الأمن السيبراني وحماية البيانات الوطنية ـ العراق نموذجاً

الباحث وليد خالد
دائرة عقارات الدولة ـ وزارة المالية ـ العراق
البريد الالكتروني waleedhameed49@yahoo.com

تاريخ التقديم للنشر ٢٠٢٥/١٠/١٥ تاريخ القبول للنشر ٢٠٢٥/١١/١٩

الملخص.

يشهد العالم المعاصر تحولاً رقمياً متسارعاً جعل من البيانات مورداً سيادياً واستراتيجياً، وأصبحت الهجمات السيبرانية تهدد أمن الدول ومؤسساتها الحيوية .في العراق، تتزايد المخاطر الرقمية بسبب ضعف البنى التحتية التقنية، وقصور التشريعات، وغياب إطار وطني متكامل لحماية البيانات والأمن السيبراني .يهدف هذا البحث إلى دراسة واقع الأمن السيبراني وحماية البيانات الوطنية في العراق، وتحليل الفجوات القانونية والتنظيمية، واستعراض تجارب عالمية يمكن الاستفادة منها، وصولاً إلى تقديم مقترحات عملية لبناء منظومة وطنية فعالة .اعتمد البحث على المنهج الوصفي والتحليلي، مع الاستفادة من الوثائق التشريعية والتقارير الدولية والمقارنة مع المعايير العالمية .وتوصلت الدراسة إلى أن العراق يفتقر إلى قانون خاص بحماية البيانات الشخصية والوطنية، ويعاني من ضعف الحوكمة الرقمية، وغياب هيئة وطنية للأمن السيبراني، مما يزيد من احتمالات الاختراق والتسريب واستهداف البنى التحتية الحرجة .وأوصى البحث بضرورة سن تشريع متكامل لحماية البيانات، وإنشاء هيئة وطنية مستقلة للأمن السيبراني، وتطوير استراتيجية وطنية، وتعزيز الشراكة بين القطاعين العام والخاص، وبناء القدرات البشرية والتقنية، واعتماد معايير دولية لضمان الامتثال والاستدامة[1].

الكلمات المفتاحية :الأمن السيبراني، حماية البيانات، العراق، السيادة الرقمية، التشريع، البنى التحتية الحرجة.

Abstract.

The contemporary world is undergoing an accelerated digital transformation in which data has become a sovereign and strategic resource. Cyberattacks increasingly threaten national security, critical institutions, and economic

stability. In Iraq, digital risks have escalated due to weak technical infrastructure, inadequate legislation, and the absence of an integrated national framework for cybersecurity and data protection. This study aims to examine the current state of cybersecurity and national data protection in Iraq, analyse legislative and regulatory gaps, and review selected global experiences that could serve as applicable models. The research adopts a descriptive-analytical methodology, relying on legislative documents, international reports, and benchmarking against global standards. The study concludes that Iraq lacks a dedicated data protection law and suffers from weak digital governance and the absence of a national cybersecurity authority, which increases the likelihood of breaches, data leakage, and attacks targeting critical infrastructure. The study recommends enacting a comprehensive data protection framework, establishing an independent national cybersecurity authority, developing a national strategy, strengthening public–private partnerships, and investing in human and technical capacity building.[2]

Keywords: Cybersecurity, Data Protection, Iraq, Digital Sovereignty, Legislation, Critical Infrastructure.

المبحث الأول :منهجية البحث.

أولاً :المقدمة.

أدى التطور المتسارع في تقنيات الاتصالات والمعلومات إلى توسع غير مسبوق في الاعتماد على الفضاء الرقمي، سواء في الإدارة الحكومية أو في القطاعات الاقتصادية أو في الخدمات العامة . وباتت البيانات الرقمية تمثل المورد الأكثر حساسية في العصر الحديث، إذ ترتبط بها القرارات السيادية والاقتصادية والأمنية .وفي هذا السياق، أصبحت الهجمات السيبرانية أحد أهم التحديات التي تواجه الدول، لأنها تستهدف بنى تحتية حيوية مثل الكهرباء والمصارف والاتصالات والمؤسسات العسكرية .ويزداد هذا التهديد في الدول التي تعاني من اضطرابات سياسية أو ضعف مؤسسي، كما

هو الحال في العراق بعد عام 2003، حيث توسعت شبكات الاتصالات والإنترنت دون وجود بنية قانونية وتقنية متماسكة لضمان أمن المعلومات وحماية البيانات .وقد ساهم هذا الواقع في اتساع فجوة الحماية الرقمية، مما يجعل العراق عرضة لهجمات منظمة تستهدف البيانات الوطنية والبنى التحتية الحرجة[3].

ثانياً :مشكلة البحث.

تتمثل مشكلة البحث في أن العراق، رغم تزايد الاعتماد على الأنظمة الرقمية في المؤسسات الحكومية والاقتصادية، ما يزال يعاني من ضعف واضح في الإطار التشريعي والتنظيمي المتعلق بالأمن السيبراني وحماية البيانات، إضافة إلى غياب هيئة وطنية موحدة تتولى إدارة المخاطر الرقمية وتنسيق الاستجابة للحوادث .كما أن المؤسسات الحكومية تفتقر إلى سياسات إلزامية لتصنيف البيانات، وإدارة الهوية الرقمية، وحماية قواعد البيانات، وإلزام الجهات بالإبلاغ عن الاختراقات، مما يجعل الدولة عرضة لمخاطر قد تمس أمنها القومي وسيادتها الرقمية[4].

ثالثاً :أهداف البحث.

يهدف البحث إلى تحقيق الأهداف الآتية:

- تحليل الإطار التشريعي والتنظيمي للأمن السيبراني وحماية البيانات في العراق.
- تحديد الفجوات القانونية والمؤسسية والتقنية التي تواجه الدولة في مجال الحماية الرقمية.
- تقييم جاهزية العراق مقارنة بالمعايير الدولية المعتمدة.
- استعراض تجارب عالمية وإقليمية ناجحة في مجال الأمن السيبراني وحماية البيانات.
- تقديم مقترحات عملية لبناء استراتيجية وطنية متكاملة تعزز الأمن السيبراني والسيادة الرقمية.

رابعاً :أهمية البحث.

تنبع أهمية البحث من كون الأمن السيبراني يمثل أحد عناصر الأمن الوطني المعاصر، إذ أصبحت الدول تواجه تهديدات رقمية لا تقل خطورة عن التهديدات العسكرية التقليدية .كما أن حماية البيانات تعد شرطاً أساسياً لنجاح التحول الرقمي، وتطوير الحكومة الإلكترونية، وتعزيز الثقة في المعاملات الإلكترونية .وتزداد أهمية هذا الموضوع في العراق بسبب التحديات الأمنية والسياسية والاقتصادية،

فضلاً عن التوسع في استخدام الخدمات المصرفية الإلكترونية، ومنصات الدفع الرقمي، والأنظمة الحكومية المرتبطة بقواعد بيانات المواطنين.

خامساً :فرضيات البحث.

ينطلق البحث من الفرضيات الآتية:

- إن غياب قانون عراقي متكامل لحماية البيانات يمثل عائقاً رئيسياً أمام بناء منظومة أمن سيبراني فعالة.
- ضعف القدرات البشرية والمؤسسية يحد من قدرة الدولة على مواجهة التهديدات الرقمية.
- إن تعزيز التعاون بين القطاعين العام والخاص يسهم في تقليل المخاطر وتحسين الاستجابة للهجمات.
- إن اعتماد المعايير الدولية وتطبيقها في المؤسسات العراقية يرفع مستوى الجاهزية الرقمية ويقلل من احتمالات الاختراق.

سادساً :منهجية البحث وأدواته

اعتمد البحث على المنهج الوصفي والتحليلي من خلال وصف واقع الأمن السيبراني في العراق، ثم تحليل التشريعات العراقية القائمة وتقييم مدى ملاءمتها للتحديات الرقمية الحديثة .كما استخدم البحث المنهج المقارن عبر دراسة نماذج عالمية مثل اللائحة العامة لحماية البيانات GDPRفي الاتحاد الأوروبي، وإطار الأمن السيبراني NISTفي الولايات المتحدة، ومعايير ISO/IEC 27001. وتم الاعتماد على أدوات البحث المتمثلة في تحليل الوثائق الرسمية والتقارير الدولية والدراسات الأكاديمية المتخصصة[5].

سابعاً :حدود البحث

تتمثل الحدود المكانية للبحث في دولة العراق، بينما تشمل الحدود الزمنية المرحلة الممتدة من عام 2003إلى عام 2025، بوصفها مرحلة التحول السياسي وتزايد الاعتماد على الإنترنت والأنظمة الرقمية .أما الحدود الموضوعية فتتمثل في دراسة التشريعات والسياسات والإجراءات المتعلقة بحماية البيانات والأمن السيبراني، دون التوسع في التفاصيل التقنية الدقيقة المتعلقة ببناء الأنظمة البرمجية.

المبحث الثاني :الإطار النظري والدراسات السابقة.

أولاً :مفهوم الأمن السيبراني.

يشير مفهوم الأمن السيبراني إلى مجموعة السياسات والتقنيات والإجراءات التنظيمية التي تهدف إلى حماية الشبكات والأنظمة وقواعد البيانات والبرمجيات من الهجمات الرقمية .ويشمل الأمن السيبراني حماية السرية (Confidentiality)وسلامة البيانات (Integrity)وتوافر الخدمة (Availability)، وهو ما يُعرف بمثلث .(CIA)كما يشمل الأمن السيبراني إدارة المخاطر، والتحقق من الهوية الرقمية، وتأمين الاتصالات، واستخدام تقنيات التشفير، وتطوير خطط الاستجابة للطوارئ .وتتزايد أهمية الأمن السيبراني في ظل اعتماد المؤسسات على الأنظمة السحابية والتطبيقات الإلكترونية وتبادل البيانات عبر الحدود[6].

ثانياً :مفهوم حماية البيانات.

حماية البيانات هي منظومة قانونية وتنظيمية تهدف إلى ضمان الاستخدام المشروع للبيانات، وتمنع جمعها أو معالجتها أو تخزينها أو مشاركتها دون موافقة قانونية .وتتعلق حماية البيانات بالخصوصية الفردية، لكنها تمتد أيضاً إلى حماية البيانات الوطنية التي تمثل قيمة استراتيجية للدولة .ومن أبرز المبادئ التي تقوم عليها حماية البيانات :الشفافية، والغاية المحددة، وتقليل البيانات، والدقة، والاحتفاظ المحدود، وسرية المعالجة، والمسؤولية القانونية للمؤسسات التي تدير البيانات[7].

ثالثاً :البيانات الوطنية والسيادة الرقمية.

أصبحت البيانات الوطنية تمثل أحد عناصر السيادة الحديثة، إذ لم تعد سيادة الدولة مقتصرة على الأرض والموارد الطبيعية، بل امتدت إلى الفضاء الرقمي .وتشمل البيانات الوطنية قواعد بيانات السكان، والسجلات المدنية، والملفات الضريبية، وبيانات النفط والطاقة، والبيانات الأمنية، وبيانات المنافذ الحدودية، وغيرها من المعلومات التي يؤدي تسريبها أو التلاعب بها إلى تهديد الأمن القومي. وفي هذا الإطار ظهر مفهوم (Digital Sovereignty)الذي يعني قدرة الدولة على التحكم ببياناتها ومنع السيطرة الخارجية عليها، سواء عبر شركات التكنولوجيا العالمية أو عبر عمليات التجسس السيبراني .ويعد توطين البيانات (Data Localization)أحد أدوات تعزيز السيادة الرقمية، إذ تسعى بعض الدول إلى فرض تخزين البيانات داخل حدودها لتقليل مخاطر نقلها إلى خوادم خارجية.

رابعاً :الجرائم السيبرانية وأشكال التهديد.

تتخذ الجرائم السيبرانية أشكالاً متعددة، منها اختراق قواعد البيانات الحكومية، والهجمات على المصارف والأنظمة المالية، وعمليات الابتزاز الإلكتروني عبر برامج الفدية (Ransomware)، والتجسس على الاتصالات، وتزوير الهويات الرقمية، إضافة إلى الهجمات الموجهة ضد البنى التحتية الحرجة مثل الكهرباء والمياه والنفط .ويلاحظ أن الجرائم السيبرانية غالباً ما تتميز بالسرعة وصعوبة التتبع، كما أنها تتجاوز الحدود الجغرافية، الأمر الذي يتطلب تعاوناً دولياً وتنسيقاً بين أجهزة الدولة والقطاع الخاص[8].

خامساً :البنى التحتية الحرجة.(Critical Infrastructure)

يقصد بالبنى التحتية الحرجة القطاعات الحيوية التي يؤدي تعطيلها أو تدميرها إلى شلل في الدولة، مثل قطاع النفط والغاز، ومنظومات الكهرباء، والاتصالات، والمصارف، والنقل، والمياه، والمستشفيات .ويزداد خطر الهجمات السيبرانية على هذه القطاعات بسبب الاعتماد على أنظمة التحكم الصناعي (SCADA)التي قد تكون قديمة أو غير محمية بشكل كاف .ويعد العراق من الدول التي تمتلك بنى تحتية حساسة في مجال الطاقة، مما يجعل أي هجوم سيبراني واسع النطاق قادراً على إحداث أضرار اقتصادية وأمنية كبيرة.

سادساً :الحوكمة الرقمية وإدارة المخاطر.

تشير الحوكمة الرقمية إلى مجموعة القواعد والسياسات والإجراءات التي تضمن إدارة الموارد الرقمية بشكل منظم وشفاف، وتحدد المسؤوليات والصلاحيات في مجال الأمن السيبراني .وتعد إدارة المخاطر من العناصر الأساسية في الحوكمة، حيث تتطلب تحديد التهديدات المحتملة، وتقييم أثرها، ثم اتخاذ إجراءات وقائية واستباقية للحد من المخاطر .وتوصي الأدبيات الدولية بضرورة وجود استراتيجية وطنية للأمن السيبراني تتضمن خططاً تنفيذية واضحة، وتحديداً للمؤسسات المسؤولة، وآليات للتنسيق بين الجهات الحكومية والقطاع الخاص[9].

سابعاً :الدراسات السابقة.

تناولت العديد من الدراسات واقع الأمن السيبراني وحماية البيانات في العراق .فقد أشار تقرير (Freedom House)لعام 2023إلى أن البيئة الرقمية العراقية تعاني من ضعف في حماية الخصوصية الرقمية، وعدم وجود ضمانات قانونية كافية تمنع استخدام البيانات من قبل الجهات غير

المختصة .كما أكد تقرير الاتحاد الدولي للاتصالات (ITU)الخاص بالعراق أن الدولة بحاجة إلى تطوير تشريعات شاملة وبناء قدرات مؤسسية، وإنشاء مركز وطني للاستجابة للطوارئ الرقمية . وفي دراسة الحمدان وحيدري (2025)تم التأكيد على أن التشريعات العراقية الحالية ما تزال تعتمد على نصوص عامة من قانون العقوبات ولا توفر حماية متخصصة للبيانات .كما تناولت بعض الدراسات الجامعية العراقية مسألة ضعف الوعي المجتمعي وغياب التدريب المتخصص في الجامعات والمعاهد التقنية .وتستنتج هذه الدراسات مجتمعة أن العراق يواجه فجوة تشريعية ومؤسسية تتطلب إصلاحاً جذرياً لتحقيق الأمن الرقمي[10].

المبحث الثالث :التطبيق والتجارب العالمية.

أولاً :واقع الأمن السيبراني في العراق.

يتميز الواقع العراقي في مجال الأمن السيبراني بتعدد الجهات الرسمية ذات العلاقة دون وجود جهة مركزية موحدة .فالمؤسسات الحكومية تعمل غالباً وفق سياسات داخلية متباينة، ولا توجد معايير إلزامية موحدة لتأمين الشبكات وقواعد البيانات .كما أن التحول الرقمي في العراق ما يزال في مراحل غير مكتملة، إذ تعتمد بعض المؤسسات على نظم ورقية وأخرى على نظم إلكترونية دون تأمين كاف .وتشير تقارير دولية إلى أن العراق يعاني من ضعف في البنية التحتية للأمن الرقمي مقارنة بالدول الأخرى، مما يجعله معرضاً للاختراقات، خصوصاً في القطاعات المالية والاتصالات والطاقة[11].

ثانياً :الإطار التشريعي والتنظيمي العراقي.

لا يوجد في العراق حتى عام 2025قانون مستقل لحماية البيانات الشخصية أو البيانات الوطنية .كما أن مشروع قانون جرائم المعلوماتية الذي طُرح منذ عام 2011لم يتم تفعيله بصورة نهائية بسبب الخلافات السياسية والتحفظات المجتمعية المتعلقة بالحريات العامة .وتعتمد الجهات الرسمية في بعض الحالات على نصوص متفرقة من قانون العقوبات وقانون الاتصالات وقوانين الخدمة المدنية، إلا أن هذه القوانين لا تتضمن أحكاماً تفصيلية لمعالجة قضايا مثل تسريب البيانات، أو الإبلاغ الإلزامي عن الاختراقات، أو المسؤولية القانونية لمشغلي قواعد البيانات[12].

ثالثاً :التحديات المؤسسية والبشرية في العراق.

من أبرز التحديات التي تواجه العراق ضعف الكوادر البشرية المتخصصة في الأمن السيبراني، وقلة برامج التدريب الوطني المستمر، فضلاً عن محدودية المختبرات التقنية في الجامعات والمعاهد .كما أن هجرة الكفاءات بعد عام 2003ساهمت في نقص الخبرات .إضافة إلى ذلك، يواجه العراق تحدياً في ضعف الثقافة الرقمية لدى الموظفين والمواطنين، مما يجعل أساليب الهندسة الاجتماعية (Social Engineering)والتصيد الإلكتروني (Phishing)أكثر نجاحاً .وتزداد هذه التحديات مع ضعف التنسيق بين المؤسسات وغياب قواعد واضحة لإدارة المخاطر الرقمية.

رابعاً :التجربة الأوروبية (GDPR)كنموذج لحماية البيانات.

تعد اللائحة العامة لحماية البيانات (GDPR)من أكثر النماذج التشريعية تطوراً في العالم، حيث تمنح الأفراد حقوقاً واسعة مثل حق الوصول إلى البيانات، وحق التصحيح، وحق النسيان، وحق الاعتراض على المعالجة .كما تلزم المؤسسات بالإبلاغ عن خروقات البيانات خلال 72ساعة، وتفرض غرامات مالية تصل إلى 4%من إجمالي الإيرادات السنوية العالمية للشركة المخالفة . وتستند GDPRإلى مبدأ أن البيانات ملك لصاحبها، وأن معالجتها يجب أن تتم وفق أساس قانوني واضح[13].

خامساً :التجربة الأمريكية (NIST Framework)وإدارة المخاطر.

يركز النموذج الأمريكي على إدارة المخاطر أكثر من التركيز على التشريعات العقابية .ويعد إطار (NIST Cybersecurity Framework)أحد أهم النماذج التي تعتمدها المؤسسات الحكومية والخاصة، إذ يحدد خمس وظائف رئيسية هي :التعرف، الحماية، الكشف، الاستجابة، التعافي . ويتميز هذا الإطار بمرونته وإمكانية تطبيقه على المؤسسات الصغيرة والكبيرة، كما يتيح بناء سياسات أمنية تدريجية وفق تقييم المخاطر .ويمكن للعراق الاستفادة من هذا الإطار في بناء خطط حماية للبنى التحتية الحرجة، خصوصاً في قطاع النفط والطاقة[14].

سادساً :تجربة إستونيا في الحكومة الرقمية.

تعد إستونيا من أبرز الدول الرائدة في الحكومة الرقمية، إذ تعتمد على الهوية الرقمية الوطنية، وتوفر خدمات حكومية إلكترونية واسعة النطاق .وقد تعرضت في عام 2007لهجمات سيبرانية واسعة أدت إلى تعطيل بعض المؤسسات، الأمر الذي دفعها إلى تطوير منظومة دفاع إلكتروني قوية وتأسيس

مركز وطني للاستجابة للطوارئ الرقمية، فضلاً عن التعاون مع حلف الناتو في مجال الدفاع السيبراني .وتؤكد تجربة إستونيا أن الأمن السيبراني لا يتحقق دون استثمار في البنية المؤسسية والوعي المجتمعي.

سابعاً :تجربة الصين وروسيا في السيادة الرقمية.

تميل بعض الدول مثل الصين وروسيا إلى تبني نموذج السيادة الرقمية الصارمة، حيث تفرض قيوداً على نقل البيانات خارج الحدود الوطنية، وتنشئ شبكات محلية بديلة وتطور تقنيات تشفير وطنية . وتعد هذه التجارب مثيرة للجدل من ناحية التوازن بين الأمن والحريات، لكنها تعكس توجه الدول نحو اعتبار البيانات جزءاً من الأمن القومي .ويمكن للعراق الاستفادة من هذه التجارب في جانب توطين البيانات الحكومية الحساسة ضمن مراكز بيانات وطنية مؤمنة، دون الوصول إلى مستوى التضييق على الحريات الرقمية.

ثامناً :تجربة الإمارات العربية المتحدة.

طورت دولة الإمارات العربية المتحدة منظومة وطنية متقدمة للأمن السيبراني من خلال إنشاء مجلس الأمن السيبراني الوطني، وإطلاق استراتيجية وطنية تركز على حماية البنى التحتية الرقمية، وتعزيز التعاون مع القطاع الخاص، وبناء قدرات بشرية عالية التدريب .كما اهتمت الإمارات بتطوير التشريعات المرتبطة بحماية البيانات والجرائم الإلكترونية، مما جعلها نموذجاً عربياً يمكن للعراق الاستفادة منه.

تاسعاً :نموذج مقترح للعراق لتعزيز الأمن السيبراني وحماية البيانات.

إن بناء منظومة وطنية للأمن السيبراني في العراق يتطلب مقاربة شاملة تشمل التشريع والمؤسسات والتقنية والوعي المجتمعي .ومن الضروري إنشاء هيئة وطنية للأمن السيبراني ترتبط بمجلس الوزراء، تكون مسؤولة عن وضع السياسات العامة، وإصدار المعايير الإلزامية، وتنسيق الاستجابة للحوادث .كما ينبغي تأسيس مركز وطني للاستجابة للطوارئ الرقمية (CERT)يعمل على مراقبة الهجمات وتحليلها وتقديم الإنذارات المبكرة .وفي الجانب التشريعي، ينبغي سن قانون لحماية البيانات الشخصية والوطنية يتضمن مبادئ الخصوصية، ويحدد حقوق الأفراد، ويلزم المؤسسات الحكومية والخاصة بحماية البيانات .إضافة إلى ذلك، ينبغي وضع نظام وطني لتصنيف البيانات إلى بيانات

عامة وحساسة وسرية وسيادية، مع تحديد ضوابط نقلها ومعالجتها .ويجب دعم هذا النموذج ببرامج تدريب وطنية في الجامعات والمعاهد، وتشجيع البحث العلمي في مجال الأمن السيبراني[15].

وفي ضوء ما سبق، فإن بناء استراتيجية وطنية عراقية للأمن السيبراني يجب أن يتضمن خارطة طريق تنفيذية على مراحل .ففي المرحلة الأولى ينبغي تطوير التشريعات وإنشاء الهيئة الوطنية ومركز الاستجابة للطوارئ .وفي المرحلة الثانية ينبغي إلزام المؤسسات بتطبيق معايير أمنية محددة، وتطوير أنظمة تصنيف البيانات، وإنشاء مراكز بيانات وطنية .أما المرحلة الثالثة فتتمثل في بناء اقتصاد سيبراني وطني يعتمد على تطوير شركات عراقية متخصصة في الأمن السيبراني، وتشجيع الابتكار والبحث العلمي، بما يخلق سوقاً وطنية توفر فرص عمل وتقلل من الاعتماد على الشركات الأجنبية.

ويمكن للعراق أيضاً أن يستفيد من مفهوم (Cyber Diplomacy)أو الدبلوماسية السيبرانية، وهو اتجاه عالمي جديد يقوم على التعاون الدولي في مواجهة الهجمات العابرة للحدود .فالهجمات السيبرانية غالباً ما يتم تنفيذها عبر شبكات دولية معقدة، مما يجعل من الصعب ملاحقة المجرمين دون تعاون دولي .ولذلك فإن انضمام العراق إلى اتفاقيات دولية مثل اتفاقية بودابست لمكافحة الجرائم السيبرانية قد يفتح المجال لتبادل المعلومات والتدريب وبناء القدرات.

ومن الناحية القانونية، فإن قانون حماية البيانات يجب أن يتضمن تحديداً واضحاً لمفهوم البيانات الحساسة، مثل البيانات الصحية والبيومترية والبيانات الأمنية، مع فرض قيود مشددة على معالجتها . كما ينبغي أن يتضمن القانون أحكاماً تتعلق بموافقة الأفراد، وحقهم في معرفة كيفية استخدام بياناتهم، وحقهم في الاعتراض، إضافة إلى تحديد المسؤولية المدنية والجنائية للمؤسسات في حال تسريب البيانات أو استخدامها بصورة غير قانونية .كما ينبغي النص على إنشاء هيئة مستقلة لحماية البيانات تكون مسؤولة عن الرقابة والتحقيق وإصدار العقوبات الإدارية.

ومن التحديات المتوقعة أيضاً أن العراق يتجه تدريجياً إلى استخدام الحوسبة السحابية في بعض المؤسسات الحكومية والخاصة، وهذا الاتجاه يوفر مزايا اقتصادية وتقنية، لكنه يخلق تحديات تتعلق بمكان تخزين البيانات والسيطرة عليها .فإذا كانت البيانات مخزنة في خوادم خارج العراق، فإنها تصبح عرضة للقوانين الأجنبية، وقد تصبح عرضة للتجسس أو الوصول غير المشروع .ولهذا فإن العديد من الدول تعتمد سياسة (Cloud Sovereignty)التي تعني ضمان أن الخدمات السحابية

تخضع للقوانين الوطنية .ويحتاج العراق إلى وضع ضوابط واضحة لتنظيم هذا القطاع وتحديد متطلبات الأمن والخصوصية.

وفي مجال الاتصالات، فإن شركات الهاتف النقال والإنترنت تعد خزانات ضخمة للبيانات، لأنها تمتلك بيانات المواقع الجغرافية للمستخدمين وسجلات الاتصالات وبيانات الدفع الإلكتروني .ولذلك فإن غياب قانون حماية البيانات يخلق خطراً مزدوجاً :الأول هو إمكانية تسرب البيانات أو بيعها، والثاني هو إمكانية استغلالها لأغراض سياسية أو أمنية غير قانونية .وتقتضي المعايير الدولية أن تكون شركات الاتصالات ملزمة بسياسات واضحة لحفظ البيانات، وبآليات تشفير، وبالإبلاغ عن الاختراقات، مع وجود جهة رقابية مستقلة.

أما قطاع النفط والغاز، فهو يمثل قلب الاقتصاد العراقي، ولذلك فإن أمنه السيبراني يرتبط مباشرة بالأمن الاقتصادي للدولة .وقد أثبتت التجارب الدولية أن الهجمات السيبرانية على المنشآت النفطية يمكن أن تسبب خسائر بمليارات الدولارات، كما حصل في بعض الهجمات العالمية التي استهدفت خطوط الأنابيب ومراكز التحكم .ومن هنا ينبغي على العراق أن يطور سياسات خاصة بأمن أنظمة التحكم الصناعي، وأن يفرض تحديثاً دورياً للبرمجيات، وعزل الشبكات الصناعية عن شبكات الإنترنت العامة، إضافة إلى تدريب العاملين في المنشآت النفطية على التعامل مع الحوادث الرقمية.

كما ينبغي التركيز على الأمن السيبراني في القطاع المصرفي العراقي بوصفه قطاعاً حيوياً يرتبط بالثقة العامة .فالمصارف العراقية، مع توسع استخدام أنظمة الدفع الإلكتروني، أصبحت عرضة لهجمات تستهدف سرقة بيانات الزبائن أو تعطيل عمليات التحويل .وفي هذا الإطار فإن اعتماد معايير أمنية مثل PCI-DSSالخاصة بحماية بيانات بطاقات الدفع يمثل خطوة ضرورية .كما أن المصارف تحتاج إلى أنظمة مراقبة مستمرة للمعاملات لاكتشاف الأنشطة المشبوهة، وإلى خطط تعافٍ رقمية لضمان استمرارية الخدمة في حال وقوع هجوم.

وتشير الأدبيات المعاصرة إلى أن بناء الأمن السيبراني لا يعتمد فقط على الأدوات التقنية مثل الجدران النارية والتشفير، بل يعتمد بصورة أساسية على إدارة الموارد البشرية والحوكمة المؤسسية. فضعف التدريب وقلة الوعي الأمني داخل المؤسسات قد يجعل من الموظف الحلقة الأضعف، حيث يتم استهدافه عبر رسائل البريد الاحتيالية أو الروابط الخبيثة، وهو ما يجعل الهندسة الاجتماعية من أكثر أدوات الاختراق نجاحاً في البيئات غير المؤهلة. لذلك فإن برامج بناء الثقافة السيبرانية تعد عنصراً حاسماً في تعزيز قدرة العراق على حماية بياناته.

ومن الجوانب المهمة التي ينبغي التوقف عندها في الحالة العراقية هو أثر البيئة السياسية والأمنية في إدارة الأمن السيبراني .فالدول التي تمر بمرحلة انتقالية غالباً ما تكون عرضة لاختراقات خارجية، لأن الانقسام المؤسسي وتعدد مراكز القرار يخلق فراغاً تنظيمياً يستغله الفاعلون السيبرانيون .كما أن بعض الهجمات الرقمية قد لا تستهدف سرقة البيانات فقط، بل قد تستهدف تعطيل الخدمات العامة وإحداث حالة من الإرباك الاجتماعي، وهو ما يعرف في الدراسات الحديثة بحروب الجيل الخامس التي تمزج بين الحرب التقليدية والحرب الإلكترونية والحرب الإعلامية.

ملاحظة تحليلية تخص الحالة العراقية.

الاستنتاجات.

1. يفتقر العراق إلى قانون شامل لحماية البيانات الشخصية والوطنية وفق المعايير الدولية.
2. غياب هيئة وطنية للأمن السيبراني يمثل ثغرة استراتيجية في منظومة الأمن الوطني.
3. ضعف البنى التحتية التقنية وقلة الاستثمار في الأمن الرقمي يزيد من مخاطر الاختراق.
4. نقص الكوادر البشرية المتخصصة يضعف قدرة العراق على الاستجابة للطوارئ الرقمية.
5. التجارب العالمية تؤكد أن الأمن السيبراني يتطلب استراتيجية وطنية وحوكمة واضحة.
6. الشراكة بين القطاعين العام والخاص تمثل عنصراً أساسياً لتعزيز حماية البيانات.
7. توطين البيانات الحساسة يعد جزءاً من تعزيز السيادة الرقمية العراقية.

التوصيات.

١ـ الإسراع في تشريع قانون عراقي متكامل لحماية البيانات الشخصية والبيانات الوطنية.

٢ـ إنشاء هيئة وطنية مستقلة للأمن السيبراني ترتبط بمجلس الوزراء وتتمتع بصلاحيات تنظيمية.

٣ـ تأسيس مركز وطني للاستجابة للطوارئ الرقمية (CERT)يعمل على الإنذار المبكر وتحليل الهجمات.

٤ـ اعتماد معايير ISO/IEC 27001وإطار NISTفي المؤسسات الحكومية والبنى التحتية الحرجة.

٦ـ وضع نظام وطني لتصنيف البيانات وتحديد مستويات السرية والصلاحيات.

٧ـ إلزام المؤسسات الحكومية بالإبلاغ عن الاختراقات خلال مدة زمنية محددة.

٨ ـ تطوير برامج تدريب وطنية بالتعاون بين الجامعات والقطاع الخاص لتأهيل مختصين في الأمن السيبراني.

٩ـ إطلاق حملات توعية وطنية حول مخاطر التصيد الإلكتروني والابتزاز الرقمي.

١٠ـ تعزيز التعاون الدولي والانضمام إلى اتفاقيات مكافحة الجرائم الإلكترونية وتبادل الخبرات.

١١ـ إنشاء مراكز بيانات وطنية مؤمنة لتوطين البيانات الحكومية الحساسة وحمايتها.

قائمة الحواشي.

15- ITU, Global Cybersecurity Index (GCI) Methodology, 2024. (ص6)

14- NIST Cybersecurity Framework, National Institute of Standards and Technology, USA. (ص6)

13- European Union, General Data Protection Regulation (GDPR), 2016. (ص6)

12- Lark Journal, The Iraqi Legislative Policy to Protect National Cyber Security, 2024. (ص6)

11- Freedom House, Iraq: Freedom on the Net 2023 Report. (ص6)

10- Al-Hamdan, S. R. S. & Heydari, A. P., The Legal Framework for Cybersecurity in Iraq, Basra Studies Journal, 2025. (ص5)

9- ITU, Global Cybersecurity Index (GCI) Methodology, 2024. (ص4)

8- Budapest Convention on Cybercrime, Council of Europe, 2001. (ص4)

7- European Union, General Data Protection Regulation (GDPR), 2016. (ص 4)

6- NIST Cybersecurity Framework, National Institute of Standards and Technology, USA. (ص4)

5- ISO/IEC 27001: Information Security Management Systems, International Organization for Standardization. (ص3)

4- Bayancenter.org, The Internet and Cyber Domain in Iraq: A Policy Void, 2022. (ص2)

3- UN-ESCWA, Iraq National Digital Development Report, 2022. (ص2)

2- Freedom House, Iraq: Freedom on the Net 2023 Report. (ص2)

1- ITU, Cybersecurity Profile: Republic of Iraq, 2025. (ص1)

قائمة المصادر والمراجع.

Freedom House, Iraq: Freedom on the Net 2023 Report.

ITU, Cybersecurity Profile: Republic of Iraq, 2025.

ITU, Global Cybersecurity Index (GCI) Methodology, 2024.

UN-ESCWA, Iraq National Digital Development Report, 2022.

Al-Hamdan, S. R. S. & Heydari, A. P., The Legal Framework for Cybersecurity in Iraq, Basra Studies Journal, 2025.

Communications and Media Commission (Iraq), Framework Regulations for Digital Platforms, 2025.

Bayancenter.org, The Internet and Cyber Domain in Iraq: A Policy Void, 2022.

Lark Journal, The Iraqi Legislative Policy to Protect National Cyber Security, 2024.

ISO/IEC 27001: Information Security Management Systems, International Organization for Standardization.

NIST Cybersecurity Framework, National Institute of Standards and Technology, USA.

Budapest Convention on Cybercrime, Council of Europe, 2001.

European Union, General Data Protection Regulation (GDPR), 2016.