International Journal of Law Research and Studies (IJLRS)
Vol. (5), No. (2)
IJLRS
February 2026
المجلة الدولية للبحوث والدراسات القانونية
الإصدار (5)، العدد (2)

الأمن السيبراني كمرفق عام: دراسة في الأساس القانوني والتنظيم الإداري

نمير علي عبد الوهاب
جامعة الفرات الأوسط التقنية، العراق
Nameer.abdulwahab@atu.edu.iq

الملخص

أنتجت الثورة الرقمية تغييرات جذرية في طبيعة مهام الدولة وأدواتها، حيث لم تعد الخدمات العامة محصورة في المجالات التقليدية مثل الأمن والدفاع والصحة والتعليم، بل توسعت لتشمل الفضاء السيبراني الذي أصبح ساحة رئيسية للنشاط الإنساني والمؤسسي. فقد أصبحت الأنظمة المعلوماتية والبنى التحتية الرقمية تشكل العمود الفقري للإدارة العامة والاقتصاد الوطني والخدمات الأساسية، مما جعل حمايتها أمر حيوي لاستقرار الدولة وأمنها.

في هذا الإطار، يتجلى الأمن السيبراني كوظيفة عامة تتولى الدولة مسؤوليتها لحماية الفضاء الرقمي من المخاطر والتهديدات المتزايدة، سواء كانت هجمات إلكترونية، أو اختراقات للبيانات، أو تعطيل للخدمات الحيوية، وقد أدى ذلك إلى إعادة تقييم الطبيعة القانونية للأمن السيبراني، ومدى إمكانية اعتباره مرفق عام يخضع لقواعد القانون العام، حيث يتعين على الدولة تنظيمه وإدارته وضمان استمراريته، وتتجلى أهمية هذه الدراسة من خلال عدة جوانب رئيسية أهمها الدور الحيوي الذي يلعبه الأمن السيبراني في حماية المنشآت والخدمات العامة الرقمية، حداثة مفهوم الأمن السيبراني كمرفق عام، وما يثيره من قضايا قانونية وتنظيمية معقدة، الحاجة إلى إطار قانوني يحدد طبيعة الأمن السيبراني وحدود تدخل الدولة في هذا المجال، وتهدف هذه الدراسة إلى تحقيق مجموعة من الأهداف المهمة وأهمها توضيح مفهوم الأمن السيبراني، مسارات تطوره، ووظائفه الأساسية، تحليل الأسس القانونية التي تجعل من الأمن السيبراني مرفقًا عامًا، دراسة الخصائص المميزة للأمن السيبراني في سياق مبادئ المرافق العامة، تسليط الضوء على التنظيم الإداري للأمن السيبراني ودور الجهات المختصة في إدارته، تدور إشكالية الدراسة إلى أي مدى يمكن اعتبار الأمن السيبراني مرفقًا عامًا، وما هي الأسس القانونية والتنظيمية التي تحكمه، واعتمدت هذه الدراسة على المنهج التحليلي الوصفي من خلال تحليل النصوص القانونية والتنظيمية المتعلقة بالأمن السيبراني، وبيان خصائصه كمرفق عام. كما تم الاستعانة بالمنهج الاستنباطي لاستخلاص القواعد العامة من المبادئ القانونية الحاكمة للمرافق العامة وتطبيقها على مجال الأمن السيبراني، وفي ختام البحث توصلنا إلى مجموعة من النتائج مفادها يعتبر الأمن السيبراني مرفق عام حديث يرتبط مباشرة بحماية النظام الرقمي العام، يستند الأساس القانوني للأمن السيبراني إلى الدستور والتشريعات المتعلقة بالأمن الوطني وحماية البيانات، يتمتع الأمن السيبراني بخصائص المرفق العام من حيث الاستمرارية والعمومية وخضوعه لإشراف الدولة.

الكلمات المفتاحية: الأمن السيبراني، المرافق العامة، الأساس القانوني، التنظيم الإداري.

International Journal of Law Research and Studies (IJLRS)
Vol. (5), No. (2)
IJLRS
February 2026
المجلة الدولية للبحوث والدراسات القانونية
الإصدار (5)، العدد (2)

Cybersecurity as a public utility: A study in legal foundations and administrative organization

Nameer Ali Abdulwahab
Al-Furat Al-Awsat Technical University, Iraq
Nameer.abdulwahab@atu.edu.iq

Abstract

The digital revolution has brought about radical changes in the nature of the state's functions and tools. Public services are no longer confined to traditional areas such as security, defense, health, and education, but have expanded to include cyberspace, which has become a primary arena for human and institutional activity. Information systems and digital infrastructure have become the backbone of public administration, the national economy, and essential services, making their protection vital to the stability and security of the state.

In this context, cybersecurity emerges as a public function for which the state assumes responsibility to protect the digital space from increasing risks and threats, whether cyberattacks, data breaches, or disruptions to vital services. This has led to a reassessment of the legal nature of cybersecurity and the extent to which it can be considered a public utility subject to the rules of public law, requiring the state to regulate, manage, and ensure its continuity. The importance of this study is evident in several key aspects, most notably the vital role cybersecurity plays in protecting digital public facilities and services; the novelty of the concept of cybersecurity as a public utility and the complex legal and regulatory issues it raises; and the need for a legal framework that defines the nature of cybersecurity and the limits of state intervention in this field. This study aims to achieve a number of important objectives, the most important of which are: clarifying the concept of cybersecurity, its developmental paths, and its basic functions; analyzing the legal foundations that make cybersecurity a public utility; examining the distinctive characteristics of cybersecurity within the framework of public utility principles; and highlighting the administrative organization of cybersecurity and the role of competent authorities in its management. The central question of this study revolves around the extent to which cybersecurity can be considered a public utility, and what These are the legal and regulatory foundations that govern it. This study adopted a descriptive analytical approach by analyzing legal and regulatory texts related to cybersecurity and outlining its characteristics as a public utility. The deductive approach was also employed to derive general

rules from the legal principles governing public utilities and apply them to the field of cybersecurity. In conclusion, the research yielded a set of findings indicating that cybersecurity is a modern public utility directly linked to the protection of the public digital system. The legal basis for cybersecurity rests on the constitution and legislation related to national security and data protection. Cybersecurity possesses the characteristics of a public utility in terms of continuity, public nature, and state oversight.

Keywords: Cybersecurity, Public Utilities, Legal Basis, Administrative Regulation.

المقدمة

أنتجت الثورة الرقمية تغييرات جذرية في طبيعة مهام الدولة وأدواتها، حيث لم تعد الخدمات العامة محصورة في المجالات التقليدية مثل الأمن والدفاع والصحة والتعليم، بل توسعت لتشمل الفضاء السيبراني الذي أصبح ساحة رئيسية للنشاط الإنساني والمؤسسي. فقد أصبحت الأنظمة المعلوماتية والبنى التحتية الرقمية تشكل العمود الفقري للإدارة العامة والاقتصاد الوطني والخدمات الأساسية، مما جعل حمايتها أمر حيوي لاستقرار الدولة وأمنها.

في هذا الإطار، يتجلى الأمن السيبراني كوظيفة عامة تتولى الدولة مسؤوليتها لحماية الفضاء الرقمي من المخاطر والتهديدات المتزايدة، سواء كانت هجمات إلكترونية، أو اختراقات للبيانات، أو تعطيل للخدمات الحيوية، وقد أدى ذلك إلى إعادة تقييم الطبيعة القانونية للأمن السيبراني، ومدى إمكانية اعتباره مرفق عام يخضع لقواعد القانون العام، حيث يتعين على الدولة تنظيمه وإدارته وضمان استمراريته.

تزداد أهمية هذا الموضوع مع تزايد الاعتماد على الحكومة الإلكترونية، والتحول الرقمي، وارتفاع معدلات الجرائم السيبرانية العابرة للحدود، مما يستدعي دراسة معمقة للأسس القانونية للأمن السيبراني، وكذلك التنظيم الإداري الذي يدير هذا المجال، بما يحقق التوازن بين حماية الأمن القومي وصون الحقوق والحريات الرقمية للأفراد.

أهمية الدراسة

تتجلى أهمية هذه الدراسة من خلال عدة جوانب رئيسية، منها:

- الدور الحيوي الذي يلعبه الأمن السيبراني في حماية المنشآت والخدمات العامة الرقمية.
- حداثة مفهوم الأمن السيبراني كمرفق عام، وما يثيره من قضايا قانونية وتنظيمية معقدة.
- الحاجة إلى إطار قانوني يحدد طبيعة الأمن السيبراني وحدود تدخل الدولة في هذا المجال.
- تسليط الضوء على العلاقة بين التنظيم الإداري الفعّال وتحقيق الأمن الرقمي المستدام.

- إسهام الدراسة في إثراء الفقه القانوني العربي في مجالات القانون الرقمي والأمن السيبراني.

أهداف الدراسة

تهدف هذه الدراسة إلى تحقيق مجموعة من الأهداف المهمة، منها:

- توضيح مفهوم الأمن السيبراني، مسارات تطوره، ووظائفه الأساسية.
- تحليل الأسس القانونية التي تجعل من الأمن السيبراني مرفقًا عامًا.
- دراسة الخصائص المميزة للأمن السيبراني في سياق مبادئ المرافق العامة.
- تسليط الضوء على التنظيم الإداري للأمن السيبراني ودور الجهات المختصة في إدارته.
- استخلاص النتائج وتقديم توصيات تسهم في تعزيز الإطار القانوني والتنظيمي للأمن السيبراني.

إشكالية الدراسة

تدور إشكالية الدراسة حول السؤال المحوري التالي:

إلى أي مدى يمكن اعتبار الأمن السيبراني مرفقًا عامًا، وما هي الأسس القانونية والتنظيمية التي تحكمه؟

ويترتب على هذا السؤال عدد من الأسئلة الفرعية، منها:

- ما هو مفهوم الأمن السيبراني، وما هي الأسباب التي تدعو إلى اعتباره مرفق عام؟
- ما هو الأساس القانوني الذي تعتمد عليه الدولة في تنظيم الأمن السيبراني؟
- كيف يتم تنظيم الأمن السيبراني إدارياً، وما مدى فعالية هذا التنظيم؟
- كيف يمكن تحقيق التوازن بين متطلبات الأمن السيبراني وضمان الحقوق والحريات الرقمية؟

منهج الدراسة

اعتمدت هذه الدراسة على المنهج التحليلي الوصفي من خلال تحليل النصوص القانونية والتنظيمية المتعلقة بالأمن السيبراني، وبيان خصائصه كمرفق عام. كما تم الاستعانة بالمنهج الاستنباطي لاستخلاص القواعد العامة من المبادئ القانونية الحاكمة للمرافق العامة وتطبيقها على مجال الأمن السيبراني.

المبحث الأول: الأساس القانوني لاعتبار الأمن السيبراني مرفقا عاما

تُعتبر تكنولوجيا المعلومات والاتصالات واحدة من أبرز الإنجازات التي شهدها العالم في العصر الحديث. فقد تمكنت هذه التقنيات، في فترة زمنية قصيرة، من الانتشار والاندماج بعمق في مختلف مجالات الحياة السياسية والاقتصادية والاجتماعية، مما أثر بشكل كبير على أساليب الإدارة العامة. وتحديداً، فقد ساهمت في تحسين أداء المرافق العامة، التي تُعتبر مشروعات تهدف إلى تحقيق المنفعة العامة، حيث تحتفظ الحكومة بالسلطة العليا في إنشائها وإدارتها وإلغائها. وقد وصلت أهمية تقديم الخدمات العامة

للمواطنين إلى حد جعل بعض الفقهاء يعتبرون الدولة مجرد مجموعة من هذه المرافق العامة.[1] إذا كانت المرافق العامة، بمختلف أنواعها، تخضع لمجموعة من المبادئ التي تهدف أساسًا إلى تحسين أدائها في تقديم الخدمات، فإن هذه المبادئ ستظل ثابتة، بل قد تتعزز إذا تم تقديم هذه الخدمات عبر نظام إلكتروني يعتمد على استخدام التكنولوجيا المتطورة. من خلال مبدأ انتظام واستمرارية عمل المرافق العامة، يمكن للمواطنين الحصول على الخدمات في أي وقت. كما يسعى مبدأ المساواة إلى دعم أولئك الذين يواجهون صعوبة في الوصول إلى شبكة المعلومات، لضمان حصولهم على نفس الخدمات الإلكترونية مثل الآخرين. وأيضًا، يساهم مبدأ التكيف مع الظروف الجديدة في تسهيل الانتقال من النظام التقليدي إلى النظام الإلكتروني، مما يؤدي إلى سرعة ودقة أكبر في إنجاز الأعمال.

المطلب الأول: مفهوم الأمن السيبراني وأبعاده:

يعتبر مفهوم الأمن السيبراني مفهوم منطور وعصري، وضروري لمتطلبات العصر، فالأمن السيبراني هو نوع من الحماية لأجهزة الحاسوب والشبكات وتطبيقات البرمجيات والأنظمة الهامة من المخاطر والاختراقات المختلفة.

ومع التقدم التكنلوجي الذي تزامن مع التطور العصري لشبكات المعلومات والأنترنت أصبح الآن السيبراني ضرورة لا غنى عنها لحماية البيانات والمعلومات الحيوية للدول والأفراد، فقد أسهم الأمن السيبراني بدور محوري في تأمين الشبكات المعلوماتية من أي اختراق أو تهديد يمسها، أي أن الأمن السيبراني يلعب دوراً حيوياً وواضحاً في حماية فضاء المعلومات الخاص بالدول والمنظمات الدولية، مما يجعله عنصراً أساسياً في السياسة العالمية[2].

فالأمن السيبراني يؤثر بفعالية من خلال السياسات الدولية التي تعتمدها الدول لحماية بياناتها وأنظمتها، وضمان أمنها المعلوماتي من محاولات الاختراق والهجمات السيبرانية الي قد تنفذها دول معادية فيما بينها، فمن دون وجود تدابير قوية للأمن السيبراني قد تتعرض الدول الحروب سيبرانية تهدد استقرارها وتثنيها عن فرض قوتها وتأثيرها على الساحة السياسية العالمية[3].

الفرع الأول: تعريف الأمن السيبراني ونشأته وتطوره:

يعرف الأمن السيبراني على أنه عبارة عن مجموعة من الأدوات المتطورة تقنياً وإدارياً وتنظيمياً، والتي يتم استخدامها لمنع الاستخدام الغير مرخص ومنع أي تدابير مسيئة الاستغلال المعلومات والبيانات

[1] أونيسي ليندة، المبادئ الضابطة للمرفق العام الإلكتروني، جامعة عباس الغرور خنشلة، مجلة الحقوق والعلوم الإنسانية، المجلد 14 / العدد 01، الجزائر،2021، ص204

[2] زينب عباس راضي، فاعلية الأمن السيبراني في السياسة العالمية (المفهوم والتدابير الأمنية للدول)، جامعة البيان كلية القانون والعلوم السياسية، مجلة أشور للعلوم القانونية والسياسية، المجلد الثاني - العدد (الأول)، العراق، ٢٠٢٥، ص ٥٥٠

[3] المرجع السابق نفسه، ص٥٥٠.

الإلكترونية وتعزيز الحماية لهذه البيانات واتخاذ جميع التدابير الضرورية الممكنة لحماية مستخدمي الفضاء السيبراني[4].

فالأمن السيبراني صار مطلباً أساسياً لكل الدول بلا استثناء لأنه يتعلق بالوقاية من المخاطر المحتملة عبر مصادر خارجية من خلال الأنترنت، فهو بمثابة الحماية للحواسيب المكتبية أو المحمولة من أي نوع من الهجمات والاختراقات التي تحدث عن طريق السيرفرات والحواسيب الأخرى، باختصار الأمن السيبراني يعمل على ضمان عدم السماح لأي شخص غير مصرح له بالولوج والوصول الى المعلومات[5].

فالأمن السيبراني يمكن تعريفه بأنه ممارسة الدفاع عن أجهزة الحواسيب والخوادم والأنظمة الإلكترونية والشبكات والبيانات المهمة من أي اختراق أو هجمة خبيثة، فالأمن السيبراني يُعرف باسم أمان تكنلوجيا المعلومات، فهو مصطلح يشمل العديد من مجالات الحماية والوقاية[6].

ويعرف الأمن السيبراني بأنه تلك التدابير التي تتخذها وتقوم بها الدول من أجل الهجوم على أنظمة معلومات العدو بهدف الحاق الضرر بها [7].

ويعرف كذلك بأنه " أي هجوم يحدث بشكل مباشر عبر شكة الكمبيوتر حيث يكون النظام الذي يتم مهاجمته عبارة عن شبكة أنترنت أو نظام كمبيوتر أو كلاهما[8] .

ويمكن الاستنتاج من التعريفات السالفة الذكريان الأمن السيبراني هو منظومة متقدمة من عدة أدوات إلكترونية وأنظمة وبرمجيات غايتها الأساس أما أيقاع أذى بالخصم ومهاجمته أو حماية بيانات ومعلومات الدولة المطورة للنظام السيبراني.

الفرع الثاني: أبعاد الأمن السيبراني:

للأمن السيبراني أبعاد عديدة وهذه الأبعاد توضح آلية عمل الأمن السيبراني وكذلك توضح هذه الأبعاد الهدف من الأمن السيبراني والهدف من وجوده في مخططات الدول، حيث يمثل الأمن السيبراني الوسيلة التكنلوجية المتطورة التي تقوم الدول بتطويرها وفق أبعاد مختلفة ومن أهم هذه الأبعاد هي الأبعاد الاجتماعية والقانونية والسياسية، وهذا ما سيتم توضيحه كالآتي:

---

[4] ربيعي حسين وسمر محمود الحروب السيبرانية: المخاطر واستراتيجيات تحقيق الأمن السيبراني الدولي والداخلي المجلة الجزائرية للأمن الإنساني، المجلد (٧)، العدد (٢)، ٢٠٢٢، ص ١٧٨

[5] فارس محمد العمارات وإبراهيم الحمامصة الأمن السيبراني المفهوم تحديات العصر) ، دار الخليج للنشر والتوزيع ط١، ٢٠٢٢، ص ١١.

[6] عبد الرحمن على اللقاني دور الأمن السيبراني في تعزيز أمن المعلومات المالية الإلكترونية، دار اليازوري العلمية للنشر والتوزيع، الأردن، ط١ ، ٢٠٢٢، ص ١٦٢.

[7] فاطمة علي أبراهيم رحاب يوسف وليد محمود السيد الأمن السيبراني والنظافة الرقمية، المجلة المصرية لعلوم المعلومات، مجلد (٩)، العدد (٢)، ٢٠٢٢، ص ٤٠١.

[8] المرجع السابق نفسه، ص ٤٠١.

1. الأبعاد الاجتماعية للأمن السيبراني:

تقوم شبكات التواصل الاجتماعي يفتح المجال للجميع للتعبير عن آرائهم السياسية وعرض طموحاتهم الاجتماعية، وأيضاً تمثل هذه الشبكات الوسيلة العصرية لتطوير المجتمع ويكون ذلك بانفتاح مجتمع ما على المجتمعات الأخرى مما يخلق الحاجة لتبادل الخبرات وتكوين أسس للتعاون[9].

فالتقدم التكنولوجي والعولمة أدى إلى أضعاف البنية التحتية، مما أصبحت هدفاً سهلاً لأي هجمة إرهابية، فالبلدان في الوقت الحاضر باتت تواجه مخاطر جمة ومن هذه المخاطر قيام الأعداء باستغلال مناطق الضعف التي تعاني منها أنظمة المعلومات الحساسة والدقيقة فالهدف الأساسي لأي عدو هو تعطيل البنية التحتية والموارد المهمة من أجل أضعاف وتهديد الأمن القومي للدولة المستهدفة [10].

2. الأبعاد السياسية للأمن السيبراني:

حثت الحروب المتتالية والتطورات السياسية التي جاءت بالتزامن مع التطورات الإلكترونية والثورة المعلوماتية اللجوء إلى تكنلوجيا الأمن السيبراني، وذلك للاستفادة منه في عمليات التجسس وسرقة المعلومات عن طريق القرصنة [11].

فعلى سبيل المثال في عام ٢٠٠١ تم اختراق مناطق عسكرية صناعية في أيران وكانت هذه المناطق مناطق حساسة عسكرياً سياسياً حيث تم اختراقها بفيروس (stuxne) ، وقد تغلغل هذا الفيروس الحواسيب الخاصة بمعامل ومصانع تخصيب اليورانيوم وقد أشارت أيران أن كل من الولايات المتحدة وإسرائيل وراء هذا الموقف والقرصنة الإلكترونية، وقد غير هذا الحادث مفهوم الأمن التقليدي لأنه شكل تهديد قوي لحدود الدول[12].

فكل دولة من حقها حماية نظامها السياسي ووجودها ومصالحها الاقتصادية في وقت أصبحت التقنيات الإلكترونية تؤثر في موازين القوى ليس على مستوى الدول فقط، بل حتى داخل المجتمع الواحد نفسه حيث أصبح من الممكن لأي فرد أن يكون لاعب سياسي في اللعبة السياسية وأصبح بإمكان أي فرد أن يضطلع على المبررات والقرارات السياسية التي تقوم حكومته باتخاذها عبر وسائل الأنترنت الحديثة المنتشرة ومقابل هذا يقوم العاملون في الأمور السياسية بالاستفادة من تقنيات الأنترنت الحديثة للترويج لسياساتهم على مستوى العالم [13].

---

[9] أدريس عطية مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، مجلة مصداقية، المجلد (١)، العدد (١)، ٢٠١٩، ص ١٠٥.
[10] إسلام فوزي، الأمن السيبراني (الأبعاد الاجتماعية والقانونية تحليل سوسيولوجي)، المجلة الاجتماعية القومية، المجلد (٥٦)، العدد (٢)، ٢٠١٩، ص ١٠٨
[11] سلمى عبد الرحيم عبد الحسن طبيعة العلاقة بين الأمن السيبراني والنمو الاقتصادي الرقمي في دول العالم، على الموقع الإلكتروني، تاريخ الزيارة ١٧ /٢٠٢٥/١ https://iaiphss.us
[12] المصدر نفسه على الموقع الإلكتروني https://iaiphss.us
[13] منى الأشقر جبور، الأمن السيبراني، التحديات ومستلزمات المواجهة، جامعة الدول العربية، المركز العربي للبحوث القانونية والفضائية اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني، بيروت ٢٠١٢٠، ص ٦.

3. الأبعاد القانونية للأمن السيبراني:

أن البعد القانوني للأمن السيبراني يتضح في غياب الإطار التشريعي والتنظيمي للتعامل مع الأعمال القانونية وغير القانونية منها والتي تتم في الفضاء السيبراني فأي نشاط سواء كان نشاط اقتصادي أو تجاري يتطلب تحديد للحقوق والواجبات للمستخدمين بشكل قانوني ، فمستخدمي التقنيات الإلكترونية عبر الفضاء السيبراني هم بحاجة قصوى إلى أطار قانوني يؤمن استخدامهم لهذه التقنيات [14]، فالنشاطات المؤسساتية والحكومية في الفضاء السيبراني يترتب عليه نتائج قانونية تستدعي أيجاد قواعد خاصة لفض النزاعات التي تنشأ عن هذه النشاطات لذا لابد من مراعاة التطورات التي جاءت بالتزامن مع ظهور التكنلوجيا والمعلومات، فبالإضافة الى حق الأنسان وحرياته المعترف بها في الدساتير أسبغت حقوق أخرى مثل حق النفاذ إلى الشبكة العالمية للمعلومات وتوسعت مفاهيم جديدة أخرى مثل أسلوب الممارسات الحديثة باستخدام التقنيات المعلوماتية وحق تكوين المدونات الإلكترونية وحق حماية ملكية البرامج المعلومات على الأنترنت[15].

4. الأبعاد الاقتصادية:

أن الأمن السيبراني مرتبط بشكل وثيق بالحفاظ على المصالح الاقتصادية لجميع الدول، وهذا الترابط الوثيق بين الاقتصاد والأمن السيبراني بأن أغلب الدول تعتمد في تعزيز اقتصادها وتطويره على الفضاء السيبراني، والذي يقوم على الأبداع والتطوير فالفضاء السيبراني أصبح مجالاً للمعاملات التجارية والمالية والصناعية والاستيراد والتصدير وكل المعاملات البنكية، ومن هنا يكمن البعد الاقتصادي للأمن السيبراني بتعزيز الأمن السيبراني للبنى التحتية الاقتصادية وتوفير كافة سبل حماية للملكية الفكرية الخاصة بالبيانات التجارية، وهذا ما يبرر دور الأمن السيبراني في حماية الاقتصاد الخاص بالدول وحماية مصلحة المستهلك[16].

المطلب الثاني: الإطار القانوني المنظم للأمن السيبراني:

في السنوات الأخيرة، أصبحت المؤسسات تعتمد بشكل متزايد على تكنولوجيا المعلومات في إدارة أعمالها، حيث تشكل شبكات الاتصال بيئة تتدفق فيها البيانات وتحتوي على خزائن المعلومات. لذا، فإن هذه الشبكات تحتاج إلى حماية تحافظ على سلامة محتوياتها وتضمن استمرارية عملها. ومع تزايد المخاطر التي تهدد سلامة البيانات المتدفقة عبر الشبكات أو المخزنة في خزائنها، وتعدد التهديدات التي تواجه استقرار وأمن تلك الشبكات مثل الفيروسات والبرامج الضارة ومحاولات الاختراق بهدف سرقة المعلومات أو التخريب، تبرز أهمية الحماية المستمرة. يتطلب الأمر تثبيت أجهزة وبرامج الحماية عند بوابات

[14] منى الأشقر جبور، السيبرانية هاجس العصر، جامعة الدول العربية المركز العربي للبحوث القانونية والقضائية، ط ١، ٢٠١٦، ص ٢٩.
[15] خالد وليد محمود، الفضاء السيبراني وتحولات القوة في العلاقات الدولية المركز العربي للنشر والتوزيع، ط1، ٢٠٢٥، ص ٢٩٣
[16] منى الأشقر جبور، مرجع سابق، ص٣١.

الشبكات المحلية وداخلها، وإدارة هذه الأدوات من منظور أمني، مع معالجة الثغرات بشكل دوري لتقليل فرص القراصنة والمنافسين والأعداء في اختراق أو سرقة أي بيانات من شبكات المعلومات.[17] .

نتيجةً لذلك، اتجهت العديد من الدول نحو وضع استراتيجيات وطنية شاملة تهدف إلى تعزيز أمن المعلومات في مجال الأمن السيبراني. يُعتبر أمن المعلومات جزءًا لا يتجزأ من مفهوم الأمن الوطني العام، الذي يشمل جميع المؤسسات والأفراد. وقد أدركت العديد من الدول أن التطورات السريعة في التكنولوجيا تطرح تهديدات خطيرة لأمن الوطن والمواطن. لذا، أصبح من الضروري اتخاذ خطوات فعالة لضمان أمن المعلومات، وذلك من خلال استراتيجيات متكاملة في مجال الأمن السيبراني لحماية الأمن الوطني بمفهومه الواسع. يعتمد الأمن السيبراني على مجموعة متنوعة من الوسائل القانونية والتقنية لمواجهة الاستخدام غير المشروع للإنترنت، بهدف حماية نظم المعلومات ووسائل الاتصالات، وبالتالي حماية الوطن والمواطنين والمؤسسات من مخاطر الأمن السيبراني.[18].

الفرع الأول: التعاون لتعزيز الأمن وحماية وتطوير البنية الإدارية:

إن الارتباط الوثيق بين البنى التحتية لتقنيات المعلومات والاتصالات، مع تزايد الاعتماد عليها من قبل الدول والأفراد والمؤسسات، يُعتبر دافعًا رئيسيًا لزيادة المخاطر. وهذا يستدعي اتخاذ تدابير وإجراءات تضمن إدارة فعّالة للمخاطر التقنية والسيبرانية، تعتمد على منهجيات تتناسب مع الأبعاد الواسعة لهذا الارتباط. وهذا الأمر ينطبق على جميع الدول، حيث يتعين على البلدان النامية، على سبيل المثال، أن تولي اهتمامًا خاصًا لأمنها السيبراني، ليس فقط لحماية نفسها، بل أيضًا لتفادي أن تصبح مصدرًا للخطر في الفضاء السيبراني.[19].

اولاً- التعاون لتعزيز الأمن:

في هذا السياق، يتوجب علينا إنشاء إطار تشريعي وتنظيمي شامل يدعم ويعزز مبادرات التعاون. فاستدامة عمل تقنيات المعلومات والاتصالات، وعلى رأسها الإنترنت، بالإضافة إلى استقرار الأمن السيبراني، تتطلب وضع سياسات فعالة لمعالجة الثغرات الأمنية والتصدي للمخاطر وتقليل آثار الجرائم. لذا، من الضروري تعزيز الجهود الرامية إلى وضع معايير ومقاييس دولية، وكذلك دعم اعتماد الأطر القانونية والتنظيمية،

[17] فايز بن عبد الله الشهري، استخدامات شبكة الإنترنت في مجال الإعلام الأمني العربي دراسة وصفية على عينة من المواقع الأمنية العربية على شبكة الإنترنت مجلة البحوث الأمنية، الرياض كلية الملك فهد الأمنية، مركز الدراسات.2011، ص١٣

[18] سامي الشواء، الغش المعلوماتي الظاهرة إجرامية مستحدثة، بحث في مؤتمر الجمعية المصرية القانون الجنائي، القاهرة، 2009، 28

[19] Understanding Cybercrime: A Guide for Developing Countries, at 72, International Telecommunication Union, April 2009, www.itu.int/TTU-D/cyb/cybersecurity/docs/itu-understandingSybercrime-guide.pdf (hereinafter "Understanding")

والاستفادة من أفضل الممارسات والتجارب الناجحة التي تعزز الثقة في الأمن السيبراني، مما يساهم في خلق بيئة ملائمة لنمو الأنشطة الاقتصادية والاجتماعية في هذا المجال.[20].

في هذا السياق، يتوجب علينا الابتعاد عن السياسات التي تتناقض مع طبيعة الإنترنت المفتوح وإمكاناته التي تشكل منصة للإبداع والنمو الاقتصادي والاجتماعي. ينبغي أن لا تتحول هذه السياسات إلى عوائق تعرقل تدفق المعلومات بحرية والوصول إليها، تحت ذريعة تحقيق الأمن والحماية. بل يجب أن تعمل سياسات الأمن على تعزيز المبادرات الفردية والجماعية التي تسعى لتحقيق الأمن والحماية بشكل فعّال.[21].

إن نجاح استراتيجيات الحماية والأمن السيبراني يتطلب تواصلاً وتكاملاً بين السياسات الأمنية واستراتيجياتها، كما ينبغي أن تكون هذه السياسات متاحة للجمهور، ليس فقط على الصعيد الوطني، بل أيضاً على المستويين الإقليمي والدولي. بالإضافة إلى ذلك، هناك حاجة ملحة لمشاركة جميع الأطراف في تطوير الحلول، بحيث تكون هذه الحلول فعالة وتؤسس لتفاهم اجتماعي وسياسي، مما يعزز فرص نجاحها وكفاءتها. كما يجب على صانعي القرار أن يأخذوا بعين الاعتبار آراء القطاعات المهنية، والخبراء، والمجتمع المدني، وغيرهم، عند صياغة التشريعات ووضع الأطر التنظيمية.[22].

ثانياً- تطوير البنية الإدارية:

تتأصل الثقة في مجال الأمن السيبراني في قدرة الجهات المعنية على التحكم في الأمور بفعالية، كما تعتمد على وضوح المسؤوليات والمرجعيات التي تتولى حماية الحقوق وإقرارها. بالإضافة إلى ذلك، تلعب القدرة على الردع وملاحقة أي عمل إجرامي أو تصرف قد يهدد استقرار المعاملات والأمن السيبراني دورًا حيويًا. ولتحقيق مكافحة فعالة، يتطلب الأمر وجود أجهزة متخصصة وعناصر تتمتع بالكفاءة والقدرة على فهم جميع جوانب إدارة أنظمة المعلومات وطرق معالجة البيانات والحقوق المرتبطة بها.[23].

تُعرف البنية التحتية بأنها مجموعة من الوسائل والقدرات التي يتم تنسيقها عادةً بواسطة هيئة مركزية للمعلومات وفقًا لما يحدده القانون الدولي. بالإضافة إلى ذلك، هناك حاجة ملحة لوجود جهة مرجعية تشرف على توثيق الحقوق، وتضع قواعد راسخة تعزز الثقة بين العاملين في مجال معالجة المعلومات

[20] عبد الرزاق سندالي، التشريع المغربي في مجال الجرائم المعلوماتية، ضمن أعمال الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر 19-20 نيسان المملكة المغربية،2017، ص٣٣.

[21] عبود السراج، مفهوم جرائم المعلوماتية، واقع وآفاق، بحث مقدم إلى المؤتمر الإقليمي الأول لمكافحة جرائم المعلوماتية الذي نظمته الجامعة الأردنية والتحد المحامين العرب خلال الفترة 18-19 كانون الثاني عام 2013، ص٥٣.

[22] Trust in the Information Society: A Report of the Advisory Board RISEPTIS, bup://www.think Inmateu: David-Olivier Jaquet-Chiffelle, ed., Identity Revolution: Multidisciplinary Perspectives, FIDIS. May 2009, http://www.fislis.net/resources/identity-evolution

[23] واثبة السعدي، الحماية الجنائية لبرامج الحاسوب، بحث مقدم إلى مؤتمر القانون والحاسوب المنعقد في جامعة اليرموك -اربد بتاريخ 12-14 تموز ،2019، ص 6.

والأنظمة المرتبطة بها، وكذلك الحقوق الناتجة عنها، في سجلات خاصة تتمتع بقيود موثوقة.[24].

ثالثاً- تعزيز وحماية الانسياب العالمي الحر للمعلومات:

يعتمد اقتصاد الإنترنت، ونموه بشكل أساسي، على حرية تدفق المعلومات. وفي حين يتوجب على الدول المختلفة وضع سياسات تعزز هذا التدفق وتدعمه، فإنها مطالبة أيضًا بتوفير إطار قانوني يحمي حقوق الخصوصية والبيانات الشخصية، بالإضافة إلى الحريات الفردية، خاصةً بالنسبة لبعض الفئات العمرية مثل الأطفال والشباب، وحقوق الملكية الفكرية. لذا، تبرز أهمية التركيز على الأمن السيبراني والعمل على تأسيس قواعد راسخة له. يرتبط تدفق المعلومات بالطبيعة المفتوحة للإنترنت، التي تعتمد بدورها على معايير ومقاييس تقنية عالمية. كما تشمل هذه السياسات المنافسة، والسوق المفتوح، والتنوع، والخدمات العابرة للحدود، مما يساهم في توفير خدمات بأسعار معقولة، ويتيح الوصول إلى الإنترنت للجميع.[25].

حماية الخصوصية: تُعد حماية الحق في الخصوصية من الركائز الأساسية لتعزيز الثقة في مجال الأمن السيبراني، وللاستفادة من إمكانيات تقنيات المعلومات والاتصالات على الأصعدة الاجتماعية والاقتصادية والثقافية. فالتحديات الراهنة المتعلقة بطرق معالجة البيانات وجمعها واستخدامها واستثمارها، قد تترك آثارًا سلبية على تجربة استخدام الإنترنت، وعلى مجموعة التقنيات المرتبطة بها، سواء من الناحية التجارية أو الاجتماعية أو الحكومية. لذا، يجب أن يتيح الإطار التشريعي والتنظيمي للمستخدمين فهم ما يحدث من ممارسات تتعلق ببياناتهم الشخصية والمعلومات التي يشاركونها عبر الإنترنت. كما ينبغي تمكينهم من ممارسة حقوقهم في إدارة تلك البيانات، بما يضمن لهم الاطمئنان بشأن الحفاظ على خصوصيتهم، وحقوقهم الفكرية، والصناعية، والأدبية. وفي هذا السياق، يمكن للتشريعات أن تستلهم من القواعد الدولية والمبادئ التي تم إقرارها عالميًا، كجزء من الأسس الضرورية للحفاظ على نمو واستقرار الأمن السيبراني[26].

الفرع الثاني: التنظيم الإداري والتشريعي لمتابعة شؤون الأمن السيبراني:

أولاً - الهيكل الإداري لمتابعة قضايا الأمن السيبراني:

تقوم كل دولة بتأسيس مجلس وطني مستقل يختص بالسلامة والأمن في الفضاء السيبراني، ليكون المرجع الأسمى في قضايا الحماية والأمان ضمن هذا المجال. وتتمثل مهامه في... [27]:

[24] محمد أمين البشري، التحقيق في الجرائم المستحدثة الرياض جامعة نايف العربية للعلوم الأمنية، مركز الدراسات والبحوث،2014، ص٢٥.
[25] واثبة السعدي، مرجع سابق ص 7.
[26] محمد أمين البشري، مرجع سابق، ص٢٦.
[27] المركز العربي للبحوث القانونية والقضائية، مجلس وزراء العدل العرب، جامعة الدول العربية، الاتفاقية العربية الحماية الفضاء السيبراني بين الواقع والطموح، 2018.

1. صياغة خطة شاملة للأمن السيبراني، ووضع السياسات اللازمة لتنفيذها.
2. الحصول على موافقة جميع الإدارات الحكومية على الاستراتيجية والسياسات المعتمدة، لضمان تنفيذها الفعّال.
3. تحديد أولويات الأمن والمبادرات الوطنية الحيوية.
4. تنسيق الجهود والمبادرات على الصعيد الوطني لتحقيق التكامل.
5. تحديد الجهات المعنية المسؤولة عن تعزيز الأمن والسلامة وبناء الثقة في الاقتصاد الرقمي.
6. تعزيز التعاون مع القطاع الخاص لمعالجة قضايا الأمن والسلامة في الفضاء السيبراني.
7. التعاون مع مختلف الأجهزة الأمنية، مثل المخابرات والأمن العام والأمن الداخلي والشرطة القضائية والجهات القضائية، لوضع معايير موحدة لردع الجرائم وملاحقتها.
8. التعاون مع الهيئات المسؤولة عن تطبيق القانون على المستويات الوطنية والإقليمية والدولية.
9. مراقبة أنظمة المعلومات الحكومية والبنية التحتية للاتصالات لضمان سلامتها.
10. الإشراف على تطوير أنظمة المعلومات المتعلقة بالهوية الرقمية وإدارتها، وتقديم التوصيات اللازمة.
11. تطوير وتنسيق الجهود الخاصة ببرامج التأهيل والتدريب وبناء القدرات في مجال الأمن والسلامة السيبرانية، بالتعاون مع الجهات الوطنية والإقليمية والعربية والدولية المعنية.[28].

يمكن للدولة أن تؤسس هيئة وطنية مستقلة رفيعة المستوى تعنى بالسلامة والأمن في الفضاء السيبراني، تتولى مسؤولية تنفيذ الاستراتيجيات والسياسات المتعلقة بالأمن والسلامة، وتنسيق الجهود الوطنية في هذا المجال. ستقوم هذه الهيئة بإدارة وتنظيم كافة الأنشطة ذات الصلة. [29] :

1. اتخاذ الإجراءات اللازمة لضمان تطبيق التدابير التي يحددها ويوصي بها المجلس الوطني.
2. متابعة مدى التزام الجهات الحكومية والخاصة بالتوصيات الصادرة عن المجلس الوطني.
3. الإشراف على تقييم مستوى السلامة والأمن، وإجراء عمليات التدقيق والمراجعة.
4. تقديم الدعم للمجلس الوطني في تنفيذ مهامه.
5. المساهمة في وضع القواعد واعتماد المعايير الدولية التي تضمن أمان الأنظمة المعلوماتية والمعلومات، وسلامة الاقتصاد الرقمي، والمصادقة على التوقيع الإلكتروني.

[28] المرجع السابق نفسه.
[29] عمر محمد يونس، الجرائم الناشئة عن استخدام الإنترنت ط1، دار النهضة العربية، القاهرة، 2015، ص٣٤.

6. مراقبة العقود التي تبرمها الدولة مع مقدمي الخدمات وجميع المستثمرين في مجال تقنيات المعلومات والاتصالات، الذين يقدمون خدمات تتعلق باستخدام هذه التقنيات.[30].

ثانياً- الإطار التشريعي لحماية الأمن السيبراني:

تلتزم كل دولة من الدول المتعاقدة بوضع أطر تشريعية وتنظيمية تستند إلى النصوص الدولية والاتفاقيات والبروتوكولات المتعلقة بحماية الفضاء السيبراني. ويشمل ذلك مكافحة الجريمة السيبرانية وتعزيز التعاون في الجرائم العابرة للحدود، بالإضافة إلى اعتماد المعايير والمقاييس الدولية اللازمة لحماية البنية التحتية للاتصالات وأنظمة المعلومات.[31].

تتعهد الدول الأعضاء بوضع القوانين المناسبة لتعزيز المشاركة الفعالة والآمنة في مجتمع المعلومات، واستغلال الفرص التي يقدمها مجتمع المعرفة، بما يساهم في تحقيق النمو والتطور، خاصة في المجالات المتعلقة بـ[32]:

1. تنظيم التجارة الإلكترونية.
2. حماية الخصوصية والحق في التعبير.
3. ضمان الحق في النفاذ إلى الشبكة العالمية للمعلومات.
4. حماية البيانات الشخصية، والبيانات الحساسة.
5. تنظيم المحتوى.
6. حماية حقوق الملكية الفكرية.
7. حماية الأطفال على الإنترنت
8. تنظيم المعاملات الإلكترونية.
9. تنظيم المسؤوليات، وخدمات الحوسبة السحابية.
10. إقرار قواعد تجريم موضوعية.
11. وضع أصول ملاحقة، ومتابعة، وتنفيذ خاصة بالجرائم السيبرانية.
12. إقرار آليات تعاون وطنية، وإقليمية ودولية.
13. إقرار الإطار التشريعي الملائم، للتعاون بين القطاعين العام والخاص، في مواجهة الجرائم السيبرانية.

[30] عبد العزيز اليوسف، التقنية في الجرائم المستحدثة بحث ضمن كتاب الظواهر الإجرامية المستحدثة وسبل مواجهتها، منشورات أكاديمية نايف للعلوم الأمنية، الرياض، 2015، ص٥٣.
[31] المركز العربي للبحوث القانونية والقضائية، مجلس وزراء العدل العرب، جامعة الدول العربية، الثالثة والعشرون من الاتفاقية العربية الحماية الفضاء السيبراني بين الواقع والطموح، 2018، ص٣١
[32] المركز العربي للبحوث القانونية والقضائية، مجلس وزراء العدل العرب، جامعة الدول العربية، المادة الثانية والعشرون من الاتفاقية العربية لحماية الفضاء السيبراني، 2018، ص٣٤.

تلتزم كل دولة من الدول المتعاقدة بضمان توافق الإجراءات والقوانين التي تتبناها في مكافحة الجريمة السيبرانية مع أفضل الممارسات الدولية السائدة في هذا المجال. ويجب أن تأخذ هذه الدول في اعتبارها الحد الأدنى المعتمد في الدول التي تمتلك أدوات تشريعية وتنظيمية، مما يتيح إمكانية تحقيق التناغم بين تشريعات الدول الأعضاء.[33].

تعتمد الدول الأعضاء، فيما يتعلق بالجرائم العابرة للحدود على مبدأ توحيد القواعد القانونية الخاصة بتجريم الأعمال الخاصة بالجرائم السيبرانية، وأصول الملاحقة والتنفيذ الخاصة بها بحيث تعتمد كل دولة القواعد القانونية التي تسمح لها باعتماد مبدأ التجريم المزدوج، وذلك بهدف إنجاح التعاون، وتفعيله[34].

المبحث الثاني: التنظيم الإداري لمرفق الأمن السيبراني

تُعتبر الحكومة الإلكترونية نهجًا حديثًا ومتقدمًا في إدارة المرافق العامة، ولكن يجب أن نوضح أن هذا لا يعني أن جميع الخدمات العامة يمكن تقديمها بالكامل عبر الإنترنت، حيث توجد العديد من الخدمات التي لا تسمح طبيعتها بتقديمها إلكترونيًا.

ومع ذلك، يمكن القول إن جميع المرافق العامة تستطيع الاستفادة من الأساليب الإلكترونية في إدارة الجوانب الإدارية، مثل استخدام الوسائط الإلكترونية لتحديد مواعيد حضور وانصراف الموظفين، وإدارة الإجازات والرواتب. كما يمكن استبدال البريد التقليدي بالبريد الإلكتروني. بالإضافة إلى ذلك، يمكن لبعض المرافق التي تتقاضى رسومًا من المواطنين مقابل خدماتها اعتماد طرق الدفع الإلكتروني لتسهيل العملية.[35].

تتعدد الأمثلة على هذا النوع من المرافق التي لا تتناسب طبيعة خدماتها مع تقديمها عبر الوسائل الإلكترونية. ومن أبرزها مرفق الأمن، الذي يتحمل مسؤولية الحفاظ على الأمن الداخلي من خلال أجهزة الأمن والشرطة. يتضح أن طبيعة الخدمة المتمثلة في حماية المواطنين لا تتيح إمكانية تقديمها إلكترونياً. ومع ذلك، يمكن استخدام الأساليب الإلكترونية في تنفيذ الجوانب أو الإجراءات الإدارية المرتبطة بهذه الخدمات.[36].

---

[33] المركز العربي للبحوث القانونية والقضائية، مجلس وزراء العدل العرب، جامعة الدول العربية المادة الثامنة والعشرون من الاتفاقية العربية الحماية الفضاء السيبراني، 2018، ص٣٥.

[34] المركز العربي للبحوث القانونية والقضائية، مجلس وزراء العدل العرب، جامعة الدول العربية المادة التاسعة والعشرون من الاتفاقية العربية الحماية الفضاء السيبراني، 2018، ص ٣٦.

[35] فياض عبد الله، رجاء كاظم حيدر عبود التعليم الإلكتروني والتعليم التقليدي دراسة تحليلية مقارنة بحث منشور في مجلة كلية بغداد للعلوم الاقتصادية الجامعة، عدد ١٩، ٢٠٠٩، ص ٢٧٦.

[36] جان سيريل، واقع وأفاق التعليم عن بعد وأثره في التعليم في العراق، بحث منشور في مجلة كلية العلوم الاقتصادية الجامعة، العدد ٢٣، ٢٠١٠، ص ٣٢٦

المطلب الأول: الوسائل الإدارية الإلكترونية:

تتبع الإدارة العامة عدداً من الوسائل التي تستطيع من خلالها الاضطلاع بالمهام المنوطة بموظفيها، وتلبية احتياجات الجمهور من الخدمات العامة. وتدور إعمال الإدارة وتصرفاتها القانونية إلى نوعين رئيسين هما:

أولاً: الإعمال التي تصدر عن الإدارة بإرادتها المنفردة ومثالها القرارات الإدارية.

ثانياً: الإعمال التي تجريها الإدارة بالاتفاق مع إرادة طرف آخر مثالها العقد الإداري.

ومع تطبيق نظام الحكومة الإلكترونية سوف يستلزم إعادة النظر في بعض جوانب الإعمال القانونية للإدارة التي من الطبيعي إن يطرأ عليها تغيير وتحول المواكبة هذا النظام ومسايرة متطلبات تطبيقه[37].

الفرع الأول: القرار الإداري الإلكتروني:

يراد بالقرار الإداري إفصاح الجهة الإدارية المختصة بالشكل الذي يتطلبه القانون عن إرادتها الملزمة بما لها من سلطة بمقتضى القوانين واللوائح لإحداث أثر قانوني معين يكون ممكناً وجائزاً قانوناً لتحقيق الصالح العام[38].

ويعرفه البعض الآخر بأنه عمل قانوني صادر بالإرادة المنفردة والملزمة لأحدى الجهات الإدارية في الدولة لإحداث تغيير في الأوضاع القانونية القائمة أما بإنشاء مركز قانوني جديد أو تعديل مركز قانوني قائم أو إلغائه[39] .

ومن هذه التعريفات يتبين أن للقرار الإداري خمسة أركان لابد من توافرها خلال إصداره والتي تتمثل بالآتي[40]:

ركن الاختصاص وهو السلطة أو الصلاحية القانونية التي يتمتع بها متخذ القرار في إصدار قراره من الناحية النوعية والمكانية والزمانية.

وبذلك فالقرار الإداري كي يكون صحيحاً ومشروعاً لابد من إن يصدر ممن يملك الصلاحية بإصداره من أعضاء السلطة الإدارية، وبخلافه يكون مشوباً بعيب عدم الاختصاص – وبذلك يكون معرضاً للإلغاء لدى الطعن به إمام القضاء [41].

ركن الشكل: وهو المظهر الخارجي الذي يصدر فيه القرار والإجراءات التي تتبع في إصداره.

---

[37] داود عبد الرازق الباز الحكومة الإلكترونية وأثرها على النظام القانوني للمرفق العام وأعمال موظفيه منشأة المعارف للنشر، الإسكندرية ٢٠٠٧، ص ٢٤٣

[38] عبد الغني بسيوني، النظم السياسية أسس التنظيم الساسي، الدار الجامعية، الإسكندرية، ١٩٨٥٠، ص ٤٦٣.

[39] عصام عبد الوهاب البرزنجي وآخرون مبادئ وإحكام القانون الإداري العاتك لصناعة الكتاب -القاهرة، ٢٠٠٧، ص ٤١٥.

[40] ماجد راغب الحلو، القانون الإداري، دار المطبوعات الجامعية الإسكندرية، ١٩٨٧، ص ٣٩٨

[41] عبد الغني بسيوني، مرجع سابق، ص ٤٧٣.

والأصل في القرارات الإدارية أنها لا تخضع لشكل معين إلا إذا نص القانون على خلاف ذلك كان يشترط القانون كتابة القرار[42] .

السبب: هو الحالة الواقعية أو القانونية التي تدفع الإدارة إلى اتخاذ القرار[43] .

المحل: فهو جوهر القرار ومادته ويتمثل بالآثار القانونية التي يحدثها القرار مباشرة والتي تتمثل بإنشاء مركز قانوني أو تعديله أو إلغائه[44] .

الغاية: فهي النتيجة النهائية التي تهدف الإدارة إلى تحقيقها من وراء إصدار القرار الإداري [45].

وحسب القاعدة العامة في إعمال السلطة الإدارية إن القرارات الإدارية يجب إن تجعل المصلحة العامة غاية لها [46].

فيما يتعلق بتأثير التطور التكنولوجي على القرارات الإدارية، فقد تم ابتكار نظام ضمن إطار الحكومة الإلكترونية يتيح للحاسوب إصدار القرارات الإدارية بشكل مستقل، دون الحاجة لتدخل بشري، ويُعرف هذا النظام باسم "الأتمتة". وبهذا، أصبح بإمكان الحاسوب أن يقوم ببعض المهام التي كان يتعين على الموظف العام القيام بها بنفسه، مما يسهل عملية اتخاذ القرارات الإدارية[47].

وقد عرفت العديد من التشريعات - نظام الأتمتة منها قانون المعاملات والتجارة الإلكترونية الصادر في دولة الإمارات العربية والذي عرف الوسيط الإلكتروني المؤتمت بأنه:

(برنامج أو نظام إلكتروني الحاسب آلي يمكن إن يتصرف أو يستجيب لتصرف بشكل مستقل كلياً أو جزئياً دون إشراف أي شخص طبيعي في الوقت الذي يتم فيه التصرف أو الاستجابة له)[48].

من بين القرارات الإدارية التي يمكن أن يتخذها الحاسب الآلي، نجد قرار تعيين موظف جديد. يتم ذلك من خلال الإعلان عن الوظيفة الشاغرة عبر البريد الإلكتروني للدائرة المعنية، بالإضافة إلى نشرها في الصحف الإلكترونية. بعد ذلك، يتم ملء الاستمارات وإرسالها عبر الإنترنت إلى الجهة الإدارية المختصة. ومن المتوقع أن يتقدم العديد من الأشخاص لشغل هذه الوظيفة، فيقوم الحاسب باختيار الأنسب بينهم، ويقوم بإبلاغه عبر بريده الإلكتروني بموعد حضوره إلى الدائرة المعنية[49].

---

[42] المرجع السابق نفسه
[43] ماجد راغب الحلو، مرجع سابق، ص ٤٧٤.
[44] عصام البرزنجي، مرجع سابق، ص ١٣٧.
[45] عصام البرزنجي، مرجع سابق، ص ٤٤٠
[46] عبد الغني بسيوني، مرجع سابق، ص ٤٩٦
[47] عمار طارق عبد العزيز، أركان القرار الإداري الإلكتروني محلة القانون للدراسات والبحوث القانونية كلية القانون – جامعة ذي قار العدد ٢، ٢٠١٠ ص ٨
[48] المادة (٢) الفقرة (١٨) من قانون المعاملات والتجارة الإلكتروني الإماراتي رقم (٢) لعام ٢٠٠٢
[49] أورنس متعب الهذال، أثر التطور الإلكتروني في الأعمال القانونية للإدارة العامة، رسالة ماجستير مقدمة الى مجلس كلية القانون – جامعة بغداد، ٢٠٠٥، ص ٨٥.

ومن وجهة نظر الباحثة إن جعل الحاسب الآلي هو مصدر القرارات الإدارية الخاصة بالتعيين يعد خير تطبيق لمبدأ المساواة في تولي الوظائف العامة كما يعد تطبيقاً للشفافية الإدارية.

وبناء على ما تقدم، يذهب البعض من الفقهاء إلى إن التحول إلى نظام الحكومة الإلكترونية يقتضي مراجعة المفاهيم التقليدية للقرار الإداري وأركانه وشروطه وعلى وجه الخصوص ركني الاختصاص والشكل[50].

فبالنسبة إلى ركن الاختصاص فقد ذكرنا أن الحاسب الآلي قد شارك الموظف العام في إصدار القرار الإداري بعد ما كان الحال يقتضي وجوب صدور القرار من جهة إدارية مختصة قانوناً.

ومن المتوقع في ظل نظام الحكومة الإلكترونية إن يتأثر الاختصاص المكاني على نحو يؤدي إلى عدم الاعتداد به في المراحل المتقدمة من تطبيق هذا النظام وخاصة عندما يتحقق التكامل بين الإدارات الحكومية المختلفة، والتنسيق فيما بينها في أداء الخدمات[51].

الفرع الثاني: العقد الإداري الإلكتروني:

تستخدم السلطة الإدارية إلى جانب القرارات الإدارية التي تصدرها بإرادتها المنفردة نظام العقود من أجل إشباع الحاجات العامة وتأمين المواد اللازمة لتسير المرافق العامة. [52]

العقد الإداري هو ذلك الاتفاق الذي يُعقد بين كيان عام بهدف إدارة أو تنظيم مرفق عام، حيث تعكس نية الجهة الإدارية استخدام أساليب القانون العام. وبالتالي، يحتوي هذا العقد على شروط غير تقليدية وغير معتادة في إطار القانون الخاص، أو يمنح المتعاقد مع الإدارة الحق في المشاركة المباشرة في إدارة المرفق العام.[53].

ويتبين من هذا التعريف خصائص العقد الإداري، حيث يجب أن تكون الإدارة طرفاً فيه، وان يتصل بمرفق عام من حيث تنظيمه أو إدارته أو استغلاله، وان نتجه نية الإدارة إلى إتباع أساليب القانون العام لدى إبرام العقد[54].

وتتعدد صور العقود الإدارية عقد - التزام أو امتياز المرافق العامة - وهو عقد إداري يتم بمقتضاه إسناد وإدارة مرفق عام اقتصادي إلى شخص من أشخاص القانون الخاص سواء كان فرداً أم شركة لمدة محدده مقابل تحصيل رسوم من المنتفعين بخدماته[55].

---

[50] اورنس متعب الهذال ، المرجع السابق نفسه، ص ٨٧

[51] داود عبد الرازق الباز، مرجع سابق، ص ٢٦٥.

[52] عثمان سلمان عيلان، أثر التطور الإلكتروني في مبادئ الوظيفة العامة، الطبعة الأولى، الناشر صباح صادق جعفر الأنباري، ٢٠١٠، ص ٤٣.

[53] عصام عبد الفتاح مطر، الحكومة الإلكترونية بين النظرية والتطبيق، دار الجامعة الجديدة الإسكندرية، مصر، ٢٠٠٨، ص ٤٦.

[54] سليمان محمد الطماوي، الأسس العامة في العقود الإدارية، مطبعة عين الشمس – القاهرة، ١٩٩١، ص ٥٩

[55] حسين عثمان محمد عثمان، أصول القانون الإداري، دار المطبوعات الجامعية - الإسكندرية، ٢٠٠٤، ص ٥١٨

وكذلك عقد – الإشغال العامة – الذي هو عبارة عن اتفاق بين الإدارة واحد الأفراد أو الشركات بقصد القيام بإنشاء أو ترميم أو صيانة عقارات الحساب شخص معنوي عام بهدف تحقيق منفعة عامة نظير المقابل المتفق عليه[56] .

فضلاً عن عقد التوريد - الذي يعرف بأنه اتفاق بين شخص معنوي من أشخاص القانون العام وفرداً أو شركة يتعهد الفرد أو الشركة بتوريد منقولات معينة للشخص المعنوي لازمة لمرفق عام مقابل ثمن معين متفق عليه. علماً بأن عقد التوريد يرد على المنقولات[57].

أما عن عقد – النقل – فهو التزام الفرد أو أحد الأشخاص بنقل المنقولات للإدارة، ويلاحظ أن عقد النقل لا يختلف في شيء عن عقد التوريد إلا في موضوع العقد.

إلى جانب عقد – تقديم المعونة وهو عقد يلتزم بمقتضاه شخص من أشخاص القانون الخاص أو العام بالمساهمة نقداً أو عيناً في نفقات مرفق عام أو إشغال عامة [58].

وبالنسبة إلى عقد – القرض العام – الذي بمقتضاه يقرض أحد الأشخاص العامة أو الخاصة مبلغاً من المال إلى الدولة مقابل فائدة سنوية محدده تدفع من قبل الدولة.

وأخيراً هناك عقد – إيجار الخدمات – وهو العقد الذي يلتزم الأفراد بمقتضاه تقديم خدماتهم الشخصية للإدارة مقابل عوض متفق عليه [59].

والحقيقة إن اعتماد الأساليب الإلكترونية من جانب الجهات الإدارية أدى إلى ظهور أنماط جديدة من العقود الإدارية وهي تلك العقود التي تبرم من خلال شبكة الإنترنت في نطاق التجارة الإلكترونية[60].

ومن المؤكد إن تظهر في مجال العقود الإدارية صور أخرى المحل العقد أو موضوعه كإبرام عقود توريد أجهزة إلكترونية، بالإضافة إلى عقود الإشغال العامة كعقد إنشاء موقع إلكتروني أو بوابة إلكترونية للجهات الإدارية يكون موضوعه خدمات معلوماتية عامة، أو توصيل المرفق العام بشبكة الإنترنت.

أما عن طرق إبرام العقد الإداري فتنحصر في المناقصة والمزايدة وطريقة الاختيار المباشر (الممارسة).

ويراد بالمناقصة بأنها مجموعة من الإجراءات التي يحددها المشرع للإدارة بهدف اختيار من يتقدم بأقل عطاء إذا أرادت الإدارة القيام بأعمال معينه أو شراء أصناف معينة.

أما المزايدة فترمي إلى التعاقد مع أي شخص يتقدم بالعطاء الأعلى إذا ما رغبت الإدارة بيع أو تأجير أملاكها.

---

[56] عصام عبد الوهاب البرزنجي، مرجع سابق، ص ٤٩٠.
[57] عبد الغني بسيوني، مرجع سابق، ص ٥٧
[58] سامي جمال الدين، أصول القانون الإداري، منشأة المعارف الإسكندرية، ٢٠٠٤، ص ٦٤٧.
[59] عصام عبد الوهاب البوزيجي ، مرجع سابق، ص ٤٩٢٩
[60] عبد الفتاح بيومي حجازي، مرجع سابق، ص ٩٢

وجدير بالذكر إن القاعدة المتبعة في كل من مصر وفرنسا تتمثل في حرية الإدارة في التعاقد إذا لم يوجد نص يفرض عليها اللجوء إلى طريقة المناقصة.

أما في العراق فأن الإدارة ملزمة بإتباع أسلوب المناقصة أو المزايدة لإبرام عقودها إلا إذا أجاز القانون خلاف ذلك[61] .

والعلة من جعل أسلوب المناقصة العامة الأصل العام في تعاقدات الإدارة هي الإتاحة الفرصة لكل من تتوافر فيه شروط المناقصة لكي يتقدم بعطائه وتتسع الفرصة إمام الإدارة لاختيار أفضل المتعاقدين واستبعاد غير الأكفاء منهم.

ونظراً لكون المناقصة تستهدف فتح الباب إمام أكبر عدد ممكن من الأفراد للتقدم إليها فأن ذلك يستلزم مراعاة مبدأ العلانية بطريقة تسمح بوصول الإعلان لأكبر عدد ممكن من المتقدمين، حيث إن مبدأ العلانية يظهر الشروط والإجراءات التي يجوز للمتنافسين التعاقد مع الإدارة على ضوءها فضلاً عن إن هذا المبدأ يوفر للإدارة فرصة اختيار أفضل العروض[62].

ولما أصبح بإمكان الإدارة إن تبرم عقودها باستخدام الوسائط الإلكترونية فلا شك إن حرية المنافسة في مجال العقد الإداري الإلكتروني ستكون أوسع في هذا الشأن كما ستكون مدعومة بصوره أكبر من خلال مبدأ العلانية لأن الإعلان سيتم من خلال شبكة الإنترنت مما يعطي فرصة لجميع المؤسسات سواء كانت صغيرة أو كبيرة للاشتراك في العملية التي تتقدم بها الإدارة ومن ثم يسهل التفاوض بينهما عن طريق البريد الإلكتروني أو غرفة المحادثة، مما يعني إن مبدأ حرية المنافسة قد تأكد أكثر في ظل العقد الإداري الإلكتروني[63].

أما عن إجراءات المناقصة أو المزايدة فتتم عبر عدة مراحل أولها الإعلان من خلال النشر في الصحف أو وسائل الإعلام المسموعة والمرئية إذا اقتضت المصلحة ذلك وتأتي بعدها مرحلة تسليم العطاء بعد انتهاء المدة القانونية وتحديد موعد لفتح العطاء حيث يتم تحليل العطاء وتدقيق الأسعار لبيان رأيها بإرساء المناقصة على أحد العطاءات، أما المزايدات فتقدم غالباً شفاهاً [64].

وما يلاحظ على هذه الإجراءات أنها تتصف بالبطء الشديد والتعقيد كما أنها تستغرق زمناً طويلاً إلى إن يتم إبرام العقد الإداري بالأسلوب التقليدي.

---

[61] عصام عبد الوهاب البرزنجي، مرجع سابق، ص ٤٩٤

[62] قيدار عبد الله صالح، إبرام العقد الإداري الإلكتروني وإثباته، بحث منشور في مجلة الرافدين للحقوق جامعة الموصل، المجلد (١٠)، العدد ٢٠٠٨،٣٧ ص ١٦٠

[63] قيدار عبد الله صالح، مرجع سابق ص ١٦١

[64] المادة التاسعة من قانون بيع وإيجار أموال الدولة العراقي رقم ٣٢ لسنة ١٩٨٦.

أما في نطاق الحكومة الإلكترونية التي تتميز بسرعة الإنجاز والكفاءة في الأداء وقلة التكاليف، فأن استخدامها في مجال المناقصات يحقق مكاسب كبيرة للأفراد أو الشركات مقدمة العطاء وكذلك بالنسبة للجهة الإدارية، فعن طريق شبكة الإنترنت يتم الإعلان عن المناقصة وبيان شروطها التفصيلية وتلقى العروض أو العطاء من المتنافسين وإرساء المناقصة على أفضل العروض المقدمة كما ذكرنا.

المطلب الثاني: سبل التحصين القانوني والتقني للعقود الإدارية الرقمية:

إن التحول الرقمي المتسارع الذي شهده المرفق العام، برزت الحاجة الماسة إلى تحصين العقود الإدارية الرقمية بمجموعة متكاملة من الضمانات القانونية والتقنية، فعلى الصعيد القانوني، تتجلى أهمية ذلك في ضرورة إرساء إطار تشريعي متين يواكب التطورات التكنولوجية، ويضمن الشرعية والمشروعية للتعاقد الإلكتروني، ويشمل ذلك على سبيل المثال، وضع نصوص قانونية واضحة تجرم الاختراقات السيبرانية وتحدد المسؤوليات المدنية والجنائية المترتبة على الإخلال بأمن البيانات، وتمكن الجهات القضائية من الفصل في النزاعات المتعلقة بالعقود الرقمية بفعالية.

وقد أبرزت العديد من الدراسات ضرورة تبني نهج تشريعي استباقي لا يكتفي بالاستجابة للتهديدات القائمة، بل يتوقع التحديات المستقبلية ويوفر حلولاً لها، مع مراعاة المبادئ الأساسية للقانون الإداري، مثل مبدأ المساواة والشفافية[65] ، كما يعد تعزيز مبدأ الحجية القانونية للتوقيع الإلكتروني وتحديد شروط صحته وإجراءاته من الركائز الأساسية التي تضمن موثوقية العقد الإداري الرقمي وتضفي عليه الشرعية اللازمة لإنفاذه قضائيا[66]، أما على الصعيد التقني فإن التحصين يتطلب تبني حلول تكنولوجية متقدمة تعزز من أمان وسلامة العقود الإدارية الرقمية، لذا فإن التحصين الفعال للعقود الإدارية الرقمية يستلزم تكاملاً بين الأبعاد القانونية والتقنية، لضمان بيئة تعاقدية آمنة شفافة، وذات حجية قانونية، تساهم في تحقيق أهداف الإدارة الإلكترونية وتعزز الثقة في التعاملات الحكومية الرقمية.

الفرع الأول: التحديات التي تواجه الأمن السيبراني في العراق:

الأمن السيبراني في العراق يواجه تحديات هائلة نتيجة للتقدم التكنولوجي السريع والتحولات الكبيرة في مجال الاتصالات والمعلومات، فيعد هدفا استراتيجيا للهجمات السيبرانية لضعف الأمان الإلكتروني في البنية التحتية الوطنية، تلك التحديات تتفاقم بسبب استخدام المؤسسات العراقية لخدمات خارجية تتيح للمعلومات المهمة تداولها في خوادم خارج الحدود الوطنية، مما يفتح بابا لاختراقات واستخدامات غير مشروعة مما ينتج عنها أعمال تجسسية، أو حتى للمساس بأمان الدول الأخرى[67] .

[65] محمود سلامة، التحول الرقمي وأثره على العقود الإدارية، دار الفكر الجامعي الإسكندرية، سنة 2019، ص 112.
[66] رجب خالده، الحجية القانونية للتوقيع الإلكتروني في التشريعات العربية، دار المعارف، القاهرة، مصر سنة 2020، ص 65
[67] عادل عبد الصادق، الإرهاب الإلكتروني، القوة في العلاقات الدولية نمط جديد وتحديات مختلفة، مركز الدراسات السياسات الاستراتيجية، القاهرة، مصر، 2009، ص 201

اولاً: ضعف البنية التحتية التكنولوجية:

أن تهديدات الأمن السيبراني يمكن اعتبارها تحديات غير مرئية تؤثر على منظومة الأمن الوطني العراقي، فالتطور التكنولوجي الذي شهده العراق في مجال الاتصالات والمعلومات والذي تزامن مع ضعف البنية الأمنية الإلكترونية التحتية الوطنية سواء أكانت أمنية، مصرفية، شخصية، أدى الوضع الراهن في العراق إلى أن يصبح ساحة مفتوحة أمام العديد من دول العالم، مما يسهل عليها اختراق المعلومات الخاصة بمؤسساته والتجسس عليها. كما تم استخدامه كمنصة لشن هجمات إلكترونية تهدد أمن المعلومات في أي دولة، بالإضافة إلى سرقة البيانات واستغلالها لأغراض الابتزاز وتنفيذ العمليات الإرهابية. وتعتمد معظم المؤسسات العراقية على الحصول على معلوماتها من أقمار صناعية تتبع خدمات خارج الحدود، مما يؤدي إلى مرور تلك البيانات عبر خوادم تلك الدول قبل أن تعود إلى العراق، وهو ما يعد خرقاً للأمن المعلوماتي. لذا، من الضروري إنشاء مجموعة من الأطر القانونية والتنظيمية والهياكل التقنية، حيث يتطلب ذلك جهوداً مشتركة بين القطاعين العام والخاص، محلياً ودولياً، لحماية الفضاء السيبراني العراقي. يجب التركيز على ضمان توفر أنظمة معلومات آمنة وحماية سرية البيانات الشخصية، واتخاذ كافة التدابير اللازمة لحماية المواطنين من مخاطر الفضاء السيبراني[68].

يشهد العراق بين الفينة والأخرى هجمات إلكترونية من قبل جماعات متطرفة وقراصنة مجهولين، تستهدف البنية التحتية الحكومية والقطاع الخاص. هذه الهجمات تؤثر سلبًا على الخدمات الحكومية، مما يعرض الأفراد والمؤسسات لمخاطر الاحتيال وسرقة الهوية. إن ضعف الأمن السيبراني ينعكس سلبًا على استقرار العراق، حيث يعرقل سير الأعمال الحكومية والتجارية، ويثني المستثمرين عن ضخ أموالهم، مما يؤدي إلى تباطؤ النمو الاقتصادي وارتفاع معدلات البطالة. لذا، يحتاج العراق إلى تعزيز بنيته التحتية لتقوية الأمن السيبراني وتمكينه من مواجهة التحديات الحديثة بفعالية، مع التشديد على أهمية تحسين القدرات الفنية والقانونية والإدارية لتحقيق أهداف الأمان السيبراني، كذلك يُسلط الضوء على حاجة البلاد إلى منظومة تعليمية تركز على دراسة الأمن السيبراني لتأهيل الكوادر البشرية وتقديم التدريب الملائم، از شهد العراق في الآونة الاخيرة استحداث 3 أقسام متخصصة في دراسة الأمن السيبراني في جامعات رئيسية منها جامعة المستنصرية، والجامعة التقنية الشمالية، وجامعة الموصل وكذلك في جامعة المستقبل، وافتتاح فروع لأكاديميات دولية لتدريس الأمن السيبراني والحوسبة السحابية في العراق، وهو تطور إيجابي يسهم في تعزيز الكفاءات في هذا المجال[69].

[68] علي زياد العلي علي حسين حميد، تكتيكات الحروب الحديثة الأمن السيبراني والحروب المعززة والهجينة، دار العربي للنشر والتوزيع، القاهرة، مصر، 2023، ص 143

[69] فارس محمد العمارات ابراهيم الحمامصة، الأمن السيبراني المفهوم وتحديات العصر، دار الخليج للنشر والتوزيع، عمان، الأردن، 2022، ص 74

ثانياً: ضعف تشريعات الأمن السيبراني:

أن استخدام التقنيات المستحدثة للتحكم في المعلومات وأساليب تجميعها ومعالجتها واختزانها وتحسين الانتفاع منها من خلال الحاسبات وثورة الاتصالات [70]، والسرعة والتطور التكنولوجي في العراق والعالم، مع وجود فجوات قانونية في مجال الإنترنت تشكل تحديا كبيرا، ففي ظل غياب معايير موحدة لقوانين الإنترنت، يصبح التنظيم أمرا حيويا، خاصة عندما تتعلق المسألة بأفراد أو كيانات من دول مختلفة ويظهر الخلل بشكل واضح عندما يتورط الهجوم السيبراني في قضايا تجاوز الحدود أذ قد يقوم المهاجمون بتنفيذ هجمات إرهابية في بلد لا تكون فيه قوانين صارمة، مما يثير تحديات في مجال تنازع القوانين، وتكمن المشكلة الحقيقية في عدم وجود سلطة مركزية على مستوى دولي تعمل على تطبيق قوانين تحمي الخصوصية وتضمن الأمان الرقمي[71]، إذ يصبح الحل لهذه التحديات هو التعاون الدولي الفعال، وفي ظل غياب سلطة دولية مركزية، يزيد نشوء ظاهرة الإرهاب الإلكتروني فهي التحديات التي تواجه الأمان الوطني، ولحماية الخصوصية وضمان الأمان السيبراني، يجب وضع معايير وسياسات تنظيمية دولية تحدد التزامات يجب اتباعها في البيئة السيبرانية لذلك أن الفجوات القانونية تجعل من الصعب إثبات الدليل المادي للاعتداءات السيبرانية، مما يجعل التحقيق والمساءلة أمورًا معقدة، ولكن يمكن أن تؤثر الهجمات السيبرانية على مستويات مختلفة، مما يبرز أهمية تنسيق الجهود الدولية لمواجهة هذه التحديات، ولتحقيق ذلك، يجب أن تلتزم الدول بالتعاون الدولي وتطوير إطار قانوني دولي ينظم الهجمات السيبرانية ويحدد العقوبات للمتورطين، وإن إقامة هياكل دولية تعمل على توحيد الجهود وتعزيز التعاون ستكون أساسية لتحقيق أمان الإنترنت ومواجهة التهديدات السيبرانية بفعالية[72].

فعدم وجود تشريعات محددة في العراق لمكافحة الهجمات السيبرانية يتيح للمهاجمين والهاكرز فرصة لتنفيذ أنشطتهم دون مواجهة عواقب قانونية جادة، يمكن أن يؤدي هذا الوضع إلى عجز في تحقيق العدالة وتطبيق القانون على المخترقين مما يزيد من التهديدات ويقلل من فعالية الاستجابة، لتحسين الأمان السيبراني في العراق، يلزم إصدار وتعزيز تشريعات فعّالة وشاملة تغطي جوانب متنوعة من الأمان السيبراني، بما في ذلك الوقاية من الهجمات، وتحقيق العدالة في حال وقوع الاختراقات، وتحديد العقوبات المناسبة للمخترقين، وفي جلسته بتاريخ 21 نوفمبر 2023 طرح البرلمان العراقي مشروع قانون جرائم

[70] زهراء عماد محمد كلنتر، تكييف الهجمات السيبرانية في ضوء القانون الدولي، مجلة الكوفة للعلوم القانونية والسياسية، 2020 المجلد 1، العدد 44/1، 2020، ص 52.

[71] صلاح مهدي هادي الشمري، زيد محمد علي اسماعيل، الأمن السيبراني كمرتكز جديد في الإستراتيجية العراقية، مجلة قضايا سياسية، كلية العلوم السياسية – جامعة النهرين العدد 62، 2020، ص281

[72] قمر ثامر صبري، الإرهاب السيبراني وأثره على الأمن القومي العراق انموذجاً"، مجلة قضايا سياسية، جامعة النهرين، كلية العلوم السياسية، بغداد، العدد 71، 2022، ص 145

المعلوماتية، بعد فشل دورات المجلس السابقة في إقراره خلال العقد المنصرم، وعلى الرغم من التعديلات المتكررة على مشروع القانون، ومع التأكيد على أهمية تنظيم عملية التواصل الإلكتروني[73].

ثالثاً: غياب الأمن الإلكتروني:

غياب الأمن الإلكتروني جعل العراق يعاني من انكشاف استراتيجي حيال أغلب بلدان العالم ومهد الطريق لهم لاختراقه والتجسس على البيانات والمعلومات بمنظومته الأمنية، بل والعمل على جعل العراق أداة لشن الهجمات الإلكترونية على الأمن المعلوماتي لدول أخرى واختراقه وسرقة معلوماتها واستخدامها لأغراض المساومة وتنفيذ أفعال إرهابية، ويتضح تأثير المخاطر السيبرانية على الأمن الوطني والاقتصاد العراقي من خلال مؤشرات عديدة، ومنها؛ عدم فعالية البنية الرقمية التحتية كما أسلفنا، حيث يعد العراق متخلفاً في مجال التبويب الرقمي وخصوصاً في المجال الاقتصادي.

فالعراق في الفضاء المعلوماتي لا يعيش عصر العزلة بيد أنه مترابط مع دول أخرى في هذا الفضاء عبر شبكات ترابطية للبنى المعلوماتية التحتية، حتى بات بالإمكان عبر ذبذبات الاتصال الرقمي تنظيف خزينة العراق من أموالها بواسطة نظاماً حاسوبياً يتم إدارته من غرفة في قرية تبعد عنه آلاف الكيلومترات، فتلك الموجات الأثيرية تهاجم مركز الثقل في تطور الدولة وتسيطر على قدرات العراق وتتحكم بكافة مقدراته، وتستهدف المراسلات الحكومية لتقوم بعملية تدمير تلك الوسائط الإلكترونية، وتستهدف الأسرار الأمنية والاقتصادية وأيضاً الاجتماعية للبلد، ليكتمل بذلك حلقات العملية التجسسية، وكذلك احتواء الفضاء السيبراني على نقاط ضعف بالإمكان توظيفها لاستغلال المصالح الاقتصادية الوطنية وتمثل تحدياً للأمن الوطني العراقي، ومنها الإرهاب والتجسس الإلكتروني والقرصنة الإلكترونية وعملية غسيل الأموال، واستخدام شبكات الإنترنت لممارسة أعمال العنف والنصب والاحتيال والاستغلال والجرائم المالية، ناهيك عن الاستخدام السلبي لمواقع التواصل الاجتماعي للقيام بإعمال مدمرة[74].

الفرع الثاني: فرص تحسين الأمن السيبراني في العراق:

تسعى الحكومة العراقية إلى تحسين فعاليتها وخدماتها من خلال تبني التقنيات الرقمية، ويعكس تحليل نموذج نضوج الحكومة الرقمية مدى تكامل هذه التقنيات في أنظمة الحكومة، ويعرض هذا السياق تحديات تبني التحول الرقمي والفرص المتاحة ويسلط الضوء على استراتيجيات العراق في تطوير حكومة رقمية تعزز التقدم والفعالية في إطار نظمها السياسية ويمكن إيجازها بالآتي[75] :

---

[73] باسم علي خريسان الأمن السيبراني في العراق قراءة في مؤشر الأمن السيبراني العالمي 2020، مركز البيان للدراسات والتخطيط، بغداد 2021، ص 9.

[74] مصطفى ابراهيم سلمان الشمري، الأمن السيبراني وأثره في الأمن الوطني العراقي، مجلة العلوم القانونية والسياسية، كلية القانون والعلوم السياسية جامعة ديالى، المجلد 10، العدد 1، 2021، ص ١٥٢.

[75] باسم علي خريسان الأمن في الفضاء السيبراني: دراسة في التهديدات واستراتيجية المواجهة مجلة كلية التراث الجامعة، بغداد، المجلد 1، العدد 36، 2023، ص 23

أولاً: حماية البنية التحتية للمعلومات الحيوية الوطنية لذلك ينبغي العمل على تقييم المخاطر التي تواجهها البنية التحتية للمعلومات الحيوية التي تتضمن وضع إطار زمني لإدارة المخاطر على البنية التحتية وتقييم التهديدات ونقاط الضعف والعواقب وإجراء تقييمات منتظمة للمخاطر التي تواجه وزارات الدولة ومؤسسات القطاعات الحيوية، وإجراء تقييمات حول مدى الترابط والاعتماد المتبادل بين مؤسسات الدولة لتحديد المخاطر التي تواجهها[76].

ثانياً: الاستجابة للحوادث والهجمات الإلكترونية وحلها والتعافي منها من خلال تداول المعلومات في الوقت المناسب والتعاون واتخاذ الإجراءات اللازمة.

ثالثاً: وضع الإطار القانوني والتنظيمي لتعزيز سلامة وحيوية الفضاء الإلكتروني.

رابعاً: تعزيز ثقافة الأمن السيبراني التي من شأنها دعم الاستخدام الأمن والمناسب للفضاء الإلكتروني.

خامساً: تطوير قوى وصقل الإمكانيات الوطنية للأمن السيبراني.

سادساً: تنمية الوعي بالمخاطر السيبرانية والحلول المتاحة، وتعزيز استخدام المنتجات والخدمات التكنلوجية الموثوق بها، ووضع استراتيجية وطنية للتصدي للأخطار ومواطن الضعف في البنية التحتية السيبرانية من قبل صانع القرار العراقي.

سابعاً: اتخاذ إجراءات دولية ومشتركة للتصدي للجرائم المعلوماتية عن طريق إبرام اتفاقيات ومواثيق دولية لمواجهة تلك الجرام والعمل على محاربتها لكن من المستحيل معرفة الحركات في الفضاء السيبراني دون رؤية استراتيجية، والمصالح هي المحفز للحراك الدولي الرقمي وأن جميع الدول يجمعها هدف واحد هو تحقيق التكامل الأمني [77].

الخاتمة

خلصت هذه الدراسة إلى أن الأمن السيبراني لم يعد مجرد إجراء تقني أو احترازي، بل أصبح وظيفة حيوية تتولى الدولة مسؤوليتها في حماية النظام الرقمي العام وضمان استمرارية الخدمات العامة. ويعكس هذا الاتجاه المتزايد نحو تنظيم الأمن السيبراني وإنشاء هياكل إدارية متخصصة تشرف عليه، طبيعته كمرفق عام يخضع لقوانين الدولة.

ومع ذلك، فإن حداثة هذا المجال وتطور التهديدات الرقمية تستدعي من المشرعين والإدارة العامة مواكبة مستمرة، سواء من حيث التشريع أو التنظيم أو التنسيق المؤسسي، لضمان تحقيق الأمن السيبراني دون المساس بحقوق الأفراد وحرياتهم بشكل غير مبرر.

[76] ظفر عبد مطر التميمي، العراق والأمن السيبراني. الفرص والتحديات، مجلة واسط للعلوم الإنسانية والاجتماعية، جامعة واسط العراق، المجلد 18، العدد 51، 2022، ص 11.

[77] مروان سالم العلي التحديات الاستراتيجية للأمن الوطني العراقي في ظل المتغيرات الدولية مجلة تكريت للعلوم السياسية، العراق، المجلد 2، العدد 20، 2020، ص 57

أولاً- النتائج:

- يعتبر الأمن السيبراني مرفق عام حديث يرتبط مباشرة بحماية النظام الرقمي العام.
- يستند الأساس القانوني للأمن السيبراني إلى الدستور والتشريعات المتعلقة بالأمن الوطني وحماية البيانات.
- يتمتع الأمن السيبراني بخصائص المرفق العام من حيث الاستمرارية والعمومية وخضوعه لإشراف الدولة.
- يلعب التنظيم الإداري المتخصص دور محوري في فعالية سياسات الأمن السيبراني.
- يواجه الأمن السيبراني تحديات قانونية وتنظيمية نتيجة التطور السريع للتقنيات والجرائم الإلكترونية.

ثانياً- التوصيات:

- ضرورة وضع تشريعات شاملة وواضحة تنظم الأمن السيبراني كمرفق عام.
- تعزيز استقلالية وكفاءة الهيئات الإدارية المعنية بالأمن السيبراني.
- دعم التنسيق بين الجهات الحكومية والقطاع الخاص في إدارة المخاطر السيبرانية.
- إدماج مبادئ حماية الحقوق والحريات الرقمية ضمن سياسات الأمن السيبراني.
- التركيز على التكوين والتدريب المستمر للموارد البشرية العاملة في مجال الأمن السيبراني.

قائمة المصادر والمراجع

1. أونيسي ليندة، المبادئ الضابطة للمرفق العام الإلكتروني، جامعة عباس الغرور خنشلة، مجلة الحقوق والعلوم الإنسانية، المجلد 14 / العدد 01، الجزائر،2021، ص204
2. زينب عباس راضي، فاعلية الأمن السيبراني في السياسة العالمية (المفهوم والتدابير الأمنية للدول)،
3. جامعة البيان كلية القانون والعلوم السياسية، مجلة أشور للعلوم القانونية والسياسية، المجلد الثاني - العدد (الأول)، العراق، ٢٠٢٥، ص ٥٥٠
4. ربيعي حسين وسمر محمود الحروب السيبرانية: المخاطر واستراتيجيات تحقيق الأمن السيبراني الدولي والداخلي المجلة الجزائرية للأمن الإنساني، المجلد (٧)، العدد (٢)، ٢٠٢٢، ص ١٧٨
5. فارس محمد العمارات وإبراهيم الحمامصة الأمن السيبراني المفهوم تحديات العصر)، دار الخليج للنشر والتوزيع ط١، ٢٠٢٢، ص ١١.
6. عبد الرحمن على اللقاني دور الأمن السيبراني في تعزيز أمن المعلومات المالية الإلكترونية، دار اليازوري العلمية للنشر والتوزيع، الأردن، ط١، ٢٠٢٢، ص ١٦٢.
7. فاطمة علي أبراهيم رحاب يوسف وليد محمود السيد الأمن السيبراني والنظافة الرقمية، المجلة
8. المصرية لعلوم المعلومات، مجلد (٩)، العدد (٢)، ٢٠٢٢، ص ٤٠١.
9. أدريس عطية مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، مجلة مصداقية، المجلد (١)، العدد (١)، ٢٠١٩، ص ١٠٥.

10. إسلام فوزي، الأمن السيبراني (الأبعاد الاجتماعية والقانونية تحليل سوسيولوجي)، المجلة الاجتماعية القومية، المجلد (٥٦)، العدد (٢)، ٢٠١٩، ص ١٠٨
11. سلمى عبد الرحيم عبد الحسن طبيعة العلاقة بين الأمن السيبراني والنمو الاقتصادي الرقمي في دول العالم، على الموقع الإلكتروني، تاريخ الزيارة ١٧ /٢٠٢٥/١ https://iaiphss.us
12. منى الأشقر جبور، الأمن السيبراني، التحديات ومستلزمات المواجهة، جامعة الدول العربية، المركز العربي للبحوث القانونية والفضائية اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني، بيروت ٢٠١٢٠، ص ٦.
13. منى الأشقر جبور، السيبرانية هاجس العصر، جامعة الدول العربية المركز العربي للبحوث القانونية
14. والقضائية، ط ١، ٢٠١٦، ص ٢٩.
15. خالد وليد محمود، الفضاء السيبراني وتحولات القوة في العلاقات الدولية المركز العربي للنشر والتوزيع، ط1، ٢٠٢٥، ص ٢٩٣.
16. فايز بن عبد الله الشهري، استخدامات شبكة الإنترنت في مجال الإعلام الأمني العربي دراسة وصفية على عينة من المواقع الأمنية العربية على شبكة الإنترنت مجلة البحوث الأمنية، الرياض كلية الملك فهد الأمنية، مركز الدراسات.2011، ص١٣.
17. سامي الشواء، الغش المعلوماتي الظاهرة إجرامية مستحدثة، بحث في مؤتمر الجمعية المصرية القانون الجنائي، القاهرة، 2009، 28
18. عبد الرزاق سندالي، التشريع المغربي في مجال الجرائم المعلوماتية، ضمن أعمال الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر 19-20 نيسان المملكة المغربية،2017، ص٣٣.
19. عبود السراج، مفهوم جرائم المعلوماتية، واقع وآفاق، بحث مقدم إلى المؤتمر الإقليمي الأول لمكافحة جرائم المعلوماتية الذي نظمته الجامعة الأردنية والتحد المحامين العرب خلال الفترة 18-19 كانون الثاني عام 2013، ص٥٣.
20. واثبة السعدي، الحماية الجنائية لبرامج الحاسوب، بحث مقدم إلى مؤتمر القانون والحاسوب المنعقد في جامعة اليرموك -اربد بتاريخ 12-14 تموز ،2019، ص 6.
21. محمد أمين البشري، التحقيق في الجرائم المستحدثة الرياض جامعة نايف العربية للعلوم الأمنية، مركز الدراسات والبحوث،2014، ص٢٥.
22. المركز العربي للبحوث القانونية والقضائية، مجلس وزراء العدل العرب، جامعة الدول العربية، الاتفاقية العربية الحماية الفضاء السيبراني بين الواقع والطموح، 2018.
23. عمر محمد يونس، الجرائم الناشئة عن استخدام الإنترنت ط1، دار النهضة العربية، القاهرة، 2015، ص٣٤.
24. عبد العزيز اليوسف، التقنية في الجرائم المستحدثة بحث ضمن كتاب الظواهر الإجرامية المستحدثة وسبل مواجهتها، منشورات أكاديمية نايف للعلوم الأمنية، الرياض، 2015، ص٥٣.
25. المركز العربي للبحوث القانونية والقضائية، مجلس وزراء العدل العرب، جامعة الدول العربية، الثالثة والعشرون من الاتفاقية العربية الحماية الفضاء السيبراني بين الواقع والطموح، 2018، ص٣١
26. المركز العربي للبحوث القانونية والقضائية، مجلس وزراء العدل العرب، جامعة الدول العربية، المادة الثانية والعشرون من الاتفاقية العربية لحماية الفضاء السيبراني، 2018، ص٣٤.

27.المركز العربي للبحوث القانونية والقضائية، مجلس وزراء العدل العرب، جامعة الدول العربية المادة الثامنة والعشرون من الاتفاقية العربية الحماية الفضاء السيبراني، 2018، ص٣٥.
28.المركز العربي للبحوث القانونية والقضائية، مجلس وزراء العدل العرب، جامعة الدول العربية المادة التاسعة والعشرون من الاتفاقية العربية الحماية الفضاء السيبراني، 2018، ص ٣٦.
29.فياض عبد الله، رجاء كاظم حيدر عبود التعليم الإلكتروني والتعليم التقليدي دراسة تحليلية مقارنة
30.بحث منشور في مجلة كلية بغداد للعلوم الاقتصادية الجامعة، عدد ١٩، ٢٠٠٩، ص ٢٧٦.
31.جان سيريل، واقع وأفاق التعليم عن بعد وأثره في التعليم في العراق، بحث منشور في مجلة كلية العلوم الاقتصادية الجامعة، العدد ٢٣، ٢٠١٠، ص ٣٢٦
32.داود عبد الرازق الباز الحكومة الإلكترونية وأثرها على النظام القانوني للمرفق العام وأعمال موظفيه منشأة المعارف للنشر، الإسكندرية ٢٠٠٧، ص ٢٤٣
33.عبد الغني بسيوني، النظم السياسية أسس التنظيم الساسي، الدار الجامعية، الإسكندرية، ١٩٨٥٠، ص ٤٦٣.
34.عصام عبد الوهاب البرزنجي وآخرون مبادئ وإحكام القانون الإداري العاتك لصناعة الكتاب -القاهرة، ٢٠٠٧، ص ٤١٥.
35.ماجد راغب الحلو، القانون الإداري، دار المطبوعات الجامعية الإسكندرية، ١٩٨٧، ص ٣٩٨
36.عمار طارق عبد العزيز، أركان القرار الإداري الإلكتروني محلة القانون للدراسات والبحوث القانونية كلية القانون – جامعة ذي قار العدد ٢، ٢٠١٠ ص ٨
37.المادة (٢) الفقرة (١٨) من قانون المعاملات والتجارة الإلكتروني الإماراتي رقم (٢) لعام ٢٠٠٢
38.أورنس متعب الهذال، أثر التطور الإلكتروني في الأعمال القانونية للإدارة العامة، رسالة ماجستير مقدمة الى مجلس كلية القانون – جامعة بغداد، ٢٠٠٥، ص ٨٥.
39.عثمان سلمان عيلان، أثر التطور الإلكتروني في مبادئ الوظيفة العامة، الطبعة الأولى، الناشر صباح صادق جعفر الأنباري، ٢٠١٠، ص ٤٣.
40.عصام عبد الفتاح مطر، الحكومة الإلكترونية بين النظرية والتطبيق، دار الجامعة الجديدة الإسكندرية، مصر، ٢٠٠٨، ص ٤٦.
41.سليمان محمد الطماوي، الأسس العامة في العقود الإدارية، مطبعة عين الشمس – القاهرة، ١٩٩١، ص ٥٩
42.حسين عثمان محمد عثمان، أصول القانون الإداري، دار المطبوعات الجامعية - الإسكندرية، ٢٠٠٤، ص ٥١٨
43.سامي جمال الدين، أصول القانون الإداري، منشأة المعارف الإسكندرية، ٢٠٠٤، ص ٦٤٧.
44.قيدار عبد الله صالح، إبرام العقد الإداري الإلكتروني وإثباته، بحث منشور في مجلة الرافدين للحقوق جامعة الموصل، المجلد (١٠)، العدد ٣٧،٢٠٠٨ ص ١٦٠
45.المادة التاسعة من قانون بيع وإيجار أموال الدولة العراقي رقم ٣٢ لسنة ١٩٨٦.
46.محمود سلامة، التحول الرقمي وأثره على العقود الإدارية، دار الفكر الجامعي الإسكندرية، سنة 2019، ص 112.

47.رجب خالده، الحجية القانونية للتوقيع الإلكتروني في التشريعات العربية، دار المعارف، القاهرة، مصر سنة 2020، ص 65
48.عادل عبد الصادق، الإرهاب الإلكتروني، القوة في العلاقات الدولية نمط جديد وتحديات مختلفة، مركز الدراسات السياسات الاستراتيجية، القاهرة، مصر، 2009، ص 201
49.علي زياد العلي علي حسين حميد، تكتيكات الحروب الحديثة الأمن السيبراني والحروب المعززة والهجينة، دار العربي للنشر والتوزيع، القاهرة، مصر، 2023، ص 143
50.فارس محمد العمارات ابراهيم الحمامصة، الأمن السيبراني المفهوم وتحديات العصر، دار الخليج للنشر والتوزيع، عمان، الأردن، 2022، ص 74
51.زهراء عماد محمد كلنتر، تكييف الهجمات السيبرانية في ضوء القانون الدولي، مجلة الكوفة للعلوم القانونية والسياسية، 2020 المجلد 1، العدد 44/1، 2020، ص 52.
52.صلاح مهدي هادي الشمري، زيد محمد علي اسماعيل، الأمن السيبراني كمرتكز جديد في الإستراتيجية العراقية، مجلة قضايا سياسية، كلية العلوم السياسية – جامعة النهرين العدد 62، 2020، ص281
53.قمر ثامر صبري، الإرهاب السيبراني وأثره على الأمن القومي العراق أنموذجاً"، مجلة قضايا سياسية، جامعة النهرين، كلية العلوم السياسية، بغداد، العدد 71، 2022، ص 145
54.باسم علي خريسان الأمن السيبراني في العراق قراءة في مؤشر الأمن السيبراني العالمي 2020، مركز البيان للدراسات والتخطيط، بغداد 2021، ص 9.
55.مصطفى ابراهيم سلمان الشمري، الأمن السيبراني وأثره في الأمن الوطني العراقي، مجلة العلوم القانونية والسياسية، كلية القانون والعلوم السياسية جامعة ديالى، المجلد 10، العدد 1، 2021، ص ١٥٢.
56.باسم علي خريسان الأمن في الفضاء السيبراني: دراسة في التهديدات واستراتيجية المواجهة مجلة كلية التراث الجامعة، بغداد، المجلد 1، العدد 36، 2023، ص 23
57.ظفر عبد مطر التميمي، العراق والأمن السيبراني. الفرص والتحديات، مجلة واسط للعلوم الإنسانية والاجتماعية، جامعة واسط العراق، المجلد 18، العدد 51، 2022، ص 11.
58.مروان سالم العلي التحديات الاستراتيجية للأمن الوطني العراقي في ظل المتغيرات الدولية مجلة تكريت للعلوم السياسية، العراق، المجلد 2، العدد 20، 2020، ص 57

1. Understanding Cybercrime: A Guide for Developing Countries, at 72, International Telecommunication Union, April 2009, www.Itu.int/TTU-D/cyb/cybersecurity/docs/itu-understandingSybercrime-guide.pdf (hereinafter "Understanding")
2. Trust in the Information Society: A Report of the Advisory Board RISEPTIS, bup://www.think Inmateu: David-Olivier Jaquet-Chiffelle, ed., Identity Revolution: Multidisciplinary Perspectives, FIDIS. May 2009, http://www.fislis.net/resources/identity-evolution