الأمن السيبراني كأحد متطلبات الأمن الدستوري دِراسة في ضمانات الدولة الحديثة

م.م. حسام سعد جاسم الزاملي

جامعة القاسم الخضراء

Email : hsamalzamly813@gmail.com

الملخص

يتناول هذا البحث موضوع العلاقة بين الأمن السيبراني والأمن الدستوري في ظل التحول الرقمي المتسارع الذي تشهده الدول الحديثة، وما يرافقه من تزايد ملحوظ في التهديدات والجرائم الإلكترونية التي تستهدف الأفراد والمؤسسات والبنى التحتية الحيوية للدولة. ويهدف البحث إلى بيان الإطار المفاهيمي لكلّ من الأمن السيبراني والأمن الدستوري، وتحليل أوجه الترابط والتكامل بينهما، مع تسليط الضوء على الضمانات التي تعتمدها الدولة لتحقيق ما يمكن تسميته بـ "الأمن السيبراني الدستوري".

وقد اعتمد البحث المنهج التحليلي الوصفي من خلال دراسة المفاهيم القانونية ذات الصلة وخلص البحث إلى أن تحقيق الأمن السيبراني لا يقتصر على الجوانب التقنية فحسب، بل يتطلب إطارًا قانونيًا وتشريعيًا متكاملًا، ومؤسسات متخصصة، وضمانات فعالة توازن بين متطلبات الأمن وحماية الحقوق والحريات. وأكد البحث أهمية التعاون الدولي في مواجهة الجرائم السيبرانية ذات الطابع العابر للحدود، وضرورة تحديث التشريعات الوطنية بما ينسجم مع التطورات التكنولوجية المتلاحقة.

الكلمات المفتاحية : الأمن السيبراني، الأمن الدستوري، ضمانات الدولة، الإطار الدستوري.

Cybersecurity as a Requirement of Constitutional Security: A Study on State Guarantees in the Modern State

Assist. Lect. Hussam Saad Jassim Al-Zamly
Al-Qasim Green University
Email : hsamalzamly813@gmail.com

Abstract

This research addresses the relationship between cybersecurity and constitutional security in light of the rapid digital transformation taking place in modern states, accompanied by a significant increase in cyber threats and crimes targeting individuals, institutions, and critical state infrastructure.

The study aims to clarify the conceptual framework of both cybersecurity and constitutional security, analyze their interrelationship and integration, and highlight the safeguards adopted by the state to achieve what may be termed "constitutional cybersecurity."

The research adopts a descriptive-analytical approach through the examination of relevant legal concepts. It concludes that achieving cybersecurity is not limited to technical aspects alone, but requires a comprehensive legal and legislative framework, specialized institutions, and effective safeguards that strike a balance between security requirements and the protection of rights and freedoms.

The study also emphasizes the importance of international cooperation in combating transnational cybercrime, as well as the necessity of continuously updating national legislation to keep pace with rapid technological developments.

Keywords: Cybersecurity, Constitutional Security , State Guarantees , Constitutional Framework.

المقدمة

يشهد العالم المعاصر تطورًا متسارعًا في مجال تكنولوجيا المعلومات والاتصالات، الأمر الذي أدى إلى انتقال العديد من الأنشطة الحكومية والاقتصادية والاجتماعية إلى الفضاء الرقمي. وقد أسهم هذا التحول في تعزيز كفاءة المؤسسات وتسهيل تقديم الخدمات العامة، إلا أنه في المقابل أوجد تحديات جديدة تمثلت في تنامي التهديدات السيبرانية التي تستهدف البنى التحتية الحيوية للدولة، والأنظمة الحكومية، والبيانات الوطنية، مما جعل الأمن السيبراني من القضايا الأساسية المرتبطة باستقرار الدولة وحماية مصالحها العليا.

ولم يعدّ مفهوم الأمن الدستوري مقتصرًا على حماية النظام السياسي أو ضمان احترام أحكام الدستور فحسب، بل امتد ليشمل حماية المقومات الأساسية التي تقوم عليها الدولة الحديثة، وفي مقدمتها الفضاء الرقمي الذي أصبح جزءًا لا يتجزأ من الأمن الوطني. فالهجمات السيبرانية قد تؤدي إلى تعطيل مؤسسات الدولة، وانتهاك الحقوق والحريات الدستورية للأفراد، وتهديد السيادة الوطنية، وهو ما يفرض على الدولة تبني منظومة قانونية ومؤسساتية فعالة لضمان الأمن السيبراني باعتباره أحد المتطلبات الجوهرية للأمن الدستوري.

ومن هذا المنطلق، تأتي هذه الدراسة لبحث العلاقة بين الأمن السيبراني والأمن الدستوري، وبيان الدور الذي تؤديه الدولة الحديثة في توفير الضمانات القانونية والمؤسساتية والتقنية الكفيلة بحماية الفضاء السيبراني، بما يسهم في تعزيز الاستقرار الدستوري وصون الحقوق والحريات وتحقيق الأمن الوطني الشامل.

أهمية البحث

تتجلى أهمية هذا البحث في عدة جوانب، أهمها:

١. إبراز أهمية الأمن السيبراني باعتباره أحد المرتكزات الحديثة للأمن الدستوري في ظل التحول الرقمي المتسارع .
٢. بيان أثر التهديدات السيبرانية على استقرار الدولة ومؤسساتها الدستورية وعلى ممارسة الحقوق والحريات العامة .

٣. تسليط الضوء على دور الدولة الحديثة في بناء منظومة متكاملة لحماية الأمن السيبراني من خلال التشريعات والسياسات العامة والمؤسسات المختصة .
٤. المساهمة في إثراء الدراسات القانونية والدستورية المتعلقة بالأمن السيبراني بوصفه موضوعًا حديثًا ومتجددًا.
٥. تقديم رؤية قانونية تساعد صناع القرار والمشرعين على تطوير الأطر التشريعية اللازمة لمواجهة المخاطر السيبرانية وتعزيز الأمن الوطني .

مشكلة البحث

تتمثل مشكلة البحث في أن التطور التكنولوجي المتسارع وما رافقه من توسع في الاعتماد على الأنظمة الرقمية قد أوجد تهديدات سيبرانية متزايدة قادرة على التأثير في أمن الدولة واستقرارها الدستوري، في وقت ما زالت فيه العديد من التشريعات والضمانات القانونية غير قادرة على مواكبة حجم هذه التحديات.

أهداف البحث

يسعى هذا البحث إلى تحقيق الأهداف الآتية:

١. بيان مفهوم الأمن السيبراني وتحديد أبعاده القانونية والدستورية .
٢. توضيح مفهوم الأمن الدستوري وبيان عناصره ومقوماته الأساسية .
٣. تحليل العلاقة بين الأمن السيبراني والأمن الدستوري في الدولة الحديثة .
٤. دراسة التهديدات السيبرانية وآثارها على استقرار المؤسسات الدستورية والحقوق والحريات العامة .
٥. التعرف على الضمانات القانونية والدستورية والمؤسساتية التي توفرها الدولة الحديثة لتحقيق الأمن السيبراني .
٦. تقييم مدى فاعلية التشريعات والسياسات المعتمدة في مواجهة المخاطر السيبرانية .
٧. تقديم مجموعة من النتائج والتوصيات التي تسهم في تعزيز الأمن السيبراني بوصفه أحد متطلبات الأمن الدستوري وضمانة لاستقرار الدولة الحديثة.

المبحث الأوّل: الإطار المفاهيمي للأمن السيبراني والأمن الدستوري

أفرز التطور التكنولوجي المتسارع، ولا سيما في مجال تقنيات المعلومات والاتصالات، تحديات قانونية ودستورية غير مسبوقة، فرضت على الدول إعادة النظر في مفاهيمها التقليدية للأمن بمختلف صوره. فلم يعدّ الأمن مقتصرًا على حماية الحدود الإقليمية أو مواجهة التهديدات العسكرية، بل امتد ليشمل الفضاء السيبراني الذي أصبح يشكل أحد أهم ميادين الصراع والتأثير في العصر الحديث. وفي هذا السياق، برز مفهوم الأمن السيبراني بوصفه أحد المرتكزات الأساسية لحماية البنى التحتية الرقمية، وضمان استمرارية عمل مؤسسات الدولة، وصون مصالح الأفراد والمجتمع من المخاطر الناجمة عن الهجمات الإلكترونية.

ويمثل الأمن الدستوري في المقابل الأساس الذي يقوم عليه استقرار الدولة الحديثة، باعتباره الضمانة الفعلية لاحترام الدستور وحماية الشرعية الدستورية، وصيانة الحقوق والحريات العامة، ومنع الانحراف في استعمال السلطة. ويكتسب هذا المفهوم أهمية خاصة في ظل التحولات الرقمية الراهنة، حيث باتت التهديدات السيبرانية قادرة على المساس المباشر بالمؤسسات الدستورية، والعمليات الديمقراطية، والنظام القانوني برمته، الأمر الذي يجعل من الأمن السيبراني عاملًا مؤثرًا في تحقيق الأمن الدستوري ذاته.

وانطلاقًا من ذلك، يهدف هذا المبحث إلى وضع إطار مفاهيمي واضح لكل من الأمن السيبراني والأمن الدستوري، من خلال بيان ماهية كل منهما، وتحديد خصائصهما وأبعادهما، بما يسهم في توضيح الأساس النظري الذي يقوم عليه البحث، ويمهد لتحليل العلاقة التفاعلية بين هذين المفهومين في المباحث اللاحقة، في ضوء متطلبات الدولة الحديثة وسيادة القانون.

المطلب الأوّل: مفهوم الأمن السيبراني وخصائصه

إن الجريمة السيبرانية – أي السيبرانية– شكل متطور من أشكال الجريمة عبر الوطنية. وتزايد ضلوع جماعات الجريمة المنظمة يزيد من تفاقم الطابع المعقد لهذه جريمة، التي تحدث في مجال الفضاء الإلكتروني الذي لا حدود له. ويمكن لمرتكبي الجرائم السيبرانية وضحاياهم أن يتواجدوا في مناطق مختلفة، ويمكن أن تتمد آثار الجريمة عبر المجتمعات في جميع أنحاء العالم، مما يبرز الحاجة إلى وضع استجابة عاجلة وديناميكية ودولية.

تتكون الجريمة السيبرانية من كلمتين: الجريمة والإنترنت. لذلك دعونا نبدأ بتعريف الجريمة لغويّا. أولًا: تظهر الجريمة في اللغة بمعنيين: الأول: الذنب. نقول جرائم وجرائم، وبمعنى ما، ارتكبت جريمة. الثاني: الجريمة، كما يقولون: "إنها جريمة في حقهم وهم جريمة في حقهم". » » ارتكب جريمة، وارتكب جريمة إذا كانت جريمته خطيرة، أي إذا كان مذنبا.[1]

تعريف السيبرانية في اللغة : كما تطرقنا سابقا بأن هي كلمة إنجليزية ، "ولقد عَّرف قاموس أكسفورد كلمة
سيبراني، أو Cyber، بأنها صفة ألي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي[٢].

يُعدّ الأمن السيبراني من المفاهيم الحديثة التي برزت نتيجة الاعتماد المتزايد على الفضاء الرقمي في إدارة شؤون الدولة وتسيير المرافق العامة وتبادل المعلومات. وقد أدى هذا التحول الرقمي إلى نشوء مخاطر وتهديدات جديدة تستهدف الأنظمة المعلوماتية والبنى التحتية الرقمية، الأمر الذي فرض على الدول ضرورة إرساء إطار قانوني ومؤسساتي متكامل يضمن حماية هذا الفضاء الحيوي. ومن هنا، أصبح الأمن السيبراني أحد المكونات الأساسية للأمن الوطني بمفهومه الشامل.

ويُقصد بالأمن السيبراني، في معناه العام، مجموعة التدابير والإجراءات الفنية والتنظيمية والقانونية التي تهدف إلى حماية الشبكات الإلكترونية، ونظم المعلومات، وقواعد البيانات، من الاختراق أو التلاعب أو التعطيل أو الاستخدام غير المشروع[٣]. ولا يقتصر هذا المفهوم على الجانب التقني فحسب، بل يمتد ليشمل الأبعاد القانونية والاستراتيجية المرتبطة بحماية مصالح الدولة والمجتمع والأفراد في البيئة الرقمية.

ومن الناحية القانونية، يُعرّف الأمن السيبراني بأنه حالة الحماية التي تكفل سرية المعلومات وسلامتها وتوافرها، وتضمن استمرارية عمل الأنظمة الإلكترونية العامة والخاصة، بما يحول دون المساس بالنظام العام أو تعريض الحقوق الأساسية للأفراد للخطر[٤]. ويُلاحظ أن هذا التعريف يُبرز الصلة الوثيقة بين الأمن السيبراني وسيادة القانون، إذ إن أي خلل في أمن الفضاء السيبراني قد يؤدي إلى انتهاك حقوق دستورية، مثل الحق في الخصوصية وحماية البيانات الشخصية.

ويتسم الأمن السيبراني بعدة خصائص تميّزه عن صور الأمن التقليدية. من أبرز هذه الخصائص الطابع العابر للحدود، حيث إن الهجمات السيبرانية غالبًا ما تنطلق من خارج الإقليم الوطني للدولة، مما يحدّ من فاعلية مبدأ الإقليمية في القانون، ويستلزم تعاونًا دوليًا وتشريعات منسجمة لمواجهتها[٥]. و يتميز الأمن السيبراني بالديناميكية والتغير المستمر، نظرًا للتطور السريع في وسائل الهجوم والدفاع الإلكتروني، الأمر الذي يفرض على المشرّع مواكبة هذا التطور من خلال تحديث القوانين والأنظمة ذات الصلة[٦]

ومن خصائص الأمن السيبراني كذلك ارتباطه الوثيق بالحقوق والحريات العامة، إذ إن الإجراءات المتخذة لتحقيقه قد تمس مباشرة حرية التعبير، وحرية الاتصال، والحق في الخصوصية. ولذلك، يشترط أن تُمارس تدابير الأمن السيبراني في إطار من الشرعية القانونية، وبما يحقق التوازن بين متطلبات الأمن وحماية الحقوق الدستورية، تفاديًا لتحول هذه التدابير إلى أداة للمساس بالحريات

العامة[٧]، وعليه، يمكن القول إن الأمن السيبراني لم يعدّ مجرد مسألة تقنية أو إدارية، بل أصبح مفهومًا قانونيًا ذا أبعاد دستورية، يفرض على الدولة الحديثة تبني سياسات وتشريعات تضمن حماية الفضاء الرقمي، وفي الوقت ذاته تحترم المبادئ الدستورية وسيادة القانون.

الفرع الأول: ماهية الأمن السيبراني وتعريفه القانوني

يُعد الأمن السيبراني من المفاهيم القانونية الحديثة التي برزت نتيجة التطور المتسارع في تقنيات المعلومات والاتصالات، وما رافقه من انتقال العديد من أنشطة الدولة والأفراد إلى الفضاء الإلكتروني. وقد أدى هذا التحول إلى نشوء مخاطر رقمية تهدد سلامة البيانات والمعلومات والبنى التحتية التقنية، الأمر الذي استدعى تدخل المشرّع والفقه القانوني لوضع إطار مفاهيمي وقانوني ينظم حماية هذا المجال الحيوي.

ويُقصد بالأمن السيبراني، في معناه العام، حماية الفضاء الإلكتروني بكافة مكوناته من نظم وشبكات ومعلومات من أي أفعال غير مشروعة تهدف إلى الاختراق أو التعطيل أو التلاعب أو الاستغلال غير القانوني.[٨] ولا يقتصر هذا المفهوم على الجانب التقني البحت، بل يمتد ليشمل الأبعاد القانونية والتنظيمية والمؤسساتية المرتبطة بحماية النظام العام في صورته الرقمية.

أما من الناحية القانونية، فيُعرَّف الأمن السيبراني بأنه مجموعة القواعد والإجراءات التي تهدف إلى ضمان سرية المعلومات وسلامتها وتوافرها، وتأمين استمرارية عمل الأنظمة الإلكترونية، بما يحول دون المساس بالمصالح العامة أو الخاصة، ويمنع الإضرار بأمن الدولة واستقرارها[٩]. ويُلاحظ أن هذا التعريف يربط الأمن السيبراني بمفهوم الأمن الوطني الشامل، باعتباره أحد مظاهر حماية السيادة في العصر الرقمي.

ويؤكد جانب من الفقه القانوني العربي أن الأمن السيبراني لم يعدّ مسألة تقنية فحسب، بل أصبح جزءًا من السياسة العامة للدولة، وأحد متطلبات حماية المرافق العامة والمؤسسات الدستورية من التهديدات المستحدثة.[١٠] كما يُعد الأمن السيبراني أداة وقائية تهدف إلى منع وقوع الاعتداءات الرقمية قبل حدوثها، من خلال تبني تشريعات ملائمة وبناء قدرات مؤسساتية متخصصة.

وعليه، فإن تحديد مفهوم الأمن السيبراني على نحو دقيق يسهم في رسم حدود التدخل القانوني للدولة في الفضاء الرقمي، ويحول دون التعسف في استعمال السلطة تحت ذريعة تحقيق الأمن، بما يضمن التوازن بين متطلبات الحماية الأمنية واحترام الحقوق والحريات الأساسية.

الفرع الثاني: خصائص الأمن السيبراني وأبعاده القانونية

يتميّز الأمن السيبراني بعدد من الخصائص التي تجعله مختلفًا عن صور الأمن التقليدية، سواء من حيث طبيعة المخاطر أو وسائل المواجهة القانونية. فالمخاطر السيبرانية تتسم بعدم المادية،

إذ تقع الاعتداءات على بيانات ومعلومات رقمية لا وجود ماديًا لها، الأمر الذي يثير إشكالات قانونية تتعلق بالإثبات وتحديد المسؤولية الجنائية أو المدنية عن الأفعال المرتكبة في الفضاء الإلكتروني(١١). وإن من أبرز خصائص الأمن السيبراني الطابع العابر للحدود، حيث إن الجرائم والهجمات السيبرانية غالبًا ما تُرتكب من خارج الإقليم الوطني للدولة، مما يحدّ من فاعلية مبدأ الإقليمية التقليدي، ويستدعي تطوير قواعد الاختصاص القضائي والتعاون الدولي لمواجهتها. ويؤكد الفقه القانوني العربي أن هذه الخاصية تفرض على الدولة تبني تشريعات مرنة تتلاءم مع طبيعة الجرائم الإلكترونية المتغير(١٢).

ويتسم الأمن السيبراني بالديناميكية والتطور المستمر، نظرًا للتقدم السريع في تقنيات المعلومات وأساليب الاختراق الإلكتروني، وهو ما يجعل القواعد القانونية الجامدة غير قادرة على الإحاطة بجميع صور الاعتداءات الرقمية. لذلك، يقتضي الأمر اعتماد سياسة تشريعية قائمة على التحديث المستمر والوقاية المسبقة، بدل الاكتفاء بالمعالجة اللاحقة للجرائم السيبرانية(١٣).

ويرتبط الأمن السيبراني ارتباطًا وثيقًا بالحقوق والحريات العامة، ولا سيما الحق في الخصوصية وحماية البيانات الشخصية وحرية الاتصال. فالتدابير الأمنية المتخذة في هذا المجال قد تؤدي، إذا لم تُقيد بضوابط قانونية واضحة، إلى المساس بهذه الحقوق. ومن ثم، يشترط أن تُمارس إجراءات الأمن السيبراني في إطار من المشروعية، وبما يحقق التوازن بين متطلبات الأمن واحترام الضمانات الدستورية(١٤).

ويُضاف إلى ذلك أن الأمن السيبراني يتسم بالطابع الوقائي، إذ لا يقتصر دوره على مواجهة الاعتداءات بعد وقوعها، بل يمتد ليشمل اتخاذ تدابير استباقية تحول دون حدوثها، من خلال سن التشريعات الوقائية، وإنشاء هيئات متخصصة، ونشر الوعي القانوني والتقني في المجتمع(١٥).

المطلب الثاني: مفهوم الأمن الدستوري وأبعاده

أصبح الأمن الدستوري في ظل التطورات الحديثة من المفاهيم الجوهرية التي تضمن استقرار الدولة وحماية النظام السياسي والقانوني، إذ يهدف إلى صون المبادئ الدستورية الأساسية، وضمان حماية الحقوق والحريات العامة، وتحقيق التوازن بين السلطات. ويتضح من دراستنا أن الأمن الدستوري يشمل مجموعة من الضمانات القانونية والمؤسساتية التي تقي الدولة من الانحراف في تطبيق الدستور أو انتهاكه(١٦). وأن تعزيز الأمن الدستوري يساهم في تعزيز ثقة المواطنين بالمؤسسات، وحماية النظام الديمقراطي، والحفاظ على سيادة القانون.

الفرع الأوّل: ماهية الأمن الدستوري وتعريفه

يمثلُ الأمن الدستوري الركيزة الأساسية لاستقرار الدولة الحديثة، ويقصد به حالة حماية الدستور واحترام أحكامه وضمان عدم انتهاك المبادئ الدستورية من قبل السلطات العامة أو الأفراد. ويعرّف

الفقه الأمن الدستوري بأنه مجموعة الضمانات القانونية والمؤسساتية التي تكفل حماية المبادئ الدستورية الأساسية، وصون الحقوق والحريات العامة، وضمان الفصل بين السلطات، ومنع الانحراف في استعمال السلطة(١٧).

ويؤكد بعض الباحثين أن الأمن الدستوري لا يقتصر على النصوص الدستورية المكتوبة، بل يشمل أيضًا الآليات العملية والضمانات القضائية والمؤسساتية، مثل المحاكم الدستورية والمجالس الرقابية، التي تكفل الرقابة على دستورية القوانين والقرارات الإدارية(١٨). كما يشمل الأمن الدستوري حماية النظام السياسي من أي تهديدات داخلية أو خارجية قد تعرّض استقرار الدولة للمخاطر.

الفرع الثاني: أبعاد الأمن الدستوري

يتسم الأمن الدستوري بأبعاد متعددة تتكامل لضمان حماية الدولة واستقرار مؤسساتها وصون الحقوق والحريات الأساسية للأفراد. ويُعد البعد القانوني من أبرز هذه الأبعاد، حيث يرتكز على احترام الدستور وسموه على القوانين الأخرى، وضمان التزام جميع السلطات التنفيذية والتشريعية والقضائية بأحكامه، بما يعزز الاستقرار القانوني ويحد من التجاوزات والانتهاكات(١٩). ويتجلى البعد المؤسساتي في وجود هيئات مستقلة، مثل المحاكم الدستورية والمجالس الرقابية، المكلفة بمراقبة تطبيق الدستور وضمان نزاهة العملية التشريعية والإدارية، ومنع أي انحراف في استعمال السلطة، مما يضمن فعالية الضمانات الدستورية ويعزز الثقة بمؤسسات الدولة(٢٠).

ويمتد البعد الحقوقي للأمن الدستوري ليشمل حماية الحقوق والحريات الأساسية للأفراد، مثل حرية التعبير وحرية الرأي والحق في الخصوصية، وضمان عدم المساس بهذه الحقوق إلا وفق ما يجيزه الدستور، وبما يحقق التوازن بين حماية الدولة وحماية الأفراد(٢١). كما يشمل الأمن الدستوري بعدًا سياسيًا، يتمثل في تعزيز الاستقرار السياسي ومنع الفوضى أو الانقلابات على النظام القائم، بما يضمن استمرار الدولة واستقرار مؤسساتها، ويُحافظ على العملية الديمقراطية في الدولة الحديثة(٢٢). ويلاحظ أن هذه الأبعاد ليست منفصلة، بل تتفاعل مع بعضها البعض، بحيث يؤدي أي قصور في أحدها إلى تأثيرات سلبية على الأبعاد الأخرى، ما يجعل الأمن الدستوري منظومة متكاملة لا يمكن تحقيقها إلا بتضافر الجوانب القانونية والمؤسساتية والحقوقية والسياسية(٢٣).

المبحث الثاني: العلاقة بين الأمن السيبراني والأمن الدستوري

أصبح من الضروري دراسة العلاقة بين الأمن السيبراني والأمن الدستوري مع التطور السريع للتكنولوجيا الرقمية والاعتماد المتزايد على الفضاء السيبراني في إدارة شؤون الدولة، إذ لم يعدّ الأمن السيبراني مجرد مسألة تقنية، بل أصبح جزءًا لا يتجزأ من منظومة الأمن الوطني والحماية الدستورية. فالتهديدات السيبرانية يمكن أن تؤثر مباشرة على استقرار المؤسسات الدستورية، وتتعرض معها الحقوق

والحريات الأساسية للأفراد، وهو ما يفرض على الدولة وضع سياسات وقوانين متكاملة تضمن حماية البنى التحتية الرقمية، في إطار احترام المبادئ الدستورية والحقوق العامة.

وينقسم هذا المبحث إلى مطلبين رئيسين: الأول يركز على الأمن السيبراني كجزء من منظومة الأمن الدستوري، والثاني يبحث انعكاسات التهديدات السيبرانية على الحقوق الدستورية.

المطلب الأول: الأمن السيبراني كجزء من منظومة الأمن الدستوري

أصبح الأمن السيبراني يشكل عنصرًا جوهريًا في منظومة الأمن الدستوري مع توسع استخدام التقنيات الرقمية والاعتماد المتزايد على الفضاء السيبراني في إدارة شؤون الدولة، إذ لم يعدّ الأمن السيبراني مجرد حماية للبنية التحتية الرقمية، بل أصبح جزءًا من آليات حماية المؤسسات الدستورية وضمان استمرار عملها بشكل سليم، بما يحقق سيادة القانون ويحمي الحقوق والحريات العامة للمواطنين[٢٤].

ويظهر أهمية دراسة الأمن السيبراني ضمن الإطار الدستوري من خلال تأثيره المباشر على استقرار الدولة، حيث يمكن للتهديدات الإلكترونية أن تعطل عمل المؤسسات التشريعية والقضائية والإدارية، أو أن تعرض بيانات المواطنين وحرياتهم الأساسية للمساس. ومن هذا المنطلق، يهدف هذا المطلب إلى توضيح دور الأمن السيبراني كجزء لا يتجزأ من الأمن الدستوري، من خلال تحليل دوره في حماية المؤسسات الدستورية، والتكامل بين الأبعاد التقنية والقانونية لضمان احترام المبادئ الدستورية[٢٥]

ويسعى المطلب إلى إبراز كيف يمكن للأمن السيبراني أن يكون أداة فعالة في صون النظام الدستوري، وضمان استقرار الدولة في مواجهة التهديدات الرقمية الحديثة، مع مراعاة التوازن بين حماية الأمن والحفاظ على الحقوق والحريات الأساسية[٢٦]

الفرع الأوّل: دور الأمن السيبراني في حماية المؤسسات الدستورية

يعتبر الأمن السيبراني اليوم أحد الركائز الأساسية في منظومة الأمن الدستوري، إذ يهدف إلى حماية المؤسسات الحكومية والهيئات الدستورية من الهجمات والاختراقات الرقمية التي قد تعطل عملها أو تضر باستقلاليتها. فالمؤسسات الدستورية، مثل البرلمان والمحاكم والهيئات الرقابية، أصبحت تعتمد بشكل متزايد على نظم المعلومات والشبكات الإلكترونية لإدارة أعمالها واتخاذ القرارات، وهو ما يجعل حماية هذه الأنظمة الرقمية جزءًا لا يتجزأ من حماية الأمن الدستوري[٢٧].

ويشير الفقه القانوني إلى أن الأمن السيبراني لا يقتصر على الجانب التقني فحسب، بل يشمل وضع قواعد وسياسات قانونية وتنظيمية تضمن سلامة البيانات والمعلومات وحماية البنية التحتية الرقمية. كما يسهم تفعيل الأمن السيبراني في تعزيز الثقة بين الدولة والمواطن، إذ يطمئن الأفراد إلى أن بياناتهم ومعلوماتهم محمية وفق إطار دستوري واضح[٢٨].

الفرع الثاني: تكامل الأمن السيبراني مع الضمانات الدستورية

يمثل دمج الأمن السيبراني ضمن منظومة الأمن الدستوري ضرورة ملحة لضمان حماية شاملة للحقوق والحريات الأساسية، وكذلك لحماية سير عمل المؤسسات الدستورية. فالأمن السيبراني لم يعد مجرد أداة لحماية البيانات التقنية، بل أصبح جزءًا من الضمانات القانونية التي تضمن عدم المساس بسيادة الدولة واستقلالية مؤسساتها، وتمنع الانحراف في تطبيق القوانين والإجراءات الدستورية(٢٩).

ويشمل التكامل بين الأمن السيبراني والضمانات الدستورية وضع سياسات متقدمة لتأمين المعلومات الرسمية والحساسة، سواء كانت بيانات انتخابية، أو سجلات قضائية، أو مراسلات حكومية، بما يضمن عدم تعرضها للاختراق أو التلاعب. كما يرتبط الأمن السيبراني بمفهوم الشفافية والمساءلة، حيث يجب أن تكون الإجراءات الأمنية مصممة بحيث تتيح رقابة مؤسساتية مستقلة على تطبيقها، بما يوازن بين حماية الأمن وصون الحقوق والحريات(٣٠).

ومن الجوانب المهمة أيضًا في هذا التكامل الاعتماد على تقنيات حديثة مثل التشفير، والأنظمة الذكية لرصد الهجمات الإلكترونية، وحماية الشبكات الحكومية من الفيروسات أو محاولات القرصنة، بما يضمن استمرار عمل المؤسسات الدستورية بشكل طبيعي. كما يشمل ذلك تدريب الكوادر البشرية على كيفية التعامل مع التهديدات السيبرانية، وتطوير آليات قانونية لملاحقة المخالفين إلكترونيًا وفق ضوابط دستورية(٣١).

ويؤكد الفقه القانوني أن نجاح منظومة الأمن السيبراني في حماية المؤسسات الدستورية يعتمد على الجمع بين الجانب القانوني والتقني والإداري، بحيث يكون كل إجراء أمني مؤطرًا قانونيًا ويخضع لرقابة دستورية، وهو ما يعكس فهمًا حديثًا للأمن الدستوري الذي يشمل حماية الفضاء الرقمي، واستمرارية عمل الدولة، وضمان الحقوق والحريات الأساسية للمواطنين(٣٢).

المطلب الثاني: انعكاسات التهديدات السيبرانية على الحقوق الدستورية

أدى التطور التكنولوجي المتسارع والاعتماد المتزايد على الأنظمة الرقمية في مختلف مجالات الحياة إلى ظهور تحديات جديدة أمام الدول الحديثة، كان من أبرزها التهديدات السيبرانية التي أصبحت تشكل خطراً حقيقياً على الحقوق والحريات الدستورية للأفراد. فالهجمات الإلكترونية لم تعد تستهدف الجوانب التقنية فقط، بل أصبحت وسيلة يمكن من خلالها المساس بحقوق أساسية كفلها الدستور، مثل الحق في الخصوصية، وحرية التعبير، والحق في الحصول على المعلومات، فضلاً عن الحقوق السياسية المرتبطة بالمشاركة في الحياة العامة(٣٣).

ويُعدّ الحق في الخصوصية من أكثر الحقوق الدستورية عرضة للانتهاك نتيجة التهديدات السيبرانية، إذ تتيح وسائل الاختراق الإلكتروني والتجسس الرقمي الوصول غير المشروع إلى البيانات

الشخصية للأفراد، بما في ذلك المراسلات الإلكترونية والمعلومات المالية والصحية وغيرها من البيانات ذات الطابع الشخصي. وقد أدرك المشرع الدستوري العراقي أهمية هذا الحق، فنص في المادة (١٧/أولاً) من دستور جمهورية العراق لسنة ٢٠٠٥ على أن: «لكل فرد الحق في الخصوصية الشخصية بما لا يتنافى مع حقوق الآخرين والآداب العامة»، كما أكدت المادة ذاتها في فقرتها الثانية حرمة المراسلات البريدية والبرقية والهاتفية والإلكترونية وعدم جواز مراقبتها أو الكشف عنها إلا لضرورة قانونية وبقرار قضائي.[٣٤] ومن ثم فإن أي اعتداء سيبراني يؤدي إلى اختراق البيانات أو تسريبها يمثل انتهاكًا مباشرًا لهذه الحماية الدستورية.

وتنعكس التهديدات السيبرانية بصورة واضحة على حرية التعبير والرأي، إذ أصبحت شبكة الإنترنت ومنصات التواصل الاجتماعي الوسيلة الأكثر انتشاراً لممارسة هذا الحق. إلا أن انتشار الهجمات الإلكترونية وحملات التضليل الرقمي واختراق الحسابات الشخصية قد يؤدي إلى تقييد قدرة الأفراد على التعبير عن آرائهم بحرية أو نشر المعلومات بصورة آمنة. وتزداد خطورة هذه الممارسات عندما تُستخدم التقنيات الرقمية لنشر الأخبار الكاذبة أو التلاعب بالمحتوى الإعلامي بهدف التأثير في الرأي العام وتوجيهه نحو مواقف معينة. وفي هذا الإطار نصت المادة (٣٨) من الدستور العراقي على ضمان الدولة لحرية التعبير عن الرأي بكل الوسائل، وحرية الصحافة والطباعة والإعلان والإعلام والنشر، الأمر الذي يفرض على الدولة واجب حماية البيئة الرقمية من الممارسات التي تهدد ممارسة هذه الحرية بصورة سليمة[٣٥].

ومن جانب آخر، تؤثر التهديدات السيبرانية في الحق في الوصول إلى المعلومات والخدمات العامة، ولا سيما بعد اتجاه الحكومات إلى اعتماد الإدارة الإلكترونية وتقديم الخدمات عبر الوسائل الرقمية. فاستهداف المواقع الحكومية أو قواعد البيانات العامة بهجمات إلكترونية قد يؤدي إلى تعطيل الخدمات الأساسية وحرمان المواطنين من الحصول على المعلومات أو إنجاز معاملاتهم بصورة طبيعية. كما أن الهجمات التي تستهدف المؤسسات الصحية أو التعليمية أو المالية قد تترتب عليها أضرار مباشرة تمس حياة الأفراد ومصالحهم الأساسية، وهو ما يجعل حماية البنية التحتية الرقمية جزءاً من مسؤولية الدولة في كفالة الحقوق الدستورية وضمان استمرارية المرافق العامة[٣٦].

ولا تقتصر آثار التهديدات السيبرانية على الحقوق الفردية فحسب، بل تمتد إلى الحقوق السياسية التي تشكل أساس النظام الديمقراطي. فمع تطور الوسائل التقنية المستخدمة في إدارة الانتخابات وحفظ بيانات الناخبين، أصبحت الأنظمة الانتخابية هدفًا محتملًا للهجمات الإلكترونية التي قد تسعى إلى التلاعب بالبيانات أو التأثير في نزاهة العملية الانتخابية. ويكتسب هذا الأمر أهمية خاصة في ضوء ما نصت عليه المادة (٢٠) من دستور جمهورية العراق لسنة ٢٠٠٥ من أن «للمواطنين رجالاً ونساءً حق المشاركة في الشؤون العامة والتمتع بالحقوق السياسية بما فيها حق التصويت والانتخاب والترشيح». ومن ثم فإن أي تهديد سيبراني يستهدف هذه الأنظمة قد يؤدي إلى المساس بالإرادة الشعبية وإضعاف الثقة بالمؤسسات الدستورية[٣٧].

وتأسيساً على ما تقدم، فإن مواجهة التهديدات السيبرانية لم تعد مجرد مسألة تقنية أو أمنية، وإنما أصبحت ضرورة دستورية لحماية الحقوق والحريات العامة وصيانة مقومات الدولة الحديثة. فكلما ازدادت قدرة الدولة على تأمين فضائها السيبراني وتعزيز الحماية القانونية والتقنية للبيانات والأنظمة الإلكترونية، ازدادت قدرتها على ضمان التمتع الفعلي بالحقوق الدستورية في البيئة الرقمية، وتحقيق التوازن بين متطلبات الأمن الوطني واحترام الحريات الأساسية للأفراد.[٣٨]

المبحث الثالث: ضمانات الدولة الحديثة في تحقيق الأمن السيبراني الدستوري

بات لزامًا على الدولة الحديثة وضع منظومة متكاملة من الضمانات لحماية الأمن السيبراني ضمن إطار دستوري واضح. مع تزايد الاعتماد على الفضاء السيبراني في إدارة شؤون الدولة والمؤسسات العامة، وتوسع التهديدات الرقمية التي قد تمس استقرار الدولة والحقوق والحريات الأساسية، فالأمن السيبراني لم يعد مجرد أداة تقنية، بل أصبح ركيزة أساسية من ركائز الأمن الدستوري، يتطلب تضافر الجوانب القانونية والتقنية والمؤسساتية لضمان حماية البيانات، وصون الحقوق، والحفاظ على استقرار المؤسسات الدستورية[٣٩]

ويهدف هذا المبحث إلى دراسة الضمانات التي تضعها الدولة الحديثة لتحقيق الأمن السيبراني الدستوري، سواء على المستوى التشريعي والمؤسساتي، أو على المستوى التقني والتعاون الدولي. فوجود هذه الضمانات لا يقتصر على الوقاية من الاختراقات والاعتداءات الرقمية فحسب، بل يشمل أيضًا وضع آليات قانونية واضحة تُحافظ على المبادئ الدستورية وتوازن بين حماية الأمن وحماية الحقوق والحريات[٤٠].

ويسلط هذا المبحث الضوء على الدور الحيوي للتشريعات الحديثة، والمؤسسات المتخصصة، والبنية التحتية التقنية، والتعاون الدولي في مواجهة التهديدات السيبرانية، مع الأخذ بعين الاعتبار المستجدات التكنولوجية المتسارعة، التي تتطلب تحديثًا مستمرًا للسياسات والإجراءات لضمان فاعلية الأمن السيبراني في حماية النظام الدستوري[٤١].

المطلب الأوّل: الضمانات التشريعية والمؤسساتية

تعدّ الضمانات التشريعية والمؤسساتية من الركائز الأساسية التي تضعها الدولة الحديثة لتحقيق الأمن السيبراني ضمن إطار دستوري متين. فالأمن السيبراني لا يقتصر على حماية الشبكات والبنى التحتية التقنية، بل يمتد ليشمل حماية الحقوق والحريات الأساسية، واستقرار المؤسسات الدستورية، واستمرارية عمل الدولة. ومن هذا المنطلق، فإن وضع تشريعات واضحة، وإنشاء مؤسسات متخصصة، وتهيئة بيئة قانونية وإدارية متكاملة يُعد ضرورة لحماية الفضاء الرقمي من التهديدات السيبرانية المختلفة[٤٢].

ويهدف هذا المطلب إلى دراسة الضمانات التشريعية والمؤسساتية التي تضعها الدولة الحديثة لمواجهة التهديدات الرقمية وحماية النظام الدستوري. و يسلط الضوء على دور القوانين، والهيئات الرقابية، والمراكز المتخصصة في حماية المعلومات، ومتابعة تنفيذ الإجراءات الأمنية، بما يعزز قدرة الدولة على حماية نفسها وحماية حقوق الأفراد(٤٣).

ومن أهم هذه الضمانات في العراق قانون الجرائم الإلكترونية رقم ١٦٠ لسنة ٢٠١٩، الذي يعالج الجرائم الإلكترونية ويحدد إجراءات الحماية، ويُلزم المؤسسات الحكومية بحماية بياناتها واتخاذ التدابير الوقائية لمنع الاختراقات، مع وجود عقوبات رادعة ضد المخالفين.(٤٤) كما ينص القانون على إنشاء وحدات متخصصة داخل الوزارات لمراقبة الأمن السيبراني وضمان تطبيق اللوائح الوطنية، بما يعزز استقرار النظام الدستوري.

وفي السياق المقارن، أكدت قوانين الأردن رقم ١٣ لسنة ٢٠١٥ بشأن حماية المعلومات والبيانات على ضرورة وضع ضوابط واضحة لحماية المعلومات الشخصية والحكومية، وتوفير آليات قانونية لمساءلة المخالفين، كما نصّت على إنشاء هيئات مختصة للإشراف على تنفيذ هذه الضمانات(٤٥). أما في مصر، فقد نص قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ على حماية البنية التحتية الرقمية ومكافحة الاختراقات الإلكترونية، مع وضع تدابير لضمان احترام الحقوق والحريات العامة ضمن حدود الدستور(٤٦).

ويشير الفقه القانوني إلى أن فعالية الضمانات التشريعية لا تقتصر على إصدار النصوص القانونية، بل تشمل تحديثها بشكل مستمر لمواكبة التطورات التقنية الحديثة، مثل التشفير المتقدم، وإنترنت الأشياء، والذكاء الاصطناعي، والتي قد تفتح المجال أمام تهديدات سيبرانية جديدة. كما يُعد تضمين الضمانات القانونية لمبادئ حماية البيانات والخصوصية جزءًا أساسيًا من التوازن بين حماية الدولة وحماية الحقوق الدستورية للأفراد(٤٧).

وتعزز الضمانات التشريعية التكامل مع الضمانات المؤسساتية، بحيث تتيح القوانين تأسيس هيئات متخصصة لمراقبة تطبيقها، مع تفعيل آليات رقابية مستقلة لضمان الالتزام بالمعايير الدستورية، وتحقيق الأمن السيبراني بشكل متكامل ومستدام(٤٨).

الفرع الأوّل: الضمانات التشريعية

تتمثل الضمانات التشريعية في مجموعة من القوانين واللوائح التي تنظم الفضاء السيبراني، وتحدد مسؤوليات المؤسسات العامة، وحقوق الأفراد، والجزاءات المقررة ضد المخالفين. وتشمل هذه التشريعات قوانين حماية البيانات، وقوانين الجرائم الإلكترونية، وقوانين حماية البنية التحتية الرقمية، بحيث تحدد الأطر القانونية للتعامل مع الهجمات السيبرانية، وتضمن حماية الحقوق والحريات العامة(٤٩).

ويؤكد الفقه القانوني أن فاعلية هذه الضمانات تعتمد على وضوح النصوص القانونية، وشموليتها لجميع أنواع التهديدات الرقمية، وتحديثها بشكل دوري لمواكبة التطورات التقنية المستمرة. كما يجب أن تراعي هذه التشريعات مبادئ الدستور، بحيث يتم تحقيق التوازن بين حماية الأمن وحماية الحقوق والحريات(٥٠).

الفرع الثاني: الضمانات المؤسساتية

تشكل الضمانات المؤسساتية جزءًا أساسيًا من منظومة الدولة الحديثة في حماية الأمن السيبراني ضمن الإطار الدستوري، إذ تهدف إلى ضمان استمرارية عمل المؤسسات الحكومية، وحماية البيانات والمعلومات الرسمية، وتأمين حقوق المواطنين ضمن الحدود الدستورية. وتشمل هذه الضمانات إنشاء هيئات متخصصة للإشراف على الأمن السيبراني، مثل مراكز الاستجابة للطوارئ السيبرانية(CERTs) ، واللجان الرقابية على المعلومات الحكومية، وهيئات حماية البيانات الشخصية، إضافة إلى هيئات وطنية لمكافحة الجرائم الإلكترونية(٥١).

ويعتمد نجاح هذه الضمانات على وضع أطر قانونية واضحة تنظم مهام هذه الهيئات وصلاحياتها، وتحدد مسؤوليات كل جهة حكومية في حماية المعلومات والبنية التحتية الرقمية. فعلى سبيل المثال، ينص قانون الجرائم الإلكترونية العراقي رقم ١٦٠ لسنة ٢٠١٩ على مسؤولية المؤسسات الحكومية عن حماية بياناتها، وتطبيق الإجراءات الوقائية لمنع الاختراقات الرقمية(٥٢). وأكدت القوانين المقارنة في الأردن ومصر على إنشاء هيئات مستقلة للأمن الرقمي، ووضع لوائح تنظيمية لحماية البيانات، بما يضمن التوازن بين حماية الأمن وحماية الحقوق والحريات(٥٣).

وتشمل الضمانات المؤسساتية أيضًا تطوير الكفاءات البشرية والتقنية من خلال برامج تدريب مستمرة للكوادر الأمنية، وإنشاء مختبرات ومحاكاة لمواجهة الهجمات السيبرانية، واستخدام الأنظمة الذكية لرصد التهديدات وتحليلها بشكل فوري. و تُعزز هذه المؤسسات التعاون الدولي مع المنظمات العالمية المعنية بالأمن السيبراني، مثل الاتحاد الدولي للاتصالات (ITU) والمنظمة الأوروبية للأمن السيبراني (ENISA)، لضمان تحديث السياسات الأمنية بما يتوافق مع المعايير الدولية(٥٤).

ومن الناحية القانونية، تعتبر استقلالية هذه المؤسسات عن التدخلات السياسية عاملًا حاسمًا في فاعلية الضمانات المؤسساتية، إذ إن وجود سلطة قضائية أو إشراف برلماني على الإجراءات المتخذة يضمن احترام المبادئ الدستورية، ومنع الانتهاكات لحقوق المواطنين، كما يتيح التدقيق في استخدام البيانات الشخصية ومراقبة تطبيق اللوائح الأمني(٥٥). ويشير الفقه القانوني إلى أن الدمج بين الضمانات المؤسساتية والتشريعية يُمثل خط الدفا ع الأول للدولة ضد التهديدات السيبرانية، ويحقق الأمن الدستوري الرقمي بشكل متكامل ومستدام(٥٦).

المطلب الثاني: الضمانات التقنية والتعاون الدولي

لم تعدّ الضمانات التشريعية والمؤسساتية وحدها كافية لحماية الأمن السيبراني ضمن الإطار الدستوري مع ازدياد الهجمات السيبرانية وتطور أساليبها بشكل سريع، بل أصبح من الضروري اعتماد ضمانات تقنية حديثة، تشمل أدوات وأنظمة مبتكرة للتصدي للاختراقات وحماية البنية التحتية الرقمية. وتشمل هذه الضمانات شبكات الحماية، التشفير، أنظمة كشف الاختراقات، والمراقبة المستمرة للشبكات، بما يضمن صون الحقوق والحريات الدستورية للأفراد واستمرارية عمل المؤسسات الحكومية(٥٧).

ويكمل هذا الجانب الضمانات التشريعية والمؤسساتية من خلال التعاون الدولي، إذ أصبح الأمن السيبراني قضية عابرة للحدود، تتطلب تبادل المعلومات، والخبرات، والتنسيق بين الدول لمواجهة التهديدات العابرة للحدود. ومن أبرز الأمثلة على ذلك، التزامات الدول بموجب اتفاقيات مثل اتفاقية بودابست لمكافحة الجرائم الإلكترونية لعام ٢٠٠١، التي تحدد إطارًا قانونيًا للتعاون الدولي في مكافحة الجرائم الرقمية، وتضع معايير لحماية البيانات والخصوصية(٥٨).

على المستوى الوطني، تنصّ بعض القوانين على استخدام الأنظمة التقنية الحديثة لتعزيز الأمن الرقمي، مثل قانون الجرائم الإلكترونية العراقي رقم ١٦٠ لسنة ٢٠١٩، الذي يتيح للجهات الحكومية المختصة استخدام الوسائل التقنية لمكافحة الاختراقات، ومراقبة الشبكات الحكومية (٥٩) ويشدد القانون على ضرورة حماية البيانات الشخصية للمواطنين وضمان عدم انتهاك الخصوصية، بما يتوافق مع المبادئ الدستورية.

ويهدف هذا المطلب إلى دراسة الضمانات التقنية التي تضعها الدولة الحديثة لحماية الفضاء الرقمي، ودور التعاون الدولي في تعزيز قدرة الدولة على مواجهة التهديدات السيبرانية، مع التركيز على أهمية تكامل الجوانب التقنية مع الأطر القانونية والمؤسساتية لتحقيق الأمن السيبراني الدستوري بشكل فعّال(٦٠).

الفرع الأوّل: الضمانات التقنية

تعتبر الضمانات التقنية من أهم الوسائل التي تعتمدها الدولة الحديثة لتحقيق الأمن السيبراني ضمن الإطار الدستوري، حيث توفر حماية فعّالة للبنية التحتية الرقمية، وأنظمة المعلومات الحكومية، والبيانات الرسمية للمواطنين. وتشمل هذه الضمانات تطبيق أنظمة التشفير المتقدمة، وجدران الحماية،

وأنظمة الكشف عن الاختراقات، وأنظمة المراقبة المستمرة للشبكات[٦١]، بما يضمن منع أي تهديدات إلكترونية قبل وقوعها، وحماية الحقوق والحريات الأساسية للمواطنين.

ويشير الفقه القانوني إلى أن الضمانات التقنية يجب أن تكون مؤطرة تشريعيًا وقانونيًا، بحيث تتكامل مع القوانين الوطنية، مثل قانون الجرائم الإلكترونية العراقي رقم ١٦٠ لسنة ٢٠١٩، الذي يسمح للجهات الحكومية المختصة باستخدام الوسائل التقنية لمراقبة الشبكات، واكتشاف الهجمات الإلكترونية، وملاحقة المخالفين[٦٢]. كما تلتزم هذه الضمانات بمبادئ حماية البيانات الشخصية والخصوصية، بما يحقق التوازن بين حماية الأمن وصون الحقوق الدستورية.

وتتضمن الضمانات التقنية أيضًا إنشاء أنظمة آلية لرصد التهديدات الإلكترونية وتحليلها بشكل لحظي، بما يسهم في اتخاذ القرارات السريعة للحد من الأضرار المحتملة، وإعداد خطط احتياطية للتعافي من الهجمات السيبرانية. كما تعتمد على تطوير الكوادر البشرية المدربة في مجالات الأمن السيبراني، وتشغيل مختبرات محاكاة للهجمات الرقمية لتدريب الموظفين الحكوميين على التعامل مع التهديدات[٦٣].

وعلى المستوى التشريعي، تتيح بعض القوانين الوطنية تنظيم استخدام هذه الأنظمة التقنية بما يحفظ الحقوق والحريات، حيث تحدد المسؤوليات الملقاة على الجهات الحكومية في حماية بيانات الأفراد، وتوضح الإجراءات الواجب اتخاذها عند حدوث اختراق، بما يتوافق مع المبادئ الدستورية[٦٤]. ويؤكد الفقه أن الجمع بين الضمانات التقنية والإطار القانوني يضمن فعالية الأمن السيبراني واستمرارية عمل المؤسسات الدستورية بشكل آمن ومستدام[٦٥].

الفرع الثاني: التعاون الدولي في مجال الأمن السيبراني

أصبح التعاون الدولي أحد الركائز الأساسية لتحقيق الأمن السيبراني ضمن الإطار الدستوري، نظرًا لطبيعة التهديدات الرقمية العابرة للحدود، والتي لا يمكن للدولة مواجهتها بمفردها. ويشمل هذا التعاون تبادل المعلومات والخبرات، والتنسيق في مواجهة الهجمات السيبرانية، وتطوير بروتوكولات مشتركة للتصدي للجرائم الإلكترونية[٦٦].

ويشير الفقه القانوني إلى أن وجود اتفاقيات دولية يُعزز قدرة الدول على حماية شبكاتها الحكومية، وضمان استمرارية عمل مؤسساتها الدستورية، وحماية الحقوق والحريات الأساسية

للمواطنين. ومن أبرز هذه الاتفاقيات اتفاقية بودابست لمكافحة الجرائم الإلكترونية (٢٠٠١)، التي وضعت إطارًا قانونيًا للتعاون بين الدول، بما في ذلك تبادل الأدلة الرقمية، وتعزيز إجراءات حماية البيانات، وملاحقة الجرائم الإلكترونية عبر الحدود[٦٧].

تبنت بعض الدول على المستوى العربي سياسات تعاون إقليمي لدعم الأمن السيبراني، مثل مبادرة جامعة الدول العربية للأمن السيبراني، التي تهدف إلى إنشاء مراكز متخصصة للتدريب وتبادل الخبرات بين الدول الأعضاء، وتعزيز القدرات التقنية للقضاء على الاختراقات والجرائم الرقمية .[٦٨] كما يشمل التعاون الدولي تبادل الخبرات مع المنظمات العالمية، مثل الاتحاد الدولي للاتصالات (ITU) والمنظمة الأوروبية للأمن السيبراني(ENISA) ، لتطبيق أفضل الممارسات التقنية والقانونية[٦٩].

وإن التزام التعاون الدولي بالمبادئ الدستورية الوطنية يعدّ من الجوانب القانونية المهمة، بما يضمن عدم المساس بالحقوق والحريات العامة، وتحديد حدود استخدام البيانات المشتركة بين الدول، ومراعاة سيادة الدولة. ويؤكد الفقه أن التنسيق الدولي يُعزز الضمانات التقنية والتشريعية، ويخلق منظومة أمنية متكاملة تحمي الدولة والمواطنين من التهديدات السيبرانية بشكل فعّال ومستدام[٧٠].

الخاتمة

خلص البحث إلى أن الأمن السيبراني لم يعدّ مجرد مسألة تقنية تقتصر على حماية الأنظمة والشبكات المعلوماتية، بل أصبح أحد المقومات الأساسية للأمن الدستوري في الدولة الحديثة. فالتوسع في استخدام التكنولوجيا الرقمية في إدارة المرافق العامة والخدمات الحكومية والعمليات الاقتصادية والاجتماعية جعل الفضاء السيبراني جزءًا من البنية الأساسية للدولة، الأمر الذي أدى إلى ظهور مخاطر وتهديدات جديدة قادرة على التأثير في استقرار المؤسسات الدستورية وممارسة الحقوق والحريات العامة.

وقد بينت الدراسة أن تحقيق الأمن الدستوري في البيئة الرقمية يقتضي وجود منظومة متكاملة من الضمانات التشريعية والمؤسساتية والتقنية، تبدأ من النصوص الدستورية التي تكفل حماية الخصوصية وحرية التعبير وسرية الاتصالات، مروراً بالتشريعات المنظمة للأمن السيبراني والجرائم الإلكترونية وحماية البيانات، وصولًا إلى إنشاء مؤسسات وطنية متخصصة تمتلك القدرة الفنية والقانونية على مواجهة التهديدات السيبرانية. كما كشفت الدراسة أن الطبيعة العابرة للحدود للهجمات السيبرانية تجعل من التعاون الدولي والإقليمي ضرورة لا غنى عنها لتعزيز الأمن السيبراني وحماية النظام الدستوري للدولة.

وتوصل البحث إلى أن نجاح الدولة الحديثة في حماية أمنها الدستوري أصبح مرتبطًا بمدى قدرتها على بناء بيئة رقمية آمنة تحقق التوازن بين متطلبات الأمن الوطني واحترام الحقوق والحريات الدستورية، بما ينسجم مع مبادئ دولة القانون ويعزز ثقة المواطنين بالمؤسسات العامة.

النتائج

١. تبين أن الأمن السيبراني أصبح أحد المتطلبات الجوهرية للأمن الدستوري بسبب الاعتماد المتزايد على التقنيات الرقمية في إدارة شؤون الدولة ومؤسساتها .
٢. كشفت الدراسة أن التهديدات السيبرانية لا تستهدف الأنظمة التقنية فحسب، وإنما تمتد آثارها إلى الحقوق والحريات الدستورية، ولا سيما الحق في الخصوصية وحرية التعبير والحق في الوصول إلى المعلومات .
٣. اتضح أن النصوص الدستورية المتعلقة بحماية الخصوصية وسرية الاتصالات تمثل الأساس القانوني الأول لحماية الأمن السيبراني في الدولة الحديثة .
٤. بينت الدراسة أن التشريعات الوطنية الخاصة بالأمن السيبراني والجرائم الإلكترونية وحماية البيانات تختلف من دولة إلى أخرى من حيث الشمول والفاعلية، الأمر الذي يؤثر في مستوى الحماية القانونية المقررة للفضاء الرقمي .
٥. أظهرت الدراسة أن فعالية الضمانات التشريعية ترتبط بوجود مؤسسات وطنية متخصصة قادرة على تطبيق تلك التشريعات ومراقبة الالتزام بها .
٦. تبين أن استقلالية الهيئات المختصة بالأمن السيبراني تشكل ضمانة أساسية لمنع التعسف في استخدام السلطات الرقمية وحماية الحقوق الدستورية للأفراد .
٧. كشفت الدراسة أن التطور التقني المتسارع يفوق في كثير من الأحيان سرعة الاستجابة التشريعية، مما يخلق فجوة قانونية قد تستغلها الجهات المهددة للأمن السيبراني .
٨. أظهرت الدراسة أن التعاون الدولي أصبح ضرورة حتمية لمواجهة الهجمات السيبرانية ذات الطابع العابر للحدود والتي يصعب على دولة منفردة التصدي لها بصورة فعالة .

التوصيات

١. إصدار قانون عراقي متكامل للأمن السيبراني يحدد اختصاصات الجهات الحكومية المعنية ويضع إطاراً قانونياً واضحاً لحماية البنية التحتية الرقمية الوطنية .
٢. الإسراع في تشريع قانون خاص بحماية البيانات الشخصية يتضمن ضوابط جمع البيانات ومعالجتها وتخزينها والعقوبات المترتبة على انتهاكها .
٣. إنشاء هيئة وطنية مستقلة للأمن السيبراني تتمتع بالشخصية المعنوية والاستقلال المالي والإداري، وتخضع لرقابة البرلمان والقضاء لضمان عدم تعارض إجراءاتها مع الحقوق الدستورية .
٤. إلزام الوزارات والهيئات الحكومية بوضع استراتيجيات دورية لإدارة المخاطر السيبرانية وإجراء اختبارات أمنية دورية للأنظمة الحكومية وقواعد البيانات الوطنية .
٥. تطوير منظومة الاستجابة الوطنية للحوادث السيبرانية من خلال إنشاء مراكز متخصصة تعمل على مدار الساعة لرصد التهديدات والتعامل معها بصورة فورية .
٦. إدراج متطلبات الأمن السيبراني ضمن معايير التحول الرقمي الحكومي وعدم إطلاق أي خدمة إلكترونية جديدة قبل التحقق من استيفائها لمتطلبات الحماية الرقمية .
٧. تعزيز التعاون مع المنظمات الدولية والإقليمية المختصة بالأمن السيبراني والاستفادة من الخبرات والتجارب المقارنة في هذا المجال .
٨. إدخال مفاهيم الأمن السيبراني والحقوق الرقمية ضمن المناهج الجامعية وبرامج التدريب الوظيفي للعاملين في المؤسسات الحكومية .
٩. إنشاء لجان مشتركة تضم خبراء قانونيين وتقنيين لمراجعة التشريعات ذات الصلة بالأمن السيبراني بشكل دوري واقتراح التعديلات اللازمة لمواكبة التطورات التقنية .
١٠. اعتماد مبدأ التوازن بين الأمن السيبراني والحقوق الدستورية عند وضع السياسات العامة، بما يمنع استخدام متطلبات الأمن ذريعة للمساس بالحقوق والحريات المكفولة دستورياً.

الهوامش

(١) خالد حسن أحمد لطفي ، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية ، دار الفكر الجامعي ، الإسكندرية ، الطبعة الأولى
٢٢٢٢: ١٣ .

(٢) د. عبد العزيز بن غرم هللا آل جار هللا ، جرائم الانترنيت وعقوباتها وفق نظام مكافحة الجرائم المعلوماتية السعودي دراسة مقارنة
(ويليه آثار العولمة على مستخدمي الانترنيت (، دار الكتاب الجامعي ، الرياض ، الطبعة الاولى ، ٢٢١٧ م ، ص ٧١.

(٣)عبد الفتاح بيومي حجازي، الجريمة المعلوماتية وحماية الأمن الرقمي، دار الفكر الجامعي، الإسكندرية، ٢٠٢٠، ص ٣٧.

(٤) محمد عبد الحميد، الأمن السيبراني: الإطار القانوني والتحديات المعاصرة، دار النهضة العربية، القاهرة، ٢٠٢١، ص ٢٥.

(5)United Nations Office on Drugs and Crime (UNODC), Cybercrime and Cybersecurity: Legal Frameworks, United Nations Publication, 2019, p. 18.

(6)OECD, Digital Security Risk Management for Economic and Social Prosperity, OECD Publishing, Paris, 2015, p. 11.

(7)European Union Agency for Cybersecurity (ENISA), Cybersecurity and Fundamental Rights, Publications Office of the European Union, 2020, p. 23.

(٨)عبد الفتاح بيومي حجازي، الجريمة المعلوماتية في التشريع العربي، دار الفكر الجامعي، الإسكندرية، ٢٠١٩، ص ٣١.

(٩) محمد عبد الحميد، الأمن السيبراني: الإطار القانوني والتشريعي، دار النهضة العربية، القاهرة، ٢٠٢١، ص ٢٤.

(١٠) محمود نجيب حسني، حماية الأمن العام في التشريعات الجنائية الحديثة، دار النهضة العربية، القاهرة، ٢٠١٦، ١٤٣.

(١١) عبد الفتاح بيومي حجازي، الجرائم الإلكترونية وإشكالات الإثبات الجنائي، دار الفكر الجامعي، الإسكندرية، ٢٠١٨، ٤٤.

(١٢)عبد الكريم علوان، الجرائم الإلكترونية وأثرها على السيادة الوطنية، دار الثقافة للنشر والتوزيع، عمّان، ٢٠٢٠، ٨١.

(١٣) محمد عبد الحميد، الأمن السيبراني وحماية البنية التحتية الرقمية، دار النهضة العربية، القاهرة، ٢٠٢١، ٣٩.

(١٤) محمد كامل ليلة، الحقوق والحريات العامة في ظل الدولة الحديثة، دار الفكر العربي، القاهرة، ٢٠١٥، ٦٦.

(١٥) يحيى الجمل، النظام الدستوري في عصر العولمة الرقمية، دار النهضة العربية، القاهرة، ٢٠١٨، ١٣٩

(١٦) عبد العزيز الزبيدي، الحقوق والحريات الدستورية في التشريع العربي، دار النهضة العربية، القاهرة، ٢٠١٧، ٥٢.

(١٧) فؤاد شرف الدين، الأمن الدستوري بين النظرية والتطبيق، دار الفكر العربي، عمّان، ٢٠١٩، ٨٨.

(١٨) محمود عبد المجيد، الرقابة الدستورية وآليات حماية الدستور، دار الثقافة القانونية، بيروت، ٢٠٢٠، ١٠١.

(١٩) عبد الله الحسن، سلوك الدولة وحماية الأمن الدستوري، دار النهضة، بغداد، ٢٠١٨، ٦٩.

(٢٠)عادل محمد، الهيئات الرقابية وآليات الرقابة الدستورية، دار الفكر القانوني، القاهرة، ٢٠١٩، ٧٧.

(٢١) أحمد محمود، حقوق الإنسان والأمن الدستوري، دار الثقافة، دمشق، ٢٠٢٠، ١٢١.

(٢٢) ناصر الزهراني، الأبعاد السياسية للأمن الدستوري، دار الفكر العربي، الرياض، ٢٠١٧، ٤٥.

(٢٣) فؤاد شرف الدين، الأمن الدستوري بين النظرية والتطبيق، دار الفكر العربي، عمّان، ٢٠١٩، ٨٨.

(٢٤) عبد الفتاح بيومي حجازي، الأمن السيبراني في حماية الدولة والمؤسسات، دار الفكر الجامعي، الإسكندرية، ٢٠٢٠، ٥٥.

(٢٥) محمود نجيب حسني، الإطار القانوني للأمن السيبراني وحماية المؤسسات الحكومية، دار النهضة العربية، القاهرة، ٢٠١٩، ٦٠.

(٢٦) فؤاد شرف الدين، الأمن السيبراني وضمان الحقوق الدستورية، دار الفكر العربي، عمّان، ٢٠١٩، ٩٨.

(٢٧)عبد الرحيم منصور، الأمن السيبراني وضمان الاستقلال المؤسسي، دار الثقافة القانونية، القاهرة، ٢٠٢١، ٧٢.

(٢٨) ياسر عبد الله، الضمانات القانونية لحماية الفضاء الرقمي في الدول العربية، دار الفكر العربي، عمّان، ٢٠٢٠، ٨٨.

(٢٩) سامي الفقي، التقنيات الحديثة ودورها في حماية المؤسسات الدستورية، دار النهضة العربية، بيروت، ٢٠١٩، ١٠٥.

(٣٠) هاني شلبي، الأمن الدستوري والأمن الرقمي: منظور قانوني مقارن، دار الثقافة، القاهرة، ٢٠٢٢، ١٣١.

(٣١) أحمد الجوهري، الأمن السيبراني والتشريعات الوطنية، دار النهضة العربية، القاهرة، ٢٠٢١، ١١٠

(٣٢) ليلى خالد، الأمن الرقمي والحقوق الدستورية في التشريع العربي، دار الفكر العربي، عمان، ٢٠١٩، ٦٧.

(٣٣) عبد الفتاح بيومي حجازي، الأمن السيبراني وحماية المعلومات في عصر التكنولوجيا الرقمية، دار الفكر الجامعي، الإسكندرية، ٢٠٢٢، ٨٥.

(٣٤) دستور جمهورية العراق لسنة ٢٠٠٥، المادة (١٧/أوّلًا وثانيًا).

(٣٥) دستور جمهورية العراق لسنة ٢٠٠٥، المادة (٣٨)؛ أحمد عبد الكريم سلامة، القانون الدستوري وحقوق الإنسان في البيئة الرقمية، دار النهضة العربية، القاهرة، ٢٠٢٣، ١٥٦.

(٣٦) محمد حسين منصور، الحماية القانونية للبيانات الشخصية والجرائم الإلكترونية، منشورات الحلبي الحقوقية، بيروت، ٢٠٢١، ١١٧.

(٣٧) دستور جمهورية العراق لسنة ٢٠٠٥، المادة (٢٠)؛ محمد فؤاد عبد الباسط، الجرائم الإلكترونية وأثرها على الحقوق والحريات العامة، دار الجامعة الجديدة، الإسكندرية، ٢٠٢٠، ٢٠١.

(٣٨)عبد الفتاح بيومي حجازي، الأمن السيبراني وحماية المعلومات في عصر التكنولوجيا الرقمية، مصدر سابق، ١٠٣.

(٣٩) نهاد عبد الرحمن، الأمن الرقمي وحماية الحقوق الدستورية، دار النهضة العربية، القاهرة، ٢٠٢١، ١٠٥.

(٤٠) زياد الحاج، التشريعات الحديثة والأمن السيبراني في الدول الحديثة، دار الثقافة القانونية، دمشق، ٢٠٢٠، ٩٧.

(٤١) أماني الخطيب، التعاون الدولي في مواجهة التهديدات السيبرانية، دار الفكر العربي، القاهرة، ٢٠٢١، ١١٠.

(٤٢) سامي الفقي، حماية الدولة والمؤسسات الدستورية في العصر الرقمي، دار النهضة العربية، بيروت، ٢٠١٩، ١٠٢.

(٤٣) ليلى خالد، الضمانات التشريعية للأمن السيبراني في الدول العربية، دار الفكر العربي، عمان، ٢٠٢٠، ٨٥.

(٤٤)قانون الجرائم الإلكترونية العراقي رقم ١٦٠ لسنة ٢٠١٩، وزارة العدل العراقية، بغداد، ٢٠١٩.

(٤٥) قانون حماية المعلومات الأردني رقم ١٣ لسنة ٢٠١٥، وزارة العدل الأردنية، عمان، ٢٠١٥.

(٤٦) قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨، الجريدة الرسمية المصرية، القاهرة، ٢٠١٨.

(٤٧) ليلى خالد، التشريعات الوطنية للأمن الرقمي وحماية الحقوق الدستورية، دار الفكر العربي، عمان، ٢٠٢٠، ٩٦.

(٤٨) نهاد عبد الرحمن، التكامل بين الضمانات التشريعية والمؤسساتية في الأمن السيبراني، دار النهضة العربية، القاهرة، ٢٠٢١، ١١٨.

(٤٩) نهاد عبد الرحمن، القوانين الوطنية لحماية الفضاء الرقمي، دار النهضة العربية، القاهرة، ٢٠٢١، ١١٦.

(٥٠) زياد الحاج، الأمن السيبراني والتشريعات الدستورية، دار الثقافة القانونية، دمشق، ٢٠٢٠، ٩١.

(٥١) أماني الخطيب، الضمانات المؤسساتية لحماية الفضاء الرقمي، دار الفكر العربي، القاهرة، ٢٠٢١، ١١٠.

(٥٢) قانون الجرائم الإلكترونية العراقي رقم ١٦٠ لسنة ٢٠١٩، وزارة العدل العراقية، بغداد، ٢٠١٩.

(٥٣) ليلى خالد، القوانين الوطنية للأمن السيبراني في الدول العربية، دار الفكر العربي، عمّان، ٢٠٢٠، ٩٢.

(٥٤) سامي الفقي، التعاون الدولي والمؤسسات الرقمية في حماية الأمن السيبراني، دار النهضة العربية، بيروت، ٢٠٢٠، ١٠٥.

(٥٥) زياد الحاج، استقلالية الهيئات السيبرانية وأثرها على الأمن الدستوري، دار الثقافة القانونية، دمشق، ٢٠٢٠، ١٠١.

(٥٦) نهاد عبد الرحمن، التكامل بين الضمانات التشريعية والمؤسساتية في الأمن السيبراني، دار النهضة العربية، القاهرة، ٢٠٢١، ١١٨.

(٥٧) صالح عبد اللطيف، الجرائم الإلكترونية وحماية البيانات في التشريعات العربية، دار الكتاب الجامعي، عمان، ٢٠١٩، ٥٤.

(٥٨)اللجنة الوزارية العربية للأمن السيبراني، دراسة مقارنة في الضمانات التقنية في مواجهة الهجمات السيبرانية، الرياض، ٢٠٢٠، ١٢.

(٥٩)خالد مصطفى، الأمن السيبراني: الإطار القانوني والتقني لمواجهة التهديدات الرقمية، دار الفكر القانوني، القاهرة، ٢٠٢٢، ١٤٣.

(٦٠) نزار صلاح، حماية البيانات الشخصية والأمن السيبراني في التشريعات العربية، دار الثقافة للنشر والتوزيع، عمّان، ٢٠٢٠، ٧٨.

(٦١) خالد مصطفى، الأمن السيبراني: الإطار القانوني والتقني لمواجهة التهديدات الرقمية، دار الفكر القانوني، القاهرة، ٢٠٢٢، ١٤٣.

(٦٢) قانون الجرائم الإلكترونية العراقي رقم ١٦٠ لسنة ٢٠١٩، وزارة العدل العراقية، بغداد، ٢٠١٩.

(٦٣) فاطمة الزهراء التومي، التشريعات الوطنية والأمن السيبراني: منظور حقوقي، دار النهضة، تونس، ٢٠٢٣، ٩٧ .

(٦٤) نزار صلاح، حماية البيانات الشخصية والأمن السيبراني في التشريعات العربية، دار الثقافة للنشر والتوزيع، عمّان، ٢٠٢٠، ٧٨.

(٦٥) مراجعة المركز العربي لدراسات الفضاء الإلكتروني، الأطر التقنية القانونية للأمن السيبراني في الوطن العربي، المركز العربي، بيروت، ٢٠٢١، ٣٤.

(٦٦) ناصر بن سليمان العيسى، التعاون الدولي في مكافحة الجرائم الإلكترونية، منشورات جامعة الملك سعود، الرياض، ٢٠٢١، ٥٩.

(٦٧) اتفاقية بودابست لمكافحة الجرائم الإلكترونية، ٢٠٠١، صادرة عن المجلس الأوروبي، بروكسل، ٢٠٠١.

(٦٨) مراجعة جامعة الدول العربية، مبادرة الأمن السيبراني العربي والتعاون الإقليمي، القاهرة، ٢٠٢٠، ٤٥.

(٦٩) خالد مصطفى، الأمن السيبراني الدولي: التعاون القانوني والتقني بين الدول، دار الفكر القانوني، القاهرة، ٢٠٢٢، ١٢٩.

(٧٠) فاطمة الزهراء التومي، التعاون الدولي والأمن السيبراني: منظور حقوقي، دار النهضة، تونس، ٢٠٢٣، ١٠٢.

قائمة المصادر

القرآن الكريم

أولاً: الكتب العربية

١. أحمد عبد الكريم سلامة، القانون الدستوري وحقوق الإنسان في البيئة الرقمية، دار النهضة العربية، القاهرة، ٢٠٢٣

٢. أحمد الجوهري، الأمن السيبراني والتشريعات الوطنية، دار النهضة العربية، القاهرة، ٢٠٢١ .

٣. أحمد محمود، حقوق الإنسان والأمن الدستوري، دار الثقافة، دمشق، ٢٠٢٠ .

٤. أماني الخطيب، التعاون الدولي في مواجهة التهديدات السيبرانية، دار الفكر العربي، القاهرة، ٢٠٢١ .

٥. أماني الخطيب، الضمانات المؤسساتية لحماية الفضاء الرقمي، دار الفكر العربي، القاهرة، ٢٠٢١ .

٦. عبد العزيز بن غرم الله آل جار الله، جرائم الإنترنت وعقوباتها وفق نظام مكافحة الجرائم المعلوماتية السعودي دراسة مقارنة (ويليه آثار العولمة على مستخدمي الإنترنت)، دار الكتاب الجامعي، الرياض، الطبعة الأولى، ٢٠١٧ .

٧. عبد العزيز الزبيدي، الحقوق والحريات الدستورية في التشريع العربي، دار النهضة العربية، القاهرة، ٢٠١٧. .

٨. عبد الله الحسن، سلوك الدولة وحماية الأمن الدستوري، دار النهضة، بغداد، ٢٠١٨ .

٩. عبد الرحيم منصور، الأمن السيبراني وضمان الاستقلال المؤسسي، دار الثقافة القانونية، القاهرة، ٢٠٢١ .

١٠. عبد الكريم علوان، الجرائم الإلكترونية وأثرها على السيادة الوطنية، دار الثقافة للنشر والتوزيع، عمّان، ٢٠٢٠ .

١١. عبد الفتاح بيومي حجازي، الجريمة المعلوماتية في التشريع العربي، دار الفكر الجامعي، الإسكندرية، ٢٠١٩ .

١٢. عبد الفتاح بيومي حجازي، الجريمة المعلوماتية وحماية الأمن الرقمي، دار الفكر الجامعي، الإسكندرية، ٢٠٢٠ .

١٣. عبد الفتاح بيومي حجازي، الجرائم الإلكترونية وإشكالات الإثبات الجنائي، دار الفكر الجامعي، الإسكندرية، ٢٠١٨ .

١٤. عبد الفتاح بيومي حجازي، الأمن السيبراني في حماية الدولة والمؤسسات، دار الفكر الجامعي، الإسكندرية، ٢٠٢٠ .

١٥. عبد الفتاح بيومي حجازي، الأمن السيبراني وحماية المعلومات في عصر التكنولوجيا الرقمية، دار الفكر الجامعي، الإسكندرية، ٢٠٢٢ .

١٦. عادل محمد، الهيئات الرقابية وآليات الرقابة الدستورية، دار الفكر القانوني، القاهرة، ٢٠١٩ .

١٧. سامي الفقي، التقنيات الحديثة ودورها في حماية المؤسسات الدستورية، دار النهضة العربية، بيروت، ٢٠١٩ .

١٨. سامي الفقي، حماية الدولة والمؤسسات الدستورية في العصر الرقمي، دار النهضة العربية، بيروت، ٢٠١٩ .

١٩. سامي الفقي، التعاون الدولي والمؤسسات الرقمية في حماية الأمن السيبراني، دار النهضة العربية، بيروت، ٢٠٢٠ .

٢٠. صالح عبد اللطيف، الجرائم الإلكترونية وحماية البيانات في التشريعات العربية، دار الكتاب الجامعي، عمّان، ٢٠١٩ .

٢١. فؤاد شرف الدين، الأمن الدستوري بين النظرية والتطبيق، دار الفكر العربي، عمّان، ٢٠١٩ .

٢٢. فؤاد شرف الدين، الأمن السيبراني وضمان الحقوق الدستورية، دار الفكر العربي، عمّان، ٢٠١٩ .

٢٣. فاطمة الزهراء التومي، التشريعات الوطنية والأمن السيبراني: منظور حقوقي، دار النهضة، تونس، ٢٠٢٣ .

٢٤. فاطمة الزهراء التومي، التعاون الدولي والأمن السيبراني: منظور حقوقي، دار النهضة، تونس، ٢٠٢٣ .

٢٥. خالد حسن أحمد لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، ٢٠٢٢ .

٢٦. خالد مصطفى، الأمن السيبراني: الإطار القانوني والتقني لمواجهة التهديدات الرقمية، دار الفكر القانوني، القاهرة، ٢٠٢٢ .

٢٧. خالد مصطفى، الأمن السيبراني الدولي: التعاون القانوني والتقني بين الدول، دار الفكر القانوني، القاهرة، ٢٠٢٢ .

٢٨. زياد الحاج، التشريعات الحديثة والأمن السيبراني في الدول الحديثة، دار الثقافة القانونية، دمشق، ٢٠٢٠ .

٢٩. زياد الحاج، الأمن السيبراني والتشريعات الدستورية، دار الثقافة القانونية، دمشق، ٢٠٢٠ .

٣٠. زياد الحاج، استقلالية الهيئات السيبرانية وأثرها على الأمن الدستوري، دار الثقافة القانونية، دمشق، ٢٠٢٠ .

٣١أ ياسر عبد الله، الضمانات القانونية لحماية الفضاء الرقمي في الدول العربية، دار الفكر العربي، عمّان، ٢٠٢٠ .

٣٢. يحيى الجمل، النظام الدستوري في عصر العولمة الرقمية، دار النهضة العربية، القاهرة، ٢٠١٨ .

٣٣. ليلى خالد، الأمن الرقمي والحقوق الدستورية في التشريع العربي، دار الفكر العربي، عمّان، ٢٠١٩ .

٣٤. ليلى خالد، الضمانات التشريعية للأمن السيبراني في الدول العربية، دار الفكر العربي، عمّان، ٢٠٢٠ .
٣٥. ليلى خالد، التشريعات الوطنية للأمن الرقمي وحماية الحقوق الدستورية، دار الفكر العربي، عمّان، ٢٠٢٠ .
٣٦. ليلى خالد، القوانين الوطنية للأمن السيبراني في الدول العربية، دار الفكر العربي، عمّان، ٢٠٢٠ .
٣٧. محمد عبد الحميد، الأمن السيبراني: الإطار القانوني والتحديات المعاصرة، دار النهضة العربية، القاهرة، ٢٠٢١ .
٣٨. محمد عبد الحميد، الأمن السيبراني: الإطار القانوني والتشريعي، دار النهضة العربية، القاهرة، ٢٠٢١ .
٣٩. محمد عبد الحميد، الأمن السيبراني وحماية البنية التحتية الرقمية، دار النهضة العربية، القاهرة، ٢٠٢١ .
٤٠. محمد حسين منصور، الحماية القانونية للبيانات الشخصية والجرائم الإلكترونية، منشورات الحلبي الحقوقية، بيروت، ٢٠٢١ .
٤١. محمد فؤاد عبد الباسط، الجرائم الإلكترونية وأثرها على الحقوق والحريات العامة، دار الجامعة الجديدة، الإسكندرية، ٢٠٢٠ .
٤٢. محمد كامل ليلة، الحقوق والحريات العامة في ظل الدولة الحديثة، دار الفكر العربي، القاهرة، ٢٠١٥ .
٤٣. محمود عبد المجيد، الرقابة الدستورية وآليات حماية الدستور، دار الثقافة القانونية، بيروت، ٢٠٢٠ .
٤٤. محمود نجيب حسني، حماية الأمن العام في التشريعات الجنائية الحديثة، دار النهضة العربية، القاهرة، ٢٠١٦ .
٤٥. محمود نجيب حسني، الإطار القانوني للأمن السيبراني وحماية المؤسسات الحكومية، دار النهضة العربية، القاهرة، ٢٠١٩ .
٤٦. ناصر الزهراني، الأبعاد السياسية للأمن الدستوري، دار الفكر العربي، الرياض، ٢٠١٧ .
٤٧. ناصر بن سليمان العيسى، التعاون الدولي في مكافحة الجرائم الإلكترونية، منشورات جامعة الملك سعود، الرياض، ٢٠٢١ .
٤٨. نزار صلاح، حماية البيانات الشخصية والأمن السيبراني في التشريعات العربية، دار الثقافة للنشر والتوزيع، عمّان، ٢٠٢٠ .
٤٩. نهاد عبد الرحمن، الأمن الرقمي وحماية الحقوق الدستورية، دار النهضة العربية، القاهرة، ٢٠٢١ .
٥٠. نهاد عبد الرحمن، التكامل بين الضمانات التشريعية والمؤسساتية في الأمن السيبراني، دار النهضة العربية، القاهرة، ٢٠٢١ .
٥١. نهاد عبد الرحمن، القوانين الوطنية لحماية الفضاء الرقمي، دار النهضة العربية، القاهرة، ٢٠٢١ .
٥٢. هاني شلبي، الأمن الدستوري والأمن الرقمي: منظور قانوني مقارن، دار الثقافة، القاهرة، ٢٠٢٢ .

ثانياً: التقارير والدراسات الدولية

1-OECD, Digital Security Risk Management for Economic and Social Prosperity, OECD Publishing, Paris, 2015.

2-European Union Agency for Cybersecurity (ENISA), Cybersecurity and Fundamental Rights, Publications Office of the European Union, 2020.

3-United Nations Office on Drugs and Crime (UNODC), Cybercrime and Cybersecurity: Legal Frameworks, United Nations Publication, 2019.

٤. اللجنة الوزارية العربية للأمن السيبراني، دراسة مقارنة في الضمانات التقنية في مواجهة الهجمات السيبرانية، الرياض، ٢٠٢٠ .

٥. مراجعة جامعة الدول العربية، مبادرة الأمن السيبراني العربي والتعاون الإقليمي، القاهرة، ٢٠٢٠ .

٦. مراجعة المركز العربي لدراسات الفضاء الإلكتروني، الأطر التقنية القانونية للأمن السيبراني في الوطن العربي، بيروت، ٢٠٢١ .

ثالثاً: الدساتير والقوانين والاتفاقيات

١. دستور جمهورية العراق لسنة ٢٠٠٥ .

٢. قانون مكافحة جرائم تقنية المعلومات المصري رقم (١٧٥) لسنة ٢٠١٨، الجريدة الرسمية المصرية، القاهرة، ٢٠١٨ .

٣. قانون حماية المعلومات الأردني رقم (١٣) لسنة ٢٠١٥، وزارة العدل الأردنية، عمّان، ٢٠١٥. .

٤. قانون الجرائم الإلكترونية العراقي رقم (١٦٠) لسنة ٢٠١٩، وزارة العدل العراقية، بغداد، ٢٠١٩ .

٥. اتفاقية بودابست لمكافحة الجرائم الإلكترونية، الصادرة عن المجلس الأوروبي، ٢٠٠١.

References

Quran

First: Arabic Books

1-Ahmed Abdel Karim Salama, *Constitutional Law and Human Rights in the Digital Environment,* Dar Al-Nahda Al-Arabia, Cairo, 2023.

2-Ahmed Al-Johari, *Cybersecurity and National Legislation*, Dar Al-Nahda Al-Arabia, Cairo, 2021.

3-Ahmed Mahmoud, *Human Rights and Constitutional Security*, Dar Al-Thaqafa, Damascus, 2020.

4-Amani Al-Khatib, *International Cooperation in Facing Cyber Threats*, Dar Al-Fikr Al-Arabi, Cairo, 2021.

5-Amani Al-Khatib, *Institutional Guarantees for Protecting Cyberspace*, Dar Al-Fikr Al-Arabi, Cairo, 2021.

6-Abdulaziz bin Gharam Allah Al Jarallah, *Internet Crimes and Their Penalties under the Saudi Anti-Cybercrime Law (A Comparative Study including the Effects of Globalization on Internet Users)*, Dar Al-Kitab Al-Jami'i, Riyadh, 1st ed., 2017.

7-Abdulaziz Al-Zubaidi, *Rights and Constitutional Freedoms in Arab Legislation*, Dar Al-Nahda Al-Arabia, Cairo, 2017.

8-Abdullah Al-Hassan, *State Conduct and Constitutional Security Protection*, Dar Al-Nahda, Baghdad, 2018.

9-Abdulrahim Mansour, *Cybersecurity and Institutional Independence Guarantee*, Dar Al-Thaqafa Al-Qanuniyya, Cairo, 2021.

10-Abdulkarim Alwan, *Cybercrime and Its Impact on National Sovereignty*, Dar Al-Thaqafa Publishing and Distribution, Amman, 2020.

11-Abdul Fattah Bayoumi Hegazy, *Information Crime in Arab Legislation*, Dar Al-Fikr Al-Jami'i, Alexandria, 2019.

12-Abdul Fattah Bayoumi Hegazy, *Information Crime and Digital Security Protection*, Dar Al-Fikr Al-Jami'i, Alexandria, 2020.

13-Abdul Fattah Bayoumi Hegazy, *Cyber Crimes and Issues of Criminal Evidence*, Dar Al-Fikr Al-Jami'i, Alexandria, 2018.

14-Abdul Fattah Bayoumi Hegazy, *Cybersecurity in Protecting the State and Institutions*, Dar Al-Fikr Al-Jami'i, Alexandria, 2020.

15-Abdul Fattah Bayoumi Hegazy, *Cybersecurity and Information Protection in the Digital Age*, Dar Al-Fikr Al-Jami'i, Alexandria, 2022.

16-Adel Mohammed, *Regulatory Bodies and Constitutional Oversight Mechanisms*, Dar Al-Fikr Al-Qanuni, Cairo, 2019.

17-Sami Al-Feki, *Modern Technologies and Their Role in Protecting Constitutional Institutions*, Dar Al-Nahda Al-Arabia, Beirut, 2019.

18-Sami Al-Feki, *Protecting the State and Constitutional Institutions in the Digital Era*, Dar Al-Nahda Al-Arabia, Beirut, 2019.

19-Sami Al-Feki, *International Cooperation and Digital Institutions in Cybersecurity Protection*, Dar Al-Nahda Al-Arabia, Beirut, 2020.

20-Saleh Abdul Latif, *Cybercrime and Data Protection in Arab Legislation*, Dar Al-Kitab Al-Jami'i, Amman, 2019.

21-Fouad Sharaf El-Din, *Constitutional Security between Theory and Practice*, Dar Al-Fikr Al-Arabi, Amman, 2019.

22-Fouad Sharaf El-Din, *Cybersecurity and Constitutional Rights Protection*, Dar Al-Fikr Al-Arabi, Amman, 2019.

23-Fatima Al-Zahraa Al-Toumi, *National Legislation and Cybersecurity: A Legal Perspective*, Dar Al-Nahda, Tunisia, 2023.

24-Fatima Al-Zahraa Al-Toumi, *International Cooperation and Cybersecurity: A Legal Perspective*, Dar Al-Nahda, Tunisia, 2023.

25-Khaled Hassan Ahmed Lotfy, *Digital Evidence and Its Role in Proving Cybercrime*, Dar Al-Fikr Al-Jami'i, Alexandria, 2022.

26-Khaled Mustafa, *Cybersecurity: Legal and Technical Framework for Facing Digital Threats*, Dar Al-Fikr Al-Qanuni, Cairo, 2022.

27-Khaled Mustafa, *International Cybersecurity: Legal and Technical Cooperation between States*, Dar Al-Fikr Al-Qanuni, Cairo, 2022.

28-Ziad Al-Hajj, *Modern Legislation and Cybersecurity in Contemporary States*, Dar Al-Thaqafa Al-Qanuniyya, Damascus, 2020.

29-Ziad Al-Hajj, *Cybersecurity and Constitutional Legislation*, Dar Al-Thaqafa Al-Qanuniyya, Damascus, 2020.

30-Ziad Al-Hajj, *Independence of Cyber Authorities and Its Impact on Constitutional Security*, Dar Al-Thaqafa Al-Qanuniyya, Damascus, 2020.

31-Yasser Abdullah, *Legal Guarantees for Protecting Cyberspace in Arab Countries*, Dar Al-Fikr Al-Arabi, Amman, 2020.

32-Yahya Al-Jamal, *The Constitutional System in the Age of Digital Globalization*, Dar Al-Nahda Al-Arabia, Cairo, 2018.

33-Laila Khaled, *Digital Security and Constitutional Rights in Arab Legislation*, Dar Al-Fikr Al-Arabi, Amman, 2019.

34-Laila Khaled, *Legislative Guarantees for Cybersecurity in Arab Countries*, Dar Al-Fikr Al-Arabi, Amman, 2020.

35-Laila Khaled, *National Legislation for Digital Security and Protection of Constitutional Rights*, Dar Al-Fikr Al-Arabi, Amman, 2020.

36-Laila Khaled, *National Cybersecurity Laws in Arab Countries*, Dar Al-Fikr Al-Arabi, Amman, 2020.

37-Mohammed Abdel Hamid, *Cybersecurity: Legal Framework and Contemporary Challenges*, Dar Al-Nahda Al-Arabia, Cairo, 2021.

38-Mohammed Abdel Hamid, *Cybersecurity: Legal and Legislative Framework*, Dar Al-Nahda Al-Arabia, Cairo, 2021.

39-Mohammed Abdel Hamid, *Cybersecurity and Digital Infrastructure Protection*, Dar Al-Nahda Al-Arabia, Cairo, 2021.

40-Mohammed Hussein Mansour, *Legal Protection of Personal Data and Cybercrime*, Al-Halabi Legal Publications, Beirut, 2021.

41-Mohammed Fouad Abdel Baset, *Cybercrime and Its Impact on Public Rights and Freedoms*, New University Publishing House, Alexandria, 2020.

42-Mohammed Kamel Leila, *Public Rights and Freedoms in the Modern State*, Dar Al-Fikr Al-Arabi, Cairo, 2015.

43-Mahmoud Abdel Majeed, *Constitutional Oversight and Mechanisms for Protecting the Constitution*, Dar Al-Thaqafa Al-Qanuniyya, Beirut, 2020.

44-Mahmoud Naguib Hosni, *Protection of Public Security in Modern Criminal Legislation*, Dar Al-Nahda Al-Arabia, Cairo, 2016.

45-Mahmoud Naguib Hosni, *Legal Framework of Cybersecurity and Protection of Government Institutions*, Dar Al-Nahda Al-Arabia, Cairo, 2019.

56-Nasser Al-Zahrani, *Political Dimensions of Constitutional Security*, Dar Al-Fikr Al-Arabi, Riyadh, 2017.

47-Nasser bin Suleiman Al-Issa, *International Cooperation in Combating Cybercrime*, King Saud University Publications, Riyadh, 2021.

48-Nizar Salah, *Personal Data Protection and Cybersecurity in Arab Legislation*, Dar Al-Thaqafa Publishing and Distribution, Amman, 2020.

49-Nihad Abdul Rahman, *Digital Security and Protection of Constitutional Rights*, Dar Al-Nahda Al-Arabia, Cairo, 2021.

50-Nihad Abdul Rahman, *Integration of Legislative and Institutional Guarantees in Cybersecurity*, Dar Al-Nahda Al-Arabia, Cairo, 2021.

51-Nihad Abdul Rahman, *National Laws for Protecting Cyberspace*, Dar Al-Nahda Al-Arabia, Cairo, 2021.

52-Hani Shalabi, *Constitutional Security and Digital Security: A Comparative Legal Perspective*, Dar Al-Thaqafa, Cairo, 2022.

Second: International Reports and Studies

1-OECD, *Digital Security Risk Management for Economic and Social Prosperity*, OECD Publishing, Paris, 2015.

2-European Union Agency for Cybersecurity (ENISA), ***Cybersecurity and Fundamental Rights,*** **Publications Office of the European Union, 2020.**

3-United Nations Office on Drugs and Crime (UNODC), ***Cybercrime and Cybersecurity: Legal Frameworks,*** **United Nations Publication, 2019.**

4-Arab Ministerial Committee for Cybersecurity, ***Comparative Study on Technical Guarantees in Facing Cyber Attacks,*** **Riyadh, 2020.**

5-Arab League Review, ***Arab Cybersecurity Initiative and Regional Cooperation,*** **Cairo, 2020.**

6-Arab Center for Cyber Space Studies Review, ***Technical and Legal Frameworks for Cybersecurity in the Arab World,*** **Beirut, 2021.**

Third: Constitutions, Laws, and Agreements

1-Constitution of the Republic of Iraq (2005).

2-Egyptian Information Technology Crimes Law No. (175) of 2018, Official Gazette of Egypt, Cairo, 2018.

3-Jordanian Cybercrime Law No. (13) of 2015, Ministry of Justice, Amman, 2015.

4-Iraqi Cybercrime Law No. (160) of 2019, Iraqi Ministry of Justice, Baghdad, 2019.

5-Budapest Convention on Cybercrime, Council of Europe, 2001.