الإطار القانوني لحماية الأمن السيبراني في العراق: (دراسة تحليلية في ضوء التشريعات الوطنية والمعايير الدولية)

الباحث. سجاد صبار رزاق الحمدان **أ.م. الهام حيدري**

مديرية تربية البصرة/ قسم الإشراف الاختصاصي **جامعة شهركرد الحكومة/ إيران**

Email : aa2680699@gmail.com

Email : e.heidary@yahoo.com

الملخص

مع التطور المتسارع في تكنولوجيا المعلومات، أصبح الأمن السيبراني ضروريًا لحماية البنية التحتية الرقمية وضمان الأمن الوطني. يواجه العراق تحديات متزايدة في تأمين فضائه السيبراني، مما يستلزم إطارًا قانونيًا متكاملًا لمكافحة الجرائم الإلكترونية. يهدف البحث إلى تحليل التشريعات العراقية المتعلقة بالأمن السيبراني، وتقييم مدى توافقها مع المعايير الدولية، مع تسليط الضوء على أوجه القصور وسبل معالجتها.

توصلت الدراسة إلى أن القوانين الحالية غير كافية لمواكبة التطورات السيبرانية، إذ تفتقر إلى تشريعات واضحة وآليات فعالة للوقاية من الهجمات الرقمية. ويوصي البحث بتحديث الإطار القانوني، واعتماد أفضل الممارسات الدولية، وتعزيز التعاون بين الجهات المعنية، لضمان استجابة أكثر فاعلية للتهديدات السيبرانية.

الكلمات المفتاحية :الأمن السيبراني، الجرائم الإلكترونية، البنية التحتية الرقمية، الأمن الوطني.

"The Legal Framework for Cybersecurity in Iraq: An Analytical Study Based on National Laws and International Standards"

Researcher. Sajjad Sabbar Razzaq Sajit Al-Hamdan
Basrah Education Directorate / Specialist Supervision
Assist. Prof. Elham Heydari
shaherkord University/ Iran
Email : aa2680699@gmail.com
Email : e.heidary@yahoo.com

Abstract

With the rapid advancement of information technology, cybersecurity has become essential for protecting digital infrastructure and ensuring national security. Iraq faces growing challenges in securing its cyberspace, necessitating a comprehensive legal framework to combat cybercrime. This study aims to analyze Iraqi cybersecurity legislation, assess its alignment with international standards, and identify gaps while proposing measures to address them.

The findings indicate that the current legal framework is insufficient to keep pace with evolving cyber threats, lacking clear regulations and effective mechanisms for mitigating such threats. The study recommends updating cybersecurity laws, adopting international best practices, and enhancing cooperation among relevant entities to ensure a more effective response to cyber threats.

Keywords: Cybersecurity, Cybercrime, Digital Infrastructure, National Security.

المقدمة

مع التطور السريع الذي يشهده العالم في مجال تكنولوجيا المعلومات والاتصالات، أصبح الفضاء السيبراني جزءًا لا يتجزأ من البنية التحتية للدول، وأداة رئيسية في تسيير مختلف القطاعات الحيوية، بما في ذلك القطاعات الاقتصادية، والسياسية، والأمنية، والاجتماعية. لم يعد الفضاء السيبراني مقتصرًا على الأنظمة الرقمية البسيطة، بل أصبح يشكل محورًا أساسيًا لعمل معظم المؤسسات، من الحكومات والشركات الكبرى إلى الأفراد في حياتهم اليومية. ومع تزايد الاعتماد على التكنولوجيا في كافة الأنشطة الاقتصادية والاجتماعية، تزايدت المخاطر المتعلقة باستخدامها، مما يجعل الفضاء السيبراني هدفًا محتملاً للتهديدات والهجمات التي تتخذ أشكالًا متعددة ومعقدة.

إن هذه التحولات التقنية جلبت معها تحديات جديدة تتعلق بأمن المعلومات وحماية خصوصية الأفراد، إذ أصبحت الهجمات السيبرانية تهدد استقرار الدول ومؤسساتها بشكل غير مسبوق. ونتيجة لتزايد هذه المخاطر، قد تجد بعض الهجمات السيبرانية نفسها قادرة على التأثير على الأمن القومي، سواء من خلال تعريض البيانات الحساسة للخطر، أو من خلال تعطيل الخدمات الحيوية التي تعتمد عليها الدول والمجتمعات. وعليه، لم يعد ممكنًا تجاهل ضرورة وجود أطر قانونية تواكب هذا التطور السريع، وتضع الحماية القانونية اللازمة للأفراد والمؤسسات على حد سواء.

وفي هذا السياق، أصبح من الأهمية بمكان أن تقوم الدول بتطوير أطر قانونية متكاملة تهدف إلى حماية الفضاء السيبراني، بحيث تكون قادرة على التصدي للتهديدات المتزايدة والمتطورة في هذا المجال. ويجب أن تكون هذه التشريعات قادرة على ضمان التوازن بين حماية الأمن العام وصون الحقوق والحريات الأساسية للأفراد، إذ إن الأمن السيبراني لا يقتصر على الدفاع عن الأنظمة الرقمية، بل يشمل أيضًا حماية حقوق المواطنين في الخصوصية، وضمان حرية الوصول إلى المعلومات بشكل آمن.

ويعد العراق من الدول التي تواجه تحديات متزايدة في هذا المجال، حيث تشهد المؤسسات الحكومية والخاصة في العراق زيادة ملحوظة في الاعتماد على التقنيات الرقمية، سواء في التواصل أو المعاملات المالية، أو حتى في تنظيم العمليات الأمنية والإدارية. هذه الزيادة في استخدام التكنولوجيا تواكبها تهديدات سيبرانية متزايدة، تستدعي من الدولة اتخاذ إجراءات عاجلة لتنظيم وحماية فضائها السيبراني. إن هذا الواقع يفرض على العراق ضرورة تحديث وتطوير تشريعاته القانونية لتواكب التطور التقني المتسارع، من خلال وضع قوانين فعّالة تضمن حماية الأنظمة والمعلومات من المخاطر السيبرانية، وتحديد المسؤوليات القانونية للمؤسسات والأفراد في مواجهة هذه التهديدات.

أولا: أهمية البحث

تنبع أهمية هذا البحث من كونه يتناول موضوعًا حديثًا وضروريًا في ظل التطور التكنولوجي المتسارع، حيث أصبحت الهجمات السيبرانية تهديدًا حقيقيًا لأمن الدول واستقرارها. وتكمن أهمية هذه الدراسة في الدور الحيوي الذي يؤديه الأمن السيبراني في حماية المصالح الوطنية والأمن المجتمعي، خصوصًا في ظل تزايد التهديدات الرقمية التي تستهدف المؤسسات الحيوية والبنى التحتية للدولة. ويصبح هذا الموضوع أكثر إلحاحًا في العراق، نظرًا لخصوصية الوضع الأمني والسياسي الذي يجعله عرضة لمخاطر الهجمات السيبرانية بشكل متزايد.

ثانيا: مشكلة البحث

يواجه العراق، كغيره من الدول، تحديات متزايدة في مجال الأمن السيبراني نتيجة التطور السريع في التكنولوجيا الرقمية، واعتماد المؤسسات الحكومية والخاصة بشكل متزايد على الأنظمة الإلكترونية. ورغم وجود بعض النصوص القانونية التي تعالج الجرائم الإلكترونية وأمن المعلومات، فإن العراق لا يمتلك حتى الآن إطارًا قانونيًا متكاملًا يُنظّم بشكل دقيق جوانب الأمن السيبراني وفق المعايير الدولية، ويُعتبر هذا قصورًا تشريعيًا. وعلى الرغم من وجود بعض النصوص القانونية في التشريعات العراقية التي تتناول بشكل غير مباشر الجوانب المرتبطة بالأمن السيبراني، فإن العراق لا يزال بحاجة إلى إطار قانوني شامل ومتكامل يعالج هذه المسألة بصورة دقيقة، ويحدد المسؤوليات القانونية، ويضع آليات فعالة للوقاية من الهجمات السيبرانية والتعامل معها حال وقوعها.

تهدف هذه الدراسة إلى تحليل الإطار القانوني لحماية الأمن السيبراني في العراق، من خلال استعراض وتحليل التشريعات الوطنية ذات الصلة، ومدى انسجامها مع المعايير الدولية المعتمدة في هذا المجال. كما تسعى الدراسة إلى الكشف عن أوجه القصور في المنظومة القانونية العراقية، مع تقديم مقترحات عملية لتعزيز الأمن السيبراني في العراق بما يواكب التطورات التكنولوجية العالمية.

ثالثا: أسئلة البحث

تبرز الإشكالية الرئيسة لهذا البحث في التساؤل الآتي:

ما مدى كفاية التشريعات العراقية الحالية في حماية الأمن السيبراني، وما مدى توافقها مع المعايير الدولية المعتمدة في هذا المجال؟

وينبثق عن هذا التساؤل الرئيس عدد من **التساؤلات الفرعية**، منها:

١. ما مفهوم الأمن السيبراني وأهميته في حماية المصالح الوطنية؟
٢. ما هي التشريعات العراقية الحالية المتعلقة بالأمن السيبراني، وما مدى فعاليتها في مواجهة هذه التهديدات؟

٣. إلى أي مدى تتوافق هذه التشريعات مع المعايير الدولية المعتمدة في حماية الأمن السيبراني؟
٤. ما هي الحلول والمقترحات التي يمكن تقديمها لتعزيز الإطار القانوني لحماية الأمن السيبراني في العراق؟

رابعاً : أهداف البحث

يهدف البحث إلى تحليل التشريعات العراقية المتعلقة بالأمن السيبراني، وبيان مدى انسجامها مع المعايير الدولية، مما يساعد في تحديد أوجه القصور التشريعي واقتراح حلول قانونية فعّالة. كما تبرز أهمية البحث في تقديمه توصيات عملية تسهم في تطوير المنظومة القانونية العراقية بما يعزز حماية المؤسسات الحكومية والخاصة من التهديدات السيبرانية. الإضافة إلى ذلك، يساهم البحث في إثراء المكتبة القانونية العراقية والعربية بمادة علمية متخصصة يمكن أن تفيد الباحثين وصنّاع القرار على حد سواء.

خامساً : نطاق البحث

ينحصر نطاق هذا البحث في دراسة وتحليل الإطار القانوني لحماية الأمن السيبراني في العراق، مع التركيز على التشريعات الوطنية ذات الصلة، مثل القوانين المتعلقة بجرائم المعلوماتية وأمن الاتصالات وحماية البيانات. ويتناول البحث أيضًا المعايير الدولية المعتمدة في مجال الأمن السيبراني، مثل المبادئ الصادرة عن الأمم المتحدة، والاتحاد الدولي للاتصالات (ITU)، ومنظمات الأمن السيبراني العالمية، بهدف تحديد مدى توافق التشريعات العراقية مع هذه المعايير.

من حيث الإطار الزمني، يركز البحث على القوانين واللوائح المعمول بها في العراق حتى تاريخ إعداد الدراسة، مع الإشارة إلى التطورات الحديثة في المجال التقني والقانوني. أما من حيث الإطار المكاني، فإن الدراسة تقتصر على الواقع القانوني في العراق مع تقديم مقارنات محدودة مع بعض الأنظمة القانونية الأخرى التي تتمتع بتجارب متقدمة في حماية الأمن السيبراني، وذلك بهدف استخلاص الدروس المستفادة وتقديم توصيات تتناسب مع البيئة القانونية العراقية.

سادساً: منهجية البحث

ولتحقيق أهداف الدراسة، سيتم الاعتماد على المنهج التحليلي المقارن، الذي يقوم على تحليل النصوص القانونية العراقية ذات العلاقة بالأمن السيبراني، مع مقارنتها بالمعايير الدولية والتشريعات المطبقة في دول أخرى ذات تجارب متقدمة في هذا المجال. ومن خلال هذه المقارنة، سيتم استخلاص النتائج ووضع التوصيات المناسبة التي تسهم في تعزيز المنظومة القانونية العراقية لحماية الأمن

السيبراني بشكل أكثر فاعلية. وتأمل الدراسة أن تقدم مساهمة علمية رصينة تُثري المكتبة القانونية العراقية، وتكون مرجعًا مفيدًا لصنّاع القرار والباحثين في مجالات القانون والتكنولوجيا على حد سواء.

خطة البحث

المبحث الأول: ماهية الأمن السيبراني وأهميته

- المطلب الأول: مفهوم الأمن السيبراني
- المطلب الثاني: أهمية الأمن السيبراني في حماية المصالح الوطنية

المبحث الثاني: الإطار القانوني للأمن السيبراني في العراق

- المطلب الأول: التشريعات الوطنية المتعلقة بالأمن السيبراني
- المطلب الثاني: دور المؤسسات الحكومية في حماية الأمن السيبراني

المبحث الثالث: المعايير الدولية للأمن السيبراني ومدى انسجامها مع التشريعات العراقية

- المطلب الأول: دور المعايير الدولية في تعزيز الأمن السيبراني وحماية الفضاء الرقمي.
- المطلب الثاني: أوجه التشابه والاختلاف بين التشريعات العراقية والمعايير الدولية

الخاتمة :

- النتائج
- التوصيات

المراجع

المبحث الأول / ماهية الأمن السيبراني وأهميته

يُعد الأمن السيبراني من الموضوعات الحديثة التي برزت نتيجة التطور السريع في تكنولوجيا المعلومات والاتصالات، وقد بات يشكل أحد العناصر الأساسية في حماية البنية التحتية الرقمية للدول والمؤسسات والأفراد على حدٍ سواء. وقد أدى تصاعد الهجمات السيبرانية إلى بروز الحاجة الملحة لإطار قانوني متكامل يُنظّم هذا المجال بما يضمن حماية المعلومات والأنظمة الإلكترونية من المخاطر المحتملة. وفي هذا السياق، يُعد تحديد مفهوم الأمن السيبراني وتوضيح أبعاده القانونية من الخطوات الأساسية لفهم آليات حمايته وتشريعاته، وهو ما سيتم تناوله في هذا المبحث. [١]

المطلب الأول/ مفهوم الأمن السيبراني

يُعد الأمن السيبراني من المفاهيم الحديثة التي برزت مع التطور المتسارع لتكنولوجيا المعلومات والاتصالات، حيث أصبح يشكل ركيزة أساسية في حماية الفضاء الإلكتروني من التهديدات السيبرانية المتزايدة. ومع ازدياد الاعتماد على التقنيات الرقمية، بات من الضروري وضع إطار قانوني وتنظيمي يضمن حماية الشبكات والأنظمة المعلوماتية من الاختراقات والهجمات الإلكترونية. وقد تنوعت تعريفات الأمن السيبراني وفقًا للجهات المختصة، حيث يُنظر إليه على أنه مجموعة من التدابير والتقنيات والسياسات التي تهدف إلى حماية الأنظمة الرقمية والشبكات الإلكترونية من أي اختراق أو استغلال غير مشروع. كما يراه بعض الباحثين على أنه لا يقتصر فقط على الحماية التقنية، بل يشمل أيضًا وضع أطر قانونية وتنظيمية تحكم استخدام الفضاء الإلكتروني وتضمن الالتزام بمعايير الحماية والأمان.[٢]

على المستوى الوطني، سعى العراق إلى تعزيز الحماية القانونية للأمن السيبراني من خلال إدراج مجموعة من النصوص الدستورية والتشريعية التي تضمن حماية البيانات الشخصية وتحد من الانتهاكات الإلكترونية. فقد نص الدستور العراقي لعام ٢٠٠٥ في المادة ١٧ على أن "للفرد حق في الحفاظ على خصوصياته الشخصية والعائلية والبيئية والمالية وغيرها، وفقًا للقانون"، مما يشكل اعترافًا صريحًا بحق الأفراد في حماية بياناتهم الشخصية من أي انتهاك إلكتروني. كما أكدت المادة ٤٠ من الدستور على أن "حرية الاتصالات البريدية والبرقية والهاتفية والإلكترونية وغيرها مكفولة، ولا يجوز مراقبتها أو التنصت عليها أو الكشف عنها إلا بموجب قانون وبقرار قضائي"، مما يضع أساسًا قانونيًا لحماية البيانات الشخصية وخصوصية المستخدمين في الفضاء الإلكتروني.[٣].

إضافة إلى ذلك، تضمنت بعض القوانين العراقية الأخرى أحكامًا تتعلق بحماية البيانات الشخصية في سياق الأمن السيبراني، مثل المادة (٧) من قانون الأحوال المدنية رقم (٦٥) لسنة ١٩٧٢، التي أكدت على سرية البيانات المسجلة في السجل المدني وعدم السماح بالاطلاع عليها إلا

من قبل الجهات المخولة قانونيًا. كما وضع قانون أصول المحاكمات الجزائية العراقي (المواد ٧٢ – ٨٣) ضوابط قانونية للتعامل مع البيانات الشخصية، بما يضمن حمايتها من الاستخدام غير المشروع أو الاختراقات السيبرانية. هذه النصوص القانونية تمثل خطوة مهمة نحو تعزيز الأمن السيبراني في العراق، لكنها لا تزال بحاجة إلى مزيد من التطوير لتتماشى مع التطورات التقنية السريعة والمتطلبات الدولية في هذا المجال.[٤]

أما على المستوى الدولي، فقد عرّف الاتحاد الدولي للاتصالات الأمن السيبراني بأنه منظومة متكاملة من السياسات والإجراءات الأمنية والممارسات الفضلى التي تُستخدم لحماية البيئة الرقمية من المخاطر السيبرانية التي قد تؤثر في الأفراد أو المؤسسات أو الحكومات. أما الهيئة الوطنية للأمن السيبراني، فقد عرفته بأنه حماية الشبكات وأنظمة تقنية المعلومات والتقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات وخدمات وبيانات من أي اختراق، أو تعطيل أو تعديل أو استخدام غير مشروع، مع شموله لمفاهيم الأمن الإلكتروني والرقمي والمعلوماتي. ويشمل الأمن السيبراني بذلك مجموعة من الآليات والإجراءات التي تهدف إلى الكشف عن التهديدات السيبرانية وإحباطها قبل أن تؤثر في الأنظمة الرقمية، مما يضمن استمرارية عملها دون انقطاع أو أضرار جسيمة.[٥]

بذلك، لا يمكن حصر الأمن السيبراني في كونه مجموعة من الإجراءات التقنية، بل هو إطار متكامل يشمل الأبعاد القانونية والتنظيمية التي تهدف إلى تأمين الفضاء السيبراني وحماية البيانات الرقمية من المخاطر الإلكترونية. ومع تزايد التهديدات السيبرانية عالميًا، بات من الضروري تطوير سياسات أكثر شمولية لتعزيز الأمن السيبراني وفقًا لأفضل الممارسات والمعايير الدولية. كما أن تعزيز الإطار القانوني الوطني يعد ضرورة ملحة لضمان بيئة رقمية آمنة، وهو ما يتطلب مواءمة التشريعات العراقية مع المعايير الدولية لمواجهة التحديات المتزايدة في هذا المجال. ورغم الجهود المبذولة في هذا السياق، لا يزال هناك العديد من التحديات التي تواجه العراق في تحقيق حماية متكاملة للأمن السيبراني، مما يستدعي تكثيف الجهود التشريعية والتقنية لضمان أمن المعلومات في المستقبل القريب.

المطلب الثاني / أهمية الأمن السيبراني في حماية المصالح الوطنية

يُعد الأمن السيبراني ركيزة أساسية في حماية المصالح الوطنية، خصوصًا في ظل التحول الرقمي المتسارع والاعتماد المتزايد على التكنولوجيا في مختلف القطاعات. في العراق، تبرز أهمية الأمن السيبراني نتيجة التهديدات الإلكترونية المتزايدة التي تستهدف البنية التحتية الحيوية، والمؤسسات الحكومية، والقطاع الخاص، مما يجعل من الضروري تبني استراتيجيات متقدمة لضمان أمن الفضاء السيبراني وحماية المصالح الوطنية من المخاطر التي قد تنعكس على الأمن القومي والاستقرار الاقتصادي والاجتماعي.[٦]

إن حماية البنية التحتية الرقمية تمثل أولوية قصوى في إطار تعزيز الأمن السيبراني، إذ تعتمد العديد من القطاعات الحيوية، مثل الطاقة، والاتصالات، والخدمات المصرفية، والأنظمة الحكومية، على التكنولوجيا الرقمية بشكل أساسي. ومع ذلك، فإن هذه القطاعات تواجه تهديدات سيبرانية متزايدة، مثل الهجمات الإلكترونية التي تستهدف أنظمة التشغيل، وسرقة البيانات، وتعطيل الخدمات، مما قد يؤدي إلى شلل اقتصادي وخسائر كبيرة. ويشكل تعزيز الأمن السيبراني في هذه القطاعات ضمانًا لاستمرارية الخدمات الأساسية وحماية الاقتصاد الوطني من الأضرار الناجمة عن الاختراقات والجرائم الإلكترونية. علاوة على ذلك، فإن الأمن السيبراني يلعب دورًا حاسمًا في حماية البيانات الوطنية والمعلومات السرية للدولة. فمع تصاعد التهديدات السيبرانية التي تستهدف المؤسسات الحكومية والأجهزة الأمنية، تزداد الحاجة إلى وضع أطر قانونية وتقنية صارمة لضمان سرية هذه المعلومات ومنع استخدامها لأغراض غير مشروعة. ويأتي الدستور العراقي لعام ٢٠٠٥ ليؤكد على هذا الجانب، حيث نصت المادة ١٧ على حماية خصوصية الأفراد، فيما أكدت المادة ٤٠ على سرية الاتصالات الإلكترونية وعدم جواز مراقبتها أو التنصت عليها إلا بموجب قانون وقرار قضائي. وهذه النصوص الدستورية توفر أساسًا قانونيًا يعزز حماية البيانات الشخصية ويحدّ من الانتهاكات السيبرانية.(٧)

إلى جانب حماية البيانات، يسهم الأمن السيبراني في تعزيز الاستقرار الاقتصادي من خلال الحد من الجرائم الإلكترونية التي تستهدف الأنظمة المصرفية، والتعاملات المالية، والمشروعات الاستثمارية. فقد أصبحت الهجمات الإلكترونية، مثل الاحتيال المالي، وغسيل الأموال، والاختراقات المصرفية، تشكل خطرًا متزايدًا على الاقتصاد العراقي، مما يستوجب تعزيز التدابير الأمنية لحماية المعاملات الرقمية وضمان بيئة آمنة للاستثمار والتجارة الإلكترونية. كما أن تعزيز الأمن السيبراني يسهم في زيادة ثقة الشركات والمستثمرين في البنية التحتية الرقمية، مما ينعكس إيجابيًا على النمو الاقتصادي والاستثمار في التكنولوجيا الحديثة.(٨).

ولا يقتصر دور الأمن السيبراني على المؤسسات والبنية التحتية فحسب، بل يمتد ليشمل حماية خصوصية الأفراد وبياناتهم الشخصية في ظل التوسع المتزايد في استخدام الإنترنت ووسائل التواصل الاجتماعي. فقد أصبح الأفراد أكثر عرضة لجرائم الاحتيال الإلكتروني، وسرقة الهوية، وعمليات الابتزاز السيبراني، مما يستدعي اتخاذ تدابير وقائية لتعزيز الوعي المجتمعي بمخاطر الفضاء السيبراني وكيفية الحماية منه. إن تعزيز الأمن السيبراني في هذا المجال يسهم في بناء بيئة رقمية أكثر أمانًا وثقة، تحمي حقوق المستخدمين وتحد من التهديدات التي تستهدف الأفراد والمؤسسات على حد سواء. ولمواجهة التحديات المتزايدة، يتطلب الأمن السيبراني في العراق نهجًا شاملاً يقوم على تحديث التشريعات، وتعزيز التنسيق بين المؤسسات الحكومية والقطاع الخاص، والاستثمار في

التقنيات الحديثة لمكافحة الجرائم السيبرانية. كما أن تطوير برامج تدريبية متخصصة في مجال الأمن السيبراني وبناء قدرات وطنية قادرة على التعامل مع التهديدات الإلكترونية يعد من الخطوات الأساسية لتعزيز الحماية السيبرانية.[٩]

المبحث الثاني / الإطار القانوني للأمن السيبراني في العراق

مع تزايد الاعتماد على الفضاء السيبراني في مختلف المجالات، أصبح وضع إطار قانوني فعّال للأمن السيبراني ضرورة استراتيجية لحماية المصالح الوطنية وتعزيز الأمن الرقمي. فالتشريعات الوطنية تعد الركيزة الأساسية في مواجهة التهديدات الإلكترونية، حيث تسهم في تحديد القواعد القانونية المنظمة لاستخدام الفضاء السيبراني، وتضع آليات قانونية لمكافحة الجرائم السيبرانية، وتحمي حقوق الأفراد والمؤسسات في هذا المجال. ولذلك، فإن تطوير إطار قانوني شامل للأمن السيبراني في العراق يعد خطوة أساسية لضمان الاستخدام الآمن والموثوق للتكنولوجيا الرقمية. وعلى الرغم من وجود عدة قوانين تتناول بعض جوانب الأمن السيبراني في العراق، إلا أن التشريعات الوطنية لا تزال بحاجة إلى إطار قانوني موحد يعالج جميع التحديات المرتبطة بحماية الفضاء السيبراني، ويحدد بوضوح أسس المسؤولية القانونية عن الجرائم الإلكترونية، وسبل التصدي لها وفق المعايير الدولية. كما تلعب المؤسسات الحكومية دورًا محوريًا في تطبيق هذه التشريعات من خلال وضع السياسات، وتعزيز البنية التحتية الأمنية، ومواجهة المخاطر السيبرانية عبر آليات وقائية واستراتيجية فعالة.

يهدف هذا المبحث إلى تحليل التشريعات الوطنية المتعلقة بالأمن السيبراني في العراق، ومدى ملاءمتها لمواجهة التحديات الراهنة في المجال الرقمي، كما يتناول دور المؤسسات الحكومية في تعزيز الأمن السيبراني، من خلال دراسة اختصاصاتها وآليات عملها في حماية الفضاء الإلكتروني، بما يضمن بيئة رقمية آمنة ومستقرة تتماشى مع التطورات العالمية في هذا المجال.

المطلب الأول/ التشريعات الوطنية المتعلقة بالأمن السيبراني

يتميز النظام القانوني العراقي بإطار تشريعي واسع يشمل مختلف المجالات القانونية، ومن بينها حماية البيانات الشخصية والأمن السيبراني، وذلك لضمان تنظيم استخدامها والحفاظ عليها من أي انتهاك أو استغلال غير مشروع. وتُعد هذه الحماية ضرورية في ظل التطور التكنولوجي السريع الذي يشهده العالم، حيث أصبحت البيانات الشخصية من الموارد الحساسة التي تتطلب تنظيمًا قانونيًا دقيقًا للحفاظ على خصوصية الأفراد وضمان عدم التعدي عليها. وقد كفل المشرّع العراقي هذا الحق من خلال عدة نصوص قانونية تسعى إلى وضع أسس قانونية لحماية البيانات الشخصية وتنظيم آلية الوصول إليها واستخدامها.[١٠]

يُعتبر قانون الأحوال المدنية رقم (٦٥) لسنة ١٩٧٢ أحد أبرز القوانين التي تتناول مسألة حماية البيانات الشخصية، إذ نصت المادة (٧) منه على سرية القيود المسجلة في السجل المدني، موضحة أن هذه المعلومات لا يجوز الاطلاع عليها إلا من قبل الشخص المعني أو الجهات المخولة رسميًا، مثل القضاء والجهات التحقيقية وضباط التجنيد، في إطار قيامهم بوظائفهم القانونية. ويؤكد هذا النص التزام القانون بمبدأ حماية الخصوصية، مع مراعاة الاستثناءات التي تفرضها مقتضيات العمل الرسمي والإجراءات القضائية، مما يعكس سعي المشرّع إلى تحقيق التوازن بين حقوق الأفراد ومتطلبات النظام القانوني والإداري.[١١]

وعلى الرغم من ذلك، فإن التشريعات العراقية الحالية المتعلقة بحماية البيانات الشخصية لا تزال تعاني من بعض أوجه القصور التي تتطلب تطويرًا لضمان حماية أكثر شمولًا لهذه البيانات. فعلى سبيل المثال، ينظم قانون أصول المحاكمات الجزائية بعض الجوانب المتعلقة باستخدام البيانات الشخصية في الإجراءات القانونية، لكنه لا يوفر ضمانات كافية تحول دون إساءة استخدامها أو تعرضها للانتهاك. وهذا يستدعي تحديث هذه التشريعات بما يتماشى مع التطورات الرقمية المتسارعة، بحيث تتضمن نصوصًا أكثر وضوحًا لحماية خصوصية الأفراد من أي استغلال غير مشروع[١٢].

وفي هذا السياق، يمثل مشروع قانون جرائم المعلوماتية محاولة لتنظيم استخدام التكنولوجيا والحد من الجرائم السيبرانية، إلا أنه أثار جدلًا واسعًا بسبب بعض مواده التي قد تؤثر في الحقوق والحريات الأساسية، بما في ذلك حماية البيانات الشخصية وحرية التعبير. وقد أظهرت دراسات متخصصة أن بعض مواد المسودة، مثل المادة (١٩)، تتعارض مع المبادئ الدولية لحقوق الإنسان، إذ إنها قد تقيد حرية التعبير وتحد من إمكانية الوصول إلى المعلومات. وبسبب هذه المخاوف، أوصت العديد من الجهات الحقوقية برفض المسودة بصيغتها الحالية، معتبرة أنها لا توفر الضمانات اللازمة لحماية حقوق الأفراد في الفضاء الرقمي.[١٣]

وقد تعرضت المسودة لانتقادات واسعة بسبب منحها السلطات صلاحيات واسعة قد تُستخدم لمراقبة الأفراد وفرض قيود مشددة على المحتوى الرقمي. فالمادة (٣) من القانون تمنح صلاحيات لمنع أي استخدام للتكنولوجيا يمكن أن يؤثر على استقلالية الدولة وأمنها الاقتصادي والسياسي والعسكري، وهو نص عام قد يؤدي إلى تقييد حرية التعبير تحت مبررات فضفاضة. كما أن المادة (٦) تحظر نشر معلومات قد تؤثر على الثقة بالنظام المالي والتجارة الإلكترونية، مما قد يحد من قدرة الأفراد والمؤسسات على انتقاد السياسات الاقتصادية والإدارية بشكل علني.[١٤]

في ظل هذه التحديات، تبرز الحاجة الملحة إلى تطوير تشريعات متوازنة تحقق الحماية الفعالة للبيانات الشخصية دون المساس بالحقوق الأساسية للأفراد. وينبغي أن تتماشى هذه التشريعات مع

المعايير الدولية لضمان عدم استخدامها كأداة لتقييد الحريات أو فرض رقابة مشددة على المواطنين. إن تحديث الإطار القانوني لحماية البيانات الشخصية، بحيث يتناسب مع التطورات التقنية الحديثة، يُعد خطوة ضرورية نحو تعزيز الأمن السيبراني وبناء بيئة قانونية عادلة تحافظ على خصوصية الأفراد وتضمن استخدامًا مشروعًا وآمنًا للمعلومات في المجتمع العراقي.

المطلب الثاني/ دور المؤسسات الحكومية في حماية الأمن السيبراني

في مختلف القطاعات، أصبح الأمن السيبراني أحد الأولويات الاستراتيجية التي تتطلب تدخلًا حكوميًا فعالًا لضمان حماية البنية التحتية الرقمية والمعلومات الحساسة. تواجه الدول، بما في ذلك العراق، تهديدات سيبرانية متنامية تستهدف مؤسساتها الحكومية والخاصة، مما يجعل من الضروري تبني سياسات وأطر قانونية متكاملة لتعزيز الأمن السيبراني والتصدي للهجمات الإلكترونية التي قد تؤثر على الاستقرار الوطني والاقتصادي. ومن هذا المنطلق، تضطلع المؤسسات الحكومية بدور أساسي في تطوير استراتيجيات الحماية، ورفع مستوى الوعي، وتعزيز التعاون بين مختلف الجهات لضمان فضاء سيبراني آمن وموثوق.[١٥]

تعد وزارة الداخلية إحدى الجهات الرئيسة المسؤولة عن الأمن السيبراني، حيث تتولى مكافحة الجرائم الإلكترونية من خلال وحداتها المختصة، وتعمل على تعزيز القدرات الأمنية في رصد التهديدات الرقمية والتحقيق فيها. كما تساهم الوزارة في نشر الوعي حول المخاطر السيبرانية من خلال برامج توعوية تستهدف المؤسسات والمواطنين، مما يسهم في تعزيز الثقافة الأمنية وتقليل فرص الاختراقات الإلكترونية. بالإضافة إلى ذلك، تتعاون الوزارة مع الجهات القضائية لضمان إنفاذ القوانين المتعلقة بالجرائم السيبرانية، مما يعزز الردع القانوني ويحد من الأنشطة الإجرامية في الفضاء الإلكتروني.[١٦] إلى جانب وزارة الداخلية، تلعب الهيئة الوطنية للأمن السيبراني دورًا محوريًا في وضع الاستراتيجيات والسياسات الوطنية لحماية البنية التحتية الرقمية للدولة. وعلى الرغم من أن الهيئة لا تزال في طور التطوير، فإنها تسعى إلى بناء منظومة أمنية متكاملة تعتمد على معايير دولية متقدمة، مع التركيز على تحسين قدرات الاستجابة للهجمات السيبرانية وتطوير أنظمة حماية متطورة. كما تهتم الهيئة بتعزيز التعاون بين الجهات الحكومية والقطاع الخاص، نظرًا لأن الأمن السيبراني يعد مسؤولية جماعية تتطلب تضافر الجهود بين مختلف الفاعلين في المجال الرقمي[١٧].

بدورها، تضطلع وزارة الاتصالات بمسؤولية تأمين الشبكات الحكومية وتطوير البنية التحتية التكنولوجية، حيث تشرف على مزودي خدمات الإنترنت لضمان الامتثال لمعايير الأمن السيبراني، كما تعمل على تنفيذ مشاريع تهدف إلى تعزيز أمن المعلومات في المؤسسات الحكومية. ومن خلال تبني تقنيات التشفير وأنظمة الحماية المتقدمة، تسعى الوزارة إلى الحد من التهديدات السيبرانية وضمان بيئة رقمية آمنة تدعم التحول الرقمي في البلاد. وعلى المستوى التشريعي، يقوم مجلس النواب العراقي

بدور هام في وضع الأطر القانونية المنظمة للأمن السيبراني، حيث يساهم في تشريع القوانين التي تعالج قضايا أمن المعلومات وحماية البيانات. ورغم وجود بعض النصوص القانونية المتعلقة بجرائم المعلوماتية، لا يزال العراق بحاجة إلى قانون شامل يعالج مختلف جوانب الأمن السيبراني بشكل أكثر تفصيلًا، ويحدد المسؤوليات بوضوح، ويضمن انسجام التشريعات الوطنية مع المعايير الدولية المعتمدة.[١٨]

وعلى الرغم من الجهود التي تبذلها المؤسسات الحكومية، فإن التحديات لا تزال قائمة، ومن أبرزها نقص الموارد التقنية والكوادر البشرية المؤهلة، إلى جانب ضعف التنسيق بين الجهات المعنية بالأمن السيبراني. كما أن التطور المستمر في أساليب الهجمات السيبرانية يستلزم تحديثًا دوريًا للأنظمة والسياسات الأمنية، مما يتطلب استثمارات مستمرة في هذا المجال. ولتجاوز هذه التحديات، من الضروري تعزيز التعاون مع الدول ذات الخبرة المتقدمة في الأمن السيبراني، والاستفادة من الخبرات الدولية في تطوير السياسات والبنى التحتية الرقمية.

لذا، يمثل الأمن السيبراني حجر الأساس في حماية الأمن الوطني وتعزيز الاستقرار الرقمي في العراق، وهو مسؤولية تتطلب تنسيقًا فاعلًا بين مختلف المؤسسات الحكومية. ومن خلال تطوير التشريعات، تعزيز البنية التحتية الرقمية، والاستثمار في التكنولوجيا والتدريب، يمكن للحكومة العراقية تحقيق مستوى متقدم من الحماية السيبرانية يواكب التحديات المتزايدة في العالم الرقمي.[١٩]

المبحث الثالث/ المعايير الدولية للأمن السيبراني ومدى انسجامها مع التشريعات العراقية

يشكل الأمن السيبراني محور اهتمام متزايد على المستويين الدولي والوطني، حيث أضحت التهديدات الإلكترونية أكثر تعقيدًا وانتشارًا، مما يستدعي تبني استراتيجيات قانونية وتنظيمية فعالة لحماية الفضاء الرقمي. في هذا الإطار، عملت العديد من المنظمات الدولية، مثل الأمم المتحدة والاتحاد الدولي للاتصالات (ITU) ومنظمة التعاون الاقتصادي والتنمية (OECD) ، على وضع معايير وإرشادات تهدف إلى توحيد الجهود الدولية وتعزيز قدرة الدول على التصدي للمخاطر السيبرانية. هذه المعايير لا تقتصر على وضع الأطر القانونية فحسب، بل تشمل أيضًا السياسات التقنية والتدابير الوقائية التي تضمن استجابة شاملة وفعالة لمختلف التهديدات الرقمية[٢٠].

على الرغم من الجهود التي يبذلها العراق في هذا المجال، إلا أن الإطار القانوني للأمن السيبراني لا يزال يواجه تحديات تتعلق بمدى تكامله مع المعايير الدولية. فالمنظومة التشريعية العراقية، رغم احتوائها على بعض الأحكام المتعلقة بحماية البيانات والجرائم الإلكترونية، تفتقر إلى إطار شامل يغطي مختلف جوانب الأمن السيبراني وفقًا للمعايير والممارسات العالمية. وعليه، فإن

تحليل مدى توافق التشريعات العراقية مع هذه المعايير يمثل خطوة ضرورية لتحديد الفجوات القانونية والتنظيمية واقتراح الإصلاحات اللازمة لتعزيز الأمن السيبراني في البلاد.[٢١]

ينقسم هذا المبحث إلى مطلبين رئيسين، حيث يتناول المطلب الأول دور المعايير الدولية في تعزيز الأمن السيبراني وحماية الفضاء الرقمي، من خلال استعراض أهم الاتفاقيات والتوصيات الصادرة عن الهيئات الدولية المتخصصة. أما المطلب الثاني، فيناقش أوجه التشابه والاختلاف بين التشريعات العراقية والمعايير الدولية، بهدف تحديد الجوانب التي تحتاج إلى تطوير لضمان بيئة سيبرانية أكثر أمانًا واستدامة.

المطلب الأول/ دور المعايير الدولية في تعزيز الأمن السيبراني وحماية الفضاء الرقمي

مع تزايد التهديدات السيبرانية التي تستهدف الاقتصادات والبنى التحتية الحيوية للدول، أصبحت الحاجة إلى وضع معايير دولية موحدة لتعزيز الأمن السيبراني أكثر إلحاحًا من أي وقت مضى. وقد أسهمت العديد من المنظمات والهيئات الدولية في تطوير أطر قانونية وتقنية تهدف إلى مكافحة الجرائم الإلكترونية التي تتجاوز الحدود الجغرافية، مما يستدعي تنسيقًا دوليًا فعالًا لمواجهتها. حيث تعد الاتفاقيات الدولية إحدى الركائز الأساسية لمكافحة الجرائم السيبرانية، حيث توفر إطارًا قانونيًا موحدًا للدول الأعضاء لمعالجة هذه التهديدات.

ومن أبرز هذه الاتفاقيات اتفاقية بودابست لمكافحة الجرائم الإلكترونية، التي أرست الأسس القانونية لمواجهة الجرائم السيبرانية على المستوى الدولي. وتشمل هذه الجرائم اختراق الأنظمة، وسرقة البيانات، والتلاعب بالمعلومات الرقمية. كما تلزم الاتفاقية الدول الأعضاء بتحديث تشريعاتها الوطنية بما يواكب التطورات التكنولوجية، وتعزز التعاون القضائي والأمني لضمان محاسبة مرتكبي هذه الجرائم حتى عبر الحدود. إلى جانب الأطر القانونية، تلعب المعايير التقنية دورًا محوريًا في تعزيز الأمن السيبراني وحماية البنى التحتية الرقمية من الهجمات المتزايدة. ومن أبرز هذه المعايير معيار ISO/IEC 27001الصادر عن المنظمة الدولية للمعايير، والذي يحدد متطلبات إدارة أمن المعلومات، بما في ذلك تقييم المخاطر، وتطبيق التدابير الوقائية، ووضع خطط استجابة للحوادث الأمنية. كما يبرز معيار ISO/IEC 27032 الذي يركز على أمن الفضاء السيبراني، حيث يقدم إرشادات لحماية الشبكات والأنظمة من الهجمات الإلكترونية المتطورة. وتساعد هذه المعايير الحكومات والمؤسسات على تبني سياسات أمنية فعالة تضمن حماية بياناتها واستمرارية عملياتها الرقمية .[٢٢]

في السياق ذاته، يؤدي المعهد الوطني للمعايير والتكنولوجيا (NIST) دورًا محوريًا في تعزيز الأمن السيبراني من خلال تطوير إطار NIST للأمن السيبراني، الذي يستند إلى خمس وظائف رئيسية: تحديد الأصول الرقمية، تطبيق التدابير الوقائية، اكتشاف التهديدات، الاستجابة للهجمات،

والتعافي من الأضرار. ويساعد هذا الإطار المؤسسات على تطوير استراتيجيات أمنية متكاملة، مما يمكنها من التصدي للهجمات الإلكترونية بفعالية، لا سيما في القطاعات الحيوية التي تتطلب مستوى عالٍ من الحماية.[٢٣]

على المستوى الدولي، يعمل الاتحاد الدولي للاتصالات (ITU) على دعم جهود تعزيز الأمن السيبراني من خلال تقديم المساعدة التقنية للدول الأعضاء، وتسهيل تبادل المعلومات حول التهديدات الإلكترونية، إلى جانب وضع استراتيجيات وطنية لحماية الأنظمة الرقمية. كما يركز الاتحاد على دعم الدول النامية في بناء بيئة إلكترونية آمنة من خلال توفير برامج تدريبية متخصصة وبناء القدرات، مما يسهم في الحد من مخاطر الهجمات الإلكترونية التي قد تهدد استقرارها الرقمي[٢٤].

إضافةً إلى الجهود القانونية والتقنية، يشكل الوعي المجتمعي عنصرًا أساسيًا في تعزيز الأمن السيبراني، حيث تعتمد فعالية أي استراتيجية أمنية على مدى إدراك الأفراد والمؤسسات للمخاطر الإلكترونية وطرق الوقاية منها. ولهذا السبب، تعمل العديد من الدول على تنظيم حملات توعوية، وإدراج مواد تعليمية متخصصة في المناهج الدراسية، إلى جانب توفير برامج تدريبية للموظفين والمتخصصين في مجال أمن المعلومات. ويسهم هذا النهج في تقليل الثغرات الأمنية التي قد يستغلها المهاجمون لاختراق الأنظمة الرقمية، مما يعزز الحماية على المستويين الفردي والمؤسسي.[٢٥]

وعلى الرغم من التقدم الملحوظ في تطوير المعايير الدولية للأمن السيبراني، لا تزال هناك تحديات تعيق تطبيقها بفعالية في بعض الدول. من أبرز هذه التحديات التفاوت التشريعي بين الدول، حيث تختلف القوانين الوطنية المتعلقة بمكافحة الجرائم الإلكترونية، مما قد يعرقل التعاون الدولي في ملاحقة المجرمين السيبرانيين. كما تواجه بعض الدول مشكلات في البنية التحتية الرقمية، مما يجعل أنظمتها أكثر عرضة للهجمات الإلكترونية. إضافةً إلى ذلك، يشكل نقص الكفاءات المتخصصة تحديًا آخر، حيث تعاني العديد من الحكومات والشركات من صعوبة في استقطاب خبراء أمن سيبراني مؤهلين لمواكبة التهديدات المتزايدة.[٢٦]

المطلب الثاني/ أوجه التشابه والاختلاف بين التشريعات العراقية والمعايير الدولية

تمثل الجرائم الإلكترونية تهديدًا متزايدًا على مستوى العالم، مما دفع العديد من الدول إلى تبني تشريعات تتماشى مع المعايير الدولية لضمان أمن الفضاء الرقمي وحماية البيانات من الهجمات السيبرانية. في هذا السياق، سعى العراق إلى تطوير منظومته القانونية لمواجهة التحديات الرقمية، إلا أن مدى انسجام هذه التشريعات مع المعايير الدولية لا يزال محل تقييم، حيث توجد بعض الجوانب التي تتوافق مع هذه المعايير، في حين أن هناك فجوات تتطلب مزيدًا من التطوير والتحديث.[٢٧]

يتجلى أحد أوجه التشابه الرئيسة في أنّ التشريعات العراقية، على غرار المعايير الدولية، تجرّم العديد من الأفعال الإلكترونية غير المشروعة، مثل الاختراق غير المصرح به، وسرقة البيانات، والاحتيال الإلكتروني. فهذه الجرائم تُعد انتهاكات صريحة للأمن السيبراني، وتحظى بتجريم واضح في القوانين الوطنية والدولية على حد سواء. كما تتماشى القوانين العراقية إلى حد ما مع اتفاقية بودابست للجرائم الإلكترونية، التي توفر إطارًا قانونيًا موحدًا لمكافحة التهديدات السيبرانية على مستوى العالم. وإلى جانب ذلك، تسعى الجهات العراقية المختصة إلى تعزيز التعاون الدولي عبر تبادل المعلومات حول الهجمات الإلكترونية مع الدول والمنظمات المعنية، وهو ما يتوافق مع النهج الذي تتبعه الاتفاقيات الدولية التي تشجع الدول على تنسيق الجهود في هذا المجال.[٢٨]

وعلى الرغم من هذا التقارب، فإن التشريعات العراقية لا تزال تواجه بعض التحديات التي تعيق تحقيق انسجام كامل مع المعايير الدولية. ومن أبرز أوجه الاختلاف أن القوانين العراقية لم تواكب بعد التطورات التقنية المتسارعة، حيث تفتقر إلى نصوص صريحة تعالج الجرائم المستحدثة، مثل هجمات الفدية والتلاعب بالبيانات عبر الذكاء الاصطناعي، والتي أصبحت من أخطر التهديدات في العصر الرقمي. كذلك، تظل العقوبات القانونية المفروضة على الجرائم السيبرانية في العراق أقل صرامة مقارنة بالمعايير الدولية، إذ تفرض بعض القوانين العالمية عقوبات قاسية تشمل السجن لمدد طويلة، وغرامات مالية كبيرة، وحجب الأنظمة المستخدمة في الهجمات، لضمان ردع فعّال للمجرمين الإلكترونيين.[٢٩]

بالإضافة إلى ذلك، لم تنص القوانين العراقية حتى الآن على إطار شامل لحماية خصوصية المستخدمين على الإنترنت، على غرار اللوائح الدولية مثل اللائحة العامة لحماية البيانات (GDPR) ، التي توفر ضمانات قانونية لحماية البيانات الشخصية وحقوق الأفراد في الفضاء الرقمي. وهذا القصور

يفتح المجال لوجود ثغرات قد تؤثر على حقوق المستخدمين في العراق، مما يستلزم تحديثًا قانونيًا يعزز من آليات حماية الخصوصية الرقمية.[٣٠]

ومن الجوانب الأخرى التي تحتاج إلى تطوير، ضعف الموارد التقنية والبشرية اللازمة لإنفاذ القوانين المتعلقة بالأمن السيبراني. فبينما تؤكد المعايير الدولية على ضرورة الاستثمار في القدرات التكنولوجية والتدريب المستمر للعاملين في هذا المجال، لا يزال العراق بحاجة إلى تطوير بنيته التحتية الرقمية وتعزيز قدراته المؤسسية لضمان تطبيق القوانين بفعالية. ويعد توفير برامج تدريبية متخصصة للعاملين في إنفاذ القانون، وإنشاء مراكز متقدمة لرصد التهديدات والاستجابة لها، من الخطوات الأساسية التي ينبغي اتخاذها لضمان مواجهة أكثر كفاءة للهجمات الإلكترونية.

ولسد الفجوات بين التشريعات العراقية والمعايير الدولية، يصبح من الضروري العمل على تحديث القوانين الوطنية بما يضمن تغطية جميع أنواع الجرائم الإلكترونية الحديثة، وتشديد العقوبات القانونية لجعلها أكثر ردعًا للمخالفين، ووضع إطار قانوني واضح لحماية البيانات الشخصية بما يواكب المعايير العالمية. كما ينبغي تعزيز التعاون مع المنظمات الدولية المختصة، والاستثمار في تطوير القدرات الفنية والبشرية في مجال الأمن السيبراني، لضمان تحقيق استجابة سريعة وفعالة للتهديدات الإلكترونية المتزايدة. وعليه، فإن تحقيق التكامل بين التشريعات العراقية والمعايير الدولية يتطلب نهجًا شاملاً يشمل إصلاحات قانونية، وتحديثات تقنية، وتعزيزًا للتعاون الدولي. ومن خلال هذه الجهود، يمكن للعراق أن يعزز أمنه السيبراني، ويحمي بنيته الرقمية من المخاطر المتنامية، ويساهم في بناء بيئة إلكترونية أكثر أمانًا واستقرارًا، تتماشى مع التوجهات العالمية الحديثة في هذا المجال[٣١].

الخاتمة

يُعد الأمن السيبراني اليوم عنصرًا جوهريًا في حماية البنية التحتية الرقمية للدول، لا سيما مع تزايد التهديدات السيبرانية وتعقيدها. وقد تناول هذا البحث الإطار القانوني للأمن السيبراني في العراق، مسلطًا الضوء على نقاط القوة والضعف في التشريعات الحالية، ومدى قدرتها على التصدي للمخاطر الرقمية المتزايدة.

أظهرت النتائج أن البيئة القانونية في العراق لا تزال تعاني من فجوات تشريعية ومؤسسية تعيق بناء منظومة سيبرانية متكاملة وفعالة. كما أن غياب التنسيق بين الجهات المعنية، وضعف الوعي المجتمعي، ونقص الكوادر المتخصصة، تشكل تحديات إضافية تتطلب استراتيجيات واضحة لمعالجتها. وفي ضوء ذلك، فإن تحقيق أمن سيبراني مستدام يتطلب تبني سياسات شاملة تستند إلى المعايير الدولية، وتعزز التعاون بين القطاعين العام والخاص، إلى جانب الاستثمار في تطوير البنية التحتية الرقمية والموارد البشرية.

بناءً على هذه المعطيات، يقدم البحث مجموعة من التوصيات التي من شأنها المساهمة في تحسين الإطار القانوني وتعزيز الحماية السيبرانية في العراق، بما يضمن بيئة رقمية أكثر أمانًا واستقرارًا.

النتائج

- الأمن السيبراني يعد مكوّنًا أساسيًا للأمن القومي والاقتصادي، خاصة مع التوسع في استخدام التكنولوجيا الرقمية.
- التشريعات العراقية الحالية غير كافية لمواجهة التهديدات السيبرانية المتزايدة، مما يستدعي مراجعة شاملة لها.
- هناك ضعف في التنسيق بين الجهات الحكومية المعنية بالأمن السيبراني، مما ينعكس سلبًا على الاستجابة الفعالة للهجمات الإلكترونية.
- تفتقر البنية التحتية الرقمية في العراق إلى التطوير الكافي الذي يمكّنها من مواجهة التحديات السيبرانية الحديثة.

- ضعف الثقافة المجتمعية حول مخاطر الأمن السيبراني يسهم في زيادة التهديدات الإلكترونية واستغلال الثغرات الأمنية.
- هناك نقص واضح في الكفاءات المتخصصة بمجال الأمن السيبراني، ما يستدعي تعزيز برامج التأهيل والتدريب المهني.

مقترحات

- تطوير البنية التحتية الرقمية عبر تبني تقنيات حديثة وتقوية الأنظمة الأمنية لمواجهة المخاطر السيبرانية المتزايدة.
- تعزيز التنسيق المؤسسي بين الجهات الحكومية والخاصة لإنشاء منظومة أمن سيبراني متكاملة تدعم الاستجابة السريعة للهجمات.
- إطلاق برامج متخصصة لبناء القدرات تستهدف تأهيل الكوادر الوطنية في مجال الأمن السيبراني من خلال شراكات مع الجامعات والمؤسسات البحثية.
- تعزيز الوعي المجتمعي حول أهمية الأمن السيبراني من خلال حملات توعوية تشمل المؤسسات التعليمية ووسائل الإعلام.
- إنشاء هيئة وطنية مستقلة للأمن السيبراني تكون مسؤولة عن وضع الاستراتيجيات، ومراقبة تنفيذها، وتنسيق الجهود بين الجهات المختلفة.

الهوامش

(١) المعداوي، أحمد محمد. حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي: دراسة مقارنة. مجلة كلية الشريعة والقانون، مصر، العدد ٣٣، ٢٠١٨، ص ١٩٢٦-٢٠٥٧.

(٢) العتيبي، زياد بن محمد عادي، جرائم السيبرانية المرتكبة عبر الوسائط الرقمية وبيان مفهومها من حيث: أشكالها، خصائصها، أركانها والدافع من ارتكابها، المجلة الاكاديمية العالمية للدراسات القانونية، المجلد ٣،العدد ١، ٢٠٢٠، ص ١٤

(٣) الدستور العراقي لعام ٢٠٠٥ في المادة ١٧.

(٤) المادة (٧) من قانون الأحوال المدنية رقم (٦٥) لسنة ١٩٧٢.

(٥) مستودع جامعة بابل للبحوث والأوراق الإلكترونية. (٣ أبريل، ٢٠١١). "فيروس الحاسوب". تاريخ الاسترداد ١٧ أغسطس، ٢٠١٨ من مستودع جامعة

http://repository.uobabylon.edu.iq/2010_2011/4_14913_742.pdf

(٦) عمر، معاوية. أهمية أمن المعلومات في مكافحة الجرائم الإلكترونية: دراسة حالة المركز السوداني لأمن المعلومات. مجلة جامعة بحري للآداب والعلوم الإنسانية، جامعة بحري، السودان، العدد ٤، (٢٠١٥)، ص ٢٣١-٢٥١.

(٧) سعاد عبد الله محمد واحمد حامد علي، الإمن السيبراني في دول مجلس التعاون لدول الخليج العربية بمنظور جهوبولتيكي معاصر، مجلة جامعة الإنبار للعلوم الإنسانية، العدد (٣)، جامعة الانبار، ٢٠٢٠، ص٣٨٢.

(8)International Organization for Migration, IOM Iraq – 2019, Technology and Innovation in Iraq, A Market Assessment of Tech Sector Businesses in Iraq, P.4.

(٩)علي زياد العلي، التحديات غير المرئية للأمن الوطني العراقي، مركز البيان للدراسات والتخطيط، مقال منشور عبر شبكة المعلومات الدولية (الإنترنت) على الموقع:

https://www.bavancenter.org /٤٥٦٥/٠٦/٢٠١٨

(١٠) بن قارة مصطفى، عائشة. الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية القانونية. المجلة العربية للعلوم ونشر الأبحاث، المجلد ٢، العدد ٥، ٢٠١٦، ص٤٤١.

(١١) المادة (٧) من قانون الأحوال المدنية رقم (٦٥) لسنة ١٩٧٢.

(١٢) أحمد قاسم فرح، النظام القانوني لمقدمي خدمات الإنترنت: دراسة تحليلية مقارنة، بحث منشور في مجلة المنارة للبحوث والدراسات، المجلد ٩، العدد ١٣، مايو ٢٠٠٧م، ص ٣٣٤.

(١٣) المادة (١٩) من مسودة قانون الجرائم المعلوماتية.

(١٤) فقرة (٤) من المادة (٦) من قانون الجرائم المعلوماتية.

(١٥) زهدور إنجي هند نجوى ريم سندس، درار نسيمة، استراتيجيات الوقاية القانونية والامنية من مهددات الامن الرقمي، المجلة الدولية لنشر البحوث والدراسات، المجلد ٢، العدد ١٦، ٢٠٢١، ص ٢٣٤.

(١٦) العتيبي، زياد بن محمد عادي، جرائم السيبرانية المرتكبة عبر الوسائط الرقمية وبيان مفهومها من حيث: أشكالها، خصائصها، أركانها والدافع من ارتكابها، المجلة الاكاديمية العالمية للدراسات القانونية، المجلد ٣، العدد ١، ٢٠٢٠، ص ١٤ وما بعدها.

(١٧) بوعقبة، نعيمة. معالجة البيانات الحساسة بين الحظر وخصوصية المعالجة: قراءة في قانون حماية المعطيات ذات الطابع الشخصي، جامعة الشاذلي بن جديد، الطارف، مجلة صوت القانون، المجلد ٩، العدد ١، ٢٠٢٢، ص٢٢٥-٢٤٥.

(١٨) بن قارة مصطفى، عائشة. الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية القانونية. المجلة العربية للعلوم ونشر الأبحاث، المجلد ٢، العدد ٥، ٢٠١٦، ص٤٤١.

(19)Nfuka, E. N., Sanga, C., & Mshangi, M. The rapid growth of cybercrimes affecting information systems in the global: Is this a myth or reality in Tanzania. International journal of information security science , vol.3 (2), 182-199.

(٢٠)عبدالسلام محمد المايل، عادل محمد الشربجي، على قابوسة، الجريمة الإلكترونية في الفضاء الإلكتروني المفهوم- الأسباب-سبُل المكافحة مع التعرض لحالة ليبيا، مجلة افاق للبحوث والدراسات سداسية، دولية محكمة، المركز الجامعى ايليزى، العدد ٤، ٢٠١٩، ص ٢٥١.

(٢١) زهدور إنجي هند نجوى ريم سندس، درار نسيمة، استراتيجيات الوقاية القانونية والامنية من مهددات الامن الرقمي، المجلة الدولية لنشر البحوث والدراسات، المجلد ٢، العدد ١٦، ٢٠٢١، ص ٢٢٨ – ٢٣٠.

(٢٢) الاتفاقية الأوروبية لجرائم الإنترنت في بودابست، المجر، في تاريخ ٢٣ نوفمبر ٢٠٠١. تُعتبر هذه الاتفاقية الأساس الأول للتعاون الدولي في مجال مكافحة الجريمة المنظمة عبر الإنترنت. وقد شارك في توقيع هذه الاتفاقية ٣٠ دولة أوروبية، بالإضافة إلى أربع دول غير أعضاء في المجلس الأوروبي وهي كندا، الولايات المتحدة الأمريكية، اليابان، وجنوب أفريقيا.

(٢٣) المبادئ التوجيهية للأمم المتحدة (١٩٩٠). تنظيم ملفات البيانات الشخصية المعدة بالحاسبة الإلكترونية. الجمعية العامة. القرار ٤٥/٩٥. متاح على الرابط: http://hrlibrary.umn.edu. تاريخ الاطلاع: ٦ يوليو ٢٠٢٠.

(24)Wang. M, et Jiang. Z.(2017). The Defining Approaches and Practical Paradox of Sensitive Data : International Journal of Communication. N.11,PP. 3286–3305.

(٢٥) محمد، مولاي، صعوبات تطبيق الإدارة الإلكترونية بالجزائر: الجريمة الإلكترونية نموذجا"، المؤتمر العالمي الأول للإدارة الإلكترونية، مركز المدينة للوسائط المتعددة، ٢٠١٠/٠٦/٠٣-٠١، طرابلس، ليبيا. (٢٠١٠).

(26) Malby, S., Mace, R., & Holterhof, A. (2013). Comprehensive study on cybercrime. New York: United nations office on drugs and crime.p.17

(27)Marwick, A. E. (2013). Status update: Celebrity, publicity, and branding in the social media age. Yale University Press.

(٢٨)أحمد قاسم فرح، النظام القانوني لمقدمي خدمات الإنترنت: دراسة تحليلية مقارنة، بحث منشور في مجلة المنارة للبحوث والدراسات، المجلد ٩، العدد ١٣، مايو ٢٠٠٧م، ص ٣٣٤.

(29) Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. Business horizons, 53(1), 59-68.

(٣٠) النظام الأوروبي لحماية البيانات (GDPR).

(٣١) زهدور إنجي هند نجوى ريم سندس، درار نسيمة، استراتيجيات الوقاية القانونية والامنية من مهددات الامن الرقمي، المجلة الدولية لنشر البحوث والدراسات، المجلد ٢، العدد ١٦، ٢٠٢١، ص ٢٣٢ – ٢٣٣.

خورامي، نعمة. التعامل مع الأمن السيبراني والمراقبة: استراتيجية إيران المزدوجة للأمن القومي٢٩ مارس ٢٠٢٤. متاح على الرابط: http://arabic.wilsoncenter.org/ar/experts/nmt-khwramy/

Valkenburg, P. M., & Peter, J. (2009). Social consequences of the Internet for adolescents: A decade of research. Current directions in psychological science, 18(1), 1-5.

المراجع

أولًا: الكتب

١. محمد، مولاي، صعوبات تطبيق الإدارة الإلكترونية بالجزائر: الجريمة الإلكترونية أنموذجا"، المؤتمر العالمي الأول للإدارة الإلكترونية، مركز المدينة للوسائط المتعددة، ٢٠١٠.

٢. خورامي، نعمة. التعامل مع الأمن السيبراني والمراقبة: استراتيجية إيران المزدوجة للأمن القومي، ٢٩ مارس ٢٠٢٤.

ثانيًا: المجلات العلمية والأبحاث

١. المعداوي، أحمد محمد. "حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي: دراسة مقارنة ".مجلة كلية الشريعة والقانون، مصر، العدد ٣٣، ٢٠١٨، ص ١٩٢٦-٢٠٥٧.

٢. العتيبي، زياد بن محمد عادي. "جرائم السيبرانية المرتكبة عبر الوسائط الرقمية وبيان مفهومها من حيث: أشكالها، خصائصها، أركانها والدافع من ارتكابها ".المجلة الأكاديمية العالمية للدراسات القانونية، المجلد ٣، العدد ١، ٢٠٢٠، ص ١٤ وما بعدها.

٣. عمر، معاوية. "أهمية أمن المعلومات في مكافحة الجرائم الإلكترونية: دراسة حالة المركز السوداني لأمن المعلومات ".مجلة جامعة بحري للآداب والعلوم الإنسانية، جامعة بحري، السودان، العدد ٤، ٢٠١٥، ص ٢٣١-٢٥١.

٤. سعاد عبد الله محمد وأحمد حامد علي. "الأمن السيبراني في دول مجلس التعاون لدول الخليج العربية بمنظور جهوبولتيكي معاصر ".مجلة جامعة الأنبار للعلوم الإنسانية، العدد (٣)، جامعة الأنبار، ٢٠٢٠، ص ٣٨٢.

٥. بن قارة مصطفى، عائشة. "الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية القانونية ".المجلة العربية للعلوم ونشر الأبحاث، المجلد ٢، العدد ٥، ٢٠١٦، ص ٤٤١.

٦. زهدور إنجي هند نجوى ريم سندس، درار نسيمة. "استراتيجيات الوقاية القانونية والأمنية من مهددات الأمن الرقمي ".المجلة الدولية لنشر البحوث والدراسات، المجلد ٢، العدد ١٦، ٢٠٢١، ص ٢٢٨-٢٣٤.

٧. بوعقبة، نعيمة. "معالجة البيانات الحساسة بين الحظر وخصوصية المعالجة: قراءة في قانون حماية المعطيات ذات الطابع الشخصي ".مجلة صوت القانون، المجلد ٩، العدد ١، ٢٠٢٢، ص ٢٢٥-٢٤٥.

٨. عبدالسلام محمد المايل، عادل محمد الشربجي، علي قابوسة. "الجريمة الإلكترونية في الفضاء الإلكتروني: المفهوم، الأسباب، سُبل المكافحة مع التعرض لحالة ليبيا ".مجلة آفاق للبحوث والدراسات، المركز الجامعي إيليزي، العدد ٤، ٢٠١٩، ص ٢٥١.

٩. أحمد قاسم فرح. "النظام القانوني لمقدمي خدمات الإنترنت: دراسة تحليلية مقارنة ".مجلة المنارة للبحوث والدراسات، المجلد ٩، العدد ١٣، مايو ٢٠٠٧، ص ٣٣٤.

ثالثًا: القوانين والتشريعات الدولية والمحلية

١. الدستور العراقي لعام ٢٠٠٥، المادة ١٧.

٢. المادة (٧) من قانون الأحوال المدنية رقم (٦٥) لسنة ١٩٧٢.

٣. المادة (١٩) من مسودة قانون الجرائم المعلوماتية.

٤. فقرة (٤) من المادة (٦) من قانون الجرائم المعلوماتية.

٥. النظام الأوروبي لحماية البيانات.(GDPR)

٦. المبادئ التوجيهية للأمم المتحدة (١٩٩٠). تنظيم ملفات البيانات الشخصية المعدة بالحاسبة الإلكترونية. الجمعية العامة. القرار ٤٥/٩٥.

رابعًا: التقارير والدراسات الرسمية

١. الاتفاقية الأوروبية لجرائم الإنترنت في بودابست، المجر، ٢٣ نوفمبر ٢٠٠١.

٢. مستودع جامعة بابل للبحوث والأوراق الإلكترونية. "فيروس الحاسوب." تاريخ الاسترداد ١٧ أغسطس ٢٠١٨ .الرابط.

References

Books

1-Mohamed, Moulay. Difficulties in Implementing E-Government in Algeria: Cybercrime as a Model. First World Conference on E-Government, Al-Madina Multimedia Center, 2010.

2-Khourami, Ne'ma. Dealing with Cybersecurity and Surveillance: Iran's Dual Strategy for National Security., March 29, 2024.

Scientific Journals and Research Papers

1-Al-Ma’dawi, Ahmed Mohamed. "Protecting User Information Privacy on Social Media Networks: A Comparative Study." Journal of the Faculty of Sharia and Law, Egypt, Issue 33, 2018, pp. 1926-2057.

2-Al-Otaibi, Ziyad bin Mohammed Adi. "Cyber Crimes Committed via Digital Media: Definition, Forms, Characteristics, Elements, and Motives." Global Academic Journal of Legal Studies, Vol. 3, Issue 1, 2020, p. 14 et seq.

3-Omar, Muawiya. "The Importance of Information Security in Combating Cybercrime: A Case Study of the Sudanese Information Security Center." Bahri University Journal for Humanities and Social Sciences, Bahri University, Sudan, Issue 4, 2015, pp. 231-251.

4-Suad Abdullah Mohammed and Ahmed Hamed Ali. "Cybersecurity in the Gulf Cooperation Council Countries from a Contemporary Geopolitical Perspective." Anbar University Journal for Humanities, Issue 3, Anbar University, 2020, p. 382.

5-Ben Qara Mustapha, Aisha. "The Right to Information Privacy Between Technological Challenges and Legal Protection." The Arab Journal of Science and Research Publishing, Vol. 2, Issue 5, 2016, p. 441.

6-Zahdoor Inji, Hind Najwa, Reem Sundus, and Drar Nasima. "Legal and Security Prevention Strategies Against Digital Security Threats." International Journal of Research and Studies Publishing, Vol. 2, Issue 16, 2021, pp. 228-234.

7-Bouakba, Naima. "Handling Sensitive Data Between Prohibition and Privacy Processing: An Analysis of the Personal Data Protection Law." Law Voice Journal, Vol. 9, Issue 1, 2022, pp. 225-245.

8-Abdelsalam Mohamed El-Mayel, Adel Mohamed Al-Sharbaji, and Ali Qaboosa. "Cybercrime in Cyberspace: Concept, Causes, and Prevention Strategies with a Focus on Libya." Afaq Journal for Research and Studies, University Center of Illizi, Issue 4, 2019, p. 251.

9-Ahmed Qasim Farah. "The Legal Framework for Internet Service Providers: A Comparative Analytical Study." Al-Manara Journal for Research and Studies, Vol. 9, Issue 13, May 2007, p. 334.

Laws and Regulations (International and National)

1-The Iraqi Constitution of 2005, Article 17.

2-Article (7) of the Civil Status Law No. (65) of 1972.

3-Article (19) of the Draft Cybercrime Law.

4-Paragraph (4) of Article (6) of the Cybercrime Law.

5-The European General Data Protection Regulation (GDPR).

6-United Nations Guidelines (1990). Regulating Personal Data Files Processed by Electronic Computers. UN General Assembly, Resolution 95/45.

Official Reports and Studies

1-International Organization for Migration (IOM), Iraq - 2019. Technology and Innovation in Iraq: A Market Assessment of Tech Sector Businesses in Iraq, p. 4.

2-The European Convention on Cybercrime, Budapest, Hungary, November 23, 2001.

3-University of Babylon Research and Electronic Papers Repository. "Computer Virus." Retrieved on August 17, 2018.