الحماية الدستورية للأمن الرقمي

م.د. اياد يوسف حيال

مدرس القانون الدستوري

جامعة كركوك/ كلية القانون والعلوم السياسية

Dr.ayad.y.2020@uokirkuk.edu.iq

Constitutional protection of digital security

Dr. Ayad yousif hayal

Lecturer in Constitutional Law

University of Kirkuk/ College of Law and Political Science

المستخلص:

أضحى الأمن الرقمي مفهومًا مركزيًا في الدراسات القانونية المعاصرة، نظرًا لارتباطه المباشر بحماية الفضاء الإلكتروني الذي بات يحتضن جانبًا واسعًا من المعاملات الإدارية والاقتصادية والاجتماعية. ويتجاوز هذا المفهوم مجرد حماية الأجهزة أو الشبكات، ليشمل منظومة متكاملة من السياسات والتشريعات والإجراءات التقنية التي تهدف إلى صون البيانات والأنظمة من الاختراق أو العبث أو التعطيل.

الوصول إلى شبكة الانترنت والذي يعد من الحقوق التي كفلتها قوانين دول عديدة فتعد الحريات الرقمية وفقا لما ورد اعلاه مصطلحا يوصف حق الافراد والتجمعات في التعبير عن آرائهم بالطريقة والكيفية عبر استخدام اجهزة الاتصال بالإنترنت وفقاً للوسائل المتاحة وشبكات التواصل الاجتماعي وتتمثل بحرية التعبير عن الرأي الرقمي، والتجمع الرقمي في منتديات افتراضية وكذلك حرية تداول المعلومات في المحتوى الرقمي

لم يعد ممكنًا فصل الأمن الرقمي عن المنظومة الدستورية، لأن أي اعتداء على البيانات أو الاتصالات أو الأنظمة الإلكترونية قد ينعكس مباشرة على ممارسة الحقوق الأساسية، وعلى استقرار المؤسسات العامة، وعلى ثقة الأفراد في الدولة. ويقتضي ذلك إعادة النظر في كيفية فهم النصوص الدستورية التقليدية، وربطها بالواقع الرقمي الجديد، بما يضمن حماية فعّالة للأمن الرقمي دون المساس بجوهر الحقوق والحريات.

الكلمات المفتاحية: (الأمن الرقمي _ شبكات التواصل _ الأمن السيبراني، حق الخصوصية)

Abstract

Digital security has become a central concept in contemporary legal studies due to its direct connection with protecting cyberspace, which now hosts a significant portion of administrative, economic, and social transactions. This concept goes beyond merely protecting devices or networks; it encompasses an

integrated system of policies, legislation, and technical procedures aimed at safeguarding data and systems from intrusion, manipulation, or disruption. Access to the Internet, which is considered a right guaranteed by the laws of many countries, has led to the emergence of **digital freedoms**. As mentioned above, this term describes the right of individuals and groups to express their opinions in various ways through the use of Internet-connected devices and social media platforms. These freedoms include digital freedom of expression, digital assembly in virtual forums, and the freedom to exchange information within digital content.

It is no longer possible to separate digital security from the constitutional framework, because any attack on data, communications, or electronic systems may directly affect the exercise of fundamental rights, the stability of public institutions, and individuals' trust in the state. This requires reconsidering how traditional constitutional texts are interpreted and linking them to the new digital reality, in order to ensure effective protection of digital security without compromising the essence of rights and freedoms.

Keywords: Digital Security – Social Media Networks – Cybersecurity – Right to Privacy.

مقدمة

أدى التحول الرقمي المتسارع، وتغلغل التقنيات الحديثة في مفاصل الحياة العامة والخاصة، إلى بروز مفهوم الأمن الرقمي بوصفه أحد المرتكزات الجوهرية لصون كيان الدولة وحماية حقوق الأفراد في آن واحد. فلم يعد الأمن محصورًا في أبعاده التقليدية، بل امتد ليشمل الفضاء السيبراني بما يحويه من بيانات، ومعاملات إلكترونية، وبنى تحتية رقمية حيوية. وفي هذا السياق، برزت الحاجة إلى إطار دستوري يحدد حدود تدخل السلطات العامة في المجال الرقمي، ويوازن بين متطلبات الأمن وحماية الحقوق والحريات الأساسية، ولا سيما الحق في الخصوصية وحرية الاتصالات والمراسلات الإلكترونية.

إن الحماية الدستورية للأمن الرقمي تمثل اليوم ميدانًا خصبًا للتأمل القانوني، لما تثيره من إشكالات تتعلق بمدى كفاية النصوص القائمة لمواجهة التحديات التقنية المتجددة، وحدود التفسير القضائي للنصوص الدستورية في ضوء الالتزامات الدولية للدولة. ومن ثمّ، يسعى هذا البحث إلى تحليل الإطار الدستوري الناظم للأمن الرقمي، وبيان مدى قدرته على استيعاب التحولات الرقمية، مع التركيز على التجربة الدستورية العراقية ومقارنتها بالاتجاهات الدولية المعاصرة، بغية إبراز مكامن القوة ونقاط القصور واقتراح مسارات تطويرية منسجمة مع دولة القانون.

إنَّ الأمن الرقمي لم يُنص عليه صراحةً في أغلب الدساتير، ومنها دستور جمهورية العراق لسنة ٢٠٠٥، وارتباطه المباشر بالحقوق والحريات الأساسية كحق الخصوصية وحرية التعبير وحرية تداول المعلومات، وهي حقوق ذات طبيعة دستورية عليا، وتحقيق التوازن بين السلطة والحرية، إذ يطرح البحث مسألة حدود تدخل الدولة في المجال الرقمي ومدى خضوعه لمبدأي الشرعية والتناسب. خاصة في ظل تطور

الجرائم السيبرانية وازدياد الاعتماد على الخدمات الرقمية. وتعزيز الرقابة الدستورية على التشريعات الرقمية، وإبراز الحاجة إلى تنظيم قانوني متوازن يمنع التعسف في استخدام أدوات المراقبة الرقمية باسم الأمن. مع تصاعد التهديدات السيبرانية والاختراقات وسرقة البيانات والهجمات على البنى التحتية الحيوية. والتحول الرقمي الشامل في مؤسسات الدولة والقطاع الخاص، مما يجعل الأمن الرقمي مسألة أمن وطني. وحماية الأفراد من انتهاك بياناتهم الشخصية خصوصاً مع توسع استخدام المنصات الرقمية، ويُعدّ الأمن الرقمي من القضايا المعاصرة التي تمسّ جوهر الحقوق والحريات الدستورية.

أولاً: أهمية البحث:

تكمن أهمية البحث في حداثة المفهوم دستورياً، فالأمن الرقمي لم يُنص عليه صراحةً في أغلب الدساتير، ومنها دستور جمهورية العراق لسنة ٢٠٠٥، وارتباطه المباشر بالحقوق والحريات الأساسية كحق الخصوصية وحرية التعبير وحرية تداول المعلومات، وهي حقوق ذات طبيعة دستورية عليا، خاصة في ظل تطور الجرائم السيبرانية وازدياد الاعتماد على الخدمات الرقمية. وتعزيز الرقابة الدستورية على التشريعات الرقمية، وإبراز الحاجة إلى تنظيم قانوني متوازن يمنع التعسف في استخدام أدوات المراقبة الرقمية باسم الأمن. مع تصاعد التهديدات السيبرانية والاختراقات وسرقة البيانات والهجمات على البنى التحتية الحيوية. والتحول الرقمي الشامل في مؤسسات الدولة والقطاع الخاص، مما يجعل الأمن الرقمي مسألة أمن وطني. وحماية الأفراد من انتهاك بياناتهم الشخصية خصوصاً مع توسع استخدام المنصات الرقمية، ويُعدّ الأمن الرقمي من القضايا المعاصرة التي تمسّ جوهر الحقوق والحريات الدستورية.

ثانياً: إشكالية البحث:

تتمثل الإشكالية الرئيسة لهذا البحث في تحديد مدى قدرة الإطار الدستوري القائم على استيعاب تحديات الأمن الرقمي، وتحقيق التوازن بين مقتضيات حماية الدولة وضمان حقوق الأفراد في الفضاء الإلكتروني، في ظل تطور سريع للتقنيات وتنوع صور الاعتداءات الرقمية. وتتفرع عن هذه الإشكالية أسئلة تتعلق بحدود التفسير الدستوري للنصوص التقليدية عند تطبيقها على وقائع رقمية مستحدثة:

١-إلى أي مدى يوفر الدستور حماية فعّالة للأمن الرقمي؟

٣-ما هو الأساس الدستوري لمفهوم الأمن الرقمي؟

٤-هل تكفي النصوص الدستورية الحالية لحمايته؟

٥-ما حدود تدخل السلطة العامة في المجال الرقمي؟

٦-كيف عالج القضاء الدستوري المقارن هذا الموضوع؟

رابعاً: أهداف البحث:

تهدف الدراسة إلى بناء تصور دستوري متكامل للأمن الرقمي يوازن بين مقتضيات حماية الدولة من التهديدات السيبرانية وضمان صون الحقوق والحريات في البيئة الرقمية، مستفيدةً من التحليل المقارن لتطوير المنظومة الدستورية الوطنية. كما تهدف الدراسة إلى ما يأتي:

١- بيان الأساس الدستوري للأمن الرقمي وتحليل مدى كفاية الحماية التي توفرها النصوص

الدستورية، مع إجراء مقارنة لاستخلاص أفضل الحلول التشريعية والقضائية.

٢- تأصيل مفهوم الأمن الرقمي دستورياً من خلال تحديد الطبيعة القانونية للأمن الرقمي.

٣- بيان علاقته بالحقوق والحريات الواردة في دستور جمهورية العراق لسنة ٢٠٠٥.

٤- تحليل نطاق الحماية الدستورية للحقوق الرقمية ومشروعية المراقبة والتقييد الإلكتروني.

٥- بيان حدود تدخل السلطة العامة في المجال الرقمي من خلال تطبيق مبدأ الشرعية.

رابعاً: منهجية البحث

يعتمد هذا البحث منهجًا تحليليًا-وصفيًا يقوم على تفكيك النصوص الدستورية ذات الصلة بالأمن الرقمي، وبيان دلالاتها في ضوء الفقه الدستوري والاتفاقيات الدولية ذات العلاقة بحماية الحقوق في الفضاء الرقمي. كما يستند إلى المنهج المقارن، من خلال استحضار بعض الاتجاهات الدولية والمعايير المرجعية في مجال الأمن الرقمي.

خامساً: خطة الدراسة:

سنقوم بالاعتماد على التقسيم الثنائي وذلك من خلال مبحثين رئيسين، ونبدأ في المبحث الأول بعنوان الإطار المفاهيمي والدستوري للأمن الرقمي، وسنقوم بتقسيم هذا المبحث إلى مطلبين:

المطلب الأول: مفهوم الأمن الرقمي وخصائصه

المطلب الثاني: الأمن الرقمي في الدستور العراقي

أما في المبحث الثاني فسنقوم بدراسة نطاق الحماية الدستورية للأمن الرقمي، وسنقوم بتقسيم هذا المبحث إلى مطلبين:

المطلب الأول: الحماية الدولية للأمن الرقمي وأثرها في تفسير النصوص الدستورية.

المطلب الثاني: الإجراءات التقنية لتعزيز أمن البيانات والمواقع الإلكترونية.

وصولاً للخاتمة والتي تتضمن أهم الاستنتاجات والتوصيات.

المبحث الأول

الإطار المفاهيمي والدستوري للأمن الرقمي

إن الإطار المفاهيمي للأمن الرقمي يرتبط بشكل اساسي بالتعريف القانوني لت لتاك الحريات من خلال تضمين المفاصل الاساسية لذلك الإطار في ضوء المفاهيم الاساسية التي تنطوي عليها وتحديد الخصائص المميزة بكونها من الحريات الاساسية للإنسان، فالحريات الرقمية على مواقع التواصل الاجتماعي وأشهرها الفيسبوك على وجه الخصوص تعد من أفضل الوسطاء للاتصال ويمكن الوصول اليها في جميع الاوقات والأماكن [١] اذ تتيح هذه المنصات الدخول المجاني مع امكانية التعبير عن الآراء وعقد المنتديات للتعبير عن الأفكار[٢].

[1] **عبدالله، أحمد، الذكاء الاصطناعي وحماية الخصوصية، دار الفكر الجامعي، الإسكندرية- مصر، ٢٠٢٣، ص ٢٣.**

[٢] **توني، حسام محمد موسى، حماية قواعد البيانات في ضوء الاتفاقيات الدولية وقانون حماية الملكية الفكرية المصري، دار النهضة العربية، القاهرة، ٢٠٢١. ص ١٢.**

وبناءً على ذلك، يتناول هذا المبحث الإطار المفاهيمي للأمن الرقمي وخصائصه، ولذلك سنقوم بتقسيم هذا المبحث إلى مطلبين، نبدأ في المطلب الأول بعنوان مفهوم الأمن الرقمي وخصائصه، أما في المطلب الثاني فسنقوم بدراسة الأمن الرقمي في الدستور العراقي.

المطلب الأول

مفهوم الأمن الرقمي وخصائصه

يتصل الأمن الرقمي اتصالًا وثيقًا بحقوق الأفراد الأساسية، إذ إن المساس بسرية البيانات أو الاتصالات قد يفضي إلى انتهاك الخصوصية، أو الإضرار بالسمعة، أو تقييد حرية التعبير، فضلًا عن تهديد الثقة في الخدمات الرقمية التي تقدمها الدولة. ومن هنا، يكتسب الأمن الرقمي بعدًا دستوريًا واضحًا، بوصفه شرطًا لازمًا لممارسة الحقوق والحريات في البيئة الرقمية، وركنًا من أركان استقرار الدولة في عصر المعلومات.

وانطلاقًا من ذلك، يتناول هذا المطلب في الفرع الأول بيان مفهوم الأمن الرقمي، وفي الفرع الثاني خصائص الأمن الرقمي وأثرها في حماية الدولة والأفراد.

الفرع الأول

تعريف الأمن الرقمي

يشكّل الأمن الرقمي أحد أبرز المفاهيم المستحدثة في الفكر القانوني المعاصر، نتيجة التحوّل العميق نحو الاعتماد على التقنيات المعلوماتية في إدارة شؤون الدولة والمجتمع. ولم يعد التعامل مع البيانات والمعلومات مسألة تقنية بحتة، بل أصبح مرتبطًا مباشرةً بحماية الحقوق والحريات، وبضمان استمرارية المرافق العامة الحيوية [٣].

بات من الضروري ضبط مفهوم الأمن الرقمي من منظور قانوني–دستوري، يراعي خصوصية الفضاء الإلكتروني وما يطرحه من مخاطر غير تقليدية. كما يقتضي الأمر التمييز بين الأمن الرقمي وغيره من المفاهيم القريبة، كأمن المعلومات والأمن السيبراني، لتحديد نطاق كل منها وحدود التداخل بينها. ولهذا سنقوم أولاً بدراسة المدخل المفاهيمي للأمن الرقمي، أما ثانياً فسنقوم بدراسة التعريف القانوني–الدستوري للأمن الرقمي، وصولاً إلى ثالثًا تمييز الأمن الرقمي عن المفاهيم القريبة.

أولًا: المدخل المفاهيمي للأمن الرقمي:

ينطلق تعريف الأمن الرقمي من إدراك أن الفضاء الإلكتروني أصبح امتدادًا طبيعيًا للحيز المادي الذي تعيش فيه الدولة والأفراد، وأن ما يجري فيه من معاملات واتصالات لا يقل أثرًا عن نظيره في العالم الواقعي. فالأمن الرقمي، في جوهره، يعبر عن حالة من الحماية الممنهجة للأنظمة المعلوماتية، والشبكات، وقواعد البيانات، والتطبيقات، من كل فعل غير مشروع يستهدف سرّيتها أو سلامتها أو توافرها .غير أن هذا التعريف التقني لا يكفي من منظور دستوري؛ إذ يتعين ربط الأمن الرقمي بمنظومة الحقوق والحريات، وبمبدأ سيادة القانون. فكل اعتداء على البيانات الشخصية،

---

[٣] شاتز، دانيال وآخرون، تعريف الأمن السيبراني، مجلة الطب الشرعي الرقمي والأمن والقانون JDFSL، جمعية الطب الشرعي الرقمي والأمن والقانون، فلوريدا، المجلد. ١٢، رقم ٢، ٢٠١٧، ص ٥٦.

أو التجسس على المراسلات الإلكترونية، أو تعطيل المنصات الرقمية العامة، ينعكس مباشرة على ممارسة الحقوق الأساسية [٤]، مثل الخصوصية، وحرية التعبير، وحق الوصول إلى المعلومات، بل وقد يمسّ الثقة في مؤسسات الدولة ذاتها .وعليه، يمكن النظر إلى الأمن الرقمي بوصفه مفهومًا مركبًا يجمع بين بعدين متلازمين: بعد تقني يتعلق بحماية البنى التحتية المعلوماتية، وبعد قانوني–دستوري يهدف إلى تنظيم تدخل السلطات العامة والجهات الخاصة في الفضاء الرقمي، بما يضمن عدم تحويل أدوات الحماية إلى وسائل للمساس بالحقوق والحريات. هذا التداخل بين البعدين هو ما يمنح الأمن الرقمي خصوصيته، ويبرر إدراجه ضمن موضوعات القانون الدستوري المعاصر.

ثانيًا: التعريف القانوني–الدستوري للأمن الرقمي:

لا يتضمن الدستور العراقي لعام ٢٠٠٥ تعريفاً صريحاً ومباشراً لمصطلح "الأمن الرقمي" أو "السيبراني" في نصوصه، لكنه يؤسس له من خلال مبادئ عامة لحماية الحقوق والحريات يركز الإطار القانوني العراقي حالياً على تطوير قوانين لمكافحة الجرائم الإلكترونية، وحماية البيانات، وضمان سرية المعلومات، ومواجهة الهجمات السيبرانية التي تهدد الأمن الوطني. حيث نصت المادة (٤٦) من الدستور العراقي على أنه: " لا يكون تقييد ممارسة أي من الحقوق والحريات الواردة في هذا الدستور أو تحديدها إلا بقانون أو بناء عليه، على ألا يمس ذل التحديد والتقييد جوهر الحق أو الحرية"[٥].

من منظور قانوني–دستوري، يمكن صياغة تعريف للأمن الرقمي على أنه: «مجموعة القواعد الدستورية والتشريعية، والسياسات العامة، والإجراءات التقنية والمؤسسية، التي تهدف إلى حماية الفضاء الرقمي للدولة، بما في ذلك البيانات والاتصالات والبنى التحتية المعلوماتية، من الأخطار والاعتداءات التي تهدد سلامتها أو سرّيتها أو توافرها، مع ضمان احترام الحقوق والحريات الأساسية للأفراد في هذا الفضاء.

.يتضمن هذا التعريف عدة عناصر جوهرية. أولها، أن الأمن الرقمي ليس مجرد إجراءات تقنية معزولة، بل هو منظومة متكاملة تستند إلى أساس دستوري يحدد حدود السلطة في مجال المراقبة، وجمع البيانات، واستخدامها. وثانيها، أن موضوع الحماية لا يقتصر على البيانات الشخصية، بل يمتد إلى الأنظمة المعلوماتية التي تدير الخدمات العامة، والاتصالات الرسمية، والمنصات التي تعتمد عليها الدولة في تسيير شؤونها. وثالثها، أن أي سياسة أو إجراء في مجال الأمن الرقمي يجب أن يخضع لمبدأ التناسب، بحيث لا تتجاوز القيود المفروضة على الحقوق والحريات ما تقتضيه الضرورة لحماية المجتمع والدولة .كما يبرز في هذا السياق دور القضاء الدستوري في رسم ملامح الأمن الرقمي، من خلال تفسير النصوص المتعلقة بالخصوصية، وحرمة

[٤] أن كل القوانين والدساتير والمواثيق تحرص على عدم جواز المساس بخصوصيته من دون حق، ومن ذلك دستور جمهورية العراق لعام 2005 فإنه يشير إشارة صريحة واضحة إلى قداسة الحق في الخصوصية لكل إنسان عراقي أسوة بالدساتير الأخرى. أشار إليه: حسين، مجباس حسين، جريمة إفشاء الأسرار والاعتداء على الحياة الخاصة، مطبعة السيماء، بغداد، العراق، ٢٠١٦، ص ٨.

[٥] المادة (٤٦) من دستور جمهورية العراق لعام ٢٠٠٥.

الاتصالات، وسيادة القانون، في ضوء الواقع الرقمي الجديد.

ثالثًا: تمييز الأمن الرقمي عن المفاهيم القريبة:

تقتضي الدقة العلمية التمييز بين الأمن الرقمي وبعض المفاهيم المتداخلة، وفي مقدمتها أمن المعلومات والأمن السيبراني. فأمن المعلومات يركّز أساسًا على حماية المعلومات، بغض النظر عن الوسيط الذي تُخزَّن أو تُنقل من خلاله، ويُعنى بضمان السرّية والسلامة والتوافر. أما الأمن السيبراني، فيتسع نطاقه ليشمل حماية الفضاء السيبراني برمّته، بما فيه من شبكات، وأجهزة، وبرمجيات، وبيانات، من الهجمات والاختراقات التي قد تنفذها جهات فردية أو جماعية أو حتى دول .في حين أن الأمن الرقمي.

يتخذ منحًى تمايز الأمن الرقمي لكونه أكثر ارتباطًا بالبناء الدستوري، إذ يركّز على تنظيم العلاقة بين الدولة والأفراد في الفضاء الرقمي، وعلى ضبط حدود تدخل السلطات العامة في مراقبة الاتصالات، وجمع البيانات، وإدارة المنصات الرقمية. فهو مفهوم يلتقي مع أمن المعلومات والأمن السيبراني في الهدف العام المتمثل في الحماية، لكنه يختلف عنهما في زاوية النظر، حيث يضع في مركز الاهتمام مسألة التوازن بين متطلبات الأمن وضمان الحقوق والحريات [٦].

إن السياسات العامة في مجال الأمن الرقمي يجب أن تُصاغ في ضوء المبادئ الدستورية، لا بوصفها مجرد استجابة تقنية لتهديدات سيبرانية. كما أن المشرّع، عند سنّ القوانين المنظمة للجرائم المعلوماتية أو لحماية البيانات الشخصية، يكون ملزمًا بمراعاة الحدود التي يرسمها الدستور، وبضمان وجود رقابة قضائية فعّالة على إجراءات المراقبة والتتبع الرقمي .وبذلك، يتضح أن تعريف الأمن الرقمي لا يقتصر على الجانب الفني، بل يمتد ليشكّل إطارًا دستوريًا ينظّم كيفية تعامل الدولة مع الفضاء الرقمي، ويضمن أن تكون حماية هذا الفضاء منسجمة مع احترام كرامة الإنسان وحقوقه الأساسية، وهو ما سيُستكمل بيانه عند تناول خصائص الأمن الرقمي وأثرها في حماية الدولة والأفراد في الفرع التالي.

الفرع الثاني

خصائص الأمن الرقمي وأثرها في حماية الدولة والأفراد

تمثّل خصائص الأمن الرقمي المدخل الأساس لفهم دوره في حماية البنية الدستورية للدولة وضمان حقوق الأفراد في الفضاء الإلكتروني. فالأمن الرقمي ليس مجرد مجموعة من الوسائل التقنية، بل هو منظومة متكاملة تتسم بسمات خاصة تميّزه عن صور الحماية التقليدية، وتجعله أكثر التصاقًا بالحقوق والحريات من أي وقت مضى .وتتجلى أهمية هذه الخصائص في كونها تحدد كيفية تصميم السياسات العامة [٧]، وصياغة التشريعات، وبناء المؤسسات المعنية بحماية الفضاء الرقمي، بما ينعكس مباشرة على استقرار الدولة وثقة الأفراد في النظام القانوني. ومن ثمّ، فإن تحليل خصائص الأمن الرقمي يتيح الكشف عن

[٦] **الحديدي، ايمن احمد، الأمن السيبرانى في ظل الانفجار المعرفي، ط١، دار اليازوردي للنشر والتوزيع، الأردن، ٢٠٢٢، ص ٤١.**

[٧] **مسكية، محمد الصغير، الفضاء السيبراني وتحديات الأمن القومي للدول، مجلة العلوم القانونية والاجتماعية، مج٧، ع٤، ٢٠٢٢، ص ٤٤٧ – ٤٦٢.**

أبعاده العميقة، وعن أثره المزدوج في حماية الدولة من جهة، وصون الأفراد من جهة أخرى.

أولًا: خصائص الأمن الرقمي المرتبطة بطبيعة الفضاء الرقمي:

أولى خصائص الأمن الرقمي أنه يتعامل مع فضاء غير مادي، متشابك، وعابر للحدود، هو الفضاء الرقمي أو السيبراني. هذا الفضاء لا يخضع للقيود الجغرافية التقليدية، ولا يمكن حصره في نطاق إقليمي ضيق، بل يمتد عبر شبكات عالمية تتداخل فيها البنى التحتية الوطنية مع منصات وخدمات عابرة للدول [٨] حيث إنَّ هذه الطبيعة اللامادية والعابرة للحدود تفرض على الأمن الرقمي أن يكون ذا طابع مرن ومتجدد، قادرًا على مواكبة التطور التقني السريع، وعلى التعامل مع تهديدات قد تنشأ خارج الإقليم الوطني، لكنها تُحدث آثارًا مباشرة داخل الدولة.

من خصائص الأمن الرقمي أنه **ديناميكي** بطبيعته، لا يستقر على صورة واحدة، بل يتطور تبعًا لتطور أدوات الهجوم والدفاع في الفضاء الرقمي .كما يتسم الأمن الرقمي بطابع **الاستمرارية**؛ إذ لا يمكن الاكتفاء بإجراءات ظرفية أو مؤقتة، لأن التهديدات الرقمية تتسم بالتكرار والتجدد، وقد تُنفّذ في أي وقت ومن أي مكان. وهذا يفرض على الدولة بناء منظومة مراقبة وحماية مستمرة، تشمل تحديث الأنظمة، وتقييم المخاطر، وتطوير القدرات البشرية والمؤسسية .إلى جانب ذلك، يتسم الأمن الرقمي بطابع **التشابك**؛ فهو لا يقتصر على قطاع واحد، بل يمسّ قطاعات متعددة: الاتصالات، المالية، الصحة، التعليم، الأمن، والخدمات العامة. هذا التشابك يجعل أي خلل في جزء من المنظومة الرقمية قادرًا على إحداث أثر متسلسل في قطاعات أخرى، وهو ما يفرض مقاربة شمولية في تصميم سياسات الأمن الرقمي.

ثانيًا: الخصائص القانونية–الدستورية للأمن الرقمي

إلى جانب الخصائص التقنية، يتميز الأمن الرقمي بجملة من السمات القانونية التي تمنحه خصوصيته في البناء الدستوري .

أول هذه السمات أنه **مرتبط جوهريًا بالحقوق والحريات الأساسية**؛ فكل إجراء يُتخذ باسم الأمن الرقمي قد يمسّ، بصورة مباشرة أو غير مباشرة، الحق في الخصوصية، وحرمة الاتصالات، وحرية التعبير، وحق الوصول إلى المعلومات. ومن ثمّ، فإن الأمن الرقمي لا يمكن أن يُفهم بمعزل عن منظومة الضمانات الدستورية التي تحكم تدخل الدولة في الحياة الخاصة للأفراد [٩].

ثانيًا، يتسم الأمن الرقمي بكونه **مجالًا لتطبيق مبدأ سيادة القانون** في صورته الحديثة؛ إذ يقتضي أن تكون جميع التدابير المتخذة في الفضاء الرقمي مستندة إلى نصوص قانونية واضحة، ومحددة، وقابلة للرقابة القضائية. فلا يجوز، في إطار دولة القانون، أن تُمارس المراقبة الرقمية أو جمع البيانات أو تتبع الاتصالات خارج إطار قانوني دقيق يحدد الشروط والقيود والضمانات .

[٨] شهيد، سنان طالب، رسم السياسة العامة للدولة العراقية في الأمن والردع السيبراني- دراسة في دستور جمهورية العراق رقم ٢٠٠٥، مجلة الكوفة للعلوم القانونية والسياسية، المجلد ١٥، العدد ٥٤، ٢٠٢٣، ص ٢٩٨.

[٩] مسكية، محمد الصغير، الفضاء السيبراني وتحديات الأمن القومي للدول، مرجع سابق، ص ٤٦١.

ثالثًا، الأمن الرقمي من مجالات التوازن الواضحة بين **السلطة والحرية؛** فهو يقوم على معادلة دقيقة تحاول التوفيق بين متطلبات حماية الدولة والمجتمع من التهديدات الرقمية، وبين ضرورة عدم تحويل هذه الحماية إلى ذريعة لانتهاك الحقوق. هذا التوازن يتجسد في مبدأ التناسب، الذي يفرض أن تكون التدابير المتخذة أقل قدر ممكن من القيود لتحقيق الهدف الأمني، وأن تخضع لرقابة فعّالة من القضاء أو الهيئات المستقلة .رابعًا، يتسم الأمن الرقمي بطابع **المؤسسية؛** إذ لا يكفي وجود نصوص قانونية، بل يجب أن تُنشأ مؤسسات متخصصة، تتمتع بالاستقلال النسبي والكفاءة الفنية، تتولى تنفيذ سياسات الأمن الرقمي في إطار من الشفافية والمساءلة. هذه المؤسسية تضمن ألا تتحول أدوات الحماية الرقمية إلى وسائل تعسفية، وتتيح في الوقت ذاته بناء خبرة تراكمية في إدارة المخاطر الرقمية.

ثالثًا: أثر خصائص الأمن الرقمي في حماية الدولة والأفراد

تنعكس خصائص الأمن الرقمي على حماية الدولة في عدة مستويات. فمن جهة، تسهم الطبيعة الشمولية والديناميكية للأمن الرقمي في تعزيز قدرة الدولة على حماية بنيتها التحتية الحيوية، مثل شبكات الكهرباء، والاتصالات، والأنظمة المالية، وقواعد البيانات السيادية، من الهجمات الرقمية التي قد تستهدف تعطيلها أو التلاعب بها. هذا البعد الوقائي يكتسب أهمية خاصة في ظل اعتماد متزايد على الأنظمة الإلكترونية في إدارة المرافق العامة .ومن جهة أخرى، يتيح الطابع المؤسسي والقانوني للأمن الرقمي للدولة أن تبني **استراتيجية وطنية متكاملة،** تستند إلى تشريعات واضحة، ومؤسسات متخصصة، وتعاون دولي في مواجهة الجرائم والهجمات الرقمية العابرة للحدود.

نستنتج أنَّ خصائص الأمن الرقمي ذات البعد الدستوري تؤدي دورًا حاسمًا في صون الحقوق والحريات .فوجود إطار قانوني واضح يحدد شروط المراقبة الرقمية، وضوابط جمع البيانات، وحقوق الأفراد في الاعتراض أو التصحيح أو المحو، يعزز الشعور بالأمان في التعامل مع المنصات والخدمات الرقمية.

المطلب الثاني
الأمن الرقمي في الدستور العراقي

يشكّل الأمن الرقمي أحد المكونات الحديثة التي باتت تتقاطع بصورة مباشرة مع البناء الدستوري في العراق، نظرًا لاتساع الاعتماد على الوسائط الإلكترونية في إدارة الشأن العام، وتزايد المخاطر الرقمية التي تستهدف الدولة والأفراد على حد سواء. وقد أفرز هذا التحوّل تحديات دستورية تتعلق بمدى كفاية النصوص القائمة لحماية الخصوصية، وضمان حرمة المراسلات الإلكترونية، وتنظيم حدود تدخل السلطات العامة في الفضاء الرقمي. كما أظهر الحاجة إلى تفسير متجدد للنصوص الدستورية التقليدية في ضوء التطورات التقنية، بما يضمن تحقيق التوازن بين متطلبات الأمن وصون الحقوق والحريات .ويكتسب هذا الموضوع أهمية خاصة في العراق، حيث يشهد البلد توسعًا في استخدام الأنظمة الرقمية الحكومية، مقابل تنامي

التهديدات السيبرانية التي تستهدف البنى التحتية الحيوية.

يتناول هذا المطلب تجليات الأمن الرقمي في الدستور العراقي من خلال فرعين، نبدأ في الفرع الأول بعنوان حماية الحق في الخصوصية وحرمة المراسلات الإلكترونية، أما في الفرع الثاني فسنقوم بدراسة مبدأ سيادة القانون وواجب الدولة في حفظ الأمن.

الفرع الأول

حماية الحق في الخصوصية وحرية المراسلات الإلكترونية

يمثّل الحق في الخصوصية وحرمة المراسلات الإلكترونية أحد أهم المرتكزات الدستورية التي تحمي الفرد في البيئة الرقمية، نظرًا لاتساع نطاق جمع البيانات وتبادل المعلومات عبر الوسائط الإلكترونية. وقد أصبح هذا الحق أكثر عرضة للانتهاك بفعل التطور التقني الذي أتاح إمكانات واسعة للمراقبة والتتبع والتخزين والتحليل. ومن ثمّ، باتت الحاجة ملحّة لإطار دستوري يضبط حدود تدخل السلطات العامة، ويضمن ألا تتحول الوسائل الرقمية إلى أدوات للمساس بالحياة الخاصة. ويكتسب هذا الموضوع أهمية خاصة في العراق، حيث يشهد الفضاء الرقمي توسعًا كبيرًا يقابله غياب تشريعات تفصيلية كافية.

أولًا: الأساس الدستوري لحماية الخصوصية وحرمة المراسلات الإلكترونية:

يشكّل الحق في الخصوصية أحد الحقوق الأساسية التي كرّستها الدساتير الحديثة، ومنها الدستور العراقي الذي نصّ في المادة (١٧) على حماية حرمة المساكن والمراسلات والاتصالات. ورغم أن النص جاء بصيغة عامة [١٠]، إلا أن مضمونه يمتد بطبيعته إلى المراسلات الإلكترونية، لأن جوهر الحماية يتعلق بصون الحياة الخاصة من التدخل غير المشروع، بغضّ النظر عن الوسيط المستخدم.

وتتجلى أهمية هذا الأساس الدستوري في أنه يضع قيدًا على السلطات العامة، فلا يجوز لها مراقبة الاتصالات أو الاطلاع على البيانات الشخصية إلا وفق شروط محددة، وبموجب قانون يحدد الحالات الاستثنائية التي تبرر هذا التدخل. كما يفرض الدستور أن تكون أي إجراءات رقابية خاضعة لرقابة قضائية فعّالة، لضمان عدم تحولها إلى وسيلة للتعسف أو المساس بحرية الأفراد.

ويُعدّ هذا الأساس الدستوري نقطة انطلاق لتفسير مدى انطباق الحماية على الوسائط الرقمية، إذ إن المراسلات الإلكترونية، بما فيها البريد الإلكتروني، وتطبيقات المحادثة، والاتصالات عبر المنصات الرقمية، أصبحت جزءًا من الحياة اليومية، ولا تختلف في طبيعتها عن المراسلات الورقية أو الهاتفية التي كانت محل حماية تقليدية.

كما أن التطور التقني أوجد تحديات جديدة، مثل جمع البيانات الوصفية، وتتبع المواقع الجغرافية، وتحليل أنماط السلوك الرقمي، وهي ممارسات قد تمسّ الخصوصية دون الاطلاع المباشر على محتوى

---

[١٠] **نصت المادة (١٧) من دستور جمهورية العراق لعام ٢٠٠٥ على أنه: " أولاً: لكل فرد الحق في الخصوصية الشخصية بما لا تنافى مع حقوق الاخرين والأداب العامة، ثانياً: حرمة المساكن مصونة، ولا يجوز دخولها أو تفتيشها أو التعرض لها إلا بقرار قضائي، وفقاً للقانون.**

المراسلات. وهذا يفرض تفسيرًا موسّعًا للنصوص الدستورية، بحيث تشمل الحماية كل ما يتعلق بالاتصالات الرقمية، سواء في محتواها أو في بياناتها المصاحبة.

ثانيًا: نطاق الحماية الدستورية للمراسلات الإلكترونية:

تتسم حماية المراسلات الإلكترونية بطابع شامل، لأنها لا تقتصر على منع الاطلاع على محتوى الرسائل، بل تمتد إلى حماية سرّية تبادلها، وضمان عدم اعتراضها أو تخزينها أو تحليلها دون سند قانوني. ويشمل نطاق الحماية عدة مستويات:

١ –حماية المحتوى الرقمي:

يشمل ذلك الرسائل النصية، البريد الإلكتروني، المحادثات عبر التطبيقات، والملفات المتبادلة. ويُعدّ أي اطلاع غير مشروع على هذا المحتوى انتهاكًا مباشرًا للحق في الخصوصية [١١].

٢ –حماية البيانات الوصفية للمراسلات:

تشمل معلومات مثل وقت الإرسال، مدة الاتصال، عنوان الـIP، الموقع الجغرافي، وهوية الأطراف المتواصلة. ورغم أنها لا تكشف المحتوى، إلا أنها قد تكشف الكثير عن نمط حياة الفرد، ما يجعل حمايتها ضرورة دستورية.

ثالثًا: التحديات الدستورية في حماية الخصوصية الرقمية وأثرها على الأفراد والدولة:

تواجه حماية الخصوصية الرقمية في العراق عدة تحديات، أبرزها غياب تشريع شامل لحماية البيانات الشخصية، وعدم وجود إطار قانوني مفصل ينظم المراقبة الرقمية. هذا الفراغ التشريعي يجعل النصوص الدستورية العامة غير كافية وحدها لمواجهة التهديدات الرقمية المعقدة، ويضع الأفراد أمام مخاطر متعددة، مثل التجسس الإلكتروني، والابتزاز، وسرقة الهوية، والتلاعب بالبيانات.

كما أن التطور التقني أوجد أدوات متقدمة للمراقبة، مثل تحليل البيانات الضخمة، وبرمجيات التجسس، وتقنيات التعرف على الوجوه، وهي أدوات قد تُستخدم دون رقابة فعّالة، ما يهدد جوهر الحق في الخصوصية. ويؤدي ذلك إلى تآكل الثقة بين المواطن والدولة، ويجعل الأفراد أكثر ترددًا في استخدام الخدمات الرقمية الحكومية.

ومن جهة أخرى، تواجه الدولة تحديًا في تحقيق التوازن بين حماية الأمن الوطني ومراعاة الحقوق الدستورية. فالتعامل مع الجرائم الإلكترونية والإرهاب الرقمي يتطلب أدوات تقنية متقدمة، لكن استخدامها دون ضوابط قد يؤدي إلى انتهاكات واسعة. ومن ثمّ، فإن بناء منظومة دستورية متكاملة لحماية الخصوصية الرقمية يسهم في تعزيز شرعية الدولة، ويمنحها القدرة على مواجهة التهديدات دون المساس بالحقوق.

كما أن حماية الخصوصية الرقمية تعزز ثقة الأفراد في البيئة الرقمية، وتشجعهم على استخدام الخدمات الإلكترونية، ما يدعم التحول الرقمي للدولة. وفي المقابل، فإن ضعف الحماية قد يؤدي إلى عزوف

[١١] أيوب، بولين انطونيوس، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، دراسة مقارنة، منشورات الحلبي، بيروت، لبنان، ٢٠٠٩، ص ١٣٢.

المواطنين عن التعامل مع المنصات الحكومية، ويعرّض البنى التحتية الرقمية لمخاطر أكبر.

نستنتج أن حماية الخصوصية وحرمة المراسلات الإلكترونية ليست مجرد حق فردي، بل هي عنصر أساسي في استقرار الدولة، وفي بناء علاقة متوازنة بين السلطة والمجتمع، وفي ترسيخ سيادة القانون في الفضاء الرقمي.

الفرع الثاني

مبدأ سيادة القانون وواجب الدولة في حفظ الأمن

يمثّل مبدأ سيادة القانون الإطار الناظم لعلاقة الدولة بالأفراد في جميع المجالات، بما فيها الفضاء الرقمي الذي أصبح جزءًا لا يتجزأ من ممارسة السلطة العامة. ويقتضي هذا المبدأ أن تُمارس الدولة صلاحياتها في حفظ الأمن ضمن حدود الدستور، وبما يضمن عدم تحول الوسائل الرقمية إلى أدوات للمساس بالحقوق والحريات. ومع توسّع التهديدات الرقمية التي تستهدف البنى التحتية والمجتمع، بات واجب الدولة في حفظ الأمن يتخذ أبعادًا جديدة تتطلب توازناً دقيقًا بين الحماية والضمانات. ومن ثمّ، فإن دراسة هذا المبدأ في سياق الأمن الرقمي تكشف عن كيفية تكيّف الدولة مع التحديات التقنية دون الإخلال بأسس الشرعية الدستورية [١٢].

أولًا: سيادة القانون كإطار ناظم للأمن الرقمي:

يُعدّ مبدأ سيادة القانون حجر الأساس في تنظيم تدخل الدولة في الفضاء الرقمي، لأنه يفرض أن تكون جميع الإجراءات الأمنية مستندة إلى قواعد قانونية واضحة، ومعلنة، وقابلة للتطبيق العام. ويعني ذلك أن الدولة لا تستطيع اتخاذ تدابير رقابية أو تقنية تمسّ الحقوق الرقمية إلا وفق قانون يحدد بدقة نطاق السلطة وشروط ممارستها، والضمانات المرافقة لها .ويكتسب هذا المبدأ أهمية خاصة في البيئة الرقمية، حيث تتوافر للدولة إمكانات واسعة للمراقبة وجمع البيانات وتحليلها بطرق قد لا تكون ممكنة في العالم المادي. ومن ثمّ، فإن سيادة القانون تمنع انزلاق السلطة نحو استخدام هذه الأدوات بصورة غير منضبطة، وتضمن أن تكون كل خطوة أمنية خاضعة لرقابة قضائية فعّالة.

ثانيًا: واجب الدولة في حفظ الأمن في البيئة الرقمية:

تتحمل الدولة واجبًا دستوريًا في حماية المجتمع من التهديدات الرقمية، سواء كانت جرائم إلكترونية، أو هجمات سيبرانية تستهدف البنى التحتية، أو محاولات اختراق للأنظمة الحكومية. ويستند هذا الواجب إلى مبدأ حماية النظام العام، وضمان استمرارية المرافق العامة، وصون الأمن الوطني .ويفرض هذا الواجب على الدولة اتخاذ تدابير متعددة، تشمل بناء قدرات تقنية متقدمة، وتطوير تشريعات حديثة، وإنشاء مؤسسات متخصصة في الأمن الرقمي. كما يتطلب التعاون مع القطاع الخاص، الذي يمتلك جزءًا كبيرًا من البنى التحتية الرقمية، ومع المجتمع الدولي لمواجهة التهديدات العابرة للحدود .غير أن هذا الواجب لا يُمارس بمعزل عن الضمانات الدستورية؛ إذ يجب أن تكون التدابير الأمنية **ضرورية ومتناسبة** مع حجم التهديد، وألا تتجاوز ما تقتضيه حماية المجتمع. فالدولة، وإن كانت مسؤولة عن حفظ الأمن، إلا أنها

---

[١٢] **صميدة، أحمد رجب سيد، *التنظيم القانوني للحق في الخصوصية المسكن، الاتصالات، البيانات الشخصية*، دار النهضة العربية، القاهرة، ٢٠٢٢، ص ٣٤.**

ملزمة في الوقت ذاته باحترام الحقوق الأساسية، وعدم استخدام الأمن الرقمي كذريعة لتوسيع سلطاتها على حساب الحريات .كما يفرض واجب حفظ الأمن على الدولة اعتماد سياسات وقائية [١٣]، لا تقتصر على مواجهة الهجمات بعد وقوعها، بل تشمل تقييم المخاطر، وتحديث الأنظمة، وتدريب الكوادر، ووضع خطط للطوارئ الرقمية. هذا البعد الوقائي يعزز قدرة الدولة على مواجهة التهديدات قبل تحولها إلى أزمات . إضافة إلى ذلك، يتطلب هذا الواجب وجود تنسيق مؤسسي بين الجهات الأمنية والقضائية والتشريعية، لضمان انسجام السياسات الرقمية مع المبادئ الدستورية، ولتجنب تضارب الاختصاصات أو تداخلها بما يضعف فعالية الحماية.

ثالثًا: التوازن بين سيادة القانون وواجب الدولة في حفظ الأمن

يمثل التوازن بين سيادة القانون وواجب الدولة في حفظ الأمن جوهر الحماية الدستورية في البيئة الرقمية. فالدولة تحتاج إلى أدوات فعّالة لمواجهة التهديدات الرقمية، لكنها في الوقت ذاته ملزمة بعدم المساس بجوهر الحقوق والحريات .يتحقق هذا التوازن من خلال عدة آليات:

- **مبدأ التناسب** :يفرض أن تكون التدابير الأمنية أقل قدر ممكن من القيود لتحقيق الهدف الأمني، وأن تُراجع دوريًا للتأكد من استمرار ضرورتها.
- **الرقابة القضائية** :تعدّ الضمانة الأهم لمنع التعسف، إذ تتيح للأفراد الطعن في الإجراءات التي تمسّ حقوقهم الرقمية، وتلزم السلطات بتقديم مبررات قانونية واضحة.
- **الشفافية والمساءلة** :تتطلب أن تُعلن الدولة عن سياساتها الرقمية، وأن تخضع مؤسسات الأمن الرقمي لرقابة برلمانية ومجتمعية، بما يعزز الثقة ويمنع الانتهاكات.
- **تحديد نطاق السلطة** :يجب أن تكون صلاحيات المراقبة الرقمية محددة بدقة، وأن تُمارس في إطار قانوني واضح يمنع التوسع غير المبرر.

نستنتج أنه يؤدي هذا التوازن إلى حماية الدولة من التهديدات الرقمية دون الإضرار بحقوق الأفراد، ويجعل الأمن الرقمي جزءًا من منظومة سيادة القانون، لا استثناءً منها. كما يعزز شرعية الدولة، ويزيد من ثقة المواطنين في البيئة الرقمية، ويضمن أن يكون التحول الرقمي قائمًا على أسس دستورية راسخة .وبذلك، يتضح أن مبدأ سيادة القانون وواجب الدولة في حفظ الأمن يشكلان إطارًا متكاملاً يضمن حماية الفضاء الرقمي، ويحقق الانسجام بين متطلبات الأمن وحقوق الأفراد، وهو ما يمهّد للانتقال إلى المبحث الثاني المتعلق بنطاق الحماية الدستورية للأمن الرقمي.

المبحث الثاني

نطاق الحماية الدستورية للأمن الرقمي

أصبح الأمن الرقمي اليوم أحد الميادين التي تتقاطع فيها اعتبارات السيادة الوطنية مع متطلبات حماية

[١٣] **الحديدي، ايمن احمد، الأمن السيبرانى في ظل الانفجار المعرفي، مرجع سابق، ص ٤١.**

الحقوق والحريات، في ظل توسّع الفضاء الإلكتروني وتزايد التهديدات العابرة للحدود. وقد فرض هذا الواقع على الدساتير الحديثة، ومنها الدستور العراقي، أن تعيد النظر في مفهوم الحماية الدستورية، بحيث لا تقتصر على المجال التقليدي، بل تمتد لتشمل البيئة الرقمية بكل ما تحمله من مخاطر وفرص. ويثير هذا التحوّل أسئلة جوهرية حول مدى قدرة النصوص الدستورية القائمة على استيعاب التحديات الرقمية، وكيفية تفسيرها بما يضمن التوازن بين مقتضيات الأمن وصون الحقوق الأساسية .كما أن التطور الدولي في مجال الأمن الرقمي، سواء من خلال الاتفاقيات أو المعايير أو التجارب المقارنة، أصبح يؤثر بصورة مباشرة في فهم نطاق الحماية الدستورية، ويقدّم نماذج يمكن الاستفادة منها في تطوير الإطار الوطني.

بناءً عليه سنقوم بتقسيم هذا المبحث إلى مطلبين، حيث نبدأ في المطلب الأول بعنوان الحماية الدولية للأمن الرقمي وأثرها في تفسير النصوص الدستورية، أما في المطلب الثاني فسنقوم بدراسة الإجراءات التقنية لتعزيز أمن البيانات والمواقع الإلكترونية.

المطلب الأول

الحماية الدولية للأمن الرقمي وأثرها في تفسير النصوص الدستورية

إن المسؤولية الدولية هي علاقة بين شخصين دوليين قوامها حدوث ضرر لشخص دولي أو أكثر نتيجة فعل عمل أو امتناع عن عمل صدر عن شخص دولي آخر. تكمن أهمية المسؤولية الدولية للأمن الرقي في القانون الدولي العام بوصفها جزءاً أساسيا من كل العلاقات الدولية القانونية، ففعالية هذا النظام تتوقف على مدى نضج قواعد المسؤولية ونموها بوصفها أداة تطور بما تكفله من ضمانات ضد التعسف، وخصوصاً فيما يتعلق بالضرر عبر الاعتداء على الأمن السيبراني[١٤].

بناءً عليه سنقوم بتقسيم هذا المطلب إلى فرعين، حيث نبدأ في الفرع الأول بعنوان الاتجاهات الدولية لتعزيز ودعم الأمن الرقمي، أما في الفرع الثاني فسنقوم بدراسة أثر القواعد الدولية في تفسير النصوص الدستورية.

الفرع الأول

الاتجاهات الدولية لتعزيز ودعم الأمن الرقمي

شهد المجتمع الدولي خلال العقدين الأخيرين تطورًا ملحوظًا في مقارباته المتعلقة بالأمن الرقمي، نتيجة تزايد الهجمات السيبرانية واتساع الاعتماد على الأنظمة الرقمية في إدارة الشأن العام والخاص. وقد دفع هذا الواقع الدول والمنظمات الدولية إلى تبني استراتيجيات ومعايير تهدف إلى تعزيز الأمن الرقمي، وضمان حماية البيانات والبنى التحتية الحيوية. وتمثل هذه الاتجاهات إطارًا مرجعيًا يمكن للدول، ومنها العراق، الاستفادة منه في تطوير سياساتها وتشريعاتها. كما تسهم في توجيه تفسير النصوص

[١٤] **الدين، احمد سيف، المسؤولية الدولية ما هيتها وآثارها وأحكامها، منشور على الموقع:** HTTPS://WWW.LEBARMY.GOV.LB/AR/CONTENT **: ، تاريخ الزيارة:٢٠٢٦/٣/٥.**

الدستورية المتعلقة بالحقوق والحريات في البيئة الرقمية.

أولًا: الإطار الدولي لحماية الأمن الرقمي:

تطوّر الإطار الدولي للأمن الرقمي عبر مجموعة من المبادرات والمعايير التي وضعتها منظمات دولية وإقليمية، مثل الأمم المتحدة، والاتحاد الأوروبي، ومنظمة التعاون الاقتصادي والتنمية. وقد ركّزت هذه المبادرات على وضع قواعد سلوك للدول في الفضاء السيبراني، وتحديد مسؤولياتها في منع الهجمات الرقمية، وحماية البنى التحتية الحيوية، وتعزيز التعاون الدولي في مواجهة الجرائم الإلكترونية

إن الأساس الحالي لشبكة الاتصالات في الفضاء السيبراني وبروتوكول التحكم بالإرسال وبروتوكول الإنترنت يعود تاريخه إلى عام ١٩٨٢، وهذا نظام اتصال قديم صمم أساساً لمجموعة صغيرة من الباحثين والأكاديميين لتبادل المعلومات فيما بينهم في بيئة منخفضة المخاطر من ناحية التعرض للانتهاك، وخطر الانتهاك يمثل صميم مشكلة تتبع الهجمات السيبرانية[١٥]، إلا إن هذه ليست المشكلة الوحيدة بل نقاط ضعف النظام تشكل صعوبات مضاعفة عندما نأخذ بنظر الاعتبار البرمجيات العديدة الموجودة حالياً.

ثانيًا: دور الاتفاقيات الدولية في تعزيز الأمن الرقمي

تلعب الاتفاقيات الدولية دورًا محوريًا في تعزيز الأمن الرقمي، لأنها تضع قواعد مشتركة للدول، وتحدد التزاماتها في حماية الفضاء الرقمي. وتساعد هذه الاتفاقيات في سد الفجوات التشريعية الوطنية، وتوفير إطار قانوني للتعاون الدولي في مواجهة التهديدات الرقمية .وتشمل هذه الاتفاقيات اتفاقيات مكافحة الجريمة المنظمة، واتفاقيات حماية حقوق الإنسان، واتفاقيات حماية البيانات، وكلها تتضمن مبادئ يمكن تطبيقها في البيئة الرقمية. فعلى سبيل المثال، تنص الاتفاقيات الدولية لحقوق الإنسان على حماية الخصوصية وحرمة المراسلات، وهي مبادئ تمتد بطبيعتها إلى الفضاء الرقمي .كما أن الاتفاقيات المتعلقة بمكافحة الإرهاب والجريمة المنظمة تفرض على الدول التزامات في مجال تبادل المعلومات، والتحقيق في الجرائم الرقمية، وتعزيز قدراتها التقنية. غير أن هذه الالتزامات يجب أن تُمارس في إطار احترام الحقوق الأساسية، وهو ما يجعل الاتفاقيات الدولية أداة لتحقيق التوازن بين الأمن والحرية .وتسهم الاتفاقيات الدولية كذلك في تعزيز التعاون بين الدول في مجال الأمن الرقمي، من خلال تبادل الخبرات، وتطوير القدرات، وتنسيق السياسات. وهذا التعاون ضروري لأن التهديدات الرقمية غالبًا ما تكون عابرة للحدود، ولا يمكن لدولة واحدة مواجهتها بمفردها.

تبقى الصكوك الدولية بحكم طبيعتها ذات نطاق جغرافي أوسع من الصكوك الإقليمية أو التشريع الوطني فيما يخص التجريم والمسائل الجنائية، كون المعاهدة تتيح المجال للتعاون بشكل مركز بشأن أنواع معينة من الجرائم، أو للنظر بعين الاعتبار إلى دواعي القلق الإقليمية، فضلاً عن النظم القانونية بمنطقة

[١٥] **ليبسون، تتبع الهجمات الإلكترونية وتعقبها: التحديات التقنية وقضايا السياسة العالمية، بحث في المركز القومي العربي، ٢٠٠٢، ص ١٤.**

محددة[١٦] . كما يمكن اعتبار اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة أساساً قانونياً للتعاون الدولي في مكافحة الجرائم الواردة في الاتفاقية، فضلاً عن الجرائم العابرة للحدود، عليه سيتم مناقشة الاتفاقيات الدولية ومدى اعتبارها كأساس قانوني لتبادل المساعدة القانونية وتسليم المجرمين [١٧].

كانت اتفاقية مكافحة الجريمة العابرة للحدود لعام ٢٠٠٠ [١٨]، من أهم التطورات القانونية التي تحققت عام ٢٠٠٠ في أروقة الأمم المتحدة، حيث كان اعتماد الجمعية العامة للأمم المتحدة اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية وبروتوكولاتها الثلاثة، وتضمنت الاتفاقية نصوصاً هامة ساهمت في بلورة مفهوم الجريمة المنظمة العابرة للحدود الوطنية [١٩].

إنَّ الاتفاقيات الدولية في أكدت على أنّ التعاون الدولي لمكافحة الجريمة يمثل احد صنوف التعاون بين الدول في علاقاتها الخارجية، وهذا ما قامت عليه معاهدة بودابست[٢٠]، ويقصد به تبادل المساعدة والعون وتضافر الجهود المشتركة بين طرفين دوليين أو أكثر لتحقيق نفع أو خدمة أو مصلحة مشتركة في مجال مواجهة التهديد الإجرامي، وما يرتبط به من مجالات أخرى، كمجال الأمن، أو تخطي مشكلات الحدود والسيادة التي قد تعترض الجهود الوطنية لملاحقة المجرمين، وتعقب مصادر التهديد، سواء كانت هذه المساعدة المتبادلة قضائية أم تشريعية أو شرطية موضوعية أم إجرائية وسواء اقتصرت على دولتين أم امتدت إقليمياً أو عالمياً، تتعدد الأسس القانونية المشتركة المؤسسة لتعاون قانوني دولي في اتفاقية بودابست لمكافحة الجرائم السيبرانية كما إنها تضمنت عدداً من المبادئ لتعاون دولي فعال وعلى النحو التالي[٢١]:

الفرع الثاني

أثر القواعد الدولية في تفسير النصوص الدستورية

أصبحت القواعد الدولية المتعلقة بالأمن الرقمي وحماية البيانات جزءًا من البيئة القانونية التي تؤثر في تفسير النصوص الدستورية، خصوصًا في الدول التي تواجه تحديات تشريعية في مواكبة التطور التقني. فالمعايير الدولية، سواء الصادرة عن الأمم المتحدة أو المنظمات الإقليمية أو الاتفاقيات متعددة الأطراف، باتت تشكّل إطارًا مرجعيًا يساعد في تحديد حدود تدخل الدولة في الفضاء الرقمي. كما أن القضاء الدستوري في العديد من الدول يستأنس بهذه القواعد عند النظر في قضايا تتعلق بالخصوصية، والمراقبة الرقمية، وحرمة الاتصالات، ما يجعلها عنصرًا مؤثرًا في تطوير الفهم الدستوري للأمن الرقمي.

أولًا: القواعد الدولية لحقوق الإنسان كأساس لتفسير الحماية الدستورية الرقمية

---

[١٦] دليل التعاون الدولي في المسائل الجنائية لمكافحة الإرهاب، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، منشورات الأمم المتحدة، نيويورك، ٢٠٠٩، ص ٢١.

[١٧] الحاملي، حسين فتحي، التعاون الدولي الأمني في تنفيذ الإحكام الجنائية، دار النهضة العربية، القاهرة، ٢٠١٤، ص ١٣٤.

[١٨] ينظر: اتفاقية مكافحة الجريمة العابرة للحدود لعام ٢٠٠٠

[١٩] أبو الوفا، أحمد، مجلس التعاون لدول الخليج العربية كمنظمة دولية، الطبعة الأولى، دار النهضة العربية، القاهرة، ٢٠٠٠، ص ٢٣٤.

[٢٠] ينظر: معاهدة بودابست لعام ٢٠٠١.

[٢١] عطا الله، إمام حسنين، جرائم تقنية المعلومات في التشريعات والصكوك العربية، دار جامعة نايف للنشر، الرياض، ٢٠١٧، ص ١٩٨.

تشكل القواعد الدولية لحقوق الإنسان، وفي مقدمتها العهد الدولي للحقوق المدنية والسياسية، الإطار الأوسع الذي تستند إليه الدول في حماية الخصوصية وحرمة الاتصالات في البيئة الرقمية. فالمادة (١٧) من العهد تحظر التدخل التعسفي أو غير المشروع في الحياة الخاصة، وهو نصّ يمتد بطبيعته إلى الفضاء الإلكتروني، لأن جوهر الحماية يتعلق بصون الفرد من المراقبة غير المبررة، بغضّ النظر عن الوسيط المستخدم .وقد أكدت لجنة حقوق الإنسان التابعة للأمم المتحدة، في تعليقاتها العامة، أن حماية الخصوصية تشمل الاتصالات الرقمية، وأن جمع البيانات على نطاق واسع يجب أن يخضع لشروط الضرورة والتناسب والرقابة القضائية. وهذا التفسير الدولي أصبح مرجعًا مهمًا للقضاء الدستوري في العديد من الدول، لأنه يقدّم معايير دقيقة لتحديد حدود تدخل الدولة في الفضاء الرقمي .كما أن الاتفاقيات الدولية المتعلقة بمكافحة الجريمة المنظمة والإرهاب تفرض على الدول التزامات في مجال التعاون الرقمي، لكنها تشدد في الوقت ذاته على ضرورة احترام حقوق الإنسان. وهذا التوازن بين الأمن والحرية يشكل قاعدة أساسية يمكن الاستناد إليها في تفسير النصوص الدستورية المتعلقة بالأمن الرقمي .وتسهم هذه القواعد الدولية في توجيه المشرّع الوطني نحو تبني تشريعات تحمي البيانات الشخصية، وتحدد شروط المراقبة الرقمية، وتضمن وجود آليات فعّالة للرقابة القضائية. كما تساعد في سد الفجوات التشريعية التي قد تعجز النصوص الدستورية العامة عن معالجتها بصورة مباشرة.

ثانيًا: المعايير الدولية لحماية البيانات وتأثيرها في تطوير الفهم الدستوري

برزت خلال السنوات الأخيرة مجموعة من المعايير الدولية المتقدمة في مجال حماية البيانات، أبرزها اللائحة العامة لحماية البيانات في الاتحاد الأوروبي (GDPR)، التي أصبحت نموذجًا عالميًا في تنظيم جمع البيانات ومعالجتها. وتقوم هذه المعايير على مبادئ أساسية، مثل الشفافية، والحد الأدنى من البيانات، والغرض المحدد، وحق الفرد في الوصول إلى بياناته وتصحيحها ومحوها .

ثالثًا: دور القضاء الدولي والمقارن في توجيه تفسير النصوص الدستورية

أصبح القضاء الدولي والمقارن أحد أهم المصادر التي يستأنس بها القضاء الدستوري عند تفسير النصوص المتعلقة بالأمن الرقمي. فقد أصدرت المحكمة الأوروبية لحقوق الإنسان أحكامًا رائدة في قضايا تتعلق بالمراقبة الرقمية، وجمع البيانات، وحرمة الاتصالات، أكدت فيها على ضرورة وجود ضمانات فعّالة، مثل الرقابة القضائية، والشفافية، وتحديد نطاق السلطة بدقة .كما أن محكمة العدل الأوروبية لعبت دورًا مهمًا في تطوير مفهوم حماية البيانات، من خلال أحكامها المتعلقة بإبطال بعض الاتفاقيات أو التشريعات التي لا توفر حماية كافية للبيانات الشخصية. وقد أثرت هذه الأحكام في العديد من الأنظمة القانونية، لأنها تقدم تفسيرًا متقدمًا لحقوق الأفراد في البيئة الرقمية .

نستنتج أنَّ تنوعت مخاطر الوسائل الرقمية على حق الحياة الخاصة بحجم التنوع التقني، وهو ما دفع

المجتمع الدولي إلى بذل المزيد من الجهود في حماية هذا الحق. تجسد ذلك بالعديد من المؤتمرات الأكاديمية المتخصصة بحقوق الإنسان والتقنية، وكان مجملها يدور حول حماية البيانات الشخصية في البيئة الرقمية بالإضافة إلى إيجاد توازن بين حق الخصوصية وحق الوصول الى المعلومات، ذلك لأن حق الخصوصية من أهم القيود التي تقيد حق الوصول الى المعلومات فتركز الجهود في اغلب الدول في العالم على حماية حق الخصوصية وحق الوصول الى المعلومات، وخلق بيئة رقمية متوازنة بين هذه الحقوق.

المطلب الثاني

الإجراءات التقنية لتعزيز أمن البيانات والمواقع الإلكترونية

إن استراتيجيات مواجهة الاختراق الرقمي تبدأ من داخل الدولة ومن صلب قوانينها الجنائية، إذ أن التشريع الجنائي مسألة ضرورية للحد من الجرائم السيبرانية، ومع ذلك توجد العديد من المشاكل تجعل التشريع الوطني وحده غير كافياً في حد ذاته ويحتاج إلى ما يدعمه من الناحية الدولية بالأخص في الجرائم العابرة للحدود الوطنية[٢٢]. حيث أنه لا يمكن التعامل مع ظاهرة الجرائم السيبرانية ما لم يكن هناك تشريعات وطنية تتعامل مع استخدام أجهزة الحاسوب وتجرم إساءة استخدامه كاتخاذه أداة للجريمة أو للتخزين البيانات غير المشروعة أو كهدف للمجرمين، إن تطوير الإجراءات التقنية لتعزيز أمن البيانات والمواقع الإلكترونية يجب أن تتسق ويتم تنسيقها مع باقي الدول، فالاتساق والمواءمة مسألة ضرورية بين البلدان في نهجها لتأطير الجرائم ومنح السلطات وتبسيط الإجراءات التحقيقية إلى حد كبير في المسائل المتبادلة وتعجيل المساعدة القانونية وتسليم المجرمين وغيرها من أشكال التعاون [٢٣].

بناءً عليه سنقوم بتقسيم هذا المطلب إلى فرعين، حيث نبدأ في الفرع الأول بعنوان التشفير الإلكتروني، أما في الفرع الثاني فسنقوم بدراسة أنظمة الكشف للحوادث الرقمية في حماية الفضاء الإلكتروني.

الفرع الأول

التشفير الإلكتروني

يمثّل التشفير الإلكتروني إحدى أهم الأدوات التقنية التي تقوم عليها منظومة الأمن الرقمي الحديثة، نظرًا لدوره المحوري في حماية البيانات والمراسلات من الوصول غير المصرح به .وقد أصبح التشفير عنصرًا أساسيًا في ضمان سرّية المعلومات وسلامتها، سواء في القطاع الحكومي أو الخاص، في ظل تزايد الهجمات الرقمية وتعقّد أساليب الاختراق .كما يشكّل التشفير وسيلة فعّالة لتحقيق التوازن بين متطلبات الأمن وحماية الخصوصية، لأنه يحدّ من قدرة أي جهة –بما فيها السلطات العامة –على الاطلاع

---

[٢٢] شوقي، محمد– وآخرون، الجرائم الإلكترونية والطب الشرعي الرقمي والسلطة القضائية، نشرته مركز ابحاث سبرينغر، ٢٠١٥، ص ٢١.

[٢٣] السنباطي، إيهاب، الترجمة الجديدة والكاملة للاتفاقية المتعلقة بالجريمة الالكترونية، بودابست عام ٢٠٠١ والبروتوكول الملحق بها، دار النهضة العربية، القاهرة، ٢٠٠٩، ص٢٨ – ٣٢.

على البيانات دون سند قانوني .ومن ثمّ، فإن دراسة التشفير الإلكتروني تعدّ مدخلًا لفهم كيفية تعزيز أمن البيانات والمواقع الإلكترونية في إطار دستوري منضبط.

أولًا :الأساس التقني للتشفير ودوره في حماية البيانات

يقوم التشفير على تحويل البيانات من صيغة قابلة للقراءة إلى صيغة مشفّرة لا يمكن فهمها إلا باستخدام مفتاح خاص، وهو ما يجعلها غير قابلة للاستغلال في حال اعتراضها أو الوصول إليها بطرق غير مشروعة .ويعتمد التشفير على خوارزميات رياضية معقدة، تتنوع بين التشفير المتماثل الذي يستخدم مفتاحًا واحدًا للتشفير وفك التشفير، والتشفير غير المتماثل الذي يعتمد على زوج من المفاتيح :أحدهما عام والآخر خاص .وتبرز أهمية التشفير في حماية البيانات أثناء انتقالها عبر الشبكات، مثل البريد الإلكتروني، والمراسلات الفورية، والمعاملات المالية، وكذلك أثناء تخزينها في قواعد البيانات أو الأجهزة المحمولة .فحتى في حال اختراق النظام أو اعتراض الاتصال، تبقى البيانات غير قابلة للاستخدام دون المفتاح الصحيح .كما يسهم التشفير في حماية سلامة البيانات، من خلال آليات التحقق من عدم التلاعب بها أثناء النقل أو التخزين، وهو ما يضمن موثوقية المعلومات ويمنع التزوير الرقمي .ويُعدّ هذا الجانب بالغ الأهمية في الأنظمة الحكومية التي تعتمد على البيانات في اتخاذ القرارات وتقديم الخدمات .إضافة إلى ذلك، يشكّل التشفير خط الدفاع الأول ضد الهجمات الرقمية التي تستهدف سرقة البيانات أو ابتزاز الأفراد والمؤسسات، مثل هجمات الفدية التي تعتمد على تشفير بيانات الضحية .وفي المقابل، فإن استخدام التشفير من قبل الجهات الشرعية يحدّ من قدرة المهاجمين على استغلال الثغرات أو الوصول إلى المعلومات الحساسة .ويكتسب التشفير أهمية خاصة في حماية البيانات الشخصية، لأنه يمنع الوصول غير المصرح به إلى المعلومات التي قد تُستخدم للإضرار بالأفراد، مثل سرقة الهوية أو التجسس أو الابتزاز .ومن ثمّ، فإن التشفير ليس مجرد أداة تقنية، بل هو عنصر أساسي في حماية الحقوق الرقمية.

ثانيًا :التشفير كضمانة للحقوق الرقمية في إطار دستوري

يمثّل التشفير الإلكتروني ضمانة أساسية للحق في الخصوصية وحرمة المراسلات، لأنه يمنع الاطلاع على محتوى الاتصالات دون إذن قانوني .وفي هذا السياق، يصبح التشفير وسيلة لتجسيد الحماية الدستورية للحقوق الرقمية، وليس مجرد تقنية محايدة . فالدساتير الحديثة، ومنها الدستور العراقي، تحمي حرمة الاتصالات والمراسلات، وهو ما يقتضي أن تكون الوسائل التقنية المستخدمة في نقل البيانات قادرة على منع أي تدخل غير مشروع .ويُعدّ التشفير الأداة الأكثر فعالية لتحقيق هذا الهدف، لأنه يضمن سرّية الاتصال حتى في حال اعتراضه. [٢٤].

كما يسهم التشفير في الحدّ من المراقبة الجماعية، التي قد تمارسها بعض الجهات الأمنية أو الشركات

[٢٤] عطا الله، إمام حسنين، جرائم تقنية المعلومات في التشريعات والصكوك العربية، مرجع سابق، ص ١٩٨.

الخاصة، لأن البيانات المشفّرة لا يمكن تحليلها أو استغلالها دون المفتاح الصحيح .وهذا يعزز مبدأ التناسب، ويمنع التوسع غير المبرر في جمع البيانات .

ثالثًا :التحديات القانونية والسياسية المرتبطة باستخدام التشفير

رغم أهمية التشفير في حماية الحقوق الرقمية، إلا أنه يثير مجموعة من التحديات القانونية والسياسية، خصوصًا فيما يتعلق بقدرة الدولة على تنفيذ واجبها في حفظ الأمن .فالتشفير القوي قد يحدّ من قدرة السلطات على الوصول إلى البيانات الضرورية للتحقيق في الجرائم أو مكافحة الإرهاب، وهو ما يثير جدلًا حول ضرورة وجود "أبواب خلفية "تسمح بفك التشفير عند الحاجة .غير أن إنشاء مثل هذه الأبواب الخلفية يشكل خطرًا كبيرًا على الأمن الرقمي، لأنها قد تُستغل من قبل جهات غير مشروعة، وتعرّض البيانات الحساسة للخطر .وقد رفضت العديد من المنظمات الدولية والخبراء هذا التوجه، لأنه يقوّض الثقة في الأنظمة الرقمية، ويضعف الحماية التقنية . كما يثير التشفير تحديات تتعلق بالمسؤولية القانونية، إذ قد تستخدمه جماعات إجرامية أو إرهابية لإخفاء أنشطتها، ما يجعل التحقيقات أكثر تعقيدًا .وهذا يفرض على الدولة تطوير قدراتها التقنية، بدلًا من إضعاف التشفير .

تواجه الدول النامية، ومنها العراق، تحديات في وضع تشريعات متوازنة تنظم استخدام التشفير، بحيث تضمن حماية الحقوق دون تعطيل قدرة الدولة على مواجهة التهديدات .ويتطلب ذلك صياغة قوانين واضحة تحدد شروط فك التشفير، والجهات المخولة بذلك، والضمانات القضائية اللازمة .كما يفرض التشفير تحديات على القطاع الخاص، الذي يجب أن يوازن بين حماية بيانات المستخدمين ومتطلبات الامتثال للقوانين الوطنية .وهذا يتطلب وجود إطار قانوني يحدد مسؤوليات الشركات، ويمنعها من استخدام التشفير كذريعة لعدم التعاون مع السلطات في الحالات المشروعة .وبذلك، يتضح أن التشفير يمثل عنصرًا أساسيًا في حماية البيانات، لكنه في الوقت ذاته يفرض تحديات تتطلب حلولًا قانونية ومؤسسية متوازنة، تضمن حماية الحقوق دون المساس بقدرة الدولة على حفظ الأمن.

الفرع الثاني

أنظمة الكشف للحوادث الرقمية في حماية الفضاء الإلكتروني

أصبحت أنظمة الكشف والاستجابة للحوادث الرقمية عنصرًا أساسيًا في منظومة الأمن الرقمي، نظرًا لتزايد الهجمات الإلكترونية وتعقّد أساليب الاختراق التي تستهدف البيانات والمواقع الإلكترونية .وتمثل هذه الأنظمة خط الدفاع الثاني بعد الإجراءات الوقائية، إذ تتيح رصد الأنشطة المشبوهة، وتحليلها، والتعامل معها في الوقت المناسب قبل أن تتحول إلى خروقات واسعة .كما تسهم في تعزيز قدرة المؤسسات على استعادة الأنظمة بعد الهجمات، وتقليل الخسائر، وضمان استمرارية العمل .ومن ثمّ، فإن دراسة هذه الأنظمة تكشف عن دورها الحيوي في حماية الفضاء الرقمي ضمن إطار دستوري يوازن بين الأمن والحقوق.

أولًا :الأساس التقني لأنظمة الكشف والاستجابة للحوادث الرقمية:

تقوم أنظمة الكشف والاستجابة للحوادث الرقمية (IDS/IPS – SIEM – EDR)على مجموعة من التقنيات التي تهدف إلى مراقبة الأنظمة والشبكات، وتحليل البيانات، واكتشاف الأنشطة غير الطبيعية التي قد تشير إلى هجوم رقمي .وتعتمد هذه الأنظمة على خوارزميات متقدمة، تشمل التحليل السلوكي، والتعلم الآلي، ومقارنة الأنماط، لتحديد التهديدات المحتملة بدقة عالية .وتبدأ هذه الأنظمة بمرحلة **جمع البيانات** من مصادر متعددة، مثل سجلات الخوادم، وحركة الشبكة، وسلوك المستخدمين، ثم تنتقل إلى مرحلة **التحليل** التي تهدف إلى تحديد الأنشطة غير المعتادة، مثل محاولات تسجيل الدخول المتكررة، أو نقل كميات كبيرة من البيانات، أو تشغيل برمجيات غير معروفة .كما تعتمد هذه الأنظمة على **قواعد معرفة مسبقة** تتضمن أنماطًا للهجمات المعروفة، مثل هجمات الحرمان من الخدمة، أو محاولات الحقن البرمجي، أو البرمجيات الخبيثة .وفي حال اكتشاف نشاط مشبوه، تقوم الأنظمة بإطلاق **تنبيه فوري**، أو اتخاذ إجراءات تلقائية مثل عزل الجهاز المصاب، أو حظر الاتصال المشبوه، أو إيقاف الخدمة مؤقتًا . وتتميز أنظمة الكشف والاستجابة بقدرتها على **تحليل الحوادث بعد وقوعها**، من خلال تتبع مسار الهجوم، وتحديد الثغرات التي استغلها المهاجمون، وتقديم تقارير تساعد في تحسين السياسات الأمنية .وهذا الجانب التحليلي يجعلها جزءًا أساسيًا من عملية التعلم المستمر في الأمن الرقمي .كما تسهم هذه الأنظمة في **تعزيز استمرارية العمل**، لأنها تقلل من زمن اكتشاف الهجمات، وتحدّ من انتشارها، وتساعد في استعادة الأنظمة بسرعة .وفي ظل الاعتماد المتزايد على الخدمات الرقمية، يصبح هذا الدور بالغ الأهمية لحماية المؤسسات الحكومية والخاصة .وبذلك، تشكل أنظمة الكشف والاستجابة للحوادث الرقمية بنية تقنية متقدمة، لا تقتصر على الرصد، بل تشمل التحليل، والتفاعل، والتعلم، وهو ما يجعلها عنصرًا محوريًا في حماية البيانات والمواقع الإلكترونية [٢٥].

ثانيًا :الدور الدستوري لهذه الأنظمة في حماية الحقوق الرقمية

تؤدي أنظمة الكشف والاستجابة للحوادث الرقمية دورًا مهمًا في حماية الحقوق الرقمية، لأنها تمنع الوصول غير المشروع إلى البيانات، وتحافظ على سرّية المعلومات وسلامتها .وهذا الدور يتقاطع مع الحماية الدستورية للخصوصية وحرمة الاتصالات، لأن أي اختراق للأنظمة الرقمية قد يؤدي إلى كشف بيانات حساسة أو التلاعب بها .وتسهم هذه الأنظمة في **منع الانتهاكات الرقمية** التي قد يتعرض لها الأفراد، مثل سرقة الهوية، أو التجسس على المراسلات، أو التلاعب بالملفات الشخصية .ومن ثمّ، فإن وجودها يعزز قدرة الدولة على حماية الحقوق الأساسية في البيئة الرقمية، ويجعل الأمن الرقمي جزءًا من منظومة الحقوق الدستورية .كما تساعد هذه الأنظمة في **ضبط حدود تدخل الدولة** في الفضاء الرقمي، لأنها توفر أدوات دقيقة لرصد الهجمات دون الحاجة إلى مراقبة

[٢٥] الظاهر، أحمد عبد، حماية البيانات الشخصية في العصر الرقمي، دار النهضة العربية، القاهرة، ٢٠٢٠، ص ٤٣.

شاملة أو جمع بيانات واسعة .[٢٦] وهذا يعزز مبدأ التناسب، ويمنع التوسع غير المبرر في المراقبة . إضافة إلى ذلك، تتيح هذه الأنظمة **إثبات الحوادث الرقمية** بطريقة موثوقة، من خلال سجلات دقيقة يمكن استخدامها في التحقيقات القضائية .وهذا يعزز مبدأ سيادة القانون، ويضمن أن تكون الإجراءات الأمنية خاضعة للرقابة القضائية .وتسهم هذه الأنظمة كذلك في **تعزيز الثقة في الخدمات الرقمية الحكومية،** لأن الأفراد يشعرون بالأمان عند استخدام المنصات الإلكترونية التي تعتمد على آليات فعّالة للكشف عن الهجمات والاستجابة لها .وهذا يشجع على التحول الرقمي، ويعزز العلاقة بين المواطن والدولة .وبذلك، يتضح أن أنظمة الكشف والاستجابة للحوادث الرقمية ليست مجرد أدوات تقنية، بل هي جزء من منظومة الحماية الدستورية التي تضمن الأمن والحرية في الفضاء الرقمي.

نستنتج أنه رغم أهمية أنظمة الكشف والاستجابة، إلا أنها تواجه تحديات قانونية ومؤسسية تتعلق بحدود استخدامها، ومسؤوليات الجهات المشغّلة لها، وضمان عدم تحولها إلى أدوات للمراقبة غير المشروعة .أول هذه التحديات يتعلق بـ حماية الخصوصية، لأن هذه الأنظمة تعتمد على جمع وتحليل كميات كبيرة من البيانات، بعضها قد يكون ذا طابع شخصي .وهذا يفرض ضرورة وجود إطار قانوني يحدد بدقة نوع البيانات التي يمكن جمعها، ومدة الاحتفاظ بها، والجهات المخولة بالاطلاع عليها.

الخاتمة

أظهر البحث أن الحماية الدستورية للأمن الرقمي أصبحت ضرورة لا يمكن الاستغناء عنها في ظل التحول الرقمي المتسارع وتزايد التهديدات السيبرانية. وقد بيّن التحليل أن الأمن الرقمي ليس مجرد إجراءات تقنية، بل هو منظومة دستورية متكاملة تقوم على حماية الخصوصية، وضبط حدود تدخل الدولة، وتعزيز سيادة القانون في الفضاء الإلكتروني. كما كشف البحث عن تأثير الاتجاهات الدولية في تطوير الفهم الدستوري للأمن الرقمي، وعن أهمية الإجراءات التقنية في حماية البيانات والمواقع الإلكترونية. وبذلك، يتضح أن بناء إطار دستوري فعّال للأمن الرقمي يمثل شرطًا أساسيًا لاستقرار الدولة وصون حقوق الأفراد.

الاستنتاجات

١. أظهر البحث أن الأمن الرقمي أصبح جزءًا أصيلًا من منظومة الأمن الشامل للدولة، وأن أي خلل في حماية الفضاء الإلكتروني قد يؤدي إلى اضطراب في المرافق العامة وتهديد للسيادة الوطنية. كما تبين أن التهديدات الرقمية تتجاوز الحدود التقليدية، ما يجعل الأمن الرقمي مسؤولية دستورية تتطلب إطارًا قانونيًا واضحًا. ويؤكد ذلك ضرورة إدماج الأمن الرقمي في السياسات الوطنية.

[٢٦] **الشكري، عادل يوسف عبد النبي، الجريمة المعلوماتية وأزمة الشرعية مجلة مركز دراسات الكوفة، النجف الاشرف، المجلد ١، الإصدار ٧، ٢٠٠٨، ص ٤٥.**

٢. بيّن البحث أن الخصوصية الرقمية وحرمة المراسلات الإلكترونية تمثلان حقوقًا دستورية يجب حمايتها في البيئة الرقمية بنفس القدر الذي تُحمى فيه في العالم المادي. وقد اتضح أن غياب تشريعات تفصيلية في العراق يضعف هذه الحماية، ويجعل الأفراد عرضة للانتهاكات. كما أظهر التحليل ضرورة تفسير النصوص الدستورية تفسيرًا موسّعًا يشمل الاتصالات الرقمية.

٣. كشف البحث أن مبدأ سيادة القانون يشكل الإطار الناظم لتدخل الدولة في الفضاء الرقمي، وأن أي إجراءات أمنية يجب أن تكون مستندة إلى قانون واضح، وخاضعة لرقابة قضائية فعّالة. كما تبين أن التوازن بين الأمن والحرية لا يتحقق إلا من خلال تطبيق مبدأ التناسب، وتحديد نطاق السلطة بدقة. وهذا يعزز شرعية الدولة ويحمي الحقوق.

٤. أظهر التحليل أن الاتجاهات الدولية، سواء في مجال حقوق الإنسان أو حماية البيانات أو مكافحة الجرائم الإلكترونية، أصبحت تؤثر بصورة مباشرة في تفسير النصوص الدستورية المتعلقة بالأمن الرقمي. كما تبين أن القضاء المقارن والدولي يقدم نماذج متقدمة يمكن الاستفادة منها في تطوير الفهم الوطني. وهذا يعزز انسجام التشريعات مع المعايير العالمية.

التوصيات

١. ضرورة إصدار تشريع وطني شامل لحماية البيانات الشخصية، يحدد بوضوح حقوق الأفراد، وواجبات الجهات العامة والخاصة، وآليات جمع البيانات ومعالجتها. ويجب أن يتضمن هذا التشريع ضمانات فعّالة للرقابة القضائية، وإجراءات واضحة للشكوى والانتصاف. كما ينبغي أن يستند إلى المعايير الدولية الحديثة.

٢. تطوير إطار قانوني ينظم المراقبة الرقمية، ويحدد شروطها وحدودها، ويضمن خضوعها لرقابة قضائية مسبقة. ويجب أن يتضمن هذا الإطار قواعد دقيقة تمنع المراقبة الجماعية، وتفرض مبدأ التناسب والضرورة. كما ينبغي أن يضمن حماية البيانات الوصفية للمراسلات، وليس المحتوى فقط.

٣. إنشاء هيئة وطنية مستقلة للأمن الرقمي وحماية البيانات، تتمتع بصلاحيات رقابية وتنظيمية، وتعمل على مراقبة الامتثال للمعايير القانونية والتقنية. ويجب أن تكون هذه الهيئة مستقلة عن السلطة التنفيذية لضمان حياديتها. كما ينبغي أن تتولى نشر الوعي الرقمي لدى المواطنين.

٤. تعزيز التعاون الدولي في مجال الأمن الرقمي، من خلال الانضمام إلى الاتفاقيات الدولية ذات الصلة، وتبادل الخبرات، وتطوير القدرات الوطنية. ويجب أن يشمل هذا التعاون مكافحة الجرائم الإلكترونية، وحماية البنى التحتية الحيوية، وتطوير آليات

الاستجابة للحوادث الرقمية. كما ينبغي الاستفادة من التجارب المقارنة.

قائمة المراجع والمصادر

أولاً: الكتب:

١. **أبو الوفا أحمد،** مجلس التعاون لدول الخليج العربية كمنظمة دولية، الطبعة الأولى، دار النهضة العربية، القاهرة، ٢٠٠٠.

٢. **صميدة ، أحمد رجب سيد** ، التنظيم القانوني للحق في الخصوصية المسكن، الاتصالات، البيانات الشخصية، دار النهضة العربية، القاهرة، ٢٠٢٢.

٣. **الظاهر، أحمد عبد،** حماية البيانات الشخصية في العصر الرقمي، دار النهضة العربية، القاهرة، ٢٠٢٠.

٤. **عطا الله، إمام حسنين،** جرائم تقنية المعلومات في التشريعات والصكوك العربية، دار جامعة نايف للنشر، الرياض، ٢٠١٧.

٥. **عبدالله، أحمد،** الذكاء الاصطناعي وحماية الخصوصية، دار الفكر الجامعي، الإسكندرية– مصر، ٢٠٢٣.

٦. **الحديدى ، ايمن احمد** ، الأمن السيبرانى في ظل الانفجار المعرفي، ط١، دار اليازوردي للنشر والتوزيع، الأردن، ٢٠٢٢.

٧. **السنباطي، إيهاب،** الترجمة الجديدة والكاملة للاتفاقية المتعلقة بالجريمة الالكترونية، بودابست عام ٢٠٠١ والبروتوكول الملحق بها، دار النهضة العربية، القاهرة، ٢٠٠٩.

٨. **أيوب، بولين انطونيوس** ، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، دراسة مقارنة، منشورات الحلبي، بيروت، لبنان، ٢٠٠٩.

٩. **توني ، حسام محمد موسى** ، حماية قواعد البيانات في ضوء الاتفاقيات الدولية وقانون حماية الملكية الفكرية المصري، دار النهضة العربية، القاهرة، ٢٠٢١.

١٠. **الحاملي، حسين فتحي** ، التعاون الدولي الأمني في تنفيذ الإحكام الجنائية، دار النهضة العربية، القاهرة، ٢٠١٤.

١١. **حسين مجباس حسين،** جريمة إفشاء الأسرار والاعتداء على الحياة الخاصة، مطبعة السيماء، بغداد، العراق، ٢٠١٦.

ثانياً: المجلات والدوريات:

١. **شاتز ، دانيال وآخرون،** تعريف الأمن السيبراني، مجلة الطب الشرعي الرقمي والأمن والقانون JDFSL، جمعية الطب الشرعي الرقمي والأمن والقانون، فلوريدا، المجلد. ١٢، رقم ٢، ٢٠١٧.

٢. **شهيد ، سنان طالب** ، رسم السياسة العامة للدولة العراقية في الأمن والردع السيبراني– دراسة في دستور جمهورية العراق رقم ٢٠٠٥، مجلة الكوفة للعلوم القانونية والسياسية، المجلد ١٥، العدد ٥٤، ٢٠٢٣.

٣. **الشكري ، عادل يوسف عبد النبي** ، الجريمة المعلوماتية وأزمة الشرعية مجلة مركز

دراسات الكوفة، النجف الاشرف، المجلد ١، الإصدار ٧، ٢٠٠٨.

٤. **ليبسون،** تتبع الهجمات الإلكترونية وتعقبها: التحديات التقنية وقضايا السياسة العالمية، بحث في المركز القومي العربي، ٢٠٠٢.

٥. **مسيكة ، محمد الصغير** ، الفضاء السيبراني وتحديات الأمن القومي للدول، مجلة العلوم القانونية والاجتماعية، مج٧، ع٤، ٢٠٢٢.

٦. **شوقي ، محمد وآخرون،** الجرائم الإلكترونية والطب الشرعي الرقمي والسلطة القضائية، نشرته مركز ابحاث سبرينغر، ٢٠١٥.

ثالثاً: الدساتير:

دستور جمهورية العراق لعام 2005

رابعاً: الاتفاقيات الدولية:

١. اتفاقية مكافحة الجريمة العابرة للحدود لعام ٢٠٠٠

٢. معاهدة بودابست لعام ٢٠٠١.

خامساً: المواقع الإلكترونية:

١. الدين احمد سيف ، المسؤولية الدولية ما هيتها وآثارها وأحكامها، منشور على الموقع:

HTTPS://WWW.LEBARMY.GOV.LB/AR/CONT.ENT