# التحديات في تطبيق قوانين حماية البيانات الشخصية في الإدارات العامة

## (دراسة مقارنة بين العراق ومصر)

**Faculty of Law-Department of Public Law, University Of Qom , Islamic Republic of Iran**

**صفاء عبد الحسين كاظم العنكوشي**

**طالب، دكتوراه، قانون عام، كلية القانون، جامعة قم الحكومية، الجمهورية الأسلامية إيران**

**safaaalankushe4@gmail.com**

**مهدي رجائي**

**Asst. Prof. Dr. Mahdi Rajaei**

**استاذ المساعد فى كلية القانون، قسم القانون العام، جامعة قم، الجمهورية الاسلامية الإيرانية**

**M.rajaei@qom.ac.ir**

**١٤٤٧هـ ٢٠٢٥م**

## الملخص

تهدف هذه الدراسة إلى تحليل أبرز التحديات التي تواجه تطبيق قوانين حماية البيانات الشخصية في الإدارات العامة، من خلال دراسة مقارنة بين التشريعين العراقي والمصري. فقد أضحى موضوع حماية البيانات الشخصية من القضايا القانونية المعاصرة ذات الأهمية البالغة، لاسيما في ظل التحول الرقمي المتسارع الذي تشهده الإدارات العامة، وما يرافقه من توسع في جمع ومعالجة وتخزين البيانات الشخصية للأفراد.وتنطلق الدراسة من إشكالية رئيسة تتمثل في مدى كفاية الأطر القانونية والتنظيمية القائمة في كل من العراق ومصر لضمان حماية فعّالة للبيانات الشخصية داخل الإدارات العامة، ومدى قدرة هذه الأطر على مواكبة التطورات التقنية المتسارعة. وتعتمد الدراسة المنهج المقارن من خلال تحليل النصوص القانونية ذات الصلة، وبيان أوجه القصور والاختلاف في التنظيم القانوني لحماية البيانات الشخصية في البلدين.وتبين الدراسة أن العراق يعاني من غياب تشريع متكامل خاص بحماية البيانات الشخصية، الأمر الذي أدى إلى تشتت القواعد القانونية وضعف الآليات الرقابية والتنفيذية، في حين خطت مصر خطوة متقدمة بإصدار قانون حماية البيانات الشخصية رقم (١٥١) لسنة ٢٠٢٠، إلا أن تطبيقه في الإدارات العامة ما زال يواجه تحديات قانونية وإدارية وتقنية، من أبرزها تعدد الاستثناءات وضعف التنسيق المؤسسي.كما توصلت الدراسة إلى أن نقص البنية التحتية التكنولوجية، وتزايد الهجمات الإلكترونية، وضعف الوعي القانوني والثقافة المؤسسية، تمثل عوامل مشتركة تعيق التطبيق الفعّال لقوانين حماية البيانات الشخصية في الإدارات العامة. وتختتم الدراسة بالتأكيد على ضرورة تطوير التشريعات، وتعزيز التنسيق المؤسسي، وبناء القدرات التقنية والبشرية لضمان حماية فعّالة للبيانات الشخصية في كل من العراق ومصر.


**الكلمات المفتاحية:**حماية البيانات الشخصية، الإدارات العامة، القانون العراقي، القانون المصري، التحول الرقمي، الأمن السيبراني.

## Abstract

This study aims to analyze the main challenges facing the implementation of personal data protection laws in public administrations through a comparative examination of the Iraqi and Egyptian legal frameworks. Personal data protection has become one of the most significant contemporary legal issues, particularly in light of the rapid digital transformation witnessed by public administrations, which has been accompanied by an expansion in the collection, processing, and storage of individuals' personal data.The study is based on a central research problem concerning the adequacy of the existing legal and regulatory frameworks in both Iraq and Egypt to ensure effective protection of personal data within public administrations, as well as their ability to keep pace with rapid technological developments. To this end, the study adopts a comparative methodology by analyzing the relevant legal texts and identifying shortcomings and differences in the legal regulation of personal data protection in the two countries.The study demonstrates that Iraq suffers from the absence of a comprehensive, dedicated personal data protection law, leading to fragmented legal rules and weak supervisory and enforcement mechanisms. In contrast, Egypt has taken a more advanced step by enacting the Personal Data Protection Law No. (151) of 2020; however, its implementation within public administrations continues to face legal, administrative, and technical challenges, most notably the multiplicity of exceptions and weak institutional coordination.Furthermore, the study concludes that inadequate technological infrastructure, the increase in cyberattacks, and the lack of legal awareness and institutional culture constitute common factors that hinder the effective implementation of personal data protection laws in public administrations. The study concludes by emphasizing the need to develop legislation, strengthen institutional coordination, and build technical and human capacities to ensure effective protection of personal data in both Iraq and Egypt.


Keywords:personal data protection, public administrations, Iraqi law, Egyptian law, digital transformation, cybersecurity.

## المقدمة

شهد العالم خلال العقود الأخيرة تحولات كبيرة في المجالات التقنية والإدارية، مما أدى إلى ظهور تحديات جديدة تتعلق بحماية البيانات الشخصية للأفراد داخل المؤسسات والإدارات العامة. فقد أصبح الاعتماد على النظم الإلكترونية وأنظمة المعلومات في معالجة البيانات الشخصية سمة أساسية للإدارة الحديثة، وهو ما رفع من أهمية وجود أطر قانونية وإدارية فعالة تضمن حماية هذه البيانات من الوصول غير المشروع أو الاستخدام السيئ. وتتفاقم هذه التحديات في الدول النامية، بما في ذلك العراق ومصر، حيث تتقاطع القوانين التقليدية مع متطلبات العصر الرقمي، ويظهر بوضوح التباين في مستوى النضج التشريعي والتنظيمي بين البلدين.

تعد حماية البيانات الشخصية أحد الركائز الأساسية لحماية حقوق الأفراد، إذ ترتبط ارتباطاً وثيقاً بالحق في الخصوصية والحق في الأمان المعلوماتي، فضلاً عن كونها عامل تمكين مهم للمواطنين في التعامل مع المؤسسات الحكومية والخاصة. ومن هذا المنطلق، ظهرت الحاجة إلى تطوير تشريعات متكاملة ووضع سياسات واضحة تضمن حماية البيانات الشخصية، سواء من خلال القوانين الوطنية أو اللوائح التنفيذية والتوجيهات المؤسسية. كما أن الإدارة الفعالة لهذه القوانين تتطلب توافر بنية تحتية تقنية متقدمة، إلى جانب وجود قدر كافٍ من التوعية القانونية والثقافية بين موظفي الإدارات العامة.

في العراق، تعاني الإدارات العامة من غياب تشريع شامل ينظم حماية البيانات الشخصية، إذ تقتصر القوانين القائمة على نصوص متفرقة ومجزأة في قوانين العقوبات، والاتصالات، أو قوانين حماية المعلومات، وهو ما يؤدي إلى ضعف التنسيق بين الجهات الحكومية وتشتت المسؤوليات الرقابية والتنفيذية. بالمقابل، شهدت مصر تقدماً ملحوظاً بإصدار قانون حماية البيانات الشخصية رقم (١٥١) لسنة ٢٠٢٠، والذي يعد خطوة مهمة نحو تنظيم عمليات جمع ومعالجة البيانات الشخصية داخل الإدارات العامة. ومع ذلك، لا يزال تطبيق هذا القانون يواجه تحديات عملية عدة، أبرزها ضعف التنسيق بين الجهات الحكومية، وقلة الوعي بين الموظفين، وانتشار الممارسات غير الآمنة في التعامل مع البيانات الرقمية.

**بيان المشكلة**

تعد حماية البيانات الشخصية من القضايا القانونية والإدارية المعاصرة التي تواجه الإدارات العامة في جميع دول العالم، لما لها من أثر مباشر على حقوق الأفراد وحرياتهم الأساسية، خصوصاً الحق في الخصوصية والأمان المعلوماتي. ومع التوسع في استخدام النظم الإلكترونية لجمع ومعالجة وتخزين البيانات، أصبحت الحاجة إلى وجود أطر قانونية وإدارية فعالة لضمان حماية هذه البيانات ضرورة ملحة، لاسيما في البلدان النامية التي ما زالت تشهد تحديات متعددة في مجال التنظيم الرقابي والتقني.

وتنبع مشكلة الدراسة من الملاحظات التالية:أولاً، ضعف التشريعات المتكاملة في بعض الدول مثل العراق، حيث يفتقر القانون العراقي إلى نصوص شاملة تحمي البيانات الشخصية، مما يؤدي إلى تشتت القواعد القانونية وتباين الإجراءات بين المؤسسات الحكومية. ثانياً، على الرغم من صدور قانون حماية البيانات الشخصية في مصر، إلا أن التطبيق العملي للقانون في الإدارات العامة ما زال يواجه تحديات عملية وتنظيمية وتقنية، تشمل ضعف التنسيق بين الجهات الحكومية، ونقص البنية التحتية الرقمية، وانتشار الممارسات غير الآمنة في التعامل مع البيانات. ثالثاً، يشكل الجانب الثقافي والتعليمي حاجزاً أمام التنفيذ الفعّال للقوانين، إذ يؤدي نقص الوعي القانوني والتقني بين موظفي الإدارات العامة إلى ضعف الالتزام بالمعايير المطلوبة، ومقاومة التغيير المؤسسي، مما يحد من فعالية أي تشريع موجود.

**أهمية البحث**

تكمن أهمية هذا البحث في كونه يعالج قضية حيوية تتعلق بحقوق الأفراد وحماية بياناتهم الشخصية في ظل التحول الرقمي المتسارع الذي تشهده الإدارات العامة. إذ يمثل فهم التحديات القانونية والإدارية والتقنية والثقافية في تطبيق قوانين حماية البيانات الشخصية خطوة أساسية لضمان حماية فعّالة للبيانات، والحد من الانتهاكات أو سوء الاستخدام.

وتزداد أهمية البحث عند النظر إلى السياق المقارن بين العراق ومصر، حيث يتيح المقارنة بين تجربتين مختلفتين في مستوى النضج التشريعي والتنفيذي، مما يوفر قاعدة معرفية لتحديد أوجه

القصور والفجوات في القوانين والإجراءات الحالية، ويساعد في استنباط الحلول العملية والتشريعية الملائمة. كما أن البحث يعزز الوعي بأهمية بناء بنية تحتية تقنية متطورة، وتطوير القدرات البشرية والتدريب المستمر للموظفين، بما يرفع من مستوى الالتزام بالقوانين ويحد من المخاطر المرتبطة بالمعالجة غير الآمنة للبيانات الشخصية.

**أهداف البحث**

يهدف البحث إلى تحقيق مجموعة من الأهداف العلمية والعملية، أهمها:

١. تحليل التحديات القانونية والإدارية التي تواجه تطبيق قوانين حماية البيانات الشخصية في الإدارات العامة في العراق ومصر.

٢. تحديد الفجوات والتقصير في التشريعات والإجراءات التنظيمية في كلا البلدين، مقارنةً بالتجارب الدولية والمعايير المعاصرة لحماية البيانات الشخصية.

٣. دراسة التحديات التقنية والتكنولوجية المتعلقة بالبنية التحتية الرقمية، وأنظمة الأمان السيبراني، وتأثيرها على حماية البيانات الشخصية في الإدارات العامة.

**منهجية البحث**

يعتمد هذا البحث على المنهج المقارن كأداة رئيسية لدراسة التحديات التي تواجه تطبيق قوانين حماية البيانات الشخصية في الإدارات العامة في العراق ومصر، من خلال تحليل النصوص القانونية، واللوائح، والتشريعات ذات الصلة، إضافة إلى استعراض الدراسات السابقة والمصادر الأكاديمية الرسمية. ويتيح المنهج المقارن تحديد أوجه التشابه والاختلاف بين التشريعين العراقي والمصري، واستخلاص الدروس المستفادة من التجربة القانونية والإدارية لكل منهما، بما يسهم في تقديم رؤية شاملة حول المشكلات القائمة وسبل معالجتها.

## المبحث الأول:التحديات القانونية والإدارية

### المطلب الأول:نقص التشريعات المتكاملة

#### الفرع الأول:غياب قوانين شاملة لحماية البيانات الشخصية في العراق

يُعدّ غياب التشريعات الشاملة أحد أبرز المعوقات التي تعترض طريق بناء منظومة فعالة لحماية البيانات الشخصية في العراق، لا سيما ضمن الإدارات العامة التي تتعامل يومياً مع بيانات حساسة تتعلق بالمواطنين والمقيمين. وعلى الرغم من الاعتراف الدستوري الصريح بحق الخصوصية، فإن هذا الحق لم يُترجم حتى الآن إلى منظومة تشريعية متكاملة قادرة على تحقيق الحماية الفعلية لهذا الحق.

**أولاً:الواقع التشريعي الحالي في العراق**

لا يوجد حتى تاريخ إعداد هذه الدراسة قانون نافذ مستقل ومتكامل لحماية البيانات الشخصية في العراق، وهو ما يترك فراغاً تشريعياً خطيراً في ظل التوسع الرقمي والإداري الذي تشهده مؤسسات الدولة. وتقتصر الإشارات القانونية ذات الصلة على نصوص متفرقة ضمن قوانين عامة، مثل:

- **دستور العراق لسنة ٢٠٠٥**، حيث تنص المادة (١٧/أولاً) على أن:"لكل فرد الحق في الخصوصية الشخصية بما لا يتنافى مع حقوق الآخرين والآداب العامة ".[١]، إلا أن هذه المادة لا تقترن بأي نص تنفيذي يوضح آليات الحماية أو الجزاء.

- **قانون تنظيم الخدمات الإلكترونية رقم ٧٨ لسنة ٢٠١٢**، والذي أورد إشارات عامة بشأن أمن البيانات، دون تخصيص أو تفصيل لحماية البيانات الشخصية[٢].

- **مشروع قانون الجرائم المعلوماتية**، الذي ما يزال في مرحلة الإقرار ولم يُفعّل حتى الآن، ويركز بشكل أكبر على الجريمة الإلكترونية دون التطرق إلى حقوق الأفراد في بياناتهم[٣].

---

(١) دستور جمهورية العراق لسنة ٢٠٠٥، المادة (١٧)، متاح على موقع مجلس النواب العراقي.

(٢) قانون تنظيم الخدمات الإلكترونية رقم ٧٨ لسنة ٢٠١٢، منشور في الوقائع العراقية، العدد ٤٢٥٥.

(٣) مسودة قانون الجرائم المعلوماتية، لجنة الأمن والدفاع البرلمانية، ٢٠١٩، غير منشورة رسمياً.

ثانياً:غياب المبادئ الأساسية لحماية البيانات

تفتقر المنظومة القانونية العراقية إلى تبني المبادئ الأساسية المعترف بها دوليًا في حماية البيانات الشخصية، مثل:

- **مبدأ الموافقة الحرة والمسبقة.**
- **مبدأ الغرض المحدد من جمع البيانات.**
- **مبدأ الحد الأدنى من البيانات.**
- **مبدأ الاحتفاظ المحدود.**
- **حق الفرد في الوصول إلى بياناته وتصحيحها أو حذفها.**

إن عدم تضمين هذه المبادئ يجعل من الصعب على الإدارات العامة وضع سياسات داخلية تحترم الحقوق الرقمية للمواطنين. وحتى في حال تبني بعض هذه المبادئ في تعليمات إدارية، فإنها تفتقر إلى القوة الإلزامية.

## الفرع الثاني:القيود القانونية والتنظيمية في التشريع المصري

على الرغم من أن مصر تُعد من أوائل الدول العربية التي سنت قانونًا مستقلاً لحماية البيانات الشخصية، وهو القانون رقم ١٥١ لسنة ٢٠٢٠، إلا أن هذا القانون لا يزال يواجه عددًا من **القيود القانونية** التي تحول دون تحقيق الحماية المتكاملة للبيانات، وخصوصًا في الإدارات العامة. فالطبيعة التنظيمية للقانون، وبعض الثغرات في أحكامه، إلى جانب تقييده في بعض الحالات لصالح اعتبارات الأمن القومي، تُعد من أبرز التحديات التي تقلل من فعاليته.

**أولاً:الإطار القانوني العام**

صدر القانون رقم ١٥١ لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية في مصر، ونُشر بالجريدة الرسمية في ١٥ أغسطس ٢٠٢٠. وقد جاء هذا القانون في إطار سعي الدولة لتنظيم بيئة البيانات المتزايدة، خاصة مع اتساع استخدام الخدمات الرقمية في الإدارات العامة والقطاع

الخاص[١]. وينص القانون في مادته الثانية على حظر جمع أو معالجة أو الإفصاح عن البيانات الشخصية إلا بموافقة صريحة من صاحب البيانات، كما يُلزم المسؤول عن المعالجة باتخاذ الإجراءات الفنية والتنظيمية اللازمة لحمايتها[٢].

**ثانيًا:القيود المتعلقة باستثناءات الجهات السيادية**

من أبرز القيود التي تؤثر على فعالية قانون حماية البيانات المصري، **الاستثناء الواسع الممنوح للجهات السيادية** .فقد نصت المادة الثالثة على أن "لا تسري أحكام هذا القانون على البيانات الشخصية التي تتم معالجتها حصريًا للأغراض الأمنية من قبل جهات الأمن القومي"، دون أن يحدد القانون المقصود بمصطلح "الأمن القومي" أو يضع ضوابط قانونية موضوعية لهذا الاستثناء[٣].

هذا الغموض يفتح الباب أمام تأويل واسع من قبل الجهات الحكومية، ويُضعف من ضمانات الحماية، لا سيما في الإدارات العامة المرتبطة بتقديم خدمات عامة تتطلب بيانات حساسة، مثل الصحة والتعليم والضمان الاجتماعي.

## المطلب الثاني:ضعف التنسيق بين الجهات الحكومية

### الفرع الأول: التنسيق بين الوزارات والمؤسسات الحكومية

تُعتبر قضية التنسيق بين الوزارات والمؤسسات الحكومية من التحديات الجوهرية التي تؤثر على فعالية تطبيق قوانين حماية البيانات الشخصية، خصوصاً في بيئة معقدة ومتعددة الجهات كالتي يشهدها العراق ومصر. إذ تعتمد حماية البيانات بشكل رئيسي على توحيد السياسات وتكامل الإجراءات بين مختلف الجهات التي تجمع وتعالج وتبادل البيانات، وهو ما يتطلب آليات واضحة للتنسيق المؤسسي والتشريعي.

---

(١) القانون رقم ١٥١ لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية، الجريدة الرسمية، العدد ٣٢ مكرر (د)، بتاريخ ١٥ أغسطس ٢٠٢٠.

(٢) المرجع نفسه، المادة (٢)

(٣) المرجع نفسه، المادة (٣)

**أولاً:أهمية التنسيق في حماية البيانات الشخصية**

تعتمد حماية البيانات الشخصية على تعاون وثيق بين الجهات الحكومية التي تدير قواعد بيانات مختلفة ومتنوعة، كالسجل المدني، الصحة، التعليم، الأمن، والمالية. هذا التنسيق يحقق:

- **توحيد معايير حماية البيانات** بما يمنع التشتت والازدواجية في تطبيق الإجراءات.
- **مشاركة الموارد الفنية والبشرية** مما يزيد من كفاءة الحماية.
- **تسهيل تبادل البيانات** بطريقة آمنة ووفقاً للضوابط القانونية.
- **تعزيز الشفافية والمساءلة** عبر آليات رقابية مشتركة.

وبدون تنسيق فعّال، تصبح جهود حماية البيانات متفرقة وغير متجانسة، مما يزيد من احتمالات تسرب البيانات أو سوء استخدامها.

ثانياً:واقع التنسيق بين الوزارات في العراق

في العراق، يشكل ضعف التنسيق بين الوزارات والمؤسسات الحكومية عائقًا رئيسيًا، يعود إلى:

- **غياب إطار تنظيمي موحد** يلزم جميع الجهات بتطبيق قواعد حماية البيانات بنفس المعايير[١].
- **عدم وجود جهة مركزية تنسق الجهود**، حيث لا توجد هيئة وطنية مستقلة تملك صلاحيات شمولية للإشراف على تطبيق حماية البيانات.
- **تنافس وتداخل الصلاحيات** بين الجهات، خاصة في ملفات الأمن والاتصالات والإعلام، ما يؤدي إلى تضارب في السياسات وتعطيل تبادل المعلومات[٢].
- **ضعف تبادل الخبرات والتدريب المشترك**، إذ تفتقر الوزارات إلى برامج مشتركة لتأهيل الكوادر وتعزيز الوعي بأهمية حماية البيانات.

---

(١) تقرير منظمة الشفافية العراقية، "التحديات في الحوكمة الرقمية"، ٢٠٢٢، ص. ١٤.

(٢) ناصر العزاوي، "إشكاليات إدارة البيانات في القطاع الحكومي العراقي"، مجلة العلوم القانونية، ٢٠٢١، ص. ١٠٢.

نتيجة لذلك، تعتمد كل وزارة أو مؤسسة على قواعد داخلية تختلف عن غيرها، ما يولد فجوات واضحة في الحماية، لا سيما في الملفات التي تتطلب تعاونًا متعدد الجهات، مثل ملفات الهوية الوطنية والخدمات الصحية.

## الفرع الثاني: دور المؤسسات الحكومية في تعزيز حماية البيانات الشخصية

يلعب دور المؤسسات الحكومية محورًا أساسيًا في تعزيز حماية البيانات الشخصية، خاصة في ظل التوسع الكبير في استخدام التقنيات الرقمية وتزايد مخاطر الاختراق أو إساءة استخدام البيانات. فهذه المؤسسات ليست فقط مسؤولة عن الالتزام بالقوانين، بل تتولى مهمة بناء ثقافة حماية البيانات وتطوير آليات فعالة لتأمين المعلومات وحفظ خصوصية الأفراد.

أولاً: المؤسسات الحكومية كجهات معنية بحماية البيانات

تتعدد المؤسسات الحكومية التي لها دور مباشر أو غير مباشر في حماية البيانات الشخصية، منها:

- **الوزارات ذات العلاقة المباشرة بالبيانات** مثل وزارات الداخلية، الصحة، التعليم، والعمل والشؤون الاجتماعية.
- **الهيئات الرقابية والتنظيمية** مثل هيئات الإعلام والاتصالات، ومراكز حماية البيانات.
- **الجهات القضائية** التي تفصل في النزاعات المتعلقة بانتهاكات الخصوصية.

ويعتمد دور هذه المؤسسات على تطوير سياسات وإجراءات داخلية تحكم معالجة البيانات، وتوفير التدريب المستمر للعاملين، بالإضافة إلى اعتماد تقنيات الحماية الحديثة.

ثانيًا: المبادرات الحكومية لتعزيز الحماية في العراق

رغم التحديات التشريعية، بدأت بعض الوزارات العراقية خطوات لتعزيز حماية البيانات الشخصية داخل إداراتها، وذلك عبر:

- **إنشاء وحدات أمن معلومات** في الوزارات الكبرى، تتولى مراقبة وحماية البيانات.
- **إصدار تعليمات داخلية** بشأن جمع ومعالجة البيانات، مثل توثيق الموافقات والحفاظ على سرية المعلومات.

- **تنظيم ورش عمل وتدريبات** لتعريف الموظفين بمخاطر التسريب وكيفية التعامل مع البيانات بشكل آمن[١].

ومع ذلك، تبقى هذه المبادرات متفرقة وتعاني من نقص في التنسيق والدعم القانوني، ما يحد من فاعليتها.

## المبحث الثاني: التحديات التقنية والتكنولوجية

### المطلب الأول: نقص البنية التحتية التكنولوجية

#### الفرع الأول: ضعف أنظمة الأمان الرقمي في الإدارات العامة

في عصر الثورة الرقمية، باتت حماية البيانات الشخصية ترتبط ارتباطاً وثيقاً بالبنية التحتية التقنية والتكنولوجية التي تعتمد عليها الجهات الحكومية والخاصة في تخزين ومعالجة هذه البيانات. وعلى الرغم من الأهمية الكبرى لأنظمة الأمان الرقمية، إلا أن الواقع في كل من العراق ومصر يعاني من ضعف واضح في هذه الأنظمة، الأمر الذي يُعد من أبرز التحديات التي تعيق تطبيق قوانين حماية البيانات الشخصية.

**أولاً: مفهوم أنظمة الأمان الرقمية وأهميتها**

تشير أنظمة الأمان الرقمية إلى مجموعة من الأدوات والتقنيات التي تهدف إلى حماية البيانات والمعلومات الرقمية من الاختراق أو الفقدان أو التلاعب. وتتضمن هذه الأنظمة:

- **جدران الحماية (Firewalls)** لمنع الدخول غير المصرح به.
- **تقنيات التشفير (Encryption)** لضمان سرية البيانات أثناء التخزين والنقل.
- **أنظمة الكشف عن الاختراق (Intrusion Detection Systems)** لرصد محاولات الهجوم.
- **آليات التحكم في الوصول (Access Control)** لتحديد من يمكنه رؤية أو تعديل البيانات.

---

(١) وزارة التخطيط العراقية، تقرير عن أمن المعلومات في الوزارات، ٢٠٢١، ص. ٣٣.

- **النسخ الاحتياطي المنتظم (Backup Systems)** للحفاظ على البيانات من الفقدان.

تكمن أهمية هذه الأنظمة في ضمان سرية وموثوقية البيانات، وهي أساس الحماية التقنية التي تكمل الجوانب القانونية والتنظيمية.

ثانياً: واقع أنظمة الأمان الرقمية في العراق

تشير الدراسات والتقارير إلى أن العراق يعاني من نقص واضح في تحديث أنظمة الأمان الرقمية المستخدمة في الإدارات العامة(١). وتتمثل أبرز المشكلات في:

- **اعتماد أنظمة قديمة وغير محدثة،** تعاني من ثغرات أمنية معروفة تعرض البيانات لمخاطر الاختراق.
- **غياب إجراءات التشفير الشاملة،** إذ لا تستخدم معظم الجهات الحكومية تقنيات التشفير لحماية البيانات أثناء التخزين أو النقل.
- **عدم وجود نظم مراقبة فعالة لرصد الهجمات السيبرانية،** مما يجعل المؤسسات عرضة لهجمات إلكترونية متكررة.
- **قلة الكوادر الفنية المؤهلة** في مجال أمن المعلومات، مما يضعف القدرة على مواجهة التحديات التقنية(٢).

هذا الواقع يجعل البيانات الشخصية في العراق عرضة للانتهاكات والهجمات، ويقلل من فاعلية تطبيق التشريعات المتعلقة بحمايتها.

## الفرع الثاني: انتشار الاستخدام غير الآمن للتكنولوجيا

تشكل التكنولوجيا الرقمية والإنترنت أدوات أساسية في إدارة البيانات الشخصية في الإدارات الحكومية، لكن انتشار الاستخدام غير الآمن لهذه التكنولوجيا يعد من أبرز التحديات التي تواجه تطبيق قوانين حماية البيانات الشخصية في العراق ومصر. ويشير هذا الاستخدام إلى ممارسات

(١) منظمة الأمم المتحدة، "تقييم البنية التحتية لتقنية المعلومات في العراق"، ٢٠٢٢، ص. ٢١.

(٢) علي حسين، "أمن المعلومات في العراق: الواقع والتحديات"، مجلة الأمن السيبراني، العدد ٥، ٢٠٢١، ص. ٧٨.

تقنية وإدارية غير كافية أو غير متوافقة مع معايير الحماية الأمنية، مما يعرض البيانات لمخاطر عالية.

**أولاً: مفهوم الاستخدام غير الآمن للتكنولوجيا**

يقصد بالاستخدام غير الآمن للتكنولوجيا كافة الممارسات التي تفتقر إلى الضوابط الأمنية اللازمة لحماية البيانات، مثل:

- استخدام برامج وتطبيقات غير محدثة أو غير موثوقة.
- اعتماد كلمات مرور ضعيفة أو مكررة.
- عدم تحديث أنظمة التشغيل والبرمجيات بانتظام.
- نقص الوعي لدى المستخدمين حول كيفية التعامل الآمن مع الأجهزة والبيانات.
- استخدام شبكات اتصال غير محمية، خاصة في البيئات الحكومية.

هذه الممارسات تسهل الوصول غير المصرح به إلى البيانات، أو تعرضها للاختراق أو التلف.

**ثانياً: واقع الاستخدام غير الآمن في العراق**

في العراق، يعاني قطاع التكنولوجيا الحكومية من انتشار استخدام تقنيات وأساليب غير آمنة نتيجة لعوامل متعددة[١]:

- ضعف الموارد المالية والتقنية، مما يدفع الجهات إلى استخدام برامج وأنظمة قديمة لا تستوفي متطلبات الأمان.
- غياب برامج تدريب وتوعية شاملة للموظفين حول كيفية التعامل الآمن مع التكنولوجيا.
- الاعتماد الكبير على الطرق التقليدية في حفظ البيانات، مع استخدام محدود للأدوات الرقمية الآمنة.
- انتشار ثقافة إهمال التحديثات الأمنية أو تأجيلها بسبب ضغط العمل أو نقص الوعي.
- كل هذه العوامل تساهم في زيادة المخاطر الأمنية على البيانات الشخصية داخل الجهات الحكومية العراقية.

(١) تقرير البنك الدولي، "تقييم الأمن السيبراني في العراق"، ٢٠٢٢، ص. ٣٨.

## المطلب الثاني: الهجمات الإلكترونية وأثرها على البيانات الشخصية

### الفرع الأول: زيادة الهجمات الإلكترونية في الإدارات العامة

تُعد الهجمات الإلكترونية من أبرز التحديات التقنية التي تواجه حماية البيانات الشخصية في الإدارات العامة، حيث تزايدت في السنوات الأخيرة بشكل ملحوظ، مما يهدد أمن المعلومات ويعرقل تطبيق التشريعات المعنية بحماية البيانات. وتعكس هذه الهجمات التوسع في الاعتماد على الأنظمة الرقمية والإلكترونية، لكنها تكشف في الوقت نفسه عن ضعف القدرات الأمنية والتقنية في المؤسسات الحكومية.

**أولاً: مفهوم الهجمات الإلكترونية وأنواعها**

تشمل الهجمات الإلكترونية مجموعة واسعة من العمليات العدائية التي تستهدف الأنظمة المعلوماتية بغرض التلاعب أو السرقة أو الإتلاف، ومن أبرز أنواعها:

- **الهجمات بالبرمجيات الخبيثة (Malware)** التي تتضمن الفيروسات، وأحصنة طروادة، وبرامج الفدية.
- **الهجمات عبر التصيد الاحتيالي (Phishing)** التي تستهدف الحصول على بيانات حساسة عبر خداع المستخدمين.
- **الهجمات التي تستغل الثغرات الأمنية (Exploits)** لاختراق الأنظمة.
- **الهجمات الموزعة لرفض الخدمة (DDoS)** التي تعطل خدمات الشبكة عن طريق إغراقها بطلبات وهمية.
- **الهجمات الداخلية** التي تنفذ من داخل المؤسسة عبر موظفين غير أمناء.

كل هذه الهجمات تؤدي إلى تهديد خطير على سرية وسلامة البيانات الشخصية.

**ثانيًا: أسباب تزايد الهجمات الإلكترونية على الإدارات العامة**

تزايدت الهجمات الإلكترونية على الإدارات العامة في العراق ومصر نتيجة عوامل عدة[١]:

(١) تقرير منظمة الأمن السيبراني العربية، "تقييم التهديدات الإلكترونية في الشرق الأوسط"، ٢٠٢٣، ص. ٤٥.

- **ضعف تحديث الأنظمة والبنية التحتية الأمنية** مما يترك ثغرات يستغلها المهاجمون.
- **انخفاض الوعي الأمني لدى العاملين في المؤسسات،** مما يسهل عمليات التصيد والهجمات الأخرى.
- **زيادة الاعتماد على الخدمات الرقمية** دون تأمين كامل للأنظمة.
- **التوترات السياسية والأمنية في المنطقة** التي قد تحفز الهجمات السيبرانية ذات الدوافع السياسية أو الاقتصادية.
- **غياب التعاون الأمني الفعال بين الجهات الحكومية** لمواجهة الهجمات بشكل موحد.

## الفرع الثاني: تدابير الأمن السيبراني لحماية البيانات الشخصية

مع تصاعد الهجمات الإلكترونية على الإدارات العامة في العراق ومصر، برزت الحاجة الملحة إلى تطبيق تدابير أمن سيبراني متقدمة تضمن حماية البيانات الشخصية وتعزز من قدرة المؤسسات على مواجهة المخاطر الإلكترونية. تمثل هذه التدابير الخط الدفاعي الأول الذي يساهم في تحقيق الامتثال القانوني، وضمان سرية وسلامة المعلومات.

**أولاً: مفهوم تدابير الأمن السيبراني**

تدابير الأمن السيبراني هي مجموعة من السياسات، الإجراءات، والتقنيات التي تهدف إلى حماية الشبكات والأنظمة والبيانات من الهجمات الإلكترونية، وتتضمن:

- **التشفير(Encryption)** :تأمين البيانات أثناء التخزين والنقل.
- **جدران الحماية(Firewalls)** :منع الدخول غير المصرح به.
- **نظم كشف ومنع التسلل(IDS/IPS)** :مراقبة وتحليل النشاطات المشبوهة.
- **المصادقة متعددة العوامل(MFA)** :تعزيز التحقق من هوية المستخدمين.
- **النسخ الاحتياطي(Backup)** :ضمان استرجاع البيانات في حالات الطوارئ.
- **التحديثات الدورية(Patch Management)** :إصلاح الثغرات الأمنية في البرمجيات.

هذه الأدوات تُستخدم ضمن إطار استراتيجي متكامل لضمان أقصى درجات الحماية.

**ثانيًا: تدابير الأمن السيبراني في العراق**

رغم التحديات، بدأ العراق في اعتماد بعض التدابير الأساسية للأمن السيبراني في الجهات الحكومية[١]:

- **إنشاء وحدات أمن المعلومات** في بعض الوزارات للإشراف على حماية البيانات.
- **اعتماد نظم جدران الحماية والتشفير الجزئي** في مؤسسات محدودة.
- **تنفيذ برامج تدريبية للموظفين** حول أساسيات الأمن السيبراني.
- **العمل على تطوير إطار وطني للأمن السيبراني**، لكن التطبيق لا يزال محدوداً بسبب قلة الموارد والتحديات التقنية.

هذه التدابير تشكل بداية مهمة لكنها بحاجة إلى توسيع وتطوير مستمر لتغطية جميع المؤسسات الحكومية.

(١) وزارة الاتصالات العراقية، "تقرير الأمن السيبراني للعام ٢٠٢٣"، بغداد، ٢٠٢٤، ص. ٢٩.

## النتائج

توصلت هذه الدراسة إلى أن تطبيق قوانين حماية البيانات الشخصية في الإدارات العامة يواجه مجموعة معقدة من التحديات المتداخلة التي تتفاوت في حدتها بين العراق ومصر، إلا أنها تشترك في تأثيرها السلبي على فعالية الحماية القانونية للبيانات الشخصية. وقد أظهرت النتائج أن الإطار التشريعي يمثل نقطة الانطلاق الأساسية في ضمان الحماية، إذ إن غياب قانون شامل ومتكامل لحماية البيانات الشخصية في العراق أدى إلى تشتت القواعد القانونية وتعدد الجهات المختصة دون وجود جهة مركزية واضحة للرقابة والتنفيذ، مما انعكس سلباً على مستوى الالتزام داخل الإدارات العامة، وفتح المجال أمام ممارسات غير منضبطة في جمع ومعالجة البيانات الشخصية.

كما بينت الدراسة أن وجود تشريع خاص بحماية البيانات الشخصية، كما هو الحال في مصر، لا يعني بالضرورة تحقيق حماية فعالة ما لم يصاحبه تطبيق عملي منظم وتنسيق مؤسسي فعال. فقد كشفت النتائج أن تعدد الاستثناءات الممنوحة لبعض الجهات الحكومية، إلى جانب ضعف التنسيق بين الوزارات والهيئات، يؤدي إلى تقليص نطاق الحماية الفعلية للبيانات الشخصية، ويجعل بعض الإدارات العامة أقل التزاماً بالضوابط القانونية المقررة. ويؤدي هذا الوضع إلى تفاوت في مستوى الحماية من جهة إلى أخرى، بما يتعارض مع مبدأ المساواة القانونية وحماية الحقوق الأساسية للأفراد.

وأظهرت النتائج أيضاً أن ضعف التنسيق بين الجهات الحكومية يعد من أبرز العوائق المشتركة في كلا البلدين، حيث لا تزال عمليات تبادل البيانات بين المؤسسات تتم في كثير من الأحيان دون وجود بروتوكولات واضحة أو أنظمة موحدة تضمن سلامة البيانات وسريتها. كما أن غياب قواعد واضحة لتحديد المسؤوليات عند حدوث انتهاكات للبيانات يؤدي إلى صعوبة المساءلة القانونية والإدارية، ويحد من فعالية آليات الرقابة والمتابعة.

## المصادر والمراجع


١. دستور جمهورية العراق لسنة ٢٠٠٥، المادة (١٧)، متاح على موقع مجلس النواب العراقي.

٢. قانون تنظيم الخدمات الإلكترونية رقم ٧٨ لسنة ٢٠١٢، منشور في الوقائع العراقية، العدد ٤٢٥٥.

٣. مسودة قانون الجرائم المعلوماتية، لجنة الأمن والدفاع البرلمانية، ٢٠١٩، غير منشورة رسمياً.

٤. القانون رقم ١٥١ لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية، الجريدة الرسمية، العدد ٣٢ مكرر (د)، بتاريخ ١٥ أغسطس ٢٠٢٠.

٥. تقرير منظمة الشفافية العراقية، "التحديات في الحوكمة الرقمية"، ٢٠٢٢، ص. ١٤.

٦. ناصر العزاوي، "إشكاليات إدارة البيانات في القطاع الحكومي العراقي"، مجلة العلوم القانونية، ٢٠٢١.

٧. وزارة التخطيط العراقية، تقرير عن أمن المعلومات في الوزارات، ٢٠٢١.

٨. .منظمة الأمم المتحدة، "تقييم البنية التحتية لتقنية المعلومات في العراق"، ٢٠٢٢.

٩. .علي حسين، "أمن المعلومات في العراق:الواقع والتحديات"، مجلة الأمن السيبراني، العدد ٥، ٢٠٢١.

١٠. تقرير البنك الدولي، "تقييم الأمن السيبراني في العراق"، ٢٠٢٢.

١١. تقرير منظمة الأمن السيبراني العربية، "تقييم التهديدات الإلكترونية في الشرق الأوسط"، ٢٠٢٣، ص. ٤٥.

١٢. وزارة الاتصالات العراقية، "تقرير الأمن السيبراني للعام ٢٠٢٣"، بغداد، ٢٠٢٤.