Tikrit University Journal For Rights Year (10) Vol (10) NO (4) Part (2) (2026) 697-718

٦٩٧

ISSN: 2519 – 6138 (Print)
E-ISSN: 2663 – 8983(On Line)

TUJR
مجلة جامعة تكريت للحقوق
Tikrit University Journal for Rights

IRAQI Academic Scientific Journals
العراقية المجلات الاكاديمية العلمية

Tikrit University Journal for Rights
Journal Homepage : http://tujr.tu.edu.iq/index.php/t

كلية القانون
College of Law

Administrative and criminal liability for breaches of cybersecurity in digital public facilities - an analytical study in light of Iraqi legislation

Associate Professor Dr. Mahdi Balavi

Department of Public Law, Faculty of Law, University of Tehran, Iran

mahdibalavi@ut.ac.ir

PhD Student RAFID SALEEM HASAN

Department of Public Law, Faculty of Law, University of Tehran, Iran

cv.sham89@gmail.com

Article info.

Article history:

- Received 22 March 2026
- Accepted 5 April 2026
- Available online 1 June 2026

Keywords:

- Corporate cybersecurity
- Digital public utility
- Administrative liability
- Criminal liability
- State employees' disciplinary law
- Gross negligence.

Abstract:

This research addresses the legal challenges arising from the transition of public administration to the digital environment, along with the associated risks that threaten the information infrastructure and citizens' personal data. The problem of the study stems from the legislative vacuum in Iraq, the absence of regulations governing institutional cybersecurity, and the inadequacy of traditional penal and disciplinary provisions to encompass crimes of technical negligence. Through an analytical–foundational approach, the research concludes that leaving systems unprotected or disclosing passwords constitutes a contemporary application of "gross negligence," which warrants criminal and administrative accountability. The study

recommends the necessity of decoupling cybercrimes from administrative information security, enacting an "Information Security Governance" law that imposes proactive disciplinary sanctions, and amending the State Employees Discipline Law to classify cyber negligence as a gross occupational violation.

المسؤولية الإدارية والجزائية عن الإخلال بالأمن السيبراني للمرفق العام الرقمي – دراسة تحليلية في ضوء التشريع العراقي

الأستاذ المشارك الدكتور مهدى بالوى

قسم القانون العام، كلية القانون ، جامعة طهران ، ايران

mahdibalavi@ut.ac.ir

طالب الدكتوراه. رافد سليم حسن عبد الرضا

قسم القانون العام، كلية القانون ، جامعة طهران ، ايران

cv.sham89@gmail.com

معلومات البحث :

تواريخ البحث:

- الاستلام : ٢٢ / اذار/ ٢٠٢٦
- القبول : ٥ / نيسان/ ٢٠٢٦
- النشر المباشر: ١/حزيران /٢٠٢٦

الكلمات المفتاحية :

- **الأمن السيبراني المؤسسي**
- **المرفق العام الرقمي**
- **المسؤولية الإدارية**
- **المسؤولية الجزائية**
- **قانون انضباط موظفي الدولة**
- **الإهمال الجسيم.**

الخلاصة: يتناول هذا البحث الإشكاليات القانونية الناجمة عن انتقال الإدارة العامة إلى البيئة الرقمية، وما يرافق ذلك من مخاطر تهدد البنية التحتية للمعلومات والبيانات الشخصية للمواطنين. تنبع مشكلة الدراسة من الفراغ التشريعي في العراق وغياب القواعد المنظمة للأمن السيبراني المؤسسي، فضلاً عن قصور النصوص العقابية والانضباطية التقليدية عن استيعاب جرائم الإهمال التقني. وقد خلص البحث من خلال المنهج التحليلي التأصيلي إلى أن ترك الأنظمة دون حماية أو إفشاء كلمات المرور يُعد تطبيقاً معاصراً لـ "الإهمال الجسيم" الذي يوجب المساءلة الجنائية والإدارية. وأوصت الدراسة بضرورة فك الارتباط بين جرائم المعلوماتية وأمن المعلومات الإداري، وتشريع قانون "حوكمة أمن المعلومات" الذي يفرض جزاءات انضباطية استباقية، مع تعديل قانون انضباط موظفي الدولة لتكييف التقصير السيبراني كمخالفة وظيفية جسيمة.

المقدمة : أولاً: التعريف بموضوع البحث

أفرز التحول الرقمي المتسارع في عمل الإدارات العامة تحديات قانونية مستحدثة تتجاوز نطاق التنظيم التقليدي للمرافق العامة، لتصل إلى مسألة تأمين البنية التحتية الرقمية وحماية البيانات الشخصية للمواطنين. إن انتقال البيانات من الخزائن الورقية إلى الخوادم السحابية يفرض بناء سياج تشريعي يحدد

بوضوح حدود المسؤولية (الإدارية والجزائية) للموظف العام وللإدارة عند حدوث اختراقات سيبرانية أو تسريب للبيانات.

أولاً: أهمية البحث

تتمثل أهمية البحث في بيان دور الأمن السيبراني في حماية المرفق العام الرقمي وضمان استمرارية خدماته، مع تحديد المسؤولية الإدارية والجزائية عند حدوث خروقات. كما يسهم في تقييم كفاية التشريع العراقي واقتراح حلول لتعزيز الحماية القانونية.

ثانياً: سبب اختيار الموضوع

يرجع اختيار الموضوع إلى حداثته، وتزايد الهجمات السيبرانية على المؤسسات الحكومية، مع وجود نقص في الدراسات العراقية المتخصصة، والحاجة لتحديد المسؤوليات القانونية في البيئة الرقمية.

ثالثاً: أهداف البحث

يهدف البحث إلى:

- توضيح مفهوم الأمن السيبراني في المرافق العامة.
- تحليل المسؤولية الإدارية والجزائية عن الإخلال به.
- تقييم التشريع العراقي وبيان أوجه القصور.
- تقديم مقترحات قانونية لتعزيز الحماية.

رابعاً: مشكلة البحث

تتمثل مشكلة البحث في مدى كفاية التشريع العراقي لتنظيم المسؤولية الإدارية والجزائية عن الإخلال بالأمن السيبراني في المرافق العامة الرقمية ، ويتفرع عنها تساؤلات حول الأساس القانوني لهذه المسؤولية وحدودها وأوجه القصور التشريعي.

وتتمحور مشكلة البحث من جهة أخرى في الإجابة عن التساؤل الآتي: إلى أي مدى تستطيع القواعد الإدارية والجزائية التقليدية في التشريع العراقي استيعاب جرائم الإهمال التقني وتحديد المسؤولية عن الإخلال بالأمن السيبراني للمرفق العام؟ ويهدف البحث إلى تشخيص الفراغ التشريعي الحالي، وإعادة تكييف النصوص العقابية والانضباطية الكلاسيكية لتتلاءم مع متطلبات الحوكمة الإلكترونية ومساءلة الموظف والقيادات الإدارية عن أمن المعلومات.

خامساً: منهجية البحث

يعتمد البحث على:

- المنهج التحليلي لدراسة النصوص القانونية.
- المنهج الوصفي لعرض الواقع القانوني.
- المنهج المقارن للاستفادة من التجارب الأخرى.
- المنهج النقدي لتقييم التشريع العراقي.

المبحث الأول: الإطار القانوني للأمن السيبراني المؤسسي والفراغ التشريعي

يُعد بناء سياج تشريعي متين خطوة تسبق أي تحول رقمي آمن. ففي ظل غياب تشريعات وطنية صريحة تُعنى بحماية البيانات وتنظيم الفضاء السيبراني المؤسسي، تجد الإدارة نفسها أمام تحديات قانونية جمة. لذا، نُسلط الضوء في هذا المبحث على الفراغ التشريعي القائم، في مطلبين نتناول في الأول المبررات القانونية الملحة لسن تشريع خاص بحماية البيانات الشخصية، ونستعرض في الثاني الإطار القانوني الحالي الناظم للأمن السيبراني للمؤسسات للوقوف على مكامن القصور فيه.

المطلب الأول: المبررات القانونية لسن تشريع حماية البيانات الشخصية.

أفرز التحول الرقمي المتسارع في عمل الإدارات العامة تحديات قانونية مستحدثة تتجاوز نطاق التنظيم التقليدي للمعاملات، وفي مقدمتها مسألة حماية البيانات الشخصية بوصفها أحد المرتكزات الجوهرية لنجاح الحوكمة الإلكترونية وبناء الثقة في التعاملات الرقمية, فقد أدى التوسع في استخدام نظم المعلومات والاتصالات إلى تعاظم حجم البيانات المتداولة بين الأفراد والجهات الرسمية، الأمر الذي جعل هذه البيانات عرضة لمخاطر الاختراق أو المعالجة غير المشروعة، بما يمسّ بصورة مباشرة حق الخصوصية الشخصية وأمن الأفراد القانوني, ولا يقف الأمر عند هذا الحد، بل إن ضرورة تقنين هذه الحماية باتت مطلباً عالمياً ملحاً يتزايد طردياً مع تطور الوسائل التقنية؛ لضمان صون الحقوق والحريات في الفضاء الرقمي[١]. وتتأكد هذه الضرورة مع التطورات التقنية الحديثة جلبت معها تحديات جديدة تتعلق بأمن المعلومات وحماية خصوصية الأفراد، إذ أصبحت الهجمات السيبرانية تهدد استقرار الدول

---

١ – ملاك عواد إسماعيل صوالحه، الجوانب القانونية لحماية خصوصية البيانات الشخصية في العصر الرقمي، مجلة القانون الدستوري والعلوم الإدارية، ، العدد (٢٩)، ألمانيا , ٢٠٢٥, ص ١٤.

ومؤسساتها بشكل غير مسبوق، وهو ما يكشف عن قصور التنظيمات القانونية التقليدية عن استيعاب هذه المخاطر المستجدة.[١]

وفي تشخيص دقيق لواقع هذا القصور في العراق، يرى البعض أن المشكلة لا تكمن فقط في غياب النص، بل في تشتت الجهود وغياب المرجعية الموحدة، إذ يعاني العراق من عدم وجود سياسة تشريعية واضحة، كما أن الأجهزة التي تعنى بالأمن السيبراني موزعة بين جهاز الأمن الوطني والمخابرات العامة ووزارة الداخلية، ولا توجد وزارة أو هيئة مستقلة للأمن السيبراني[٢], هذا التشتت المؤسسي يعرقل وجود رؤية تشريعية شاملة تحمي البيانات الشخصية بفاعلية.

وعلى الرغم من وجود نصوص قانونية متفرقة في التشريع العراقي تمسّ بعض جوانب حماية البيانات، كقواعد سرية السجلات المدنية أو القيود المفروضة على تداول بعض المعلومات، إلا أن هذه النصوص لا ترقى إلى مستوى تشريع متكامل يعالج البيانات الشخصية بوصفها حقًا مستقلاً ذا طبيعة رقمية, إذ يلاحظ أن قانون الأحوال المدنية رقم (١٥) لسنة ١٩٧٧، على سبيل المثال، وإن كان قد كفل سرية القيود المسجلة في السجل المدني، إلا أن نطاق هذه الحماية يظل محدودًا بطبيعة البيانات التقليدية، ولا يمتد ليشمل المعالجة الإلكترونية الواسعة للبيانات أو تداولها عبر المنصات الرقمية الحكومية، الأمر الذي يبرز فجوة تشريعية واضحة في هذا المجال[٣], وهذا القصور يبرز الحاجة الماسة لمغادرة مربع النصوص العامة المتناثرة والانتقال إلى تشريع خاص وشامل يواكب الفراغ التشريعي ويغطي المعالجة الإلكترونية الواسعة للبيانات، وهو المسار الذي بات ضرورة لا غنى عنها لسد الفجوة التشريعية الواضحة في المنظومة القانونية الوطنية[٤].

ويرى الباحث أن جوهر الإشكالية في حماية البيانات لا يكمن فقط في حمايتها من الاختراق الخارجي (وهو الجانب الأمني)، بل في حمايتها من التعسف الإداري الداخلي؛ أي كيفية تعامل الموظف

---

١ – سجاد صبار رزاق الحمدان، إلهام حيدري، الإطار القانوني لحماية الأمن السيبراني في العراق– دراسة تحليلية في ضوء التشريعات الوطنية والمعايير الدولية، مجلة دراسات البصرة، العدد (٦٢)، ٢٠١٥، ص ٩١.

٢ – سامر محي عبد الحمزة، السياسة التشريعية العراقية لحماية الأمن السيبراني الوطني– دراسة في ضوء مبادئ القانون الدولي العام، مجلة لارك للفلسفة واللسانيات والعلوم الاجتماعية، جامعة واسط، المجلد (٣)، العدد (٤٦)، ٢٠٢٢، ص ٥٢٣.

٣ – سجاد صبار رزاق الحمدان، إلهام حيدري، مصدر سابق , ص ٩٩.

٤ – ملاك عواد إسماعيل صوالحه، مصدر سابق , ص ١٤.

العام مع بيانات المواطن أثناء ترويج المعاملة, فغياب قانون ينظم دورة حياة البيانات داخل الإدارة (جمعاً، وتخزيناً، وإتلافاً) يجعل بيانات المواطنين عرضة للاستغلال أو البيع أو الإهمال بلا رادع إداري واضح، مما يزعزع الثقة الرقمية التي هي أساس انخراط المواطن في نظام الحوكمة.

ولم تكن السلطة التشريعية غائبة تماماً عن هذا المشهد، بل كانت هناك محاولات لتدارك هذا النقص، ففي الخامس من حزيران ٢٠٢٢، أعلنت لجنة الأمن والدفاع في مجلس النواب العراقي عزمها على إعادة تقديم مشروع قانون جرائم المعلوماتية[١] إلا أن تأخر إقرار هذا القانون وبقاءه في أروقة التشريع يعزز من حالة الفراغ القانوني ويؤكد الحاجة للإسراع في حسم هذه المنظومة التشريعية.

ومما يعزز مبررات سن هذا التشريع ضرورة التمييز الدقيق بين أنواع البيانات، وهو ما تفتقده القواعد العامة الحالية في القانون العراقي, فالمتطلبات القانونية الحديثة تستلزم التفريق بوضوح بين البيانات الشخصية العادية (كالاسم والعنوان) والبيانات الحساسة (كالبصمة البيومترية، والسجلات الصحية، والمعتقدات، والآراء السياسية), هذا التمييز ضروري لفرض حماية مشددة على البيانات الحساسة واشتراط إذن مسبق وصريح لمعالجتها نظرًا لخطورة المساس بها على الحياة الخاصة للأفراد، وهو ما يستدعي من المشرع العراقي التدخل لتقنين هذا التصنيف لضمان شمولية الحماية وتحديد مستوياتها بما يتناسب مع طبيعة البيانات المعالجة[٢].

ويزداد هذا الفراغ التشريعي وضوحًا عند النظر إلى متطلبات الحوكمة الإلكترونية، التي تقوم في جوهرها على تبادل البيانات بين الإدارات المركزية واللامركزية، وربط قواعد المعلومات الوطنية، وتمكين المواطن من إنجاز معاملاته عن بُعد. فغياب إطار قانوني خاص لحماية البيانات الشخصية يُضعف الثقة في الأنظمة الإلكترونية، ويجعل المواطن مترددًا في إيداع معلوماته ووثائقه عبر المنصات الرقمية، وهو ما ينعكس سلبًا على كفاءة إنجاز المعاملات الإدارية. وفي هذا الصدد، يرى البعض أن 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[٣].

---

١ – محمد كاظم هادي عنجور المنصوري، الواقع التشريعي للأمن السيبراني في العراق– التحديات والطموحات، مجلة العلوم الإنسانية والطبيعية، المجلد (٦)، العدد (٨)، ٢٠٢٥، ص ٥٧١.

٢ – ملاك عواد إسماعيل صوالحه، مصدر سابق, ص١٦.

٣ – سجاد صبار رزاق الحمدان، إلهام حيدري، مصدر سابق , ص ١٠٠.

كما تبرز المبررات القانونية لسنّ تشريع خاص بحماية البيانات الشخصية من زاوية الالتزامات الدولية والمعايير المقارنة، إذ تسعى العديد من الدول إلى مواءمة تشريعاتها الوطنية مع المعايير الدولية ذات الصلة بالأمن السيبراني وحماية الخصوصية الرقمية. ومن أهم هذه المعايير التي تفرض سن التشريع ضرورة إنشاء جهة مؤسساتية مستقلة[١] تتولى الرقابة والإشراف على حماية البيانات, وجود مثل هذه الهيئة يعد ضمانة إجرائية لا غنى عنها لمنح التراخيص، وتلقي الشكاوى، ومراقبة مدى التزام الجهات المعالجة للبيانات بالقانون، وهو فراغ مؤسسي يعاني منه النظام القانوني الحالي الذي يفتقر لجهة مركزية متخصصة بهذا الشأن[٢], ويلاحظ في هذا الإطار أن التشريعات العراقية، وإن كانت تجرّم بعض الأفعال الإلكترونية غير المشروعة، إلا أنها لا تزال تواجه تحديات تعيق تحقيق انسجام كامل مع المعايير الدولية، ولا سيما تلك المتعلقة بتنظيم جمع البيانات ومعالجتها والرقابة على استخدامها[٣]. ويؤدي هذا التباين إلى إضعاف مركز العراق في البيئة الرقمية الدولية، ويحدّ من قدرته على بناء منظومة حوكمة إلكترونية متكاملة وآمنة.

ومن جهة أخرى، فإن حماية البيانات الشخصية تمثل شرطًا سابقًا لضمان فعالية الأمن السيبراني المؤسسي، إذ لا يمكن الحديث عن أمن رقمي حقيقي في ظل غياب قواعد واضحة تحدد التزامات الجهات الإدارية في جمع البيانات، وحدود استخدامها، وآليات مساءلتها عند الإخلال بها, وقد أشار بعض الباحثين إلى أن ضعف البنية التشريعية، إلى جانب محدودية الموارد التقنية والبشرية، يؤدي إلى وجود ثغرات قد تؤثر على حقوق المستخدمين، مما يستلزم تدخلاً تشريعيًا واضحًا يضع قواعد دقيقة لحماية البيانات ويعزز من آليات الإنفاذ القانوني[٤], كما أن التشريع الخاص يوفر مظلة للمسؤولية الجنائية الرادعة التي تميز بين المسؤول عن المعالجة و المعالج وتفرض عقوبات تتناسب مع جسامة الانتهاك، سواء كانت عقوبات سالبة للحرية أو غرامات مالية مشددة، وهو ما يعالج القصور في

---

١ – خصص الفصل الرابع من دستور جمهورية العراق لسنة ٢٠٠٥ لبيان الهيئات المستقلة وذكر في المادة ١٠٢ الى المادة ١٠٧ مجموعة من الهيئات في حين نصت المادة ١٠٨ على ما يلي " يجوز استحداث هيئات مستقلة أخرى حسب الحاجة والضرورة بقانون"

٢ – ملاك عواد إسماعيل صوالحه، مصدر سابق, ص ٢٠.

٣ – سجاد صبار رزاق الحمدان، إلهام حيدري، مصدر سابق , ص ١٠٤.

٤ – سجاد صبار رزاق الحمدان، إلهام حيدري، مصدر سابق , ص ١٠٥.

النصوص العقابية التقليدية التي قد لا تغطي صور الاعتداءات الرقمية المستحدثة على البيانات، مما يستوجب نصاً خاصاً لردع الانتهاكات التي تطال الخصوصية الرقمية[١].

وتأسيسًا على ما تقدم، يتبين أن سنّ تشريع خاص لحماية البيانات الشخصية في العراق لم يعد ترفًا تشريعيًا، بل ضرورة قانونية تفرضها متطلبات الدستور، وعلى المستوى الدستوري، يُلاحظ أن الدستور الحالي لسنة ٢٠٠٥ لم يرد فيه الحق في حماية البيانات الشخصية بصورة صريحة, انما تناول بالتنظيم الحق ضمناً, وهنا نجد على المشرع الدستوري العراقي إضافة نص يخص حق حماية البيانات الشخصية أسوة بحقوق الإنسان الأخرى وذلك لإضفاء الحماية الدستورية على البيانات الشخصية[٢], فالنصوص الحالية (كالمادة ١٧ و٤٠) تحمي الخصوصية والمراسلات بشكل عام دون تخصيص دقيق للبيانات الرقمية.

ومبادئ الحوكمة الإلكترونية، وحاجة المواطن إلى ضمانات فعّالة تحمي خصوصيته في البيئة الرقمية. فنجاح إنجاز معاملات المواطنين إلكترونيًا لا يقاس بسرعة الإجراء وحدها، بل بمدى ما توفره الدولة من حماية قانونية لبياناتهم، وبقدرتها على بناء ثقة مستدامة بين الإدارة والمواطن في ظل التحول الرقمي المتنامي.

المطلب الثاني: الإطار القانوني الناظم للأمن السيبراني للمؤسسات الحكومية.

يعاني التنظيم القانوني للأمن السيبراني في العراق من قصور واضح في مواجهة التحديات المستحدثة، إذ لا تزال المنظومة التشريعية تعتمد بشكل أساسي على القواعد العامة في قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩, ورغم أن هذا القانون تضمن نصوصاً عقابية تتعلق بجرائم النشر والتهديد والمساس بالأخلاق العامة، إلا أنه لم يعد يتماشى مع التطور التقني الهائل، ولا يستوعب الكم المتزايد من المشكلات التي تُعرض على المحاكم يومياً، مما يجعل المشرع العراقي متأخراً في وضع الحدود اللازمة لمنع الإضرار بالمصالح العامة والخاصة في الفضاء الرقمي، والاكتفاء بنصوص وُضعت لبيئة تقليدية مغايرة للواقع الحالي[٣].

---

١ – ملاك عواد إسماعيل صوالحه، مصدر سابق, ص ٢١.

٢ – شميم مزهر راضي، الحق في حماية البيانات الشخصية في ظل دستور جمهورية العراق لسنة ٢٠٠٥، مجلة جامعة الإمام جعفر الصادق (ع) للدراسات القانونية، العدد الرابع، ٢٠٢٢، ص ١٦٣.

٣ – محمد كاظم هادي عنجور المنصوري، مصدر سابق , ص ٥٧٠.

ولا تتوقف التحديات القانونية عند حدود النصوص العقابية، بل تمتد لتشمل القواعد الحاكمة للمسؤولية المدنية والتعويض، إذ تصطدم القواعد التقليدية بصعوبات إجرائية في البيئة الرقمية، حيث أن: مسألة الاثبات هنا قد تكون غاية في الصعوبة خصوصاً إذا ما علمنا ان الذي يدير البيانات ويتولى معالجتها والتعامل معها انما هو شخص محترف بتقنيات الوسط الالكتروني وأن صاحب البيانات من النادر أن يكون على درجة من الاحتراف بتقنيات الوسط الرقمي، وهذا ما يعني ضياع حق المضرور بالمطالبة بالضمان في حالة عدم تمكنه من اثبات التعدي ومجاوزة الواجب المفروض على صاحب الوسط الرقمي ومعالج البيانات[١].

وعلى صعيد التطبيق القضائي، يتأسس التزام الإدارة بالتعويض على المادة (٢١٩)[٢] من القانون المدني العراقي رقم (٤٠) لسنة ١٩٥١ المعدل التي تقرر مسؤولية الإدارة عن الأضرار الناجمة عن أعمال موظفيها، فضلاً عن خضوعها للقواعد العامة للمسؤولية التقصيرية التي تستلزم توافر أركان الخطأ والضرر والعلاقة السببية وفقاً للمادة (٢٠٤)[٣] من القانون ذاته, وفي هذا الصدد، يرى الباحث أن تطبيق هذه القواعد التقليدية في بيئة الحوكمة الإلكترونية يصطدم بعقبة إثبات ركن الخطأ إذ يفتقر المواطن – الذي تتعرض بياناته للانتهاك– إلى القدرة الفنية اللازمة لتحديد سبب الخلل، وما إذا كان نتاجاً لخطأ مرفقي (إهمال الموظف) أم لسبب أجنبي (هجوم سيبراني)، مما يستدعي تدخلاً تشريعياً لتبني مبدأ المسؤولية المفترضة تخفيفاً لعبء الإثبات التقني عن المتضرر.

---

١ – د. اسامة عبد الواحد التهامي، نطاق الحماية القانونية للبيانات الشخصية والمسؤولية التقصيرية عن معالجتها –دراسة في القانون الإماراتي، مجلة البحوث القانونية والاقتصادية، كلية الحقوق جامعة المنصورة، العدد (٦٧) ، ٢٠١٨, ص ٦٤٥ .

٢ – تنص المادة (٢١٩) من القانون المدني العراقي رقم (٤٠) لسنة ١٩٥١ المعدل على ما يلي " ١ – الحكومة والبلديات والمؤسسات الاخرى التي تقوم بخدمة عامة وكل شخص يستغل احد المؤسسات الصناعية او التجارية مسؤولون عن الضرر الذي يحدثه مستخدموهم، اذا كان الضرر ناشئاً عن تعد وقع منهم اثناء قيامهم بخدماتهم. ٢ – ويستطيع المخدوم ان يتخلص من المسؤولية اذا اثبت انه بذل ما ينبغي من العناية لمنع وقوع الضرر او ان الضرر كان لا بد واقعاً حتى لو بذل هذه العناية.

٣ – تنص المادة (٢٠٤) من القانون المدني العراقي رقم (٤٠) لسنة ١٩٥١ المعدل على ما يلي "كل تعد يصيب الغير بأي ضرر آخر غير ما ذكر في المواد السابقة يستوجب التعويض".

وقد واجهت المحاولات التشريعية لسد هذا الفراغ عقبات دستورية وسياسية، ولا سيما فيما يتعلق بمشروع قانون جرائم المعلوماتية, فقد شهدت الأروقة التشريعية جدلاً واسعاً حول مسودات هذا القانون (نسخة ٢٠١١ ونسخة ٢٠١٨)، حيث اصطدمت هذه المشاريع بالمخاوف المتعلقة بالحريات العامة, فقد انتُقدت المسودات لاحتمالية تعارضها مع المادة (٣٨) من الدستور العراقي التي تكفل حرية الرأي والتعبير، فضلاً عن تعارضها مع الاتفاقيات الدولية، مما أدى إلى سحب نسخة ٢٠١١ وتجميد نسخة ٢٠١٨ وسط مطالبات بتعديلها لضمان عدم استخدامها كأداة لتقييد الحريات بدلاً من حماية الأمن السيبراني[١].

وفي محاولة لتدارك هذا الفراغ التشريعي عبر حلول تنفيذية، أصدرت مستشارية الأمن الوطني في عام ٢٠٢٢ (استراتيجية الأمن السيبراني العراقي) لتكون بمثابة خارطة طريق توفر تدابير متماسكة لحماية البنية التحتية الحيوية للمعلومات. وقد تضمنت هذه الاستراتيجية تشكيل (فريق وطني مشترك للاستجابة للحوادث السيبرانية) يتولى مهام تأمين الشبكات ومراكز البيانات الوطنية، وتنسيق الجهود بين القطاعين العام والخاص، ليكون هذا الإجراء التنظيمي بمثابة حل مؤقت لملء الفراغ الذي خلفه غياب القانون المختص[٢].

وتبرز في هذا السياق إشكالية جوهرية تتمثل في الخلط المفاهيمي لدى المشرع العراقي بين قانون جرائم المعلوماتية وبين قانون أمن المعلومات, فالمشرع لم يتمكن من التمييز الدقيق بينهما؛ إذ يُعنى الأول بتجريم الأفعال ومعاقبة الجناة، بينما يركز الثاني على حماية البيانات والمعلومات كأصول رقمية ومعالجتها. هذا الخلط أدى إلى غياب رؤية تنظيمية تحمي المعلومة بحد ذاتها، حيث تُعتبر البيانات مدخلات أساسية، وتصبح معلومات ذات قيمة عند معالجتها، وهو جانب وقائي يختلف تماماً عن الجانب العقابي الذي ركزت عليه مسودات القوانين المقترحة[٣].

ولا يقف الإشكال عند هذا الحد، بل يمتد ليشمل عجز المصطلحات القانونية التقليدية عن استيعاب الديناميكية التقنية للنشاط السيبراني، إذ أن وسائل المعالجة الرقمية تعكس بمضمونها وطبيعتها

---

١ – محمد كاظم هادي عنجور المنصوري، مصدر سابق , ص ٥٧٢.

٢ – د. ثابت سلطان محمد، تعزيز استراتيجيات الأمن السيبراني في العراق والدول العربية وموائمتها مع أهداف التنمية المستدامة، المجلة العراقية للعلوم الاقتصادية، السنة الثالثة والعشرون، عدد خاص، ٢٠٢٥، ص ٤٠ – ٤٧.

٣ – محمد كاظم هادي عنجور المنصوري، مصدر سابق , ص ٥٧٢.

وذاتها صورة من صور التعامل التي لا يمكن حصرها ولا التكهن بها في ظل مجتمع المعلومات وصناعة المعرفة المفتوح على مصراعيه امام الكثير والكثير من التقنيات الرقمية والتكنولوجية الذكية[١].

وفيما يتعلق بحماية المؤسسات من الإرهاب الإلكتروني، فإن النصوص الدستورية (المواد [٢]٧، ٣٢١[٣]، ٧٣[٤]) وقانون جهاز مكافحة الإرهاب لسنة ٢٠٠٨، ركزت على الإرهاب بمفهومه المادي التقليدي، ولم تُشر صراحة في مضامينها إلى الإرهاب الإلكتروني وآثاره المدمرة على المجتمع والمؤسسات, فرغم أن أهداف جهاز مكافحة الإرهاب تتضمن مجابهة واستئصال الإرهاب بجميع أشكاله، إلا أن غياب النص الصريح على البعد السيبراني يُضعف الغطاء القانوني اللازم لمواجهة الهجمات التي تستهدف البنى التحتية الرقمية للدولة، والتي قد تؤدي إلى انهيار اقتصادي أو اجتماعي نتيجة تعطيل الأنظمة الحيوية[٥].

ويذهب الباحث إلى أن الاعتماد على استراتيجيات صادرة عن السلطة التنفيذية لتنظيم الأمن السيبراني للمؤسسات، وإن كان حلاً مؤقتاً، إلا أنه يفتقر إلى عنصر الإلزام القانوني والجزائي تجاه الإدارات المقصرة, فالاستراتيجية توجه ولا تعاقب، بينما يتطلب انتظام سير المرفق العام الإلكتروني وجود نصوص قانونية تفرض عقوبات مسلكية وجنائية على المسؤول الإداري الذي يتسبب بإهماله في توقف الخدمة الرقمية أو ضياع البيانات، لضمان أن يكون الأمن السيبراني واجباً وظيفياً لا مجرد خيار فني.

---

١ – إخلاص مخلص إبراهيم وزياد طارق جاسم، المسؤولية التقصيرية عن التعامل بالبيانات الشخصية في الوسط الرقمي، وقائع المؤتمر العلمي الدولي التاسع للقضايا القانونية (ILIC9)، جامعة تيشك الدولية، 2024, ص ٤.

٢ – تنص المادة (٧) من دستور جمهورية العراق لسنة ٢٠٠٥ على ما يلي " أولاً : – يحظر كل كيانٍ أو نهجٍ يتبنّى العنصرية أو الإرهاب أو التفكير أو التطهير الطائفي، أو يحرض أو يمهد أو يمجد أو يروج أو يبرر له، وبخاصة البعث الصدامي في العراق ورموزه، وتحت أي مسمىً كان، ولا يجوز أن يكون ذلك ضمن التعددية السياسية في العراق، وينظم ذلك بقانون. ثانياً : – تلتزم الدولة بمحاربة الإرهاب بجميع أشكاله، وتعمل على حماية أراضيها من أن تكون مقراً أو ممراً أو ساحة لنشاطه"

٣ – تنص المادة (٢١/ ثالثا) من دستور جمهورية العراق لسنة ٢٠٠٥ على ما يلي " ثالثاً : – لا يمنح حق اللجوء السياسي إلى المتهم بارتكاب جرائم دولية أو إرهابية، أو كل من الحق ضرراً بالعراق" .

٤ – تنص المادة (٧٣ / اولا) من دستور جمهورية العراق لسنة ٢٠٠٥ على ما يلي "يتولى رئيس الجمهورية الصلاحيات الآتية: أولاً : – إصدار العفو الخاص بتوصية من رئيس مجلس الوزراء، باستثناء ما يتعلق بالحق الخاص، والمحكومين بارتكاب الجرائم الدولية والإرهاب والفساد المالي والإدراي .

٥ – محمد كاظم هادي عنجور المنصوري، مصدر سابق , ص ٥٧٣– ٥٧٤.

وقد أفرز غياب الغطاء التشريعي الموحد واقعاً مؤسسياً يتسم بالتشتت, إذ تفتقد الدولة لمؤسسة تخصصية موحدة للأمن السيبراني، بل توجد أقسام موزعة في دوائر مختلفة تعمل كل منها بمفردها، فعلى سبيل المثال، أنشأت وزارة الداخلية مركزاً للأمن السيبراني يركز على الجريمة الإلكترونية ومكافحة الإرهاب الإلكتروني، بينما أطلق جهاز الأمن الوطني منصة خاصة للأمن السيبراني لحماية الأمن المجتمعي, في حين استحدثت وزارة التعليم العالي أقساماً علمية متخصصة في الجامعات لرفد الدولة بالكوادر, هذا التعدد في المرجعيات الأمنية والتنفيذية، في ظل غياب قانون يحدد التراتبية والاختصاص، يؤدي إلى ضعف التنسيق وغياب الرؤية الموحدة لمواجهة التهديدات[١].

ويرى الباحث أن استمرار الفراغ التشريعي في مجال الأمن السيبراني للمؤسسات الحكومية يعود سببه الرئيس إلى عقدة الارتباط بين الأمن السيبراني وحرية التعبير, فكلما طُرح مشروع قانون لحماية الفضاء الرقمي، تم اختزاله في نصوص عقابية تطال المدونين والمستخدمين، مما يثير حفيظة الرأي العام ويعطل التشريع. والحل يكمن في فك هذا الارتباط، من خلال تشريع قانون حوكمة أمن المعلومات ذي طابع إداري وفني بحت، يُلزم المؤسسات الحكومية (المركزية واللامركزية) بمعايير تحصين الشبكات وحماية البيانات، بعيداً عن النصوص العقابية التي يمكن أن تظل ضمن قانون العقوبات أو قانون خاص بالجرائم الإلكترونية، وذلك لضمان عدم تعطيل حماية المرفق العام الإلكتروني بذريعة الخوف على الحريات.

المبحث الثاني: نطاق المسؤولية الإدارية والجزائية عن الخروقات السيبرانية

إن القاعدة القانونية المستقرة تقضي بتلازم السلطة مع المسؤولية، ولما كانت الإدارة تحتكر سلطة تسيير المرفق العام الرقمي، فإنها تتحمل تبعات أي خلل يمس أمنه, وفي ظل غياب نصوص عقابية حديثة، تبرز أهمية تطويع القواعد الكلاسيكية لتستوعب جرائم العصر الرقمي. وعليه، نُكرس هذا المبحث لبيان نطاق المساءلة، وذلك عبر مطلبين: يركز الأول على المسؤولية الإدارية والانضباطية للموظف والقيادة الإدارية عن خرق البيانات، في حين يُعالج الثاني المسؤولية الجزائية الناشئة عن الإضرار العمدي وغير العمدي بالبنية الرقمية

المطلب الأول: المسؤولية الإدارية والانضباطية عن خرق البيانات.

---

١ – د. ثابت سلطان محمد، المصدر السابق، ص ٤٨.

بالتطبيق على وحدات الإدارة اللامركزية، تنهض المسؤولية الإدارية والانضباطية للمحافظ وموظفي الإدارة المحلية (الكوادر التقنية في المحافظة) عندما يثبت ارتكابهم لمخالفات وظيفية تتعلق بأمن المعلومات وعدم المحافظة على سرية بيانات المواطنين المتاحة لهم عبر "الإدارة الطرفية". ويُعد قانون انضباط موظفي الدولة والقطاع العام رقم (١٤) لسنة ١٩٩١ المعدل الإطار الحاكم لهذه المسؤولية. حيث تضمنت المادة (٤) من هذا القانون النص على ما يلي "يلتزم الموظف بالواجبات الآتية : ... سادساً – المحافظة على اموال الدولة التي في حوزته او تحت تصرفه واستخدامها بصورة رشيدة .سابعاً : كتمان المعلومات والوثائق التي يطلع عليها بحكم وظيفته او اثناءها اذا كانت سرية بطبيعتها او يخشى من افشائها الحاق الضرر بالدولة او بالاشخاص او صدرت اليه اوامر من رؤسائه بكتمانها ويبقى هذا الواجب قائماً حتى بعد انتهاء خدمته، ولا يجوز له ان يحتفظ بوثائق رسمية سرية بعد احالته على التقاعد او انتهاء خدمته بأي وجه كان...."[١]

إن قواعد البيانات التي تتعامل معها المحافظة إلكترونياً تُعد من قبيل المعلومات والوثائق السرية وكذلك أموال الدولة بالمعنى الواسع للمال العام (الأصول الرقمية) فإذا قام الموظف المحلي بإهمال حماية حاسوبه، أو شارك كلمة المرور الخاصة به مما أدى إلى اختراق واجهة النظام الطرفية، فإنه يكون قد أخلّ بواجباته الوظيفية, وبناءً عليه تُفرض عليه إحدى العقوبات الانضباطية المنصوص عليها في المادة (٨) من ذات القانون، والتي تتدرج من (لفت النظر، الإنذار، التوبيخ، قطع الراتب) وتصل إلى (العزل) في حال كانت المخالفة تشكل خطراً جسيماً على مصالح الدولة وأمن بيانات مواطنيها[٢].

---

١ – المادة (٤ / سادسا وسابعا) من قانون انضباط موظفي الدولة والقطاع العام رقم (١٤) لسنة ١٩٩١ المعدل .

٢ – تنص المادة (٨) من قانون انضباط موظفي الدولة والقطاع العام رقم (١٤) لسنة ١٩٩١ المعدل العقوبات التي يجوز فرضها على الموظف هي: اولاً : لفت النظر : ويكون بإشعار الموظف تحريرياً بالمخالفة التي أرتكبها وتوجيهه لتحسين سلوكه الوظيفي ويترتب على هذه العقوبة تأخير الترفيع او الزيادة مدة ثلاثة اشهر. ثانياً : الإنذار : ويكون بإشعار الموظف تحريرياً بالمخالفة التي ارتكبها وتحذيره من الإخلال بواجبات وظيفته مستقبلاً ويترتب على هذه العقوبة تاختر الترفيع او الزيادة مدة ستة اشهر. ثالثاً : قطع الراتب : ويكون بحسم القسط اليومي من راتب الموظف لمدة لا تتجاوز عشرة ايام بأمر تحريري تذكر فيه المخالفة التي ارتكبها الموظف وأستوجبت فرض العقوبة ، ويترتب عليها تأخير الترفيع او الزيادة وفقاً لما يأتي: أ– خمسة اشهر في حالة قطع الراتب لمدة لا تتجاوز خمسة ايام. ب– شهر واحد عن كل يوم من ايام قطع الراتب في حالة تجاوز مدة العقوبة خمسة ايام. رابعاً : التوبيخ : ويكون بإشعار الموظف تحريرياً بالمخالفة التي ارتكبها والأسباب التي جعلت سلوكه غير مرض ويطلب اليه وجوب اجتناب المخالفة وتحسين سلوكه الوظيفي ويترتب على هذه العقوبة تأخير الترفيع او الزيادة مدة سنة واحدة . خامساً : إنقاص الراتب : ويكون بقطع مبلغ

المسؤولية السياسية والإدارية (القصور في التنفيذ والإشراف): تكتسب هذه المسؤولية أهمية بالغة لكونها تتعلق بالمحافظ بصفته الرئيس التنفيذي الأعلى في المحافظة، وتتأسس على فكرة أن التفويض الإداري الواسع يقابله عبء ثقيل في الرقابة والتوجيه, وتتفرع هذه المسؤولية في التعامل مع حوادث خرق البيانات المحلية إلى شقين:

أ- المسؤولية السياسية (المساءلة أمام السلطة التشريعية المحلية): لا تقتصر المساءلة في العمل الإداري على العقوبات الوظيفية، بل ترتقي إلى مستوى المحاسبة السياسية من قبل مجلس المحافظة بصفته السلطة الرقابية, فإذا تعرضت بيانات المحافظة للخرق نتيجة غياب الرؤية الأمنية، أو عدم تخصيص المحافظ لمبالغ كافية من الموازنة المحلية لتطوير أنظمة

من راتب الموظف بنسبة لا تتجاوز (١٠%) من راتبه الشهري لمدة لا تقل عن ستة اشهر ولا تزيد على سنتين ويتم ذلك بأمر تحريري يشعر الموظف بالفعل الذي ارتكبه ويترتب على هذه العقوبة تأخير الترفيع او الزيادة مدة سنتين. سادساً : تنزيل الدرجة : ويكون بأمر تحريري يشعر في الموظف بالفعل الذي ارتكبه ويترتب على هذه العقوبة. أ- بالنسبة للموظف الخاضع لقوانين او انظمة او قواعد او تعليمات خدمة تأخذ بنظام الدرجات المالية والترفيع، تنزيل راتب الموظف الى الحد الأدنى للدرجة التي دون درجته مباشرة مع منحه العلاوات التي نالها في الدرجة المنزل منها (بقياس العلاوة المقررة في الدرجة المنزل اليها) ويعاد الى الراتب الذي كان

يتقاضاه قبل تنزيل درجته بعد قضائه ثلاث سنوات من تاريخ فرض العقوبة مع تدوير المدة المقضية في راتبه الأخير قبل فرض العقوبة. ب- بالنسبة للموظف الخاضع لقوانين او انظمة او قواعد او تعليمات خدمة تأخذ بنظام الزيادة كل سنتين، تخفيض زيادتين من راتب الموظف ويعاد الى الراتب الذي كان يتقاضاه قبل تنزيل درجته بعد قضائه ثلاث سنوات من تاريخ فرض العقوبة مع تدوير المدة المقضية في راتبه الاخير قبل فرض العقوبة. ج- بالنسبة للموظف الخاضع لقوانين او انظمة او قواعد او تعليمات خدمة تاخذ بنظام الزيادة السنوية، تخفيض ثلاث زيادات سنوية من راتب الموظف مع تدوير المدة المقضية في راتبه الاخير قبل فرض العقوبة. سابعاً : الفصل : ويكون بتنحية الموظف عن الوظيفة مدة تحدد بقرار الفصل يتضمن الاسباب التي أستوجبت فرض العقوبة عليه على النحو الآتي: أ- مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات اذا عوقب الموظف باثنتين من العقوبات التالية او باحداها لمرتين وارتكب في المرة الثالثة خلال خمس سنوات من تاريخ فرض العقوبة الاولى فعلا يستوجب معاقبته بإحداها: ١- التوبيخ. ٢- انقاص الراتب. ٣- تنزيل الدرجة .ب- مدة بقائه في السجن اذا حكم عليه بالحبس او السجن عن جريمة غير مخلة بالشرف وذلك إعتباراً من تاريخ صدور الحكم عليه ، وتعتبر مدة موقوفيته من ضمن مدة الفصل ولا تسترد منه انصاف الرواتب المصروفة له خلال مدة سحب اليد. ثامناً : العزل : ويكون بتنحية الموظف عن الوظيفة نهائياً ولا تجوز إعادة توظيفه في دوائر الدولة والقطاع العام ، وذلك بقرار مسبب من الوزير في إحدى الحالات الآتية: أ- اذا ثبت ارتكابه فعلاً خطئاً يجعل بقائه في خدمة الدولة مضراً بالمصلحة العامة. ب- اذا حكم عليه عن جناية ناشئة عن وظيفته او ارتكبها بصفته الرسمية. ج- اذا عوقب بالفصل ثم اعيد توظيفه فارتكب فعلاً يستوجب الفصل مرة اخرى".

الحماية الطرفية، أو تقاعسه عن تنفيذ سياسات الحوكمة الرقمية، فإنه يضع نفسه تحت طائلة الاستجواب والإقالة. و تستند هذه المسؤولية إلى المادة (٧/ ثامناً) من قانون المحافظات رقم (٢١) لسنة ٢٠٠٨ المعدل[١]، التي تمنح مجلس المحافظة حق "استجواب المحافظ" وإصدار قرار بـ "الإقالة" في حال ثبوت (الإهمال الجسيم في أداء الواجب والمسؤولية). وفي سياق الإدارة الرقمية، يُعد التفريط بأمن قواعد البيانات، أو ترك الحواسيب والشبكات المحلية دون حماية وبرامج وتحديثات دورية، صورة تطبيقية حديثة وصريحة لـ "الإهمال الجسيم" الذي يبرر الإطاحة بالمحافظ سياسياً لفقده أهلية إدارة المرفق العام.

ب- المسؤولية الإدارية عن الإخلال بواجب (الإشراف والتفتيش): تنهض هذه المسؤولية عندما يُخل المحافظ بواجباته كقائد إداري، بمعزل عن المساءلة السياسية للمجلس. فحدوث خرق في الأجهزة الطرفية (الموجودة داخل الدوائر) يُعد دليلاً على وجود فوضى إدارية أو ضعف في الرقابة الداخلية. أذ يمارس المحافظ بموجب المادة (٣١/ رابعاً) من قانون المحافظات غير المنتظمة في اقليم ، صلاحية (الإشراف على سير العمل في الدوائر المرتبطة

---

١ – تنص المادة (٧/ ثامناً) من قانون المحافظات رقم (٢١) لسنة ٢٠٠٨ المعدل على ما يلي "يختص مجلس المحافظة بما يلي :..... ثامنا: ١- استجواب المحافظ أو احد نائبيه بناءا على طلب ثلث اعضائه وعند عدم قناعة الأغلبية البسيطة بأجوبة المستجوب يعرض للتصويت على الإقالة في جلسة ثانية ويعتبر مقالا بموافقة الأغلبية المطلقة لعدد أعضاء المجلس ويكون طلب الإقالة أو التوصية بها مستندا على احد الأسباب الحصرية الآتية : أ – عدم النزاهة أو استغلال المنصب الوظيفي. ب – التسبب في هدر المال العام. ج – فقدان احد شروط العضوية. د – الإهمال أو التقصير المتعمدين في أداء الواجب والمسؤولية. ٢- لمجلس النواب إقالة المحافظ بالأغلبية المطلقة بناءاً على اقتراح رئيس الوزراء لنفس الأسباب المذكورة أعلاه . ٣- يعد المحافظ مقالاً عند فقدانه لأحد الشروط المنصوص عليها في المادة (٥) من هذا القانون . ٤- للمحافظ أن يعترض على قرار الإقالة , أمام المحكمة الاتحادية العليا خلال خمسة عشر يوماً من تاريخ تبليغه بالقرار وعلى المحكمة أن تبت في الاعتراض خلال شهر من تاريخ تسجيله وعليه في هذه الحالة أن يقوم بتصريف أعمال المحافظة اليومية لحين البت في الاعتراض. ٥ – يقوم مجلس المحافظة بعد نهاية مدة الطعن المشار إليها في الفقرة (٤) أعلاه أو تصديق قرار الإقالة من قبل المحكمة الاتحادية العليا في حالة وقوع اعتراض عليه بانتخاب محافظ جديد وفقاً لأحكام البند (٧) من هذه المادة خلال مدة أقصاها ثلاثين يوماً من تاريخ التصديق أو انتهاء مدة الطعن."

بالمحافظة وتفتيشها)[١]. إن واجب "الإشراف والتفتيش" لا يقتصر على متابعة الدوام الرسمي أو الإجراءات الورقية، بل يمتد حتماً ليشمل الرقابة الصارمة على "بيئة العمل الرقمية فإذا ثبت أن خرق البيانات حدث بسبب عدم تفعيل المحافظ لدوائر الرقابة التقنية، أو عدم متابعته لالتزام الموظفين بضوابط أمن المعلومات، فإنه يُعد مقصراً إدارياً. هذا القصور في السيطرة على النهايات الطرفية للشبكة المحلية يجعله مسؤولاً عن الفراغ الإداري الذي هيأ بيئة خصبة للاختراق، حتى وإن لم يقم بتسريب البيانات بشخصه.

المطلب الثاني: المسؤولية الجزائية عن الإضرار العمدي وغير العمدي بالبنية الرقمية.

لا تقف حماية البيانات عند حدود العقاب الإداري، بل تتعداه إلى المساءلة الجنائية إذا ارتقت المخالفة إلى مصاف الجريمة, وفي هذا السياق، يُعد قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩ المعدل المرجعية الأساسية لتكييف جرائم تسريب البيانات الرقمية والإضرار بها ووفقا لما يلي:

أ- جريمة إفشاء الأسرار الوظيفية: تضمنت المادة (٣٢٧) من قانون العقوبات العراقي النص على ما يلي: "يعاقب بالحبس مدة لا تزيد على ثلاث سنوات وبالغرامة التي لا تزيد على ثلثمائة دينار او باحدى هاتين العقوبتين كل موظف او مكلف بخدمة عامة افشى امرا وصل الى علمه بمقتضى وظيفته لشخص يعلم وجوب عدم اخباره به. وتكون العقوبة السجن اذا كان من شأن هذا الافشاء ان يضر بمصلحة الدولة.[٢]".

ينطبق هذا النص بشكل مباشر على موظفي المحافظة الذين يمتلكون حق الوصول إلى بيانات المواطنين الرقمية فإذا قام الموظف باستغلال صلاحيته الطرفية لسحب بيانات مواطنين وتسريبها أو بيعها لجهات خارجية، فإنه يُسأل جزائياً عن جريمة إفشاء الأسرار الوظيفية، وتطال هذه المسؤولية المحافظ كفاعل أصلي أو شريك إذا ثبت تواطؤه أو إصداره أوامر غير قانونية بهذا الشأن.

ب-جريمة الإضرار العمدي وغير العمدي بأموال الدولة: كما عالج المشرع حالات إحداث الضرر المادي أو المعنوي بالبنية الرقمية، حيث نصت المادة (٣٤٠) على ما يلي:"يعاقب

---

١ – تنص المادة (٣١ / رابعا) من قانون المحافظات غير المنتظمة في اقليم رقم ٢١ لسنة ٢٠٠٨ المعدل على ما يلي "يمارس المحافظ الصلاحيات الآتية :..... رابعا : الإشراف على سير المرافق العامة في المحافظة وتفتيشها ما عدا المحاكم والوحدات العسكرية والجامعات والكليات والمعاهد ....."

٢ – المادة (٣٢٧) من قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩ المعدل.

بالسجن مدة لا تزيد على سبع سنوات او بالحبس كل موظف او مكلف بخدمة عامة احدث عمدا ضررا باموال او مصالح الجهة التي يعمل فيها او يتصل بها بحكم وظيفته او باموال الاشخاص المعهود بها اليه[١]".

كما تضمنت المادة ٣٤١ على ما يلي "يعاقب بالحبس مدة لا تزيد على ثلاث سنوات او بغرامة لا تزيد على ثلثمائة دينار كل موظف او مكلف بخدمة عامة تسبب بخطئه الجسيم في الحاق ضرر جسيم باموال او مصالح الجهة التي يعمل بها او يتصل بها بحكم وظيفته او باموال او مصالح الاشخاص المعهود اليه ان كان ذلك ناشئا عن اهمال جسيم باداء وظيفته او عن اساءة استعمال السلطة او عن اخلال جسيم بواجبات وظيفته[٢]".

ولغرض التكييف القانوني السليم للسلوك الوظيفي في البيئة الرقمية، يرى الباحث ضرورة إعادة تفسير مفهومي (الخطأ الجسيم) و (الإهمال الجسيم) الواردين في نص المادة (٣٤١) من قانون العقوبات العراقي بما ينسجم مع طبيعة العمل الإداري في ظل الحوكمة الإلكترونية. فهذه المفاهيم القانونية صيغت في الأصل في إطار الإدارة التقليدية التي كانت تعتمد على الوثائق الورقية والموجودات المادية، الأمر الذي جعل صور الإهمال المرتبطة بها تدور غالباً حول الإخلال بحفظ الأموال أو الوثائق أو الممتلكات العامة.

ففي الإدارة التقليدية، قد يُعد من قبيل الإهمال الجسيم ترك أبواب الدائرة مفتوحة، أو الإخلال بواجب حفظ السجلات والوثائق الرسمية، أو التفريط في الأموال العامة. غير أن التحول نحو الإدارة الرقمية يفرض إعادة قراءة هذه المفاهيم في ضوء الواقع التقني الجديد الذي أصبحت فيه البيانات الرقمية والأنظمة المعلوماتية تمثل جزءاً أساسياً من موجودات المرفق العام. فالمرفق الإداري الحديث لا يقوم فقط على المبنى والملفات الورقية، بل يعتمد بصورة متزايدة على الخوادم وقواعد البيانات والمنصات الرقمية التي تحتوي على معلومات حساسة تتعلق بالمواطنين والمؤسسات.

وعليه، فإن صور الإهمال الجسيم في البيئة الرقمية ينبغي أن تُفهم على نحو يتلاءم مع طبيعة المخاطر المرتبطة بإدارة الأنظمة المعلوماتية. فمثلاً، إن تقاعس الموظف المختص أو المسؤول الإداري عن تحديث برامج الحماية الإلكترونية, أو إهماله في تطبيق إجراءات الأمن السيبراني المعتمدة، أو استخدام كلمات مرور ضعيفة أو مشاركتها مع الآخرين، أو ترك الأنظمة الرقمية دون إجراءات حماية كافية، قد يؤدي إلى اختراق الأنظمة الحكومية أو تسريب بيانات المواطنين. وهذه الأفعال، وإن كانت

---

١ – المادة (٣٤٠) من قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩ المعدل.

٢ – المادة (٣٤١) من قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩ المعدل.

تبدو للوهلة الأولى أخطاء تقنية بسيطة، إلا أنها في حقيقتها قد تشكل إهمالاً جسيماً متى ما ترتب عليها ضرر جسيم يمس أمن المعلومات أو حقوق الأفراد.

ومن ثم يرى الباحث أن هذه الممارسات تمثل تطبيقاً معاصراً وصريحاً لمفهوم الإهمال الجسيم الوارد في المادة (٣٤١) من قانون العقوبات العراقي، لأن الموظف العام يكون في هذه الحالة قد أخل إخلالاً واضحاً بواجبات الحيطة والحذر التي تفرضها طبيعة وظيفته، ولا سيما عندما يتعلق الأمر بحماية البيانات الحكومية أو البنية التحتية الرقمية للمرفق العام. وبناءً على ذلك، فإن ثبوت مثل هذا الإهمال إذا أدى إلى اختراق الأنظمة المعلوماتية أو تسريب بيانات المواطنين يوجب مساءلة الموظف جنائياً وفقاً لأحكام القانون، باعتبار أن البيانات الرقمية أصبحت اليوم جزءاً من المال العام أو من المصالح التي يلتزم الموظف بحمايتها وصيانتها.

تُشكل هاتان المادتان ركيزة أساسية في معالجة الإخفاقات التقنية للإدارة العامة، فإذا أهملت الإدارة (سواء كانت مركزية أو لامركزية) تطبيق معايير الأمان المتاحة لها (مثل ترك الحواسيب الطرفية مفتوحة للعموم، أو عدم استخدام برامج الحماية من الفيروسات على الأجهزة)، مما أدى إلى دخول فيروس دمر بيانات الدائرة، فإن الموظف التقني أو الإداري المقصر يُسأل وفق المادة ٣٤١ لارتكابه خطأ جسيماً ناتجاً عن إهمال ومخالفة للأنظمة. وبالمقابل، إذا كان الضرر الجسيم ناتجاً عن سقوط الخوادم المركزية أو ضعف بروتوكولات التشفير الوطنية، فإن المسؤولية الجزائية وفق هاتين المادتين تنتقل لتطال الموظفين والقيادات في الجهة المجهزة للنظام، وتُعفى الإدارة المُشغلة لكون الخلل قد وقع خارج نطاق سيطرتها الفنية.

الخاتمة

بتوفيق من الباري عز وجل اتممنا البحث بموضوع (المسؤولية الإدارية والجزائية عن الإخلال بالأمن السيبراني للمرفق العام الرقمي – دراسة تحليلية في ضوء التشريع العراقي) وقد توصلنا الى جملة من النتائج والتوصيات نبينها في الاتي :

أولاً: الاستنتاجات

١– – يشكل الأمن السيبراني ركناً أساسياً في ضمان استمرارية عمل المرفق العام الرقمي وحماية بياناته

٢– يفتقر التشريع العراقي إلى تنظيم متكامل وواضح للمسؤولية القانونية الناشئة عن الإخلال بالأمن السيبراني.

٣– تتسم المسؤولية الإدارية بالاتساع لتشمل الموظف والجهة الإدارية عند الإهمال أو التقصير في حماية الأنظمة.

٤– تقوم المسؤولية الجزائية عند توافر أركان الجريمة السيبرانية، سواء بفعل عمدي أو إهمال جسيم.

٥– يوجد تداخل بين المسؤوليتين الإدارية والجزائية، مع غياب معايير دقيقة للفصل بينهما.

٦– تعاني المنظومة القانونية من ضعف في الإجراءات الوقائية والرقابية المتعلقة بالأمن السيبراني.

٧– غياب قانون وطني مستقل لحماية البيانات الشخصية والأمن السيبراني المؤسسي يُعد إغفالاً تشريعياً خطيراً، وأن الاعتماد على القواعد المدنية أو العقابية التقليدية لم يعد كافياً لردع الانتهاكات الرقمية أو تحديد المسؤولية التقصيرية بدقة.

٨– البيانات الرقمية والأنظمة المعلوماتية أصبحت جزءاً لا يتجزأ من "المال العام"، وأن تقاعس الموظف أو الإدارة عن تحديث برامج الحماية أو مشاركة كلمات المرور يمثل تطبيقاً معاصراً للإهمال الجسيم الوارد في المادة (٣٤١) من قانون العقوبات العراقي.

ثانياً: التوصيات

١ –ضرورة سن تشريع عراقي خاص بالأمن السيبراني ينظم المسؤولية الإدارية والجزائية بشكل واضح.

٢ –تحديث القوانين القائمة (العقوبات، انضباط موظفي الدولة) بما يتلاءم مع الجرائم السيبرانية.

٣ –وضع معايير قانونية دقيقة لتحديد حالات الإهمال والتقصير في المجال السيبراني.

٤ –تعزيز الرقابة الإدارية وتفعيل أنظمة التدقيق الأمني داخل المؤسسات الحكومية.

٥ –تدريب الموظفين على إجراءات الأمن السيبراني ورفع مستوى الوعي القانوني والتقني.

٦ –إنشاء جهة وطنية مختصة بالإشراف على الأمن السيبراني في المرافق العامة.

٧ –الاستفادة من التجارب الدولية في تطوير الإطار التشريعي والتنظيمي.

٨ –نوصي المشرع العراقي بفك الارتباط بين مشاريع جرائم المعلوماتية (التي تستهدف الأفراد) وبين الحاجة الملحة لتشريع قانون حوكمة أمن المعلومات المؤسسي ذي الطابع الإداري والوقائي، والذي يُلزم دوائر الدولة بتحصين شبكاتها كالتزام وظيفي صارم.

٩–ندعو إلى تعديل (قانون انضباط موظفي الدولة والقطاع العام رقم ١٤ لسنة ١٩٩١ المعدل) بإدراج نصوص صريحة تُكيّف (الإهمال السيبراني المؤسسي) كمخالفة وظيفية جسيمة تستوجب عقوبات رادعة تطال الموظف المباشر والقيادات الإدارية المشرفة عليه على حد سواء.

قائمة المصادر والمراجع

أولاً: البحوث والمجلات العلمية

١– إخلاص مخلص إبراهيم، وزياد طارق جاسم، المسؤولية التقصيرية عن التعامل بالبيانات الشخصية في الوسط الرقمي، وقائع المؤتمر العلمي الدولي التاسع للقضايا القانونية(ILIC9) ، جامعة تيشك الدولية، ٢٠٢٤.

٢– د. أسامة عبد الواحد التهامي، نطاق الحماية القانونية للبيانات الشخصية والمسؤولية التقصيرية عن معالجتها – دراسة في القانون الإماراتي، مجلة البحوث القانونية والاقتصادية، كلية الحقوق جامعة المنصورة، العدد (٦٧)، ٢٠١٨.

٣– د. ثابت سلطان محمد، تعزيز استراتيجيات الأمن السيبراني في العراق والدول العربية وموائمتها مع أهداف التنمية المستدامة، المجلة العراقية للعلوم الاقتصادية، عدد خاص، ٢٠٢٥.

٤– سامر محي عبد الحمزة، السياسة التشريعية العراقية لحماية الأمن السيبراني الوطني – دراسة في ضوء مبادئ القانون الدولي العام، مجلة لارك للفلسفة واللسانيات والعلوم الاجتماعية، جامعة واسط، المجلد (٣)، العدد (٤٦)، ٢٠٢٢.

٥– سجاد صبار رزاق الحمدان، وإلهام حيدري، الإطار القانوني لحماية الأمن السيبراني في العراق – دراسة تحليلية في ضوء التشريعات الوطنية والمعايير الدولية، مجلة دراسات البصرة، العدد (٦٢)، ٢٠١٥.

٦– شميم مزهر راضي، الحق في حماية البيانات الشخصية في ظل دستور جمهورية العراق لسنة ٢٠٠٥، مجلة جامعة الإمام جعفر الصادق (ع) للدراسات القانونية، العدد الرابع، ٢٠٢٢.

٧- محمد كاظم هادي عنجور المنصوري، الواقع التشريعي للأمن السيبراني في العراق – التحديات والطموحات، مجلة العلوم الإنسانية والطبيعية، المجلد (٦)، العدد (٨)، ٢٠٢٥.

٨- ملاك عواد إسماعيل صوالحه، الجوانب القانونية لحماية خصوصية البيانات الشخصية في العصر الرقمي، مجلة القانون الدستوري والعلوم الإدارية، ألمانيا، العدد (٢٩)، ٢٠٢٥.

ثانياً: الدساتير والقوانين

١- دستور جمهورية العراق لسنة ٢٠٠٥.

٢- القانون المدني العراقي رقم (٤٠) لسنة ١٩٥١ المعدل.

٣- قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩ المعدل.

٤- قانون انضباط موظفي الدولة والقطاع العام رقم (١٤) لسنة ١٩٩١ المعدل.

٥- قانون المحافظات غير المنتظمة في إقليم رقم (٢١) لسنة ٢٠٠٨ المعدل.