى جانب الأهداف العسكرية كافة جوانب الحياة بما في ذلك البنى التحتية وشبكات النقل والطاقة والأنظمة المالية[٢].

---

(1) Ney, Joseph, S. (2011). Power and national security in cyberspace America's cyber future, center for a new America security, volume 2, p 16.

(٢) لمزيد من التفاصيل ينظر: تامر سعيد عبد اللطيف محمود، الاستمرارية والتغير في استراتيجية الأمن السيبراني للولايات المتحدة الأمريكية في المدة من ٢٠٠٩ إلى ٢٠٢٤، مجلة العلوم السياسية، العدد ٦٩، ٢٠٢٥، ص ٢٧١ وما بعدها.

ومن أهم المبادرات التي اتخذتها الحكومة الأمريكية مبادرة "Zero Trust Architecture" التي تتبناها المؤسسات الفيدرالية.

أما من حيث إجراءات الضبط الإداري الإلكتروني، فهناك التزام على كافة المؤسسات الفيدرالية بتطبيق نموذج "Zero Trust" لحماية البيانات الحكومية. وهو ما ترتب عليه تقليل فرص اختراق قواعد بيانات المواطنين، مما يعزز الثقة العامة ويمنع الفوضى المعلوماتية. ومن أهم المؤسسات المعنية بالأمن السيبراني على المستوى الفيدرالي وزارة الداخلية والدفاع، مكتب الأمن الإلكتروني والاتصالات، مركز حماية البنى التحتية الوطنية، إضافة إلى قطاع جرائم الحاسب الآلي. كذلك تم اعتماد خطة تسمح بإعطاء الأولوية للوكالات الاستخباراتية الأمريكية لأجل مجابهة المخاطر الإلكترونية التي تهدد الحكومة والبنى التحتية الحيوية للدولة[١].

المطلب الثاني: تجربة العراق وبعض الدول العربية في مجال الأمن السيبراني

كما هو الحال على المستوى الدولي والذي شهدنا فيه الجهود المشتركة أو الفردية لمواجهة المخاطر المتعددة التي قد تنال من الامن القومي لتلك الدول فان الدول العربية قد سعت هي الاخرى الى الحد من تلك المخاطر وان كان يعاب عليها أنها كانت مقتصرة على المستوى الفردي، فقد حاول العراق ان يتخذ بعض الاجراءات المهمة لمواجهة خطر انتهاك سيادته وأمنه القومي والداخلي، كما واجهت بعض الدول العربية هذه المخاطر من خلال الكثير من الإجراءات القانونية والمادية وهذا ما سنبينه في تجربة العراق وبعض الدول العربية.

الفرع الأول: جهود العراق في مجال الأمن السيبراني

العراق دولة ذات تاريخ ممتد عبر آلاف السنين، وهي مهد للعديد من الحضارات، البابلية والسومرية والآشورية، وتمتلك العديد من الثروات الطبيعية، إضافة إلى موقعها المتميز، وإمكاناتها البشرية، وتنوعها الثقافي[٢]، ورغم أن العراق بدأت نهضتها الصناعية مبكراً، فهي كدولة تمتلك ثروات نفطية وتعدينية مؤهلة لأن تكون في مصاف الدول المتقدمة صناعياً؛ إلا أنها مرت بكثير من الأحداث السياسية والحروب التي عطلت من تقدمها وتحقيق نهضتها الشاملة.

---

[١] ميهوب وسام، نموذج الولايات المتحدة الأمريكية في مجال الأمن السيبراني: بين ضرورة الهجوم وإمكانات الدفاع، مجلة البيان للدراسات القانونية، المجلد ٨، العدد ٢، ديسمبر ٢٠٢٣، ص ١٣١.

[2] العراق: التاريخ، الخريطة، العلم، السكان، والحقائق. موقع بريتانيكا على الرابط التالي:

https://www.britannica.com/place/Iraq

وفي ظل التطورات التكنولوجية التي يشهدها العالم والتي زادت وتيرتها في السنوات الأخيرة، وتسارعت كافة دول العالم لتوطين التكنولوجيا في المجالات المختلفة، كان على الحكومة العراقية ألا تتخلف عن مسايرة هذا الواقع الجديد، ورغم دخول الانترنت العراق مبكراً إلا أن استخدامه كان على نطاق ضيق حتى عام ٢٠٠٣، حيث تغيرت الأوضاع كثيراً فزاد عدد المستخدمين لشبكة الانترنت، ومُدت خطوط الاتصالات اللاسلكية عبر الاقمار الصناعية، وتزايد عدد مقدمي الخدمات الرقمية[١].

ثم في العام ٢٠٠٤ بدأت العراق أولى خطواتها نحو اعتماد نهج متكامل للحكومة الإلكترونية من أجل التنمية المحلية والوطنية، وبما يتماشى مع استراتيجية التنمية الوطنية العراقية والأهداف الإنمائية، وتم توقيع مذكرة تفاهم وقعت بين وزير الابتكار والتكنولوجيا الإيطالي ووزير العلوم والتكنولوجيا العراقي ونتج عن هذا التعاون تدشين شبكة جديدة لربط الوزارات العر اقيه، وإنشاء بنية تحتية أساسية لتوفير الخدمات الرقمية تبع ذلك استراتيجية الوكالة الأمريكية للتنمية الدولية لتعزيز الخدمات الرقمية العامة في العراق بهدف استعادة الخدمات الأساسية وتحسين حوكمة القطاع، وفي عام ٢٠٠٩ قامت الحكومة بالبدء في تنفيذ برنامج الحكومة الإلكترونية[٢].

بيد أن الواقع يشير إلى أن عملية التحول الرقمي في العراق تأخرت نسبياً مقارنة ببعض دول الجوار، كما أنها تسير ببطء سواء على الجانب السياسي والحكومي أو على جانب التشريعات المنظمة للمجالات التكنولوجية، وهو الأمر الذي يرجع إلى العديد من العوامل السياسية والاقتصادية والأمنية، ونتج عنها مجموعة من التحديات التي أبطأت من عملية دمج التكنولوجيا في كافة القطاعات، وتمثلت هذه التحديات في ضعف النية التحتية الرقمية، التأخر الكبير في إعداد الكوادر البشرية المؤهلة للانتقال بالمؤسسات الحكومية من نطاق العمل التقليدي إلى الأنظمة الرقمية، ونقص الخبرة وافتقار العديد من المؤسسات للتجارب والممارسات الرقمية، وكل هذه الاسباب تقلل من قدرة الجهات المختصة على امتلاك نماذج رقمية لأداء الخدمات.

التحدي الأكبر الذي يواجه الحكومة للحفاظ على الفضاء الإلكتروني يتمثل في توفير الأمن السيبراني الذي يحمي المؤسسات والأفراد من التهديدات والهجمات الإلكترونية وذلك لعدة أسباب منها:

---

[١] هناء عدالت حسن المختار، تطور المعلوماتية في فئات المجتمع العراقي والمصري حسب المؤشرات الثلاث (الأعمال والأشخاص والحكومات) لسنة ٢٠١٦، دراسة مقارنة، المجلد ١٤، العدد ٣، يوليو ٢٠١٣، ص ٣٩١٤ وما بعدها.

[٢] لمزيد من التفاصيل ينظر: على صباح محمد، وعبد الرحمن محمد عيسى، توظيف التكنولوجيا الحديثة في مؤسسات الدولة (العراق نموذجا)، مجلة كلية دجلة الجامعة، المجلد ٧، العدد ٣، أيلول ٢٠٢٤، ص ٥٦٦ وما بعدها.

أولاً-غياب وضعف التشريعات التنظيمية واللوائح الإدارية:

وذلك بسبب غياب تشريع للأمن السيبراني حتى الآن، والقانون الوحيد يتضمن بنودًا تتعلق بحماية البيانات وتنظيم الفضاء الرقمي هو الاتصالات والمعلوماتية رقم ١٥٩ لسنة ١٩٨٠، لكنه لا يغطي الأمن السيبراني بشكل شامل. إضافة إلى بعض الأوامر الوزارية والتنظيمية الصادرة من وزارة الداخلية وهيئة الإعلام والاتصالات لتنظيم التعامل مع الابتزاز الإلكتروني وبعض الاختراقات.

أما قانون مكافحة الجرائم الإلكترونية رقم ١٢ لسنة ٢٠٠٨ فرغم أنه يهدف إلى تنظيم استخدام التكنولوجيا من خلال إطار قانوني ملزم، إلا أنه جاء قاصراً عن مواكبة التغيرات الحديثة مثل الجرائم الإلكترونية المتطورة وحماية البيانات. ونفس الأمر ينطبق على قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩ المعدل فهو وغن كان يعالج بعض القضايا مثل التشهير أو الإساءة لكنه أيضاً لا يغطي كافة الجرائم الرقمية الحديثة[١].

كما أن قانون حماية المستهلك رقم ١ لسنة ٢٠١٠ يتضمن بعض البنود القليلة التي يمكن تطبيقها على التجارة الإلكترونية لكنه غير قادر على تقديم حماية للعديد من الجرائم كالاحتيال الرقمي أو الابتزاز أو سرقة بيانات العملاء وغيرها من الجرائم الإلكترونية الاخرى.

إن عدم وجود تشريعات محددة لحماية البيئة الرقمية في العراق يعرض المؤسسات والأفراد لخطر التعرض لهجمات سيبرانية من قبل المهاجمين والهاكرز، الذين يتمكنون من تمرير نشاطهم الإجرامي دون عقوبة تردعهم، كما أن ذلك يعطل حركة سلطات الضبط في وقاية المجتمع من هذا النوع من الجرائم قبل وقوعها لعدم بسبب عدم وجود الضوابط والإجراءات التي تمكن سلطات الضبط من عدم أداء وظيفتها في الحفاظ على البيئة الرقمية، ويترتب على هذا زيادة في الهجمات السيبرانية وتغيب العدالة التي ينشدها المجتمع[٢].

ثانياً- ضعف البنية التحتية وغياب الأمن الإلكتروني:

---

(1) لمزيد من التفاصيل ينظر: طلال ناظم الزهيري، إطار تشريعي مقترح للحد من الجرائم الإلكترونية وتعزيز الأخلاقيات الرقمية في العراق، مجلة آفاق للأبحاث السياسية والقانونية، المجلد ٨، العدد ١، ٢٠٢٥، ص ٧٥ وما بعدها.

(2) للمزيد ينظر: رعد خضير صليبي، تعزيز الأمن السيبراني في العراق: التحديات والفرص، مجلة دراسات دولية، العدد ٩٩، ٢٠٢٤، ص ٥١٨ وما بعدها.

يعاني العراق من ضعف في البنية التحتية الرقمية على كافة المستويات والقطاعات سواء الأمنية أو المصرفية أو الشخصية، وهوما يسهل من عمليات الاختراق والتجسس على البيانات، وزيادة فرص السطو عليها والتلاعب بها بغرض الابتزاز أو ارتكاب الجرائم أو قد تستخدم لتنفيذ أعمال إرهابية وتخريبية تهدد أمن واستقرا النظام العام. ولعل من عوامل تأخر العراق في إنشاء بنية تحتية قوية يرجع إلى عدم قدرة شبكات الإنترنت على مواكبة التطورات التكنولوجية السريعة، علاوة على المشاكل التي يعاني منها قطاع للكهرباء، وكذلك غياب الربط الإلكتروني بين الجهات الحكومية. إضافة إلى عدم توفير العدد الكافي من أجهزة الحاسوب في المؤسسات الحكومية.

وعلى الجانب الإداري هناك نقص في الكوادر الفنية والبرامج التدريبية والموارد اللازمة لتنفيذ القوانين التكنولوجية وللتعامل مع قضايا التكنولوجية، إضافة إلى عدم الاستعانة بالأدوات الحديثة في التحقيق والملاحقة، وهو ما يقلل من قدرة الأجهزة المعنية من التصدي للتهديدات الإلكترونية.

ومع تزايد اعتماد المجتمع العراقي على التكنولوجيا الرقمية أصبح من اللازم العمل من قبل الحكومة على تبني سياسات تكفل بيئة رقمية آمنة وموثوقة حتى تنال ثقة المواطنين والمقيمين، وخاصة في ظل سعي الحكومة لجذب الاستثمارات الأجنبية لتنفيذ خطط التنمية[١]. وفي الأونة الأخيرة أطلقت الحكومة العراقية بعض المبادرات لتحديث القوانين القديمة وتبني تشريعات جديدة تتعلق بالتكنولوجيا الحديثة. كما تم إنشاء وحدات متخصصة في الجرائم الإلكترونية داخل أجهزة الشرطة لتعزيز القدرة على مكافحة الجرائم الرقمية بفعالية[٢].

ثالثاً: الاستراتيجية الوطنية للأمن السيبراني في العراق:

أطلقت الحكومة العراقية الاستراتيجية الوطنية للأمن السيبراني وهي "استراتيجية الاستعداد الوطني لتوفير تدابير متماسكة وإجراءات استراتيجية لضمان أمن وحماية الوجود العراقي في الفضاء السيبراني، وحماية البنية التحتية الحيوية للمعلومات، وبناء ورعاية مجتمع إنترنت موثوق به. عادة، تتألف استراتيجية الأمن السيبراني الوطنية من عدة استراتيجيات قصيرة ومتوسطة وطويلة الأمد تغطي جميع الأولويات الوطنية، وتعالج التعرض الوطني للمخاطر السيبرانية. هنالك تهديدات سيبرانية رئيسية في جميع أنحاء العالم التي تضر بالمصلحة الوطنية. مثل؛ الجريمة الإلكترونية– الإرهاب الإلكتروني –

---

[١] توركان إبراهيم علي، الحكومة الإلكترونية وأثرها على ابرام العقود الإلكترونية، مجلة كلية القانون للعلوم القانونية والسياسية، املجلد١٠، العدد ٣٩، ٢٠٢١، ص ٤٣.

[2] https://osamatumalegal.com/ar/blog

الصراع السيبراني –التجسس السيبراني إساءة معاملة الأطفال واستغلالهم عبر الانترنت"[١]. ومن انعكاس تلك الستراتيجية فقد لم انشاء بعض المراكز والادترات لضمان حماية الأمن اليبراني منها:

– مركز الأمن السيبراني:

في يناير ٢٠٢٥ أطلقت الحكومة العراقية مبادرة إنشاء مركز الأمن السيبراني ليكون أحد قطاعات وزارة الداخلية، ثم تحول بعد ذلك إلى كيان مستقل، ويختص هذا المركز ببعض المهام التي تعزز من الأمن الرقمي ومن ذلك:

– مكافحة الابتزاز الإلكتروني الذي يستهدف المؤسسات والمواطنين وضبط وملاحقة مرتكبيه.

– حماية المنصات الحكومية من التهديدات السيبرانية.

– التصدي للإرهاب الإلكتروني والمنصات ذات الأفكار المتطرفة أو الهدامة

– كشف التهديدات والهجمات السيبرانية وتحليلها، وتقييم المخاطر الناجمة عنها بما يمكن من الوقاية والحد منها.

– تدريب وتنمية الكوادر الأمنية الرقمية وتأهيلها للتعامل مع التهديدات الإلكترونية.

رابعاً: خارطة التعاون الرقمي:

خلال مؤتمر ITEX ٢٠٢٥ لتعزيز الوعي السيبراني أعلنت هيئة الإعلام والاتصالات عن خارطة للتعاون في المجالات الرقمية من خلال برامج تدريبية مع شركات تقنية عالمية، مع التوسع في إنشاء مراكز للأمن السيبراني في كافة المحافظات العراقية[٢]، وتشمل هذه الخارطة على عدة محاور وهي:

- تطوير التشريعات الرقمية.
- تعزيز التوقيع الإلكتروني.
- إنشاء بنية تحتية سيبرانية وطنية.
- بناء شراكات مع القطاع الخاص والجامعات.

---

[١] للمزيد ينظر: استراتيجية الأمن السيبراني في العراق، مستشارية الأمن الوطني، امانة سر اللجنة الفنية العليا لامن الاتصالات والمعلومات.على الربط التالي
https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/00056_06_iraqi-cybersecurity-strategy.pdf

[2] https://www.alamssar.com/437293

ويقترح الباحث على الحكومة الإسراع في تنفيذ خطط واستراتيجيات الأمن السيبراني تتضمن سن وتحديث التشريعات اللازمة التي تمس المجالات الحيوية والحساسة لتتناسب مع التطورات المتسارعة للتكنلوجيا الرقمية، مع الاستفادة من التجارب الدولية الرائدة في مجال الأمن السيبراني، والتركيز على الاهتمام بالتعاون الدولي، إضافة إلى توفير الدعم السياسي والمالي اللازم، إضافة عمل حملات أعلانية وعقد الندوات لتوعية المواطنين بمخاطر الهجمات السيبرانية.

الفرع الثاني: جهود بعض الدول العربية في مجال الأمن اليبراني

أولاً: جهود المملكة الأرنية الهاشمية في مجال الأمن السيبراني:

تعد المملكة الأردنية الهاشمية من بين الدول العربية الرائدة في مجال الأمن السيبراني، حيث حققت تقدمًا ملحوظاً على المستويين الإقليمي والدولي، حيث أشار التقرير الأخير للمؤشرات الوطنية للأمن السيبراني (NCSI) إلى حلول الأردن في الترتيب الأول عربيًا والعشرون عالميًا بنسبة بلغت ٧٣.٣٣٪، وهو ما يعكس الاهتمام المتزايد من جانب حكومة المملكة وسعيها المستمر نحو تطوير خطط الأمن السيبراني بشمولية تؤكد من خلالها تكاملها مع الجهود العالمية لمواجهة الهجمات والتهديدات الإلكترونية.

كما يؤكد تقرير الربع الثالث لتقدم سير العمل في البرنامج التنفيذي لرؤية التحديث الاقتصادي ٢٠٢٣-٢٠٢٥، فإن هذا الترتيب الجديد للمملكة يمثل خطوة بالغة الأهمية ويعزز من مكانة الأردن كمركز إقليمي للأمن السيبراني، وينبئ عن فاعلية السياسات المتخذة في هذا المجال الحيوي، مما يعزز من ثقة المستثمرين سواء الأجانب أو الوطنيين [١].

وتجدر الإشارة إلى أن المشرع الأردني ومن خلال ما أصدرته من تشريعات لتنظيم البيئة الرقمية قد عزز من المجهودات التي اتخذتها الحكومة في مجال الأمن السيبراني، حيث أصدر **قانون الأمن السيبراني الأردني رقم ١٦ لسنة ٢٠١٩م**، والذي يرمي إلى تحقيق بعض الأهداف أهمها حماية المملكة من تهديدات حوادث الأمن السيبراني، إضافة إلى تطوير قدرات الردع والمراقبة والإنذار لتحقيق استجابة مرنة لحوادث الأمن السيبراني والتخفيف من الاضرار الناجمة عنها، مع العمل على بناء قدرات أمن

(1) https://www.almamlakatv.com/news/154844

سيبراني وطني يضمن مواجهة التهديدات التي تعترض أنظمة المعلومات والبنى التحتية، وكذلك رفع مستوى الأمن الوطني العام والشامل للمؤسسات والأفراد[١].

ومن الأهداف أيضاً خلق بيئة أمنة لأجل جذب الاستثمارات الخارجية ومحفزة للاقتصاد الوطني، خاصة في ظل تسارع التطور في أنظمة المعلومات وتنامي حجم الخدمات الحكومية لمراقبة الفضاء السيبراني الوطني ورصد وتوثيق حوادث الأمن السيبراني.

كما أصدرت المملكة قانون الجرائم الإلكترونية الأردني رقم ١٧ لسنة ٢٠٢٣، وقانون حماية البيانات الشخصية رقم ٢٤ لسنة ٢٠٢٣، ونظام ترخيص مقدمي خدمات الأمن السيبراني رقم ٧٦ لسنة ٢٠٢٤، الصادر في ٢٠٢٤/١٠/٢٢، وهذا النظام الأخير صادر بمقتضى البند (٤) من الفقرة (ب) من المادة ٦ والمادة ١٨من قانون الأمن السيبراني رقم ١٦ لسنة ٢٠١٩.

أ- **المجلس الوطني للأمن السيبراني** [٢]: تم إنشاء المجلس الوطني للأمن السيبراني بموجب نص المادة ٣/أ من قانون الأمن السيبراني الأردني رقم ١٦ لسنة ٢٠١٩، وهو مؤسسة وطنية عامة تهدف إلى بناء منظومة قوية وفعالة للأمن السيبراني. ويشكل المجلس من رئيس يعين بإرادة ملكية سامية وعدد من الأعضاء يمثلون كل من وزارة الاقتصاد الرقمي والريادة، البنك المركزي، القوات المسلحة الأردنية، مديرية الأمن العام، المركز الوطني للأمن وإدارة الأزمات، وثلاثة اعضاء يسميهم مجلس الوزراء يتم اختيارهم لمدة سنتين قابلة للتجديد لمرة واحدة على أن يكون اثنان منهم من ذوي الخبرة في القطاع الخاص. كما بينت المادة ٤ من ذات القانون مهام وصلاحيات المجلس، أهمها إقرار الاستراتيجيات والسياسات والمعايير المتعلقة بالأمن السيبراني.

ب- **المركز الوطني للأمن السيبراني** [٣]: نصت المادة ٥/أ من قانون الأمن السيبراني الأردني سالف الذكر على أن: "يُنشأ في المملكة مركز يسمى (المركز الوطني للأمن السيبراني) يتمتع بشخصية اعتبارية ذات استقلال مالي وإداري وله بهذه الصفة تملك الأموال المنقولة وغير المنقولة والقيام بجميع التصرفات القانونية اللازمة لتحقيق أهدافه بما في ذلك إبرام العقود وحق التقاضي وينوب عنه في الإجراءات القضائية وكيل إدارة قضايا الدولة".

---

[١] د. محمد السعيد القزعة، د. طارق السيد أبوعقيل، المواجهة الجنائية، مصدر سابق، ص٤٧٨.

[٢] لمزيد من التفاصيل ينظر: موقع المركز الوطني للأمن السيبراني الأردني على الرابط التالي:
https://ncsc.jo/Ar/List/Regulation_AR

[3] صدر نظام المركز الوطني للأمن السيبراني رقم ١ لسنة ٢٠٢٠وذلك استناداً لنص الفقرة ٣ من المادة ٧ من قانون الامن السيبراني رقم ١٦ لسنة ٢٠١٩. نشر هذا النظام بالجريدة الرسمية ، العدد رقم ٥٦١٤ بتاريخ ٢٠٢٠/١/٢.

كما بينت المادة ٦/أ أن الهدف من المركز هو بناء منظومة فعالة للأمن السيبراني على المستوى الوطني وتطويرها وتنظيمها لحماية المملكة من تهديدات الفضاء السيبراني ومواجهتها بكفاءة وفاعلية بما يضمن استدامة العمل والحفاظ على الأمن الوطني وسلامة الأشخاص والممتلكات والمعلومات. وبحسب المادة ٦/ب يتولى المركز العديد من المهام من بينها، إعداد استراتيجيات وسياسات ومعايير الأمن السيبراني ومراقبة تطبيقها ووضع الخطط اللازمة لتنفيذها ورفعها للمجلس لإقرارها. ويسعى المركز كذلك إلى تطوير عمليات الأمن السيبراني وتدريب وتأهيل وتوعية وتثقيف موظفي القطاع العام والخاص وكافة فئات المجتمع وإكسابهم المعرفة والمهارات اللازمة للحد من المخاطر والتهديدات وفقاً لأفضل الممارسات، وكذلك تحديد معايير الأمن السيبراني وضوابطه، وتصنيف حوادث الأمن السيبراني في ضوء التعليمات الصادرة عنه، وإعداد مشروعات التشريعات ذات العلاقة بالأمن السيبراني بالتعاون مع الجهات المعنية ورفعها للمجلس.

ثانياً: المملكة العربية السعودية:

يمثل الأمن السيبراني في السعودية جزءًا أساسيًا من رؤية المملكة العربية ٢٠٣٠، حيث تسعى المملكة إلى حماية المعلومات والبيانات الرقمية من الهجمات الإلكترونية[١]. ففي السنوات الأخيرة، استثمرت المملكة العربية السعودية بكثافة في الأمن السيبراني وقد تضمن ذلك؛ إنشاء الهيئة الوطنية للأمن السيبراني (NCA) وتطوير الاستراتيجية الوطنية لأمن المعلومات (NISS) كما أصدرت الهيئة الوطنية للأمن الإلكتروني لوائح وإرشادات جديدة لتحسين ممارسات الأمن السيبراني في القطاعين الحكومي والخاص، مع التركيز على رفع مستوى الوعي العام حول تهديدات الأمن السيبراني وأفضل الممارسات[٢].

واعتبرت السعودية أن مسالة الأمن السيبراني في السعودية تأتي كأولوية وطنية، وقد عبرت المملكة عن طموحها في أن تكون رائدة عالميًا في هذا المجال من خلال مجموعة من الاستراتيجيات والمبادرات التي تشرف عليها الهيئة الوطنية للأمن السيبراني. وقد حققت المملكة تقدمًا كبيرًا، حيث احتلت مراكز متقدمة في مؤشرات الأمن السيبراني العالمية.

---

[١] لمزيد من التفاصيل حول الأمن السيبراني في المملكة العربية السعودية ينظر: المنصة الوطنية على الرابط التالي: https://my.gov.sa/ar/content/cybersecurity

[2] https://nca.gov.sa/ar/#:~:text

وفي يونيو ٢٠٢١ تم الإعلان عن تحقيق السعودية المرتبة الثانية عالميا من بين ١٩٣ دولة، والمركز الأول على مستوى الوطن العربي والشرق الأوسط وقارة آسيا في المؤشر العالمي للأمن السيبراني، الذي تصدره وكالة الأمم المتحدة المتخصصة في تكنولوجيا المعلومات والاتصالات "الاتحاد الدولي للاتصالات"، محققةً بذلك قفزة بـ ١١ مرتبة عن العام ٢٠١٨م، وبأكثر من ٤٠ مرتبة منذ إطلاق رؤية السعودية ٢٠٣٠ حيث كان ترتيبها ٤٦ عالميًا في نسخة المؤشر للعام ٢٠١٧م. وفي يونيو ٢٠٢٤ ووفقاً لتقرير الكتاب السنوي للتنافسية العالمية لعام ٢٠٢٤ الصادر عن مركز التنافسية العالمي بسويسرا، حققت السعودية المرتبة الثانية عالمياً بعد الولايات المتحدة الامريكية في مؤشر الأمن السيبراني.

وتشمل جهود الأمن السيبراني في رؤية السعودية ٢٠٣٠ تطوير استراتيجيات وتقنيات متقدمة للتصدي للهجمات الرقمية، تعزيز الوعي والمهارات في مجال الأمن السيبراني، وتطبيق معايير عالمية لحماية المعلومات في البيئات الرقمية.، حيث تسعى المملكة إلى ضمان استقرار البنية التحتية الرقمية وحماية مصالحها الاستراتيجية في ظل عالم رقمي متطور ومليء بالتحديات[١].

كما تلتزم المملكة العربية السعودية بتأمين بنيتها التحتية الرقمية من خلال استراتيجيات شاملة وتقنيات متطورة وأطر تنظيمية. وتهدف هذه الإجراءات إلى حماية المواطنين والشركات والمؤسسات من التهديدات المتطورة، مع تعزيز الوعي وبناء القدرات والتعاون العالمي. وهو ما يسهم تطلعات المملكة الرامية إلى إرساء منظومة رقمية مرنة وآمنة، تتماشى مع رؤية ٢٠٣٠.

أ- الهيئة الوطنية للأمن السيبراني:

وعلى مستوى التنظيمات والمؤسسات الحكومية أنشأت المملكة الهيئة الوطنية للأمن السيبراني، والتي تأسست عام ٢٠١٧، تتمثل مهمتها في حماية المصالح الحيوية والبنية التحتية الحيوية والخدمات الحكومية. كما تشرف على أطر العمل الوطنية للأمن السيبراني، وتشدد الهيئة على مسؤولية الجهات في الامتثال للأمن السيبراني. وتضطلع بالعديد من المسؤوليات على النحو التالي:

- إعداد الاستراتيجية الوطنية للأمن السيبراني وتنفيذها.
- إدارة مخاطر الأمن السيبراني عبر البنية التحتية الحيوية والقطاعات ذات الأولوية.
- تشغيل مراكز الأمن السيبراني الوطنية للمراقبة والاستجابة للحوادث وتبادل المعلومات.

---

[١] سمية مشرف عبد الله العمري، الأمن السيبراني ودوره في رفع مستوى الأمن العام للدولة "المملكة العربية السعودية أنموذجاً" دراسة في الجغرافيا السياسية، مجلة مركز الخدمة للاستشارات البحثية، المجلد٢٦، العدد٧٧، كلية الاداب، جامعة المنوفية، يناير ٢٠٢٤، ص١٠: ١٢

- بناء القدرات الوطنية في مجال الأمن السيبراني من خلال التدريب والترخيص والمعايير المهنية.
- تمثيل المملكة العربية السعودية في مسائل الأمن السيبراني العالمي.
- تعزيز الابتكار وتحسين استثمارات الأمن السيبراني.

ب- المركز الوطني للاستجابة لطوارئ الحاسب الآلي(CERT)

يُعد المركز الوطني للاستجابة لطوارئ الحاسب الآلي (CERT) جزءًا من الهيئة الوطنية للأمن السيبراني، ويعمل على التوعية بالأمن السيبراني، وإصدار التحذيرات بشأن التهديدات الناشئة ومعالجة الثغرات الأمنية. كما يقود حملات التوعية ويتعاون مع فرق الاستجابة العالمية ويوفر الموارد في الوقت المناسب[١].

ت- البوابة الوطنية لخدمات الأمن السيبراني (حصين):

تمكن بوابة حصين الوطنية الجهات والأفراد من خلال توفير أحدث منصات الأمن السيبراني. وتشمل أهدافها في تعزيز البنية التحتية الوطنية للأمن السيبراني، تمكين الجهات من تحقيق أهدافها في مجال الأمن السيبراني، تحسين الإنفاق الحكومي في مجال الأمن السيبراني. وتعزيز الخبرات المحلية في مجال الأمن السيبراني.

وعلى الجانب التشريعي اهتم المنظم السعودي بحماية البيئة الرقمية[٢]، فأصدر نظام مكافحة الجرائم المعلوماتية وبينت المادة الثانية من هذا النظام الأهداف التي يرمي إلى تحقيها وهي" :يهدف هذا النظام إلى الحد من وقوع جرائم المعلوماتية، وذلك بتحديد هذه الجرائم والعقوبات المقررة لكل منها، وبما يؤدي إلى ما يأتي:

- المساعدة على تحقيق الأمن المعلوماتي.
- حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية
- حماية المصلحة العامة، والأخلاق، والآداب العامة.

---

[١] ينظر: المنصة الوطنية على الرابط التالي:
https://my.gov.sa/ar/content/cybersecurity#section-2

[٢] د. فهد بن عابد الشمرى، الإطار القانوني لحماية البيانات الشخصية فى تشريعات المملكة العربية السعودية، دراسة تحليلية، مجلة البحوث الفقهية والقانونية، العدد٤٣، كلية الشريعة بدمنهور، جامعة الأزهر، اكتوبر ٢٠٢٣، ص ١٦٥٢: ١٦٥٣.

الخاتمة

على الرغم من كم الفوائد الإيجابية الناجمة عن التطور التقني إلا أن هذا التطور قد كشف في العقدين الأخيرين عن كم من المخاطر لا يمكن الاستهانة به وعلى نحو قد شكل تهديدًا قويًا لأمن واستقرار المجتمعات، وأدى إلى تحول اهتمامات المجتمع الدولي من كيفية الاستفادة من المزايا الناجمة عن التطور التقني، إلى التفكير في وضع الخط والاستراتيجيات التي تستهدف الحد من مخاطره وما يفرضه من التحديات. ومما لا شك فيه أن هذه التحديات الكبيرة قد فرضت على سلطات الضبط العديد من الالتزامات التي تثقل كاهلهم، وتجعل من الصعوبة مواجهتها بالوسائل والسبل التقليدية، الأمر الذى دفع العديد من الدول إلى تبني خطط تستهدف تطوير الأداء في المجال الأمني من خلال الاهتمام بالأجهزة المعنية بوظيفة الضبط الإداري في سبيل تقديم كل آليات الدعم للقائمين على هذه الأجهزة للنهوض بالأعباء الملقاة على عواتقهم.

ومن خلال ما عرضنا له من أفكار في طيات هذا البحث قد توصلنا إلى مجموعة من النتائج والتوصيات يمكن تلخيصها على النحو التالي:

النتائج:

١- تلعب التطورات التكنولوجية وما ارتبط بها من عمليات التحول الرقمي، إضافة إلى ظهور تقنيات الذكاء الاصطناعي الدور الأهم والأقوى في تشكيل الواقع المجتمعي مما ترتب عليه تغير في طبيعة وشكل العلاقات.

٢- لا زالت العراق في حاجة لتضافر كافة الجهود للتصدي للمخاطر التقنية، وبالأخص في الجانب التشريعي، والجوانب المرتبطة بالبنية التحتية.

٣- مع تزايد تعقيد الهجمات السيبرانية وتكرارها، أصبحت ضرورة حماية مجالاتنا الرقمية أمرًا بالغ الأهمية. وأن ما يرتبط بها من تحديات غيرت من المفاهيم التقليدية للقيادة والسيطرة سواء ما تعلق منها بالأعمال المدنية أو ما كان منها يخص المجالات العسكرية.

٤- فرض التطور التقني المتسارع العديد من التحديات كما أضاف عبئًا جديدًا على الأجهزة المعنية بالضبط الإداري.

٥- تشكل الهجمات السيبرانية واستغلال التقنية الحديثة في ارتكاب الجرائم تهديدًا للأمن القومي.

٦- تلعب أنظمة الأمن السيبراني دوراً حيوياً لا غنى عنه في حماية البيانات والمعلومات سواء ما تعلق منها ببيانات الأفراد أو المؤسسات وبصفة خاصة المنظمات والأجهزة التابعة للدولة، فالأمن السيبراني هو جدار الحماية الأول للحفاظ على الخصوصية وضمان سرية البيانات.

التوصيات:

١- يجب على الهيئات الحكومية العمل باستمرار على تحديث وتطوير آلياتها ووسائلها، ومن خلال تبني استراتيجيات جادة وقائمة على أسس علمية وتقنية حديثة تمنحها القدرة على مجابهة التحديات والمخاطر المختلفة الناتجة عن الاستخدام غير المشروع من قبل مرتكبي الهجمات السيبرانية.

٢- إلزام الشركات التي تستخدم بيانات الأفراد بتضمين تطبيقاتها معايير الشفافية والموثوقية، ومراعاة التنوع والشمول والمساواة، ووضع آليات ووسائل أمنية قائمة على التقنيات الحديثة لضمان مستويات عالية من الحماية ضد الهجمات السيبرانية.

٣- نوصي الحكومة العراقية بسرعة العمل على ايجاد بيئة تشريعية متوازنة ومرنة لتتواكب مع التطورات السريعة في المجالات التقنية بحيث تتناسب مع كل ما هو جديد وأن تكون على إطلاع دائم ومستمر بأي تتطور.

٤- دعوة الحكومة العراقية إلى ضرورة العمل على زيادة الاهتمام بالعنصر البشري وتطوير الأجهزة المعنية بوظيفة الضبط الإداري من خلال التدريب المستمر للأفراد في سبيل الاعداد الجيد للنهوض بمهامهم على الوجه الأكمل ، وتزويدهم بكافة الأجهزة المتطورة التي تساعدهم على أداء وظائفهم.

٥- اتخاذ خطوات جادة لتوعية المواطنين بالمخاطر والتحديات التي يتعرض لها المجتمع في الفضاء الرقمي، وذلك من خلال تضمين موضوعات التكنولوجيا وبصفة خاصة الذكاء الاصطناعي والأمن السيبراني ضمن المناهج والمقررات التعليمية بكافة المراحل التعليمية سواء مراحل التعليم الأساسي أو المرحلة الجامعية.

٦- نأمل الحكومة العراقية أن تتبنى خطط للحماية من الهجمات السيبرانية على غرار ما اتخذه الإتحاد الأوروبي من إجراءات تشريعية وتقنية، وأن يشمل ذلك وضع رؤية شاملة للتعاون والتنسيق على المستوى الوطني والدولي لوضع التدابير المناسبة لتنظيم وإدارة المخاطر التي تهدد أمن الشبكات وأنظمة المعلومات.

٧- نوصي الحكومة العراقية بالاستفادة من تجارب الدول الرائدة تكنولوجيا وبصفة خاصة في مجال الأمن السيبراني، مع التركيز على نقل الخبرات من خلال عقد الشركات مع المؤسسات المتخصصة محليا وعالمياً.

قائمة المصادر

أولاً: المصادر باللغة العربية:

١. أميره محمد ابراهيم ساتي، الجريمة المعلوماتية في النظام السعودي، مجلة الأندلس للعلوم الإنسانية والاجتماعية، جامعة الأندلس للعلوم والتقنية، العدد ٧٥، يونيو ٢٠٢٣.
٢. أنور رسلان، وجيز القانون الإداري، ط ٣، بدون دار نشر، ٢٠٠٤.
٣. إيمان محمد الشورة، الأمن السيبراني في البنوك الإسلامية الأردنية، كلية الشريعة، الجامعة الأردنية، ٢٠٢٠.
٤. تامر سعيد عبد اللطيف محمود، الاستمرارية والتغير في استرتيجية الأمن السيبراني للولايات المتحدة الأمريكية في المدة من ٢٠٠٩ إلى ٢٠٢٤، مجلة العلوم السياسية، العدد ٦٩، ٢٠٢٥.
٥. جيهان سعد محمد الخضري وآخرون، الأمن السيبراني والذكاء الاصطناعي في الجامعات السعودية" دراسة مقارنة"، مجلة تطوير الأداء الجامعي، المجلد ١٢، العدد ١، ٢٠٢٠.
٦. حسين أحمد مقداد عبد اللطيف، دور الضبط الإداري في الحد من مخاطر الفضاء الإلكتروني في مصر وفرنسا، مجلة العلوم القانونية والاقتصادية، العدد الأول، السنة الخامسة والستون، يناير ٢٠٢٣.
٧. خالد ظاهر عبد الله جابر السهيل، دور التشريعات الجزائية في حماية الأمن السيبراني بدول مجلس التعاون الخليجي، مجلة البحوث الفقهية والقانونية، جامعة الأزهر، كلية الشريعة والقانون، دمنهور، العدد ٣٨، يوليو ٢٠٢٢.
٨. دعاء محمد ابراهيم بدران، التشريعات الممكنة للضبط الإداري والأمني لمكافحة الانحراف الفكري عبر منصات التواصل الاجتماعي، مجلة البحوث الفقهية والقانونية، كلية الشريعة والقانون بدمنهور، جامعة الأزهر، العدد ٤٠، يناير ٢٠٢٣.
٩. رعد خضير صليبي، تعزيز الأمن السيبراني في العراق: التحديات والفرص، مجلة دراسات دولية، العدد ٩
١٠. سامي حسن نجم الحمداني، وحسين طلال مال الله العزاوي، دور الضبط الإلكتروني في مكافحة الشائعات المخلة بالأمن العام، مجلة جامعة تكريت للحقوق، المجلد ٥، العدد ١، ج١، سبتمبر/ ايلول ٢٠٢٠.
١١. سعيد مفلح حمود الصويلح، الدور الإستشرافي للذكاء الاصطناعي في إدارة الأزمات الأمنية، مجلة الفكر الشرطي، المجلد ٣٢، العدد ١٢٧، اكتوبر ٢٠٢٣.
١٢. سلامة فضل الشامي، جرائم الاعتداء على الحق في الخصوصية في ضوء التطور التكنولوجي، رسالة ماجستير، أكاديمية الإدارة والسياسة للدراسات العليا وجامعة الأقصى بغزة، ٢٠١٨.

١٣. سمية مشرف عبد الله العمري، الأمن السيبراني ودوره في رفع مستوى الأمن العام للدولة "المملكة العربية السعودية أنموذجاً" دراسة في الجغرافيا السياسية، مجلة مركز الخدمة للاستشارات البحثية، المجلد٢٦، العدد٧٧، كلية الاداب، جامعة المنوفية، يناير ٢٠٢٤

١٤. صلاح الدين رجب فتح الباب صميدة، المواجهة التشريعية لمخاطر الذكاء الاصطناعي في ضوء المعايير الدولية، المحور الأول: دراسات في القضايا القانونية المستجدة بكافة مجالاتها، المؤتمر الدولي العلمي الثاني، القضايا القانونية المستجدة، مجلة كلية القانونTwejer ، جامعة سوران، أربيل، الفترة من ٢٢-٢١-٤-٢٠٢٤، المجلد ٧، العدد ١، ٢٠٢٤.

١٥. صلاح الدين رجب فتح الباب، أثر استخدام تقنيات الذكاء الاصطناعي على النظام العام، مجلة الفكر الشرطي، مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، الإمارات، المجلد ٣٣، العدد ١٣١، أكتوبر ٢٠٢٤.

١٦. طارق السيد محمود أبوعقيل، تقنيات الذكاء الاصطناعي ودورها في تسهيل الإرهاب الإلكتروني ومكافحته، مجلة جامعة الزيتونة الأردنية للدراســـات القانونية، المجلد الخامس، اصدار خاص، ٢٠٢٤.

١٧. طلال ناظم الزهيري، إطار تشريعي مقترح للحد من الجرائم الإلكترونية وتعزيز الأخلاقيات الرقمية في العراق، مجلة آفاق للأبحاث السياسية والقانونية، المجلد ٨، العدد ١، ٢٠٢٥.

١٨. عبد الحميد بسيوني: الذكاء الاصطناعي والوكيل الذكي، دار الكتب العلمية للنشر والتوزيع، القاهرة، بدون تاريخ نشر، ص١٩.

١٩. عبد الفتاح المالحي، الإطار القانوني لحماية الحق في الخصوصية في عصر الرقمنة، مجلة الباحث للدراسات القانونية والقضائية، العدد ٥٦، يوليو ٢٠٢٣.

٢٠. على آل مداوي، الأمن السيبراني، تعريفه-أهميته- أنواعه-استراتيجيات للوقاية من الهجمات السيبرانية، مجلة الدراسات الدولية، العدد ٣٤، ١٤٤٥هـ/٢٠٢٣.

٢١. فارس محمد العمارات، ابراهيم الحمامصة، الأمن السيبراني المفهوم وتحديات العصر، دار الخليج للنشر والتوزيع، عمان، الأردن، ٢٠٢٢.

٢٢. فهد بن عابد الشمري، الإطار القانوني لحماية البيانات الشخصية في تشريعات المملكة العربية السعودية، دراسة تحليلية، مجلة البحوث الفقهية والقانونية، العدد٤٣، كلية الشريعة بدمنهور، جامعة الأزهر، اكتوبر ٢٠٢٣.

٢٣. ماجد راغب الحلو، القانون الإداري، دار الجامعة الجديدة، الإسكندرية، ٢٠٠٦.

٢٤. محمد السعيد القزعة، طارق السيد أبوعقيل، المواجهة الجنائية لاستخدام الويب المظلم في الاعتداء على البيانات الشخصية، مجلة جرش للبحوث والدراسات، المجلد٢٥، العدد٢(ب)، الأردن، ٢٠٢٥.

٢٥. محمد جمال جبريل وآخرون، القانون الإداري، الجزء الثاني، النشاط الإداري، الإسراء للطباعة، القاهرة، ب. ت.
٢٦. محمد رفعت عبد الوهاب، مبادئ وأحكام القانون الإداري، دار المطبوعات الجامعية، الإسكندرية، ٢٠٠٢.
٢٧. محمد سعد أحمد، دور التأمين في مواجهة المخاطر الناشئة عن الذكاء الاصطناعي وتكنولوجيا المعلومات، دراسة تحليلية، مجلة مصر المعاصرة، الجمعية المصرية للاقتصاد السياسي والتشريع، القاهرة، العدد ٥٤٣، يونيو ٢٠٢١.
٢٨. محمد سعيد الهاجري، دور الأمن السيبراني في تحقيق الأمن الإلكتروني بدولة قطر، مجلة قراءات علمية في الأبحاث والدراسات القانونية والإدارية، العدد ٣٢، ٢٠٢٤.
٢٩. محمد طه ابراهيم الفليح، الجريمة السيبرانية في النظام القانوني الأردني، مجلة الزرقاء للبحوث والدراسات الإنسانية، المجلد الرابع والعشرون، العدد الأول، ٢٠٢٤.
٣٠. محمد عبد العال السناري، مبادئ ونظريات القانون الإداري، دراسة مقارنة، ٢٠٠٤/٢٠٠٥.
٣١. محمد عبد الله المنشاوي، جرائم الإنترنت في المجتمع السعودي، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، ٢٠٠٣.
٣٢. محمد محمود مكاوي، البيئة الرقمية بين سلبيات الواقع وآمال المستقبل، مجلة المعلوماتية، العدد ٩، ٢٠٠٥.
٣٣. مصلح محمود الصرايرة، القانون الإداري، الكتاب الأول، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، ٢٠١٢.
٣٤. منى الأشقر جبور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والفضائية، ٢٠١٢.
٣٥. ميهوب وسام، نموذج الولايات المتحدة الأمريكية في مجال الأمن السيبراني: بين ضرورة الهجوم وإمكانات الدفاع، مجلة البيان للدراسات القانونية، المجلد ٨، العدد ٢، ديسمبر ٢٠٢٣.
٣٦. وائل أحمد عبد الله صبرة، التحديات الأخلاقية التي تواجه العلم والتكنولوجيا في عصر البيانات الضخمة، مجلة كلية الآداب، جامعة سوهاج، العدد ٥٣، ٢٠١٩.
٣٧. وليد السيد سليم، ضمانات الخصوصية في الإنترنت، دار الجامعة الجديدة، ٢٠١٢.
٣٨. يارا حافظ الجندي، البيانات الشخصية بين التهديد والحماية، دراسة فى ضوء أحكام القانون رقم ١٥١ لسنة ٢٠٢٠، مجلة الدراسات القانونية والاقتصادية، المجلد ٩، العدد ٤، كلية الحقوق، جامعة مدينة السادات، ديسمبر ٢٠٢٣.
٣٩. يوسفي سفيان، وكلثوم مسعودي: الأمن الفكري وتحديات الأمن السيبراني "دراسة نظرية"، مجلة الباحث، مج ١٦، ع ٢ ،٢٠٢٤.

ثانياً: المصادر باللغة الأجنبية:

1. Abou El Seoud, Mahinour. Exploring the Potential of E-Government in Reducing Corruption –Case of Egypt. 2024. American University in Cairo, Master's Thesis. AUC Knowledge Fountain.pp.8-12. https://fount.aucegypt.edu/etds/2207.
2. Alemayehu Tegegn, D. (2024). The role of science and technology in reconstructing human social history: effect of technology change on society. *Cogent Social Sciences*, *10*(1). https://doi.org/10.1080/23311886.2024.2356916
3. Alibasic, A., Al Junaibi, R., Aung, Z., Woon, W. L., & Omar, M. A. (2017). Cybersecurity for smart cities: A brief review. In Data Analytics for Renewable Energy Integration: 4th ECML PKDD Workshop, DARE 2016, Riva del Garda, Italy, September 23, 2016, Revised Selected Papers 4 (pp. 22-30). Springer International Publishing. https://link.springer.com/chapter/10.1007/978-3-319-50947-1_3
4. Ana Paula Brandão and Isabel Camisão, 'Playing the Market Card: The Commission's Strategy to Shape EU Cybersecurity Policy' (2022) 60 Journal of Common Market Studies 1335; Helena Carrapico and André Barrinha, 'The EU as a Coherent (Cyber)Security Actor?' (2017) 55 Journal of Common Market Studies 1254, 1259.
5. Araz Taeihagh, Governance of artificial intelligence, POLICY AND SOCIETY 2021, VOL. 40, NO. 2, p.138. https://doi.org/10.1080/14494035.2021.1928377
6. Chih-Che Suna , Adam Hahna , Chen-Ching Liu,.(2018). Cyber Security of a Power Grid: State-of-the-Art, International Journal of Electrical Power & Energy Systems, Volume 99, July 2018, Pp. 45-56. https://doi.org/10.1016/j.ijepes.2017.12.020
7. Christian Djeffal, Artificial Intelligence and Public Governance: Normative Guidelines for Artificial Intelligence in Government and Public Administration, January 2020, pp.277-290. DOI: 10.1007/978-3-030-32361-5_12
8. Dimitra Markopoulou, Vagelis Papakonstantinou, Paul de Hert, (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation, Computer Law & Security Review,Volume 35, Issue 6, November 2019, pp.1-11. http://www.sciencedirect.com/
9. Edwards, D.J. (2024). Data Protection. In: Critical Security Controls for Effective Cyber Defense. Apress, Berkeley, CA. pp. 57-96 https://doi.org/10.1007/979-8-8688-0506-6_3
10. Elif Kiesow Cortez. (2020). Data Protection Around the World: An Introduction. Privacy Laws in Action, Pp. 1-6.
11. Haenlein. Siri, .in my Hand, who's the Fairest in the Land? On the Interpretations, Illustrations and Implications of Artificial Intelligence, Business Horizons. (1) 62.
12. Herman P The military-technical revolution. Def Analysis 10(1):91–95. https://doi.org/10.1080/07430179408405608
13. Herscovici, A. (2023). Beyond Episteme: The Concept of Order. In: Value, Historicity, and Economic Epistemology. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-21157-7_8
14. Hoadley DS, Lucas NJ (2018) Artificial intelligence and national security. Congressional Research Service, Washington, DC.
15. https://unesdoc.unesco.org/ark:/48223/pf0000369455_ara
16. Isakov Abror Fakhriddinovich, Urozov Fakhridin Isakovich, Abduzhapporov Shahboz Muzaffar Ugli, Isokova Mukhlisa Fakhriddin kizi. (2024). ENHANCING CYBERSECURITY: PROTECTING DATA IN THE DIGITAL AGE, Innovations in Science and Technologies" ilmiy-elektron jurnal. Vo.1, No.1 Pp.40-48.
17. Jed Odermatt, 'The European Union as a Cybersecurity Actor' in Steven Blockmans and Panos Koutrakos (eds), Research Handbook on EU Common Foreign and Security Policy (Edward Elgar Publishing 2018) 359
18. Julian Richards, Cyber-War: The Anatomy of the Global Security Threat, PALGRAVE MACMILLAN, 2014, P.3-6. DOI: 10.1057/9781137399625.0001

19. Kathryn C. Seigfried-Spellar, Gary R. Bertoline, and Marcus K. Rogers. (2011). Internet Child Pornography, U.S. Sentencing Guidelines, and the Role of Internet Service Providers, Digital Forensics and Cyber Crime,Third International ICST Conference, ICDF2C 2011, Dublin, Ireland, October 26-28, 2011, Springer, pp. 17-30. file:///C:/Users/vip/Downloads/978-3-642-35515-8.pdf
20. Kneuper, R. (2025). Technical and Organizational Implementation of Data Protection. In: Data Protection for Software Development and IT. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-70639-8_6
21. M. Martellini (ed.), Cyber Security Deterrence and IT Protection for Critical Infrastructures, SpringerBriefs in Computer Science, DOI: 10.1007/978-3-319-02279-6_1
22. Mahira, D. F., Rohmahwatin, D. S., & Suciningtyas, N. D. (2020). Strengthening Multistakeholder Integrated through Shared Responsibility in the face of Cyber Attacks Threat. Lex Scientia Law Review, 4(1), 59-69. https://doi.org/10.15294/lesrev.v4i1.38191
23. MarshMcLennan, Global cyber terrorism incidents on the rise,2021. https://www.mmc.com/insights/ publications/2018/nov/global cyber-terrorism-incidents-on-the-rise.html.
24. Masike Malatji, Alaa Tolah. (2024): Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI, p 1-2. https://link.springer.com/article/10.1007/s43681-024-00427-4
25. Mayer-Schönberger, V., & Cukier, K. (2013). Big data: A revolution that will transform how we live, work, and think. Houghton Mifflin Harcourt.
26. Morten Bay, (2016). WHAT IS CYBERSECURITY? In search of an encompassing definition for the post-Snowden era, French Journal For Media Research pp. 4-9. https://www.researchgate.net/publication/308609163_WHAT_IS_CYBERSECURITY_In_search_of_an_encompassing_definition_for_the_post-Snowden_era
27. Neil J. Smelser, Paul B. Baltes, History of Technology, International Encyclopedia of the Social & Behavioral Sciences, Pergamon, 2001, Pages 6852-6857, https://doi.org/10.1016/B0-08-043076-7/02648-6. https://www.sciencedirect.com/science/article/pii/B0080430767026486
28. Ney, Joseph, S. (2011). Power and national security in cyberspace America's cyber future, center for a new America security, volume 2, p 16.
29. Pier Giorgio Chiara, (2024). Towards a right to cybersecurity in EU law? The challenges ahead, Computer Law & Security Review, Volume 53, July 2024, 105961. Pp. 1-9. http://www.elsevier.com/locate/clsr
30. Reza Montasari, Cyber Threats and National Security: The Use and Abuse of Artificial Intelligence, p.680.
31. Robert McLaughlin and Hitoshi Nasu .(2014). New Technologies and the Law of Armed Conflict, p.2. https://link.springer.com/book/10.1007/978-90-6704-933-7
32. Rohit Kalakuntla, Anvesh Babu Vanamalaand Ranjith Reddy Kolipyaka, Cyber Security, HOLISTICA – Journal of Business and Public Administration,Volume 10 (2019): Issue 2, pp. 115-128. DOI: https://doi.org/10.2478/hjbpa-2019-0019
33. Sharma, R. (2012). Study of Latest Emerging Trends on Cyber Security and its challenges to Society. International Journal of Scientific & Engineering Research, 3(6).
34. Sk Tahsin Hossain, Tan Yigitcanlar, Kien Nguyen, Yue Xu, Cybersecurity in local governments: A systematic review and framework of key challenges, Urban Governance, Volume 5, Issue 1, 2025, Pages 1-19. https://doi.org/10.1016/j.ugj.2024.12.010.
35. Tai, M.C. (2020). The Impact of Artificial Intelligence on Human Society and Bioethics. Tzu Chi Medical Journal, 32(4), 339-343. http://doi:10.4103/tcmj.tcmj_71_20
36. Tom Kirkham, The critical role of administrative controls in cybersecurity, https://tomkirkham.com/the-critical-role-of-administrative-controls-in-cybersecurity/
37. Tzavara, V., Vassiliadis, S. Tracing the evolution of cyber resilience: a historical and conceptual review. Int. J. Inf. Secur.23, 1695–1719 (2024). https://doi.org/10.1007/s10207-023-00811-x

المصادر الإلكترونية:

https://energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Shttps://icscert.uscert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdfector.pdf
https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security
https://www.dataguard.com/cyber-security/
https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/165893/VNK_2024_13.pdf
https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/75353/92016_Information_Security_Strategy_for_Finland.pdf?sequence=1&isAllowed=y
https://www.cnbcarabia.com/128373/2024/21/09
https://www.europarabct.com
https://www.cnbcarabia.com/128373/2024/21/09
https://privacyhq.com/news/world-data-privacy-rankings-countries/
https://www.almamlakatv.com/news/154844
https://ncsc.jo/Ar/List/Regulation_AR
https://my.gov.sa/ar/content/cybersecurity
https://nca.gov.sa/ar/#:~:text
https://blog.uniqkey.eu/eu-cybersecurity-regulations/
https://www.kiteworks.com/risk-compliance-glossary/eu-cybersecurity-act/
https://www.trade.gov/country-commercial-guides/eu-cyber-security
https://ec.europa.eu/digital-single-market/en/nis-cooperation-group
https://business.gov.nl/amendment/nis2-directive-protects-network-information-systems/
https://rm.coe.int/budapest-convention-in-arabic/1680739173
https://www.hostgator.com/help/article/how-to-generatedownload-a-full-backup
https://www.fortinet.com/resources/cyberglossary/what-is-web-security
Data Protection and Privacy Legislation Worldwide | UN Trade and Development (UNCTAD)
https://www. gchq.gov.uk/files/GCHQAIPaper.pdf