قوائم المحتويات متاحة على المجلات الاكاديمية العراقية
مجلة البحوث والدراسات الاسلامية
الصفحة الرئيسية للمجلة: https://djisrs.dws.gov.iq

الأساليب والآليات الفعّالة لحماية البيانات الشخصية في الإدارات العامة

(دراسة مقارنة بين العراق ومصر)

Effective Methods and Mechanisms for the Protection of Personal Data in Public Administrations:

A Comparative Study between Iraq and Egypt

صفاء عبد الحسين كاظم العنكوشي/ طالب، دكتوراه، قانون عام، كلية القانون، جامعة قم الحكومية، الجمهورية الأسلامية إيران *

مهدي رجائي/ أستاذ المساعد في كلية القانون، قسم القانون العام، جامعة قم، الجمهورية الاسلامية الإيرانية*

Keywords: Personal data protection, public administrations, legislation, enforcement mechanisms, Iraq, Egypt.

Abstract

This study aims to identify the effective methods and mechanisms for protecting personal data in public administrations through a comparative analysis of the Iraqi and Egyptian experiences, in light of the rapid development in the use of digital technologies within government institutions. The protection of personal data has gained increasing importance due to its close connection with safeguarding the right to privacy and preserving individuals' fundamental rights and freedoms, as well as its role in enhancing trust between citizens and public administration.The study is based on the hypothesis that the effectiveness of personal data protection cannot be achieved merely through the existence of legal texts; rather, it requires an integrated framework that includes clear legislation, effective enforcement mechanisms, an advanced technical infrastructure, and the promotion of legal awareness and institutional culture. The research adopts the comparative method to analyze the legislative and regulatory frameworks in Iraq and Egypt, with a focus on the required legal amendments, the role of governmental bodies and the private sector in implementing data protection laws, and the importance of awareness-raising and training in supporting the practical application of these laws.The study demonstrates that Iraq faces an urgent need to enact a comprehensive personal data protection law that is consistent with international standards, while the Egyptian experience requires continuous development of the Personal Data Protection Law and the restriction of exceptions granted to public administrations. It also concludes that strengthening institutional oversight, activating monitoring and review mechanisms, and expanding training and awareness programs constitute essential elements for ensuring effective and sustainable protection of personal data in public administrations. The study concludes by emphasizing that the adoption of these methods and mechanisms contributes to establishing a modern public administration that respects individuals' privacy and kee ps pace with the requirements of digital transformation in Iraq and Egypt.

معلومات المقال

تاريخ المقال:

الإرسال:٢٠٢٦/١/١٨م

المراجعة:٢٠٢٦/١/٢٣م

القبول: ٢٠٢٦/٢/١م

الكلمات المفتاحية:

حماية البيانات الشخصية، الإدارات العامة، التشريع، آليات التنفيذ، العراق، مصر

الملخص

تهدف هذه الدراسة إلى بيان الأساليب والآليات الفعّالة لحماية البيانات الشخصية في الإدارات العامة، من خلال دراسة مقارنة بين التجربتين العراقية والمصرية، في ظل التطور المتسارع في استخدام التقنيات الرقمية داخل المؤسسات الحكومية. وتكتسب حماية البيانات الشخصية أهمية متزايدة لارتباطها الوثيق بحماية الحق في الخصوصية وصون الحقوق والحريات الأساسية للأفراد، فضلاً عن دورها في تعزيز الثقة بين المواطن والإدارة العامة. تنطلق الدراسة من فرضية مفادها أن فعالية حماية البيانات الشخصية لا تتحقق بمجرد وجود نصوص قانونية، وإنما تتطلب منظومة متكاملة تشمل تشريعات واضحة، وآليات تنفيذ فعّالة، وبنية تقنية متطورة، إلى جانب نشر الوعي القانوني والثقافة المؤسسية. وتعتمد الدراسة المنهج المقارن لتحليل الأطر التشريعية والتنظيمية في العراق ومصر، مع التركيز على التعديلات القانونية المطلوبة، ودور الهيئات الحكومية والقطاع الخاص في تنفيذ قوانين حماية البيانات، فضلاً عن أهمية التوعية والتدريب في دعم التطبيق العملي لهذه القوانين. وتبين الدراسة أن العراق يواجه حاجة ملحّة إلى سن تشريع متكامل خاص بحماية البيانات الشخصية يتوافق مع المعايير الدولية، بينما تتطلب التجربة المصرية تطويراً مستمراً لقانون حماية البيانات الشخصية وتقييد الاستثناءات الممنوحة للإدارات العامة. كما توصلت الدراسة إلى أن تعزيز الرقابة المؤسسية، وتفعيل آليات المتابعة والمراجعة، وتوسيع برامج التدريب والتوعية، تمثل عناصر أساسية لضمان حماية فعّالة ومستدامة للبيانات الشخصية في الإدارات العامة. وتختتم الدراسة بالتأكيد على أن تبني هذه الأساليب والآليات يسهم في ترسيخ إدارة عامة حديثة تحترم خصوصية الأفراد وتواكب متطلبات التحول الرقمي في العراق ومصر.

* Corresponding author at: **Safaa Abdul Hussein Kazem Al-Ankooshi/ PhD Candidate in Public Law, College of Law, Qom State University, Islamic Republic of Iran.**

*** Mahdi Rajaei/ Assistant Professor, College of Law, Department of Public Law, University of Qom, Islamic Republic of Iran.**

safaaalankushe4**@gmail.com**

M.rajaei@qom.ac.ir

١.المقدمة

أصبحت حماية البيانات الشخصية في الإدارات العامة من المتطلبات الأساسية لبناء إدارة حديثة وفعّالة، خاصة في ظل التحول الرقمي المتسارع الذي تشهده الدول المعاصرة. فالتوسع في استخدام الأنظمة الإلكترونية وقواعد البيانات الرقمية في تقديم الخدمات العامة أدى إلى تضاعف حجم البيانات الشخصية التي تجمعها الإدارات العامة وتعالجها، الأمر الذي يفرض ضرورة اعتماد أساليب وآليات فعّالة تضمن حماية هذه البيانات من الانتهاك أو الاستغلال غير المشروع. ولم يعد الاكتفاء بالنصوص القانونية التقليدية كافياً لتحقيق هذه الحماية، بل بات من الضروري تطوير منظومة متكاملة تجمع بين التشريع والتنفيذ والرقابة والتوعية.

وتبرز أهمية البحث في الأساليب والآليات الفعّالة لحماية البيانات الشخصية في الإدارات العامة عند ملاحظة أن ضعف التطبيق العملي للقوانين، حتى في حال وجودها، يؤدي إلى تقويض الثقة بين المواطن والمؤسسة الحكومية، ويعرض الحقوق الأساسية للأفراد للخطر. فالإدارة العامة، بحكم طبيعة مهامها، تتعامل مع بيانات حساسة تتعلق بالهوية والحالة الصحية والاجتماعية والاقتصادية للأفراد، مما يجعل أي خلل في حمايتها ذا آثار قانونية واجتماعية خطيرة. ومن هنا، فإن دراسة الآليات العملية التي تكفل التطبيق السليم لقوانين حماية البيانات الشخصية تمثل خطوة جوهرية نحو تعزيز سيادة القانون وحماية الخصوصية.

١.١.بيان المشكلة

تواجه الإدارات العامة في كل من العراق ومصر تحديات متعددة في مجال حماية البيانات الشخصية، لا تقتصر على الجوانب التشريعية فحسب، بل تمتد لتشمل ضعف آليات التنفيذ والمتابعة، وقصور البنية المؤسسية والتقنية، إضافة إلى محدودية الوعي القانوني والثقافي لدى الموظفين والمواطنين. فعلى الرغم من إدراك أهمية حماية البيانات الشخصية بوصفها جزءاً من حماية الحق في الخصوصية، إلا أن التطبيق العملي للأساليب والآليات الكفيلة بتحقيق هذه الحماية لا يزال دون المستوى المطلوب.

وتتمثل مشكلة الدراسة في أن غياب تشريع متكامل في العراق، يقابله وجود إطار قانوني في مصر يواجه تحديات تتعلق بفعالية التنفيذ واتساع الاستثناءات الممنوحة للإدارات العامة، مما يؤدي إلى تفاوت مستوى الحماية من جهة إلى أخرى، ويضعف الثقة في قدرة المؤسسات الحكومية على صون البيانات الشخصية. كما أن ضعف التنسيق بين الجهات الحكومية، ومحدودية دور الهيئات الرقابية، وقلة إشراك القطاع الخاص في منظومة الحماية، كلها عوامل تسهم في استمرار أوجه القصور في التطبيق العملي لقوانين حماية البيانات الشخصية.

٢.١.أهمية البحث و اهدافه

تنبع أهمية هذا البحث من معالجته للأساليب والآليات الفعّالة لحماية البيانات الشخصية في الإدارات العامة، بوصفها أحد المرتكزات الأساسية لضمان

احترام الحق في الخصوصية وتعزيز الثقة بين المواطن والمؤسسات الحكومية. فمع تزايد الاعتماد على التقنيات الرقمية في تقديم الخدمات العامة، أصبحت البيانات الشخصية أكثر عرضة للمخاطر والانتهاكات، مما يستوجب البحث في الوسائل العملية الكفيلة بتفعيل الحماية القانونية المقررة لها.

١.٣. أهداف البحث

يهدف هذا البحث إلى تحقيق مجموعة من الأهداف العلمية والعملية، تتمثل فيما يأتي:

١. بيان الأساليب القانونية الفعّالة لتطوير التشريعات الوطنية الخاصة بحماية البيانات الشخصية في العراق ومصر، في ضوء المعايير الدولية المعاصرة.
٢. تحليل آليات التنفيذ والمتابعة المعتمدة في الإدارات العامة، وبيان دور الهيئات الحكومية والرقابية في ضمان التطبيق السليم لقوانين حماية البيانات الشخصية.
٣. توضيح دور القطاع الخاص في دعم منظومة حماية البيانات الشخصية، ومدى التزامه بالضوابط القانونية في جمع ومعالجة البيانات.

١.٤.منهجية البحث

يعتمد هذا البحث على **المنهج المقارن** في دراسة الأساليب والآليات الفعّالة لحماية البيانات الشخصية في الإدارات العامة، من خلال تحليل التشريعات الوطنية والأنظمة القانونية المعتمدة في كل من العراق ومصر، مع التركيز على أوجه التشابه والاختلاف بين التجربتين. ويسهم هذا المنهج في تقييم مدى كفاية التعديلات التشريعية القائمة، وقياس مستوى توافقها مع المعايير الدولية لحماية البيانات الشخصية، بما يساعد على استخلاص نماذج قانونية وتنظيمية قابلة للتطبيق في كلا البلدين.

٢.المبحث الأول: تطوير التشريعات الوطنية

١.٢.المطلب الأول: التعديلات القانونية المطلوبة في العراق.

١.١.٢.الفرع الأول: مقترحات لتطوير قانون حماية البيانات الشخصية في العراق

تُعتبر القوانين الوطنية لحماية البيانات الشخصية العمود الفقري في أي نظام يهدف إلى حماية خصوصية الأفراد وضمان أمان بياناتهم. وفي العراق، يواجه التشريع الحالي تحديات جوهرية تتطلب مراجعة وتحديث لتواكب التطورات التكنولوجية والمعايير الدولية. لذلك، تبرز الحاجة إلى وضع مقترحات تطويرية محددة تقود إلى صياغة قانون متكامل وفعّال لحماية البيانات.

أولاً: الوضع القانوني الراهن في العراق

يُعَد قانون حماية البيانات الشخصية في العراق محدودًا نسبيًا، إذ لا يوجد حتى الآن تشريع شامل وموحد ينظم جمع ومعالجة البيانات الشخصية على المستوى الوطني[١]. وتعتمد بعض المؤسسات على أنظمة عامة أو على مواد متفرقة في قوانين أخرى، مما يخلق فجوات في الحماية ويؤثر سلبًا على حقوق الأفراد.

ثانيًا: ضرورة تطوير التشريع وفقًا للمعايير الدولية لمواكبة التغيرات السريعة في مجال التكنولوجيا الرقمية، ينبغي على العراق تبني إطار قانوني ينسجم مع معايير حماية البيانات الدولية، مثل:

(١) وزارة العدل العراقية، "تقرير واقع التشريعات الرقمية في العراق"، بغداد، ٢٠٢٢، ص. ٢٧.

– **اللائحة العامة لحماية البيانات** (GDPR) الأوروبية التي تعتبر نموذجًا متقدمًا في تنظيم حماية البيانات.

– التوصيات الصادرة عن **اللجنة الدولية لحماية الخصوصية** والهيئات الدولية ذات الصلة.

ذلك يتطلب تعديل القوانين لتشمل:

– تعريف واضح وشامل للبيانات الشخصية وأنواعها.

– مبادئ قانونية تنظم جمع واستخدام البيانات.

– حقوق الأفراد مثل حق الوصول والتصحيح والحذف.

– آليات للرقابة والتفتيش.

– عقوبات رادعة للانتهاكات.

٢.١.٢.الفرع الثاني: التوافق مع المعايير الدولية في حماية البيانات الشخصية.

يُعد التوافق مع المعايير الدولية أحد أهم المحاور التي يجب أن تستند إليها التشريعات الوطنية لحماية البيانات الشخصية، وذلك لضمان فعالية الحماية ومواءمتها مع التطورات العالمية في مجال الخصوصية والأمن السيبراني. وهذا يكتسب أهمية خاصة للعراق الذي يسعى إلى تحديث نظامه القانوني في ضوء التجارب العالمية، ولا سيما في ظل التفاعل المتزايد مع الاقتصاد الرقمي والتبادل الدولي للبيانات.

أولاً: أهمية التوافق الدولي في التشريعات الوطنية

يرتكز التوافق مع المعايير الدولية على عدة أسباب رئيسية[١]:

– **حماية حقوق الأفراد:** تكفل الاتفاقيات والمعايير الدولية حقوق الأفراد في الخصوصية والسرية.

– **تيسير التجارة الإلكترونية:** يسهل التوافق تبادل البيانات بين الدول ويعزز التعاون التجاري الرقمي.

– **تعزيز الثقة الدولية:** يرفع من ثقة الشركاء الدوليين والمؤسسات العالمية بالتشريعات الوطنية.

– **التصدي للهجمات السيبرانية:** يتيح تبادل الخبرات والتنسيق في مواجهة التهديدات العابرة للحدود.

ثانياً: أبرز المعايير الدولية المتعلقة بحماية البيانات

١. **اللائحة العامة لحماية البيانات** (GDPR) التي صدرت عن الاتحاد الأوروبي عام ٢٠١٦، والتي تُعد من أقوى التشريعات في العالم، حيث تقدم إطارًا متكاملًا لحماية البيانات الشخصية، وتفرض شروطًا صارمة على جمع ومعالجة البيانات، مع حقوق واسعة للأفراد[٢].

٢. **المبادئ التوجيهية لمنظمة التعاون الاقتصادي والتنمية** (OECD) بشأن حماية الخصوصية والتدابير عبر الوطنية في مجال حماية البيانات، والتي توفر معايير أساسية لتصميم القوانين والسياسات[٣].

٣. **اتفاقية المجلس الأوروبي رقم ١٠٨** المتعلقة بحماية الأفراد تجاه معالجة البيانات ذات الطابع الشخصي، والتي تمثل أول اتفاقية دولية في هذا المجال[٤].

٢.٢.المطلب الثاني: التعديلات القانونية المطلوبة في مصر

١.٢.٢.الفرع الأول: تحديث وتوسيع قانون حماية البيانات الشخصية المصري

شهدت مصر في السنوات الأخيرة خطوات مهمة نحو تنظيم حماية البيانات الشخصية، إذ صدر قانون حماية

(١) الهيئة الوطنية للامتثال العراقي، "أهمية التوافق الدولي في حماية البيانات"، ٢٠٢٤، ص. ٣٣.

(٢) الاتحاد الأوروبي، "اللائحة العامة لحماية البيانات"(GDPR) ، ٢٠١٦.

(٣) منظمة التعاون الاقتصادي والتنمية(OECD) ، "المبادئ التوجيهية بشأن حماية الخصوصية"، ٢٠١٣.

(٤) مجلس أوروبا، "اتفاقية حماية البيانات رقم ١٠٨"، ١٩٨١.

البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠، والذي يمثل إطارًا تشريعيًا متطورًا مقارنة بالمراحل السابقة[١]. إلا أن التطبيق العملي للقانون والكفاءة في الحماية تتطلبان مراجعات وتعديلات تسهم في توسيع نطاق الحماية وتحسين آليات التنفيذ.

أولاً: أبرز ملامح قانون حماية البيانات المصري الحالي

ينص القانون المصري على تنظيم جمع ومعالجة البيانات الشخصية بوضوح، ويوفر حقوقًا للأفراد مثل حق الوصول والتصحيح والاعتراض، ويُلزم الجهات المعنية بالحصول على موافقة صريحة قبل استخدام البيانات[٢]. كما أنشأ القانون "الهيئة الوطنية للبيانات الشخصية" كمؤسسة مستقلة تشرف على تطبيق القانون وتراقب ممارسات حماية البيانات.

ثانيًا: أسباب الحاجة لتحديث القانون وتوسيعه

رغم الجوانب الإيجابية في القانون، فإن هناك أسبابًا تدعو إلى تحديثه وتوسيعه، منها[٣]:

– ظهور تقنيات جديدة مثل الذكاء الاصطناعي، وإنترنت الأشياء، والتي تتطلب تنظيمًا خاصًا.

– وجود ثغرات في بعض مواد القانون تتعلق بالبيانات الحساسة والبيانات المنقولة عبر الحدود.

– الحاجة لتقوية العقوبات والجزاءات لضمان ردع المخالفين.

– تحسين التنسيق بين الجهات الحكومية المختلفة والقطاع الخاص.

– ضرورة تضمين مواد خاصة بحماية الأطفال والبيانات الطبية.

٢.٢.٢.الفرع الثاني: تعزيز القوانين الخاصة بالخصوصية في الإدارات العامة في مصر

تُعد الإدارات العامة في مصر من أهم الجهات التي تتعامل مع كميات هائلة من البيانات الشخصية لمواطنين وأفراد مختلفين، مما يجعل حماية هذه البيانات وحفظ الخصوصية من الأولويات التي يجب أن تحظى باهتمام تشريعي وتنفيذي متزايد. وعلى الرغم من وجود قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠، إلا أن هناك حاجة ماسة إلى تعزيز القوانين والإجراءات الخاصة بالخصوصية داخل الإدارات الحكومية لضمان تطبيق فعال ومتسق.

أولاً: أهمية الخصوصية في الإدارات العامة

تعمل الإدارات العامة على جمع ومعالجة بيانات حساسة مثل البيانات الصحية، المالية، والبيانات المتعلقة بالحياة الشخصية للمواطنين، ولذلك فإن أي خلل في حماية هذه البيانات قد يؤدي إلى انتهاكات جسيمة للحقوق، ويُضعف ثقة الجمهور في المؤسسات الحكومية[٤]. كما أن حفظ الخصوصية يسهم في تحسين جودة الخدمات وتعزيز الشفافية.

ثانيًا: الوضع التشريعي الحالي في مصر

ينص قانون حماية البيانات المصري على التزامات عامة للجهات الحكومية والخاصة، لكنه لا يحدد بشكل تفصيلي آليات خصوصية خاصة للإدارات العامة، مما يترك فراغًا في التطبيق الفعلي داخل

(١) قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠، الجريدة الرسمية، العدد ٤٥، ٢٠٢٠.

(٢) الهيئة الوطنية للبيانات الشخصية المصرية، "تقرير أداء العام الأول"، القاهرة، ٢٠٢٢، ص. ٢٣.

(٣) المركز المصري للسياسات الرقمية، "تحديات حماية البيانات في مصر"، ٢٠٢٣، ص. ٣٧.

(٤) وزارة التخطيط المصرية، "دراسة حول خصوصية البيانات في القطاع العام"، القاهرة، ٢٠٢٢، ص. ٢٩.

المؤسسات الحكومية[١]. كما أن العديد من اللوائح التنفيذية التي تضبط حماية البيانات في الجهات الحكومية لا تزال في طور الإعداد أو التنفيذ.

٣.المبحث الثاني: آليات التنفيذ والمتابعة

١.٣.المطلب الأول: دور الهيئات الحكومية في تنفيذ قوانين حماية البيانات الشخصية

١.١.٣.الفرع الأول: الجهات المسؤولة عن الرقابة والتطبيق في العراق ومصر

يشكل دور الجهات الحكومية المختصة في الرقابة وتنفيذ قوانين حماية البيانات الشخصية حجر الأساس لضمان فاعلية هذه القوانين وحماية حقوق الأفراد. تختلف طبيعة هذه الجهات ومسؤولياتها بين العراق ومصر، لكنها تتقاطع في الهدف الأساسي وهو توفير بيئة قانونية وإدارية تضمن سلامة البيانات الشخصية.

أولاً: الجهات المسؤولة في العراق

– **وزارة الاتصالات وتقنية المعلومات:** تُعد الجهة الرئيسية التي تتولى وضع السياسات الفنية والتقنية المتعلقة بحماية البيانات، وتنسيق الجهود مع الوزارات والمؤسسات الأخرى[٢].

– **الهيئة الوطنية للاتصالات وتقنية المعلومات:** تعمل على مراقبة تنفيذ المعايير التقنية، وضمان حماية المعلومات والبيانات، ولها صلاحيات متابعة المخالفات واتخاذ الإجراءات اللازمة.

– **الجهات القضائية:** تتولى معالجة الدعاوى القضائية المتعلقة بانتهاك حقوق حماية البيانات، مع وجود توجه متزايد لإنشاء وحدات قضائية متخصصة في الجرائم الإلكترونية.

– **الوزارات والمؤسسات العامة:** تقع على عاتقها مسؤولية تنفيذ القانون داخلياً، من خلال تعيين مسؤولين عن حماية البيانات وتفعيل السياسات الرقابية.

ثانيًا: الجهات المسؤولة في مصر

– **الهيئة الوطنية للبيانات الشخصية:** هي الجهة الرقابية الرسمية التي تأسست بموجب قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠، وتتمتع بصلاحيات واسعة تشمل التفتيش، التحقيق، فرض الغرامات، والتوعية[٣].

– **وزارة الاتصالات وتكنولوجيا المعلومات:** تساهم في دعم البنية التحتية التقنية وتطوير أنظمة حماية البيانات، بالتعاون مع الهيئة الوطنية.

– **الهيئات القضائية:** تلعب دورًا في تطبيق العقوبات على المخالفين للقانون، ويُنظر إلى تطوير القضاء المختص بالجرائم الإلكترونية كأولوية لتعزيز تنفيذ القانون.

– **الإدارات والمؤسسات الحكومية:** مسؤولة عن تنفيذ القوانين داخل حدود اختصاصها، وتعيين موظفي حماية البيانات.

٢.١.٣.الفرع الثاني: تحسين آليات المتابعة والمراجعة في تنفيذ قوانين حماية البيانات الشخصية

تعتبر آليات المتابعة والمراجعة من الركائز الأساسية لضمان تطبيق فعال ومستدام لقوانين حماية البيانات الشخصية في الإدارات العامة، حيث تسهم هذه الآليات في الكشف المبكر عن الانتهاكات، وتصحيح المسارات

(١) قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠، الجريدة الرسمية، العدد ٤٥، ٢٠٢٠.

(٢) وزارة الاتصالات العراقية، "تقرير حماية البيانات والأمن السيبراني"، بغداد، ٢٠٢٣، ص. ٤٠.

(٣) الهيئة الوطنية للبيانات الشخصية المصرية، "التقرير السنوي ٢٠٢٣"، القاهرة، ٢٠٢٤، ص. ٣٦.

القانونية والإجرائية، وتعزيز ثقة الأفراد والمؤسسات في منظومة حماية البيانات.

أولاً: أهمية آليات المتابعة والمراجعة

تمكّن آليات المتابعة والمؤشرات المراقبة من:

– تقييم مدى التزام الجهات الحكومية والخاصة بأحكام القانون.

– رصد حالات الانتهاك والتجاوز.

– قياس أثر القوانين على حماية البيانات الشخصية.

– تحسين السياسات والإجراءات باستمرار بناءً على نتائج المراجعة[١].

ثانيًا: الوضع الحالي لآليات المتابعة في العراق ومصر

– في العراق، تفتقر بعض الجهات إلى آليات متابعة منتظمة، وتعتمد بشكل كبير على التقييمات الخارجية أو التقارير الدورية غير المنهجية، مما يحد من فعالية الرقابة[٢].

– في مصر، رغم وجود الهيئة الوطنية للبيانات الشخصية التي تقوم بدور الرقابة، إلا أن آليات المتابعة تحتاج إلى تطوير، خصوصًا من حيث التوسع في نطاق الرقابة وتفعيل دور الشكاوى وتحليل البيانات[٣].

٢.٣.المطلب الثاني: دور القطاع الخاص في حماية البيانات الشخصية

١.٢.٣.الفرع الأول: التعاون بين القطاع العام والخاص في حماية البيانات الشخصية

يُعد التعاون بين القطاعين العام والخاص من العوامل الأساسية لتحقيق حماية فعالة للبيانات الشخصية، حيث يتقاطع عملهما في معالجة كميات ضخمة من البيانات ويواجهان تحديات مشتركة في الأمن والخصوصية. وتبرز أهمية هذا التعاون في صياغة وتنفيذ سياسات شاملة تضمن حماية الحقوق وحماية البيانات من الانتهاك.

يتميز القطاع الخاص بقدرته التقنية وخبرته في إدارة البيانات الرقمية، بينما يمتلك القطاع العام السلطة القانونية والتنظيمية لضمان الامتثال[٤]. الجمع بين هذين القطاعين يحقق:

– تطوير معايير وأدوات حماية موحدة.

– تبادل الخبرات والمعلومات حول التهديدات السيبرانية.

– تعزيز قدرة الطرفين على مواجهة الانتهاكات والاختراقات.

– دعم جهود التوعية والتدريب للموظفين.

ثانيًا: أشكال التعاون بين القطاع العام والخاص في العراق ومصر

– **المبادرات المشتركة:** تتبنى بعض الحكومات برامج ومشروعات مشتركة مع الشركات التقنية لتطوير حلول أمنية متقدمة[٥].

٢.٢.٣.الفرع الثاني: فرض الالتزامات القانونية على الشركات الخاصة في جمع ومعالجة البيانات الشخصية

مع تزايد دور القطاع الخاص في جمع ومعالجة البيانات الشخصية، أصبح من الضروري فرض التزامات قانونية وتنظيمية واضحة على هذه الشركات لضمان احترام حقوق الأفراد وحماية بياناتهم من الانتهاكات.

---

(١) مركز الدراسات القانونية والتنظيمية، "أهمية المتابعة في تطبيق قوانين حماية البيانات"، القاهرة، ٢٠٢٣، ص. ٢٧.

(٢) وزارة الاتصالات العراقية، المرجع السابق، ص. ٤٥.

(٣) الهيئة الوطنية للبيانات الشخصية المصرية، التقرير السنوي ٢٠٢٣، ص. ٣٩.

(٤) منظمة التعاون الاقتصادي والتنميةOECD ، "التعاون بين القطاعين العام والخاص في الأمن السيبراني"، ٢٠٢٢، ص. ١٥.

(٥) وزارة الاتصالات العراقية، "تقرير الشراكات التقنية"، بغداد، ٢٠٢٣، ص. ٣٨.

يشمل ذلك شركات التكنولوجيا، الاتصالات، التسويق، والخدمات المالية وغيرها، التي تتعامل مع كميات ضخمة من المعلومات الحساسة.

أولاً: أهمية فرض الالتزامات القانونية على الشركات الخاصة

إن فرض التزامات على الشركات الخاصة يحقق:

– ضمان الشفافية في كيفية جمع واستخدام البيانات.

– توفير حماية فعالة للبيانات من خلال اتباع معايير أمنية صارمة.

– تمكين الأفراد من معرفة كيفية التعامل مع بياناتهم.

– تحفيز الشركات على تبني ممارسات أخلاقية ومسؤولة.

ثانيًا: الإطار القانوني والتنظيمي في العراق ومصر

– **في العراق:** بالرغم من وجود قوانين عامة لحماية البيانات، إلا أن الإطار التنظيمي الخاص بفرض الالتزامات على الشركات الخاصة لا يزال في مراحل التطوير، ويعاني من ضعف في التنفيذ والمراقبة(١).

– **في مصر:** قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠ وضع قواعد واضحة للشركات الخاصة تتضمن شروطًا لجمع البيانات، موافقة الأفراد، والحفاظ على سرية البيانات، مع وجود عقوبات على المخالفين(٢).

٤.المبحث الثالث: تعزيز التوعية والتدريب

١.٤.المطلب الأول: البرامج التدريبية لموظفي الإدارات العامة

١.١.٤.الفرع الأول: تصميم برامج تدريبية متخصصة لموظفي الإدارات العامة في مجال حماية البيانات الشخصية

تُعد البرامج التدريبية المتخصصة من الركائز الأساسية لتعزيز قدرات الموظفين في الإدارات العامة على حماية البيانات الشخصية، حيث تسهم في رفع الوعي القانوني والتقني، وتطوير مهارات التعامل مع البيانات بما يتوافق مع القوانين والتشريعات الوطنية والدولية.

أولاً: أهمية تصميم برامج تدريبية متخصصة

– **رفع الوعي القانوني:** تعريف الموظفين بحقوق الأفراد وواجباتهم القانونية تجاه البيانات الشخصية، مما يقلل من حالات الانتهاك غير المقصود(٣).

– **تعزيز المهارات التقنية:** تزويد الموظفين بالمعرفة والأدوات التقنية الضرورية لحماية البيانات والتعامل مع التهديدات السيبرانية.

– **تحسين جودة الأداء:** تطبيق الإجراءات السليمة في جمع ومعالجة البيانات يساهم في تحسين كفاءة العمل والخدمات الحكومية.

– **بناء ثقافة حماية البيانات:** ترسيخ ممارسات مستدامة تحافظ على سرية وأمن المعلومات.

ثانيًا: مكونات تصميم البرامج التدريبية المتخصصة

١. **تحليل الاحتياجات التدريبية:** دراسة واقع المهارات والمعرفة لدى الموظفين لتحديد الثغرات.

(١) وزارة الاتصالات العراقية، "تقرير حماية البيانات والخصوصية"، بغداد، ٢٠٢٣، ص. ٥٠.

(٢) قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠، الجريدة الرسمية، ٢٠٢٠، ص. ١٨.

(٣) المركز الدولي لحماية البيانات، "أهمية التدريب في حماية البيانات"، ٢٠٢٢، ص. ١٢.

٢. **تحديد الأهداف التدريبية:** وضع أهداف واضحة ترتبط بمتطلبات القانون والسياسات المؤسسية.

٢.١.٤.الفرع الثاني: تطبيق التدريب المستمر على حماية البيانات الشخصية

إن التدريب المستمر للموظفين في الإدارات العامة يُعد من أهم آليات ضمان الامتثال الفعّال والمستدام لقوانين حماية البيانات الشخصية، إذ لا يكفي إجراء تدريب أولي لمرة واحدة، بل يجب أن تتضمن خطة التدريب الحكومية برامج دورية ومحدثة تراعي التغيرات القانونية والتقنية المستمرة في مجال الخصوصية والأمن السيبراني.

أولًا: أهمية التدريب المستمر في تعزيز ثقافة الحماية

١. **مواكبة التغيرات التشريعية والتقنية:** تساعد الدورات المتكررة الموظفين على فهم المستجدات في القانون الوطني والمعايير الدولية (مثل اللائحة العامة لحماية البيانات(GDPR ، مما يضمن استمرار التزامهم بالمتطلبات القانونية[١].

٢. **الحد من الأخطاء البشرية:** تُعد الأخطاء البشرية من أبرز أسباب تسرب البيانات، والتدريب المتكرر يقلل منها عن طريق التذكير المستمر بالإجراءات الأمنية.

٣. **بناء ثقافة حماية مؤسسية:** التدريب المستمر يُرسّخ سلوكًا مؤسسيًا قائمًا على احترام البيانات، ما يعزز من مكانة المؤسسات العامة كمؤسسات تحترم حقوق الأفراد.

٤. **تحسين الاستجابة للطوارئ:** تمارين المحاكاة العملية ضمن التدريبات تساهم في تحسين الاستجابة لحالات اختراق البيانات أو الهجمات الإلكترونية.

ثانيًا: الوضع الحالي للتدريب المستمر في العراق ومصر

– **في العراق:** لا تزال أغلب برامج التدريب تُنفّذ على نطاق محدود وغير منتظم، وغالبًا ما تُجرى كردّ فعل لحوادث معينة بدلًا من كونها جزءًا من خطة إستراتيجية مستدامة[٢].

– **في مصر:** تم إطلاق مبادرات من الهيئة الوطنية لحماية البيانات، تضمنت دورات تدريبية موسمية، لكن هناك حاجة لتوسيع نطاقها وتحويلها إلى برامج مؤسسية مدمجة ضمن عمل الإدارات العامة[٣].

٢.٤.المطلب الثاني: حملات التوعية بحقوق حماية البيانات الشخصية

١.٢.٤.الفرع الأول: حملات التوعية عبر وسائل الإعلام ووسائل التواصل الاجتماعي

تعد حملات التوعية الموجهة للمواطنين عبر وسائل الإعلام التقليدية والحديثة ركيزة أساسية لتعزيز فهم المجتمع بأهمية حماية البيانات الشخصية وحقوق الخصوصية. تسهم هذه الحملات في نشر المعلومات بشكل واسع، وتكوين وعي جماهيري يضغط باتجاه احترام التشريعات والامتثال لها.

أولاً: أهمية حملات التوعية الإعلامية

١. **الوصول الجماهيري الواسع:** تمكن وسائل الإعلام من نقل الرسائل إلى شرائح واسعة من المجتمع، بما في ذلك الفئات الأقل اطلاعًا بالتقنيات الرقمية[٤].

---

(١) European Union Agency for Cybersecurity (ENISA), "Guidelines on Continuous Training for Data Protection," 2022, p. 1.٩

(٢) وزارة التخطيط العراقية، "تقرير تقييم القدرات المؤسسية"، بغداد، ٢٠٢٣، ص. ٥١.

(٣) الهيئة المصرية لحماية البيانات الشخصية، "الدليل التدريبي السنوي"، القاهرة، ٢٠٢٣، ص. ٣٣.

(٤) اليونسكو، "تأثير الإعلام على الثقافة الرقمية"، ٢٠٢٢، ص. ٤٥.

٢. **التكرار والتعزيز:** يتيح الإعلام تكرار الرسائل التوعوية، مما يعزز ترسيخ المعلومات ويشجع على السلوكيات الآمنة.

٣. **التنوع في الصيغ:** تشمل التلفزيون، الإذاعة، الصحف، والمنصات الرقمية، ما يلبي احتياجات أعمار وبيئات مختلفة.

ثانيًا: استراتيجيات الحملات على وسائل التواصل الاجتماعي

١. **التخصيص والشرائح المستهدفة:** استخدام أدوات الاستهداف للإعلانات المدفوعة على فيسبوك، تويتر، وإنستجرام لعرض رسائل تتناسب مع أعمار واهتمامات مختلفة(١).

٢. **المحتوى التفاعلي:** إعداد فيديوهات قصيرة، إنفوجرافيكس، واستطلاعات رأي تشجع المتابعين على التفاعل والمشاركة في نشر التوعية.

٣. **التعاون مع المؤثرين:** إشراك الشخصيات العامة والمدونين التقنيين لنشر رسائل حماية البيانات، مما يزيد من المصداقية والوصول(٢).

٢.٢.٤.الفرع الثاني: توظيف التكنولوجيا الحديثة في نشر الوعي بحماية البيانات الشخصية

أصبح استخدام التكنولوجيا في نشر الوعي حول حماية البيانات الشخصية ضرورة ملحة، ليس فقط لأنها وسيلة عصرية وسريعة للوصول إلى الجمهور، بل لأنها تتماشى مع طبيعة الموضوع ذاته الذي يرتبط بالعالم الرقمي والافتراضي. وبفضل أدوات الذكاء الاصطناعي، الواقع المعزز، وتطبيقات الهاتف الذكي، يمكن للحكومات والمؤسسات توسيع قاعدة التوعية المجتمعية بطرق مبتكرة وأكثر تفاعلية.

١. **الوصول السريع والواسع:** التكنولوجيا تُتيح إيصال الرسائل التوعوية إلى جمهور متنوع وفي مناطق نائية عبر الإنترنت(٣).

٢. **الرسائل المخصصة:** تمكن الخوارزميات من تصميم محتوى توعوي يتناسب مع سلوكيات واهتمامات المستخدمين.

٣. **التفاعل الفوري:** توفر التطبيقات والمنصات التقنية قنوات تواصل مباشرة وفورية للاستفسار والتبليغ.

٥. النتائج

أظهرت نتائج هذا الفصل أن حماية البيانات الشخصية في الإدارات العامة لا يمكن أن تتحقق بصورة فعّالة إلا من خلال تبني منظومة متكاملة من الأساليب والآليات التي تجمع بين التطوير التشريعي، وفعالية التنفيذ، ورفع مستوى الوعي والتدريب. فقد تبين أن التشريعات تمثل الأساس القانوني للحماية، إلا أن فعاليتها تظل محدودة ما لم تُدعّم بآليات تنفيذ واضحة ومؤسسات رقابية قادرة على فرض الالتزام وضمان التطبيق العملي للنصوص القانونية.

وأوضحت النتائج أن العراق يواجه حاجة ملحّة إلى سن تشريع متكامل خاص بحماية البيانات الشخصية، يحدد بشكل دقيق مفاهيم البيانات، وحقوق الأفراد، والتزامات الإدارات العامة، مع إنشاء جهة مستقلة تتولى الإشراف والرقابة. كما بينت النتائج أن غياب

(١) منصة Hootsuite ، "Social Media Targeting Strategies 2023"، ٢٠٢٣.

(٢) مركز بحوث التواصل الاجتماعي، "فاعلية المؤثرين في التوعية الرقمية"، ٢٠٢٣، ص. ٢٨.

(٣) منظمة التعاون الاقتصادي والتنمية OECD ، "Digital Government in the MENA Region"، ٢٠٢٢، ص. ٧٨.

هذا الإطار التشريعي الموحد يؤدي إلى استمرار التباين في الممارسات الإدارية، ويضعف القدرة على مساءلة الجهات التي تنتهك قواعد حماية البيانات. وفي المقابل، أظهرت الدراسة أن وجود قانون خاص بحماية البيانات الشخصية في مصر يمثل خطوة إيجابية، إلا أن فعالية هذا القانون تتأثر بمدى تحديثه المستمر وقدرته على مواكبة التطورات التقنية، فضلاً عن ضرورة تقليص الاستثناءات التي تحد من نطاق تطبيقه داخل الإدارات العامة.

المصادر والمراجع

١. وزارة العدل العراقية، "تقرير واقع التشريعات الرقمية في العراق"، بغداد، ٢٠٢٢، ص. ٢٧.
٢. الهيئة الوطنية للامتثال العراقي، "أهمية التوافق الدولي في حماية البيانات"، ٢٠٢٤، ص. ٣٣.
٣. الاتحاد الأوروبي، "اللائحة العامة لحماية البيانات (GDPR)"، 2016.
٤. منظمة التعاون الاقتصادي والتنمية (OECD)، "المبادئ التوجيهية بشأن حماية الخصوصية"، ٢٠١٣.
٥. مجلس أوروبا، "اتفاقية حماية البيانات رقم ١٠٨"، ١٩٨١.
٦. قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠، الجريدة الرسمية، العدد ٤٥، ٢٠٢٠.
٧. الهيئة الوطنية للبيانات الشخصية المصرية، "تقرير أداء العام الأول"، القاهرة، ٢٠٢٢، ص. ٢٣.
٨. المركز المصري للسياسات الرقمية، "تحديات حماية البيانات في مصر"، ٢٠٢٣، ص. ٣٧.
٩. وزارة التخطيط المصرية، "دراسة حول خصوصية البيانات في القطاع العام"، القاهرة، ٢٠٢٢، ص. ٢٩.
١٠. قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠، الجريدة الرسمية، العدد ٤٥، ٢٠٢٠.
١١. وزارة الاتصالات العراقية، "تقرير حماية البيانات والأمن السيبراني"، بغداد، ٢٠٢٣، ص. ٤٠.
١٢. الهيئة الوطنية للبيانات الشخصية المصرية، "التقرير السنوي ٢٠٢٣"، القاهرة، ٢٠٢٤، ص. ٣٦.
١٣. مركز الدراسات القانونية والتنظيمية، "أهمية المتابعة في تطبيق قوانين حماية البيانات"، القاهرة، ٢٠٢٣، ص. ٢٧.
١٤. وزارة الاتصالات العراقية، المرجع السابق، ص. ٤٥.
١٥. الهيئة الوطنية للبيانات الشخصية المصرية، التقرير السنوي ٢٠٢٣، ص. ٣٩.
١٦. منظمة التعاون الاقتصادي والتنمية OECD، "التعاون بين القطاعين العام والخاص في الأمن السيبراني"، ٢٠٢٢، ص. ١٥.
١٧. وزارة الاتصالات العراقية، "تقرير الشراكات التقنية"، بغداد، ٢٠٢٣، ص. ٣٨.
١٨. وزارة الاتصالات العراقية، "تقرير حماية البيانات والخصوصية"، بغداد، ٢٠٢٣، ص. ٥٠.
١٩. قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠، الجريدة الرسمية، ٢٠٢٠، ص. ١٨.
٢٠. المركز الدولي لحماية البيانات، "أهمية التدريب في حماية البيانات"، ٢٠٢٢، ص. ١٢.

٢١. وزارة التخطيط العراقية، "تقرير تقييم القدرات المؤسسية"، بغداد، ٢٠٢٣، ص. ٥١.

٢٢. الهيئة المصرية لحماية البيانات الشخصية، "الدليل التدريبي السنوي"، القاهرة، ٢٠٢٣، ص. ٣٣.

٢٣. اليونسكو، "تأثير الإعلام على الثقافة الرقمية"، ٢٠٢٢، ص. ٤٥.

٢٤. مركز بحوث التواصل الاجتماعي، "فاعلية المؤثرين في التوعية الرقمية"، ٢٠٢٣، ص. ٢٨.

25. OECD، "Digital Government in the MENA Region"، 2022.٧٨ ، ص.

26. Hootsuite، "Social Media Targeting Strategies 2023"، 2023.

27. .European Union Agency for Cybersecurity (ENISA), "Guidelines on Continuous Training for Data Protection," 2022, p. 19.