



الثغرات والتحديات التشريعية التي تواجه حماية البيانات الشخصية في التشريع العراقي والمصري

## الثغرات والتحديات التشريعية التي تواجه حماية البيانات الشخصية في التشريع العراقي والمصري

قاسم محمد سعودي الفارسي

Email: [qasimmohamed620@gmail.com](mailto:qasimmohamed620@gmail.com)

دكتوراه القانون العام / جامعة قم / كلية القانون

محسن ملك افضلى الاردكانى

جامعة قم / كلية القانون

Email: [mohsenmalekafzali@yahoo.com](mailto:mohsenmalekafzali@yahoo.com)

[malekafzali@miu.ac.ir](mailto:malekafzali@miu.ac.ir)

**الكلمات المفتاحية:** الثغرات، التحديات، البيانات الشخصية، التشريع العراقي، التشريع المصري.

### كيفية اقتباس البحث

الفارسي، قاسم محمد سعودي ، محسن ملك افضلى الاردكانى، الثغرات والتحديات التشريعية التي تواجه حماية البيانات الشخصية في التشريع العراقي والمصري، مجلة مركز بابل للدراسات الانسانية، تشرين الأول ٢٠٢٦، المجلد: ١٦، العدد: ١٠ .

هذا البحث من نوع الوصول المفتوح مرخص بموجب رخصة المشاع الإبداعي لحقوق التأليف والنشر ( Creative Commons Attribution ) تتيح فقط للآخرين تحميل البحث ومشاركته مع الآخرين بشرط نسب العمل الأصلي للمؤلف، ودون القيام بأي تعديل أو استخدامه لأغراض تجارية.

Registered في

**ROAD**

Indexed في

**IASJ**

## Legislative Gaps and Challenges Facing Personal Data Protection in Iraqi and Egyptian Legislation

**Qasim Mohammed Saudi Al-Farsi**

Department of Public Law, College of Law, University of Qom, Qom,  
Iran

**Mohsen Malik Afzali Ardakani**

University of Qom / Faculty of Law

**Keywords :** Gaps, challenges, personal data, Iraqi legislation, Egyptian legislation.

### How To Cite This Article

Al-Farsi, Qasim Mohammed Saudi, Mohsen Malik Afzali Ardakani, Legislative Gaps and Challenges Facing Personal Data Protection in Iraqi and Egyptian Legislation, Journal Of Babylon Center For Humanities Studies, October 2026, Volume:16, Issue 10.



This is an open access article under the CC BY-NC-ND license  
(<http://creativecommons.org/licenses/by-nc-nd/4.0/>)

[This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.](#)

### Abstract:

This research aims to analyze the adequacy of constitutional and legislative frameworks in Iraq and Egypt regarding the provision of effective legal protection for personal data. It seeks to identify key gaps and challenges facing such protection, highlight similarities and differences between the two systems, and evaluate the role of the judiciary and competent authorities in addressing legislative deficiencies and handling emerging digital violations. Additionally, the study aims to leverage the Egyptian experience to enhance the Iraqi legal framework. The research derives its significance from the contemporary nature of personal data protection and its direct link to the right to privacy, the protection of individual freedoms, and digital security. The core problem addressed is the adequacy of Iraqi and Egyptian legislation in confronting gaps and challenges arising from technological advancement, as well as their capacity to regulate the collection, processing, storage, transfer, and





disclosure of personal data and to provide effective means of countering digital violations. This issue is particularly acute in Iraq due to the lack of a comprehensive, specialized legislative framework and the fragmentation of protection measures across various legal provisions; in Egypt, the challenge lies in the effectiveness of implementing specialized legislation and its ability to keep pace with rapid technological developments. The study employs a comparative approach to contrast the legal frameworks for personal data protection in Iraq and Egypt and to identify points of convergence and divergence. It also utilizes a descriptive-analytical method to examine relevant constitutional and legislative texts. The research yields several findings, most notably a clear disparity between the two systems regarding the level of legislative regulation. Iraq still requires a specialized, comprehensive legislative framework that defines the concept of personal data, the rights of data subjects, and the obligations of data controllers; in contrast, Egyptian legislation offers a more specialized and clear regulatory structure, though there remains a need to enhance enforcement and oversight mechanisms to address technological advancements. The study also revealed that while constitutional protection of privacy and communications serves as a crucial foundation in both legal systems, it is insufficient on its own to counter modern digital infringements.

#### المخلص

يهدف البحث إلى تحليل مدى كفاية القواعد الدستورية والتشريعية في العراق ومصر في توفير حماية قانونية فعالة للبيانات الشخصية، والكشف عن أبرز الثغرات والتحديات التي تواجه هذه الحماية، وبيان أوجه الاتفاق والاختلاف بين النظامين، فضلاً عن تقييم دور القضاء والجهات المختصة في مواجهة النقص التشريعي والتعامل مع الاعتداءات الرقمية المستحدثة، والاستفادة من التجربة المصرية في تطوير الإطار القانوني العراقي. وتتبع أهمية البحث من حادثة موضوع حماية البيانات الشخصية وارتباطه المباشر بالحقوق في الخصوصية وحماية الحريات الفردية والأمن الرقمي، وتتمثل إشكالية البحث في مدى كفاية التشريعات العراقية والمصرية في مواجهة الثغرات والتحديات الناشئة عن التطور التكنولوجي، ومدى قدرتها على تنظيم عمليات جمع البيانات الشخصية ومعالجتها وتخزينها ونقلها والإفصاح عنها، وتوفير وسائل فعالة لمواجهة الاعتداءات الرقمية؛ إذ تبرز الإشكالية في العراق بصورة أكبر بسبب عدم اكتمال الإطار التشريعي المتخصص وتوزع الحماية بين نصوص قانونية متفرقة، بينما تتمثل في مصر في مدى فاعلية تطبيق التنظيم التشريعي المتخصص وقدرته على مواكبة التطورات التقنية المتسارعة. واعتمد البحث على المنهج المقارن لمقارنة التنظيم القانوني لحماية البيانات



الشخصية في العراق ومصر وتحديد أوجه الاتفاق والاختلاف بينهما، كما اعتمد على المنهج الوصفي التحليلي لتحليل النصوص الدستورية والتشريعية ذات الصلة، وقد توصل البحث إلى مجموعة من النتائج، أهمها وجود تفاوت واضح بين النظامين في مستوى التنظيم التشريعي؛ فالعراق ما زال بحاجة إلى إطار تشريعي متخصص ومتكامل يحدد مفهوم البيانات الشخصية وحقوق أصحابها والتزامات الجهات القائمة على معالجتها، في حين يمتلك التشريع المصري تنظيمًا أكثر تخصصًا ووضوحًا، مع استمرار الحاجة إلى تطوير آليات التطبيق والرقابة لمواجهة المستجدات التقنية. كما أظهرت الدراسة أن الحماية الدستورية للخصوصية والاتصالات تمثل أساسًا مهمًا في كلا النظامين، لكنها لا تكفي وحدها لمواجهة الاعتداءات الرقمية الحديثة.

### المقدمة

أدى التطور المتسارع في تكنولوجيا المعلومات والاتصالات والتحول المتزايد نحو البيئة الرقمية إلى جعل البيانات الشخصية من أهم العناصر التي تعتمد عليها المؤسسات الحكومية والخاصة في تقديم الخدمات وإدارة المعاملات واتخاذ القرارات، الأمر الذي أدى في الوقت ذاته إلى تزايد المخاطر التي تهدد خصوصية الأفراد وسلامة بياناتهم، نتيجة سهولة جمعها ومعالجتها وتخزينها ونقلها وتبادلها إلكترونيًا. وقد أفرز هذا التطور صورًا جديدة من الاعتداءات، كالوصول غير المشروع إلى البيانات، وتسريبها، وإساءة استخدامها، ومعالجتها دون سند قانوني، الأمر الذي جعل حماية البيانات الشخصية تمثل تحديًا تشريعيًا وقانونيًا متزايد الأهمية، يتطلب وجود قواعد واضحة ومتكاملة تواكب التطورات التقنية وتحقق التوازن بين مقتضيات التحول الرقمي من جهة، وحماية الحق في الخصوصية والحريات الفردية من جهة أخرى.

لذلك تتمثل مشكلة البحث في التساؤل عن مدى كفاية التشريعات العراقية والمصرية في مواجهة الثغرات والتحديات القانونية التي أفرزها التطور التكنولوجي في مجال حماية البيانات الشخصية، ومدى قدرة القواعد الدستورية والتشريعية القائمة على تنظيم عمليات جمع البيانات ومعالجتها وتخزينها ونقلها والإفصاح عنها، فضلًا عن مدى فاعلية الآليات القانونية في مواجهة الاعتداءات التي تتعرض لها البيانات الشخصية. الأمر الذي يثير التساؤل الرئيس الآتي: إلى أي مدى نجح التشريع العراقي والمصري في معالجة الثغرات والتحديات التشريعية التي تواجه حماية البيانات الشخصية وتوفير حماية قانونية فعالة للخصوصية الرقمية؟

وتتمثل أهمية البحث في كونه يتناول أحد الموضوعات القانونية الحديثة التي ترتبط بصورة مباشرة بحماية الحياة الخاصة والحقوق والحريات الفردية، ولا سيما مع التوسع في استخدام الوسائل الإلكترونية والأنظمة الرقمية في مختلف مجالات الحياة. كما تبرز أهميته



العلمية في تحليل مدى كفاية التنظيم القانوني لحماية البيانات الشخصية في العراق ومصر، والكشف عن أوجه القصور والثغرات التي قد تحد من فعالية هذه الحماية، فضلاً عن بيان أوجه الاتفاق والاختلاف بين النظامين القانونيين.

ويهدف البحث إلى بيان وتحليل الثغرات والتحديات التشريعية التي تواجه حماية البيانات الشخصية في التشريع العراقي والمصري، وتقييم مدى كفاية القواعد القانونية القائمة في توفير حماية فعالة للبيانات والخصوصية الرقمية، فضلاً عن تحديد أوجه القوة والقصور في التنظيم القانوني لكل من العراق ومصر.

كما اعتمد البحث على المنهج المقارن من خلال إجراء مقارنة بين التشريع العراقي والمصري في مجال حماية البيانات الشخصية، وبيان أوجه الاتفاق والاختلاف بينهما وتحديد مواطن القوة والقصور في كل نظام قانوني، كما تم الاعتماد على المنهج الوصفي التحليلي لتحليل النصوص الدستورية والتشريعية والقواعد القانونية ذات الصلة بحماية البيانات الشخصية والخصوصية الرقمية، وبيان مدى ملاءمتها للتطورات التقنية الحديثة.

### المبحث الأول: غياب وقصور التشريع الخاص

يُعدّ غياب أو قصور التشريع الخاص بحماية البيانات الشخصية من أبرز التحديات التي تواجه ضمان الخصوصية الرقمية، ولا سيما في ظل التطور المتسارع في وسائل جمع البيانات ومعالجتها وتخزينها.

**المطلب الأول: القصور التشريعي والمؤسسي في حماية البيانات الشخصية في العراق ومصر**  
تواجه حماية البيانات الشخصية في كل من العراق ومصر تحديات كبيرة على الصعيد التشريعي والمؤسسي حيث أن التطور التكنولوجي السريع لم يواكبه دائماً إطار قانوني متكامل مما أدى إلى وجود ثغرات تشريعية وأطر تنظيمية غير مكتملة وتتمثل هذه الثغرات والتحديات في عدة مستويات تشمل التشريعات النافذة، والهيكل المؤسسية وآليات الرقابة والتنفيذ وهو ما يحد من قدرة الحكومات على فرض سيادتها على البيانات الشخصية للمواطنين والمنظمات الخاصة بشكل فعال فلا يوجد حتى الآن قانون شامل يحكم حماية البيانات الشخصية على مستوى الدولة الاتحادية إذ تقتصر القوانين النافذة على بعض النصوص الجزئية في قانون أصول المحاكمات الجزائية وقوانين مكافحة الجرائم الإلكترونية وإساءة استخدام الهواتف المحمولة والإنترنت ويقتصر دور هذه النصوص على تنظيم حالات محددة مثل الرقابة على المراسلات والمكالمات الهاتفية بموجب أوامر قضائية دون تحديد شامل للحقوق والالتزامات المتعلقة بمعالجة البيانات الشخصية من قبل الجهات الحكومية أو الخاصة<sup>1</sup>. ويؤدي هذا النقص التشريعي إلى ظهور عدة ثغرات من





أبرزها:

١. غياب هيئة مركزية مستقلة لمراقبة ومعالجة البيانات الشخصية، مما يحد من قدرة الرقابة على منع الانتهاكات، وغياب تعريف واضح للبيانات الشخصية وأنواعها، مما يترك المجال واسعاً لتأويل السلطة القضائية أو الجهات التنفيذية عند التعامل مع الانتهاكات. فعدم وجود نصوص صريحة لتطبيق العقوبات على الجهات الخاصة التي تساء استخدام البيانات وبالتالي تقتصر الإجراءات على الأفراد فقط. وضعف حماية الأطفال والمراهقين من المخاطر الرقمية مثل التعرض للمحتوى الضار أو إساءة استخدام البيانات الشخصية عبر الإنترنت، وهو ما يشير إلى قصور واضح في التغطية التشريعية.<sup>٢</sup>

ورغم وجود قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠ في مصر وإنشاء الهيئة الوطنية للبيانات الشخصية، إلا أن التطبيق العملي للقانون يواجه تحديات كبيرة، أبرزها:

١. ضعف البنية التحتية المؤسسية للهيئة الوطنية، خاصة فيما يتعلق بالرقابة التقنية على معالجة البيانات في المؤسسات الخاصة. والافتقار إلى التعاون بين الجهات الحكومية المختلفة مثل النيابة العامة ووزارة الاتصالات والجهات الرقابية، مما يؤدي إلى بطء معالجة الانتهاكات.

٣ تحديات التنفيذ الرقمي والقضائي عند التعامل مع الجرائم الإلكترونية العابرة للحدود، إذ تتطلب الجرائم الإلكترونية مثل الاحتيال المالي أو الابتزاز الرقمي تعاوناً دولياً وإجراءات قضائية معقدة. وعدم التوازن بين حماية الخصوصية والحق في الأمن القومي، حيث تترك بعض المواد القانونية هامشاً واسعاً للحكومة للتدخل في البيانات الشخصية بذريعة الأمن القومي، وهو ما قد يشكل تهديداً للحقوق الفردية إذا لم يتم ضبطه بمعايير واضحة.

ويشترك العراق ومصر في العديد من التحديات المتعلقة بحماية البيانات الشخصية، ومن أبرزها:

١. التطور السريع للتكنولوجيا بالمقابل البطء النسبي في تحديث التشريعات، مما يجعل بعض الجرائم الإلكترونية الجديدة خارج نطاق النصوص القانونية. والجرائم العابرة للحدود التي تتطلب تعاوناً دولياً ومتابعة دقيقة، وهو ما يعاني منه العراق بشكل خاص بسبب ضعف التشريعات الدولية المطبقة على الجرائم السيبرانية. ونقص التدريب والخبرة الفنية للقضاة والهيئات الرقابية في مجال الجرائم الإلكترونية والتحقيقات الرقمية، مما يقلل من فعالية تطبيق القانون<sup>٣</sup>، وغياب التوعية العامة بحقوق البيانات الشخصية لدى المواطنين، مما يؤدي إلى عدم قدرتهم على المطالبة بحقوقهم أو الإبلاغ عن الانتهاكات.

ولتحسين الإطار القانوني وحماية البيانات الشخصية في العراق ومصر لابد من إنشاء هيئة مركزية مستقلة في العراق على غرار الهيئة الوطنية للبيانات الشخصية في مصر لمراقبة

المعالجة والإشراف على جميع الجهات الحكومية والخاصة وتحديث التشريعات الوطنية بشكل دوري لمواكبة التطورات التكنولوجية، مع وضع تعريفات دقيقة للبيانات الشخصية وحقوق الأفراد المتعلقة بها. وتعزيز التعاون بين السلطات القضائية والهيئات التنفيذية والمجتمع المدني لضمان فعالية الرقابة على استخدام البيانات وتنظيم برامج تدريبية للقضاة والجهات الرقابية في مجالات التحقيق الرقمي والجرائم الإلكترونية وتوعية المواطنين بحقوقهم وواجباتهم فيما يتعلق بالبيانات الشخصية لضمان المشاركة الفعالة في حماية خصوصيتهم.

يُعد غياب أو قصور التشريع الخاص بحماية البيانات الشخصية من أبرز التحديات التي تواجه الحكومات في العراق ومصر، حيث أن التطور التكنولوجي السريع واستخدام الإنترنت والوسائل الرقمية في جمع ومعالجة البيانات الشخصية لم يُواكب دائما بتشريعات واضحة وشاملة مما أدى إلى ثغرات قانونية تؤثر على حماية خصوصية الأفراد وضمان سيادة الحكومة على البيانات فلا يوجد حتى الآن قانون شامل ينظم معالجة البيانات الشخصية على مستوى الدولة الاتحادية، فالنصوص النافذة تتوزع على قوانين مختلفة مثل قانون أصول المحاكمات الجزائية رقم ٢٣ لسنة ١٩٧١، وقانون مكافحة جرائم المعلوماتية، وقانون منع إساءة استخدام الهواتف المحمولة والإنترنت في إقليم كردستان رقم ٦ لسنة ٢٠٠٨، ويترتب على هذا النقص التشريعي العديد من المشكلات العملية، منها:

١. غياب حماية شاملة للبيانات الشخصية، إذ تركز النصوص الحالية على بعض الإجراءات الجزئية مثل مراقبة المكالمات الهاتفية والرسائل الإلكترونية بأمر قضائي دون تنظيم واضح لمعالجة البيانات في المؤسسات الحكومية أو الخاصة.

٢. عدم تحديد أنواع البيانات الشخصية والبيانات الحساسة، مما يترك المجال واسعا لتأويل السلطة التنفيذية والقضائية عند التعامل مع الانتهاكات المحتملة.

٣. غياب العقوبات الواضحة على الجهات الخاصة التي تسيء استخدام البيانات، حيث تقتصر الجزاءات غالبا على الأفراد المتسببين في الانتهاكات.

٤. ضعف الإطار المؤسسي الرقابي، إذ لا توجد هيئة مركزية مستقلة تعنى بمراقبة ومعالجة البيانات الشخصية، ما يحد من قدرة الحكومة على ممارسة سيادتها بشكل فعال<sup>٤</sup>.

أما في مصر، فقد تم إصدار قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠ وإنشاء الهيئة الوطنية للبيانات الشخصية وهو تقدم ملحوظ مقارنة بالوضع العراقي إلا أن التشريع المصري يعاني من عدة نقاط ضعف تشريعية وتطبيقية منها ضعف البنية التحتية المؤسسية للهيئة، خاصة في مجال الرقابة التقنية على معالجة البيانات لدى الجهات الخاصة ما يحد من

فاعلية تطبيق القانون. وتداخل بعض النصوص مع قوانين أخرى مثل قانون حماية المستهلك وقانون مكافحة جرائم المعلوماتية، مما يؤدي إلى غموض في تحديد المسؤوليات والسلطات عند وقوع الانتهاكات والتحديات التنفيذية في الجرائم الإلكترونية العابرة للحدود، إذ أن النصوص الحالية لا تكفل تعاوناً دولياً فعالاً مع الدول الأخرى لمعالجة الجرائم المتعلقة بالبيانات.<sup>٥</sup>

والافتقار إلى نصوص واضحة لحماية الأطفال والشباب من المخاطر الرقمية مثل المحتوى الضار أو إساءة استخدام البيانات الشخصية على الإنترنت على الرغم من وجود إشارات عامة في القانون لحماية الفئات الضعيفة وإن غياب التشريع الخاص يؤثر مباشرة على قدرة الحكومة على ممارسة سيادتها على البيانات الشخصية للمواطنين والمنظمات الخاصة، حيث يؤدي إلى<sup>٦</sup>:

١. تفاوت مستوى الحماية بين الجهات الحكومية والخاصة، إذ قد تستغل بعض الجهات الخاصة البيانات دون رقابة فعالة، بينما تلتزم الجهات الحكومية جزئياً بالمعايير القانونية.
٢. زيادة المخاطر على الخصوصية وحرية الأفراد، إذ يصبح المواطنون أقل قدرة على التحكم في بياناتهم أو رفع دعاوى ضد الانتهاكات.
٣. ضعف ثقة المجتمع في استخدام الخدمات الرقمية، بما يشمل المؤسسات الحكومية والخاصة، مما يحد من الاستفادة الكاملة من التحول الرقمي والتنمية التكنولوجية.

ومن ثم، يتضح أن غياب أو قصور التشريع الخاص يعد من أكبر العقبات أمام ضبط وحماية البيانات الشخصية وضمان ممارسة الحكومة لسيادتها القانونية والتنظيمية على هذه البيانات في كلا البلدين.

### المطلب الثاني: صور الاعتداء على البيانات الشخصية وقصور الحماية القانونية

فقد شهدت السنوات الأخيرة توسعاً كبيراً في استخدام الشبكات الاجتماعية والمنصات ومواقع التسوق الإلكترونية، الأمر الذي أدى إلى إمكانية جمع معلومات شخصية عن الأفراد تتجاوز بكثير المعلومات التي يحتفظون بها بأنفسهم خارج الإنترنت بالطرق التقليدية وتمثل هذه المواقع مصدراً أساسياً لجمع البيانات الشخصية، بما في ذلك تتبع المواقع التي زارها المستخدم مسبقاً عبر بروتوكول الإنترنت (IP) وملفات تعريف الارتباط (Cookies) مما يزيد من تعقيد حماية الخصوصية الرقمية كما يتيح الاستخدام المتزايد للإنترنت في الاتصالات ومخازن البيانات الرقمية فرصاً أكبر لاعتراضها وانتهاك خصوصيتها، بما في ذلك استهداف ما يُعرف بمستودعات الأسرار الإلكترونية حيث تخزن البيانات الشخصية بشكل مركزي، ما يجعلها عرضة للاختراق وقد أشار الفقهاء إلى أن العقول الإلكترونية تستطيع جمع أكبر قدر ممكن من المعلومات الشخصية ودمجها وتنظيمها لتكوين صورة متكاملة عن الفرد وهو ما يشكل تهديداً

ملموساً على الحياة الخاصة الرقمية للأشخاص<sup>٧</sup>.

أولاً: جمع المعلومات الشخصية عن طريق استخدام تقنيات الإنترنت: تقوم معظم المواقع الإلكترونية بما في ذلك مواقع العلاقات الاجتماعية ومواقع البريد الإلكتروني، والتسوق بجمع بيانات المستخدمين مباشرة مثل الاسم واللقب والعمر والمستوى التعليمي والحالة الاجتماعية وأرقام البطاقات الائتمانية، وأحياناً بيانات حساسة أخرى مثل الموقع الجغرافي واهتمامات المستخدم<sup>٨</sup>، كما تجمع بعض البيانات تلقائياً عند تصفح الإنترنت، مثل عنوان الكمبيوتر (IP)، ونوع المتصفح، ووقت وتاريخ زيارة المواقع، ووقت الاتصال بالشبكة، مما يمثل تهديداً للخصوصية الرقمية إذا لم يتم تنظيم هذه الممارسات قانونياً حيث ينص الدستور العراقي على حماية الخصوصية والاتصالات في المادتين (١٧) و(٤٠)<sup>٩</sup>، بما يشمل بيانات المستخدمين على الإنترنت، لكنه يفتقر إلى تشريع موحد يحدد حقوق الأفراد والتزامات الجهات التي تجمع البيانات، بينما جاء قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠ ليضع إطاراً واضحاً لمعالجة البيانات الشخصية وحماية الخصوصية الرقمية، بما يتوافق مع المعايير الدولية للأمم المتحدة والاتحاد الأوروبي<sup>١٠</sup>.

ثانياً: ملفات تعريف الارتباط (Cookies): ان ملفات الكوكيز هي ملفات نصية يرسلها خادم الموقع إلى جهاز المستخدم لتخزين بيانات شخصية تتعلق بالمستخدم وجهازه بما في ذلك عنوان الإنترنت وطريقة الاتصال والمواقع التي تم زيارتها ونوع الجهاز والمعالج والبيانات المدخلة في استمارات التسجيل و تستخدم هذه الملفات لتسهيل استخدام المواقع، لكن الاحتفاظ بها وسرقتها يمكن أن يسهل اختراق الحسابات الشخصية والصفحات المدارة عبر الإنترنت، بما يشكل تهديداً للخصوصية الرقمية<sup>١١</sup>.

ثالثاً: البريد غير المرغوب فيه (Spam): ويشكل البريد الإلكتروني غير المرغوب فيه تهديداً للخصوصية الرقمية إذ غالباً ما يكون مجهول المرسل ويستهدف أعداداً كبيرة من المستلمين ويتضمن أحياناً برمجيات خبيثة كما يتم الحصول على عناوين البريد من مجموعات الدردشة والإعلانات على الإنترنت، ما يؤدي إلى تلوث الشبكات والملفات الرقمية.

رابعاً: فقدان البيانات الشخصية: ان جمع البيانات الشخصية وإنشاء قواعد بيانات لها يزيد من احتمالية فقدانها أو تعرضها للاختراق. فمثلاً، فقدت إحدى الشركات في فرنسا عام ٢٠٠٦ أسطوانة تحتوي على بيانات ٩٠٠٠ عامل، بينما تشير الإحصاءات إلى فقدان ١٦٢ مليون ملف شخصي عام ٢٠٠٧ مقارنة بـ ٤٩ مليون ملف عام ٢٠٠٥. وتتعدد صور الاعتداء على البيانات الشخصية لمستخدمي شبكات التواصل الاجتماعي، ومن أبرزها:

١. الاختراق الإلكتروني للحسابات واستخدام البيانات الشخصية لأغراض تجارية أو دعائية.
  ٢. استغلال ملفات الكوكيز لمتابعة سلوك المستخدم وتوجيه الإعلانات له.
  ٣. التصيد الاحتيالي والرسائل المزعجة التي تهدد أمان المستخدم وشبكة الاتصالات.
  ٤. فقدان البيانات نتيجة سوء التخزين أو الهجمات الإلكترونية على قواعد البيانات.
- ويشترط قانون حماية البيانات الشخصية، وفق المادة السابعة، ألا يتم جمع أو معالجة أي بيانات شخصية إلا بموافقة صريحة من صاحب البيانات، ما يُعرف بمبدأ الرضا الحر<sup>١٢</sup>، وقد برزت حالات اعتداء على الخصوصية الرقمية نتيجة جمع البيانات دون رضا المستخدم، مثل قضية شركة جوجل "جوجل ستريت فيو" في عامي ٢٠٠٩ و ٢٠١٠، حيث جمعت الشركة بيانات حساسة تتعلق بالمحتوى الشخصي للمستخدمين، بما في ذلك كلمات المرور ورسائل البريد الإلكتروني عبر شبكات الواي فاي، ما أدى إلى فرض غرامة مالية قدرها ١٠٠ ألف يورو من قبل اللجنة القومية للمعلوماتية والحريات في فرنسا، وتعهدت جوجل بالتخلص من البيانات المخزنة كما اعتبرت محكمة النقض الفرنسية أن جمع عناوين البريد الإلكتروني دون علم أصحابها يعد جمعاً غير مشروع للبيانات الشخصية ويستحق العقوبة، حتى لو لم يتم الاحتفاظ بهذه العناوين ومن أبرز القضايا في هذا السياق قضية Google, Inc . FTC، المتعلقة بوضع ملفات كوكيز على متصفح Safari، مما مكن الشركة من تتبع نشاط المستخدمين دون علمهم، لتحقيق أهداف تجارية وإعلانية، وانتهت القضية بتسوية خارج المحكمة بدفع جوجل غرامة قدرها ٢٢.٥ مليون دولار<sup>١٣</sup>.
- وينص القانون على ضرورة أن يكون جمع البيانات الشخصية لغرض محدد وشرعي، وفق المادة ٦/٢ من قانون حماية البيانات الشخصية، ويجب أن تحقق المصلحة المشروعة<sup>١٤</sup> وتعد البيانات الشخصية عنصراً رئيسياً في الإعلانات الرقمية والتسويق الإلكتروني، حيث يتم بيع بيانات المستخدمين لشركات الإعلانات بهدف إعداد قواعد بيانات تحدد احتياجاتهم ورغباتهم، وهو ما يعرف بـ بروفایل العميل ويزداد الخطر عندما يقدم المستخدم بياناته طوعية على شبكات التواصل الاجتماعي، مثل فيسبوك وماي سبيس دون وعيه الكامل بإعادة استخدام هذه البيانات لأغراض تجارية، وتنظيمها ونشرها دون تمكين صاحب البيانات من ممارسة حقوقه عليها.
- وقد أكدت محكمة النقض الفرنسية أن بيع بيانات المستخدمين لمعلنين يمثل جمع بيانات شخصية غير مشروع، وهو ما دفع اللجنة القومية للمعلوماتية والحريات إلى مطالبة فيسبوك بإعلام المستخدمين بكافة ملفاتهم الشخصية، بما في ذلك الآراء السياسية والدينية كما يتم جمع البيانات الشخصية عبر الإنترنت عن طريق ملفات الكوكيز، التي تخزن على جهاز المستخدم

و تُرسل إلى مواقع تجارية لإرسال عروض دعائية تستهدف المستخدم بناءً على اهتماماته وسلوكه الرقمي، وهو ما يشكل انتهاكاً للخصوصية الرقمية إذا لم يكن الهدف مشروعاً وواضحاً حيث ان غياب تشريع محدد في العراق يحظر استخدام البيانات الشخصية لأغراض تجارية دون موافقة المستخدم يعرض الأفراد لانتهاكات محتملة على شبكة الإنترنت.<sup>١٥</sup>

ووفق المادة ٣٤ من قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠، يلتزم من يجمع البيانات الشخصية أو يعالجها باتخاذ كافة الاحتياطات اللازمة لضمان أمن البيانات ومنع أي تغيير أو إتلاف لها من قبل أشخاص غير مخولين<sup>١٦</sup>، وتعد قواعد البيانات المتصلة بالإنترنت هدفاً سهلاً للقراصنة الذين يستخدمون أساليب متطورة مثل ملفات التجسس وبرامج الاختراق للوصول إلى المعلومات الشخصية للمستخدمين<sup>١٧</sup>، بما في ذلك البريد الإلكتروني والصفحات الشخصية، مما يمثل اعتداء صارخاً على خصوصية الفرد ويمكن للاختراق أن يؤدي أيضاً إلى انتهاك حرمة الشرف والاعتبار عبر الإنترنت، من خلال نشر محتوى خاص بالفرد أو استخدام بياناته الشخصية للتهديد والابتزاز، ويشمل ذلك الصور أو محتوى رسائل البريد الإلكتروني.<sup>١٨</sup>

أما عن التشهير الرقمي يعني نشر وقائع أو بيانات تمس سمعة الفرد أو كرامته، ويُعد انتهاكاً لحقه في الخصوصية، خصوصاً عند نشر هذه المعلومات عبر الشبكات الاجتماعية، وهو ما يشكل سبباً لإقامة دعاوى مدنية على أساس المسؤولية التقصيرية.<sup>١٩</sup>

وان الابتزاز الرقمي يحدث عندما يهدد شخص بنشر معلومات أو صور شخصية للحصول على مكاسب مادية أو معنوية ومن الأمثلة الواقعية في الولايات المتحدة، قضية State v. Noll في ولاية إنديانا، حيث هدد الجاني بنشر صور جنسية فاضحة للضحية إذا لم تلب طلباته، وأيدت المحكمة اعتبار ذلك تهديداً مجرماً وفق قانون ولاية إنديانا<sup>٢٠</sup>، وفي مصر، يواجه القانون تحديات في معاقبة الابتزاز الإلكتروني إذا كان التهديد شفاهة مباشرة، إذ ينص قانون العقوبات المصري، المادة ٣٢٧ على أن التهديد يجب أن يكون كتابة أو عن طريق شخص آخر لتطبيق العقوبة ما يترك ثغرة قانونية في حماية الضحايا من الابتزاز الرقمي<sup>٢١</sup>، أما في العراق، ورغم ضمان الدستور للخصوصية في المواد ١٧ و ٤٠، إلا أن غياب تشريع محدد للجرائم الرقمية يجعل متابعة الابتزاز والتشهير عبر الإنترنت تحدياً كبيراً، خصوصاً مع استخدام تقنيات متطورة للاختراق الرقمي<sup>٢٢</sup>. أما اعتراض الاتصالات فيعني الاستحواذ على محتوى المحادثات أو الاتصالات الرقمية دون موافقة الطرفين، وهو انتهاك للخصوصية الرقمية وتستخدم في ذلك أساليب متقدمة مثل التنصت على المكالمات الهاتفية أو رسائل الإنترنت، بما يوازي التطور

التقني في مجالات الاتصال الرقمي<sup>٢٣</sup>.

ومن الأمثلة الدولية على ذلك: برنامج Carnivore الذي طوّره وكالة التحقيقات الفيدرالية الأمريكية (FBI) للتجسس على الاتصالات الرقمية. وشبكة Echelon العالمية للتجسس التي أسستها وكالة الأمن القومي الأمريكية (NSA) بالتعاون مع جهات استخباراتية أوروبية، والتي تستهدف كافة أنواع الاتصالات الرقمية، سواء السلكية أو اللاسلكية أو عبر الأقمار الصناعية.

حيث ان انتهاك الحق في الخصوصية الرقمية والتجسس على الاتصالات يتعارض مع المبادئ الدولية لحقوق الإنسان، خاصة مع ما ورد في إعلان الأمم المتحدة بشأن الخصوصية الرقمية<sup>٢٤</sup>، الذي أكد على ضرورة حماية الاتصالات الرقمية ومنع التدخل التعسفي فيها<sup>٢٥</sup>، وأن استخدام الاسم عبر الشبكات أمر لا غنى عنه لإجراء المعاملات المختلفة من إنشاء حسابات خاصة وتسوق وغيرها، ولهذا يقتضي الأمر حمايته من كافة صور الاعتداء عليه ولأهمية الاسم كأحد الحقوق للصيقة بالشخصية، أولاه المشرع حماية قانونية خاصة به في القانون المدني بالمادة ٥١، والتي تنص على أن لكل من نازعه الغير في استعمال اسمه بلا مبرر، ومن انتحل الغير اسمه دون حق، أن يطلب وقف هذا الاعتداء مع التعويض عما يكون قد لحقه من ضرر وبالتالي تكون صور الاعتداء على الحق في الاسم هما المنازعة والانتحال<sup>٢٦</sup>.

والمنازعة تعني اعتراض شخص من الغير على تسمية الشخص باسمه، أي إنكاره استعماله لهذا الاسم، ويتضح ذلك في الشركات التي تقدم الخدمات الإلكترونية عبر الشبكة مثل البريد الإلكتروني، الصفحات الشخصية في مواقع التواصل الاجتماعي أو خدمات تسجيل الدومين لمواقع مرتبطة بنشاط المستخدم، إذ يعتبر اعتراض الشركات على استخدام الاسم في الدومين أو البريد الإلكتروني أو اسم المستخدم نوعاً منازعة في الاسم<sup>٢٧</sup>، أما الانتحال فيقصد به استعمال الاسم بشكل غير مشروع من جانب الغير، بالتسمي به في مواجهة الناس دون مبرر وفي هذه الحالة شائعة على مواقع شبكات التواصل الاجتماعي، وقد تترافق مع الاختراق للصفحة الشخصية، حيث يستخدم المخترق اسم الشخص للسب أو القذف أو الابتزاز، مما يسبب أضراراً جسيمة للشخص صاحب الاسم<sup>٢٨</sup>، وبخصوص نشر الفيديوهات عبر وسائل التواصل الاجتماعي، فإن ذلك يعد انتهاكاً للحق في الصورة في العالم الافتراضي، كما ورد في قضية بتصوير Dharun Ravi حيث قام الطالب The State of New Jersey vs Dharun Ravi زميل له عبر كاميرا الويب ونشر الفيديو على الإنترنت مما أدى إلى أضرار جسيمة للضحية وانتحارها، وأدانت المحكمة انتهاك الخصوصية<sup>٢٩</sup>.

أما تجميع البيانات الشخصية لحساب الدولة، فيجوز وفق القانون الفرنسي بعد الحصول على

ترخيص رسمي، سواء لمعالجة البيانات المتعلقة بأمن الدولة أو منع الجرائم الجنائية، أو التعامل مع بيانات حساسة مثل الأصل العرقي أو الحالة الصحية أو البيانات البيومترية، وإلا يعتبر التجميع غير مشروع ويعاقب عليه بالسجن والغرامة<sup>٣٠</sup>، وبذلك يتضح أن الدول أو الحكومات قد ترتكب اعتداءات على البيانات الشخصية من خلال التنصت واعتراض الاتصالات، التجسس أو حتى بالتعاون مع الشبكات مما يجعل المسؤولية مشتركة بين الجهات الحكومية والشركات المشغلة للخدمات الرقمية أما عن الجرائم المتعلقة بالبيانات الشخصية المعالجة إلكترونياً، فإن الحماية الجزائية لحرمة الحياة الخاصة في عصر تقنية المعلومات الحديثة شهدت تطوراً في نطاقها ومشتملاتها، وأصبح من الضروري توفير الحماية الجنائية لحرمة الحياة الخاصة من صور الاعتداء التي تمس البيانات الشخصية للأفراد. ولتحقيق ذلك، يجب تحديد ماهية المعلومات والبيانات التي تعرض خصوصية الأفراد للانتهاك ضمن مجتمع المعلومات الإلكترونية<sup>٣١</sup>، يجري التمييز بين المعلومات المجهولة التي لا تدل ولا يستدل منها على شخص معين، فهي لا تتمتع بخصوصية. والمعلومات القابلة للتعرف على الشخص التي تسمح بالتصرف على شخص معين، وقد تكون معلومات موضوعية مثل الاسم الموطن الحالة المدنية الوظيفة العقوبات التي تعرض لها الشخص، فهي من مميزات الشخصية. ومعلومات ذاتية تحمل رأياً شخصياً عن الغير. وفي الغالب تتعلق المعلومات الموضوعية والذاتية بالحياة العامة للأفراد، غير أن المعلومات الاسمية المخزنة في بنوك المعلومات تمس حرمة الحياة الخاصة للأفراد، وتعرف البيانات الاسمية بأنها البيانات الشخصية المتعلقة بحرمة الحياة الخاصة للفرد، مثل حالته الصحية المالية الوظيفية المهنية، والعائلية عند معالجتها إلكترونياً.

وتبرز خطورة تقنيات المعلومات الحديثة على حرمة الحياة الخاصة عند جمع البيانات الاسمية تخزينها، تشغيلها، أو استخراجها من ذاكرة النظام وإيصالها للغير، سواء كانت جهة حكومية أو غير حكومية، أو شخصاً طبيعياً. ومن ثم تقع جريمة التخزين غير المشروع للبيانات الشخصية متى تم ذلك دون رضا صاحبها أو لاستخدامها لأغراض غير مخصصة لها.<sup>٣٢</sup>

وتتحقق هذه الجريمة حتى إذا كانت الحكومات هي من قامت بأفعال التخزين للبيانات الشخصية، ما دام ذلك دون سند قانوني أو خارج الحالات المصرح بها قانونياً، أو دون أمر قضائي إلا أن التخزين يكون مشروعاً إذا تم وفق القانون أو لمقتضيات الصالح العام، كما هو الحال في الدول التي تطبق الحكومة الإلكترونية بموجب قوانين نافذة.<sup>٣٣</sup>

فيما يخص التشريع العربي، ينص القانون العراقي رقم ٣٠ لسنة ٢٠١٩ بشأن حماية البيانات الشخصية على وجوب الحصول على موافقة صريحة من صاحب البيانات قبل أي معالجة أو

تخزين، ويعاقب على التخزين أو الإفشاء غير المشروع للبيانات الشخصية بالسجن وغرامات مالية<sup>٣٤</sup>، أما القانون المصري رقم ١٥١ لسنة ٢٠٢٠ فيلزم كل جهة تقوم بمعالجة البيانات الإلكترونية باتخاذ التدابير اللازمة لحمايتها ويجرم الإفشاء أو الاستخدام غير المشروع للبيانات الشخصية<sup>٣٥</sup>.

أما عن أركان جريمة التخزين غير المشروع فمنها: الركن الأول: محل الجريمة البيانات الشخصية، الركن المادي: حفظ أو تخزين البيانات على نحو غير مشروع باستخدام وسائل تقنية غير مشروعة أو معالجة بيانات يحظر القانون معالجتها، والركن المعنوي القصد الجنائي القائم على العلم والإرادة، بحيث يعلم الجاني بالطبيعة الشخصية للبيانات وعدم مشروعية تخزينها وتنتج إرادته لحفظها أو تخزينها خلافاً للقانون<sup>٣٦</sup>.

أما عن جريمة المعالجة الإلكترونية للبيانات الشخصية دون ترخيص، فتقع هذه الجريمة عندما يقوم المسؤول عن معالجة البيانات بمعالجتها في غير الأحوال المصرح بها قانونياً، أو بعد انتهاء الترخيص الممنوح<sup>٣٧</sup>. فالركن المادي المعالجة الإلكترونية للبيانات الشخصية دون التقيد بالإجراءات القانونية، وتشمل جميع أشكال المعالجة حتى وإن كان الخطأ غير عمدي.

الركن المعنوي: القصد الجنائي أو الخطأ غير العمدى، بحيث يعلم الجاني بأن المعالجة تتم دون ترخيص وأنه ينتهك القانون، وعن جريمة تجاوز الغرض من المعالجة، فتتطلب هذه الجريمة وجود الركن المادي: استغلال البيانات الشخصية بما يتجاوز الغاية المصرح بها قانونياً، مثل الكشف عن مصادر ثروة صاحب البيانات أو معلومات خاصة بحياته الشخصية، الركن المعنوي القصد الجنائي العام، بمعرفة الجاني بأن فعله انحرف عن الغرض القانوني للمعالجة مع عدم اعتبار البواعث أو الأهداف التي دفعت الجاني لارتكاب الفعل<sup>٣٨</sup>.

وفيما يتعلق بالإطار القانوني في العراق ومصر، يُنظم قانون حماية البيانات العراقي (٢٠١٩) هذه الجرائم ويعاقب عليها بالسجن والغرامات المالية، بينما القانون المصري رقم ١٥١ لسنة ٢٠٢٠ يعاقب على تجاوز الغاية من معالجة البيانات، مؤكداً ضرورة الالتزام بالغرض المحدد للمعالجة الإلكترونية<sup>٣٩</sup>.

### المبحث الثاني: دور القضاء في سد النقص التشريعي

يؤدي القضاء دوراً مهماً في سد النقص التشريعي المتعلق بحماية البيانات الشخصية، من خلال تفسير النصوص القائمة وتطبيقها على المستجدات الرقمية بما يكفل حماية الخصوصية. وتبرز أهمية هذا الدور في العراق ومصر في تحقيق التوازن بين حقوق الأفراد ومتطلبات الأمن والمصلحة العامة في ظل التطور المتسارع للجرائم الإلكترونية.

### المطلب الأول: الدور التفسيري والرقابي للقضاء في حماية البيانات الشخصية

يُعد القضاء أحد الأعمدة الرئيسية في حماية البيانات الشخصية وحفظ الحقوق الرقمية للمواطنين في ظل غياب أو قصور التشريعات الخاصة، إذ يلعب دوراً تكميلياً في سد الثغرات القانونية وتفسير النصوص النافذة بما يحقق التوازن بين حماية الخصوصية وممارسة الحكومة لسيادتها على البيانات.

وفي العراق فإن غياب قانون شامل لحماية البيانات الشخصية يجعل القضاء يعتمد على مجموعة من النصوص الجزئية، أبرزها قانون أصول المحاكمات الجزائية رقم ٢٣ لسنة ١٩٧١، وقانون مكافحة جرائم المعلوماتية، إضافة إلى القانون رقم ٦ لسنة ٢٠٠٨ في إقليم كردستان بشأن منع إساءة استخدام الهواتف المحمولة والإنترنت حيث يقوم القضاء العراقي بتفسير النصوص الجزئية بما يتوافق مع مبادئ حماية البيانات الشخصية فعلى سبيل المثال، يستخدم القاضي نص المادة ٧٤ من قانون أصول المحاكمات الجزائية لإصدار أوامر مراقبة المكالمات الهاتفية أو الاطلاع على المراسلات عندما يكون هناك دلائل قوية على وقوع جريمة مع مراعاة التوازن بين حق الفرد في الخصوصية ومتطلبات التحقيق الجنائي.<sup>٤٠</sup>

وسد الثغرات في الجرائم الرقمية، إذ يلجأ القضاء إلى توسيع مفهوم "الأدلة الرقمية" واعتبارها جزءاً من الأدلة المادية، رغم عدم وجود نص صريح يشمل هذه البيئة الإلكترونية وذلك لضمان تطبيق القانون على الجرائم المعلوماتية والرقابة على الإجراءات الحكومية والخاصة، من خلال التأكد من أن الجهات التي تقوم بمعالجة البيانات الشخصية تتقيد بالمبادئ العامة للعدالة وحرية الأفراد، مع استثناء الحالات التي تقتضيها الضرورة الأمنية أو القانونية.<sup>٤١</sup>

أما في مصر، مع صدور قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠ وإنشاء الهيئة الوطنية للبيانات الشخصية، يلعب القضاء دوراً رقابياً وتفسيرياً أيضاً، من حيث تفسير القانون بما يوازن بين حماية الخصوصية وحرية تداول المعلومات إذ تصدر المحاكم أحكاماً تحدد نطاق السلطة المخولة للهيئة الوطنية وللجهات الخاصة عند معالجة البيانات الشخصية، مع مراعاة الحقوق الدستورية للأفراد<sup>٤٢</sup> وسد الثغرات المتعلقة بالجرائم الإلكترونية العابرة للحدود، حيث يعتمد القضاء المصري على اتفاقيات التعاون الدولي في التحقيق وملاحقة الجناة عند وجود نقص في النصوص الوطنية، مما يعكس مرونة القضاء في مواجهة تحديات التحول الرقمي.<sup>٤٣</sup>

وحماية الفئات الضعيفة، بما في ذلك الأطفال والشباب، من خلال إصدار أحكام قضائية تفرض قيوداً على نشر المحتوى الضار أو استخدام البيانات الشخصية بطرق تعرض هذه الفئات للخطر رغم أن القانون الجديد لا يحتوي على نصوص تفصيلية لكل المخاطر المحتملة، حيث يلعب

القضاء دوراً محورياً في تعزيز سيادة الحكومة على البيانات الشخصية من خلال تحديد نطاق السلطة المخولة للجهات الحكومية والخاصة، بما يقلل من الانتهاكات ويضمن التزام المؤسسات بالمعايير القانونية والأخلاقية وضمان المساواة القانونية، حيث يمكن للمتضررين رفع دعاوى أمام القضاء عند تعرض بياناتهم الشخصية للتسريب أو سوء الاستخدام وتوفير قاعدة سابقة للأحكام القضائية وتساعد على تفسير النصوص المستقبلية وتطوير التشريعات بما يتماشى مع التطورات التكنولوجية وهو ما يعكس وظيفة القضاء التكميلية في سد النقص التشريعي وتحقيق التوازن بين مصالح الدولة وحماية حقوق الأفراد. ويكفل الدستور حرمة المراسلات والاتصالات ويقرر حمايتها، إلا أن هذه الحرمة ليست مطلقة، فكفالة الحق في سرية المراسلات والاتصالات لا تعني التضحية بحق المجتمع، بل يجب تحقيق التوازن بين حقوق الأفراد وحررياتهم من جهة، ومصلحة المجتمع وأمنه من جهة أخرى<sup>٤٤</sup>.

وبناء عليه، أجازت النصوص الدستورية المساس بهذه الحرمة بشروط وضوابط محددة وفق القانون واستجابت القوانين الإجرائية لتلك الضوابط في قوانين الإجراءات الجنائية وأصول المحاكمات الجزائية وتعد فرنسا من الدول السبقة في وضع تنظيم تشريعي لسرية المراسلات والاتصالات. وبخصوص السلطة المختصة بإصدار الأذن بمراقبة الرسائل والاتصالات، أما قانون الإجراءات الجنائية المصري، فقد أجاز، بالمثل، لقاضي التحقيق إصدار أمر بضبط الرسائل ومراقبة المكالمات الهاتفية أو تسجيل الأحاديث الخاصة في أماكن مغلقة إذا كان هو المباشر للتحقيق، بينما إذا تولت النيابة العامة التحقيق، فإن القاضي الجزائي هو المختص بالإذن لها بمراقبة المكالمات وضبط الخطابات والرسائل والاطلاع عليها متى كان لذلك فائدة<sup>٤٥</sup>. كما أتاح القانون المصري لرئيس المحكمة الابتدائية المختصة، في حالة وجود دلائل قوية على استخدام مرتكب إحدى الجرائم المنصوص عليها في المادتين (١٦٦) مكرر و ٣٠٨ (مكرر) من قانون العقوبات لجهاز هاتفي أن يأمر بوضع الجهاز تحت المراقبة بناء على تقرير مدير عام مصلحة التلغراف والتليفونات وشكوى المجني عليه، وللفترة التي يحددها القانون أما بالنسبة لقانون أصول المحاكمات الجزائية العراقي، فقد جاء خالياً من نص تنظيمي مباشر لضبط المراسلات والاتصالات، إلا أن البعض يرى أنه طالما أن الدستور العراقي يسمح بإفشاء أسرار المراسلات والاتصالات متى ما كانت ضرورة العدالة والأمن تقتضي ذلك، فلا يمنع القانون ذلك<sup>٤٦</sup>.

كما تنص المادة (٧٤) من قانون أصول المحاكمات الجزائية العراقي على أن قاضي التحقيق يمكنه إصدار أمر كتابي لتقديم الأوراق أو الأشياء الموجودة لدى الشخص والتي تفيد التحقيق

في ميعاد معين مما يعني أن المراسلات، إن لم تقدم طواعية، يجوز إجبار الشخص على تقديمها، ويمكن القاضي التحقيق مراقبة المكالمات الهاتفية إذا رآها مفيدة للتحقيق، علماً بأن المكالمات الهاتفية تعتبر من باب الرسائل الشفوية. ولقد اشترطت غالبية القوانين التي تولت تنظيم مراقبة المحادثات الخاصة وإجراءات الاطلاع على الرسائل والبرقيات الشخصية، عدة شروط منها:

أولاً: وقوع جريمة: لا يجوز اللجوء إلى إجراءات ضبط المراسلات ومراقبة الاتصالات بوصفها من وسائل التحري عن الجرائم ما لم تكن هناك دلائل قوية وقرائن قاطعة على وقوع جريمة، إذ أن القيام بذلك بدون سبب يفضي إلى انتهاك حرمة الأفراد وخصوصياتهم بدعوى التحري عن الجرائم. ويقع تقدير كفاية القرائن واختيار توقيت الإجراء على عاتق الجهة المختصة، وتخضع هذه القرارات لمراقبة محكمة الموضوع وقد اشترط قانون الإجراءات الجنائية الفرنسي لسنة ١٩٥٧ المعدل بالقانون رقم ٦٤٣ لسنة ١٩٧٠ وفق المادتين (٨٠-٨١)، أن تكون الجريمة المراد التحري عنها جرائم خاصة جداً يصعب إثباتها بطرق الإثبات العادية، مثل جرائم الرشوة والتهديد. أما قانون الإجراءات الجنائية المصري، فقد نص في المادة (٩٥) على أن تكون الجريمة المرخص باتخاذ هذه الإجراءات جنائية أو جنحة يعاقب عليها بالحبس مدة تزيد على ثلاثة أشهر، أي أن نوع العقوبة يمثل معياراً لاختيار الجريمة، كما أكدت محكمة النقض المصرية أن الأصل في إصدار أوامر التفتيش وتسجيل المحادثات هو حماية الأدلة الجنائية ولا يصح إلا لضبط جنائية أو جنحة وقعت بالفعل مع وجود أدلة كافية.

ثانياً: وجوب أن تكون هناك فائدة في إظهار الحقيقة: اللجوء إلى اتخاذ هذه الإجراءات هو أمر استثنائي يفرضه الضرورة والفائدة المنتظرة منه في الكشف عن غموض الجريمة أو ضبط الجناة. فإذا تبين أن هذه الإجراءات لا تخدم هذا الهدف، تصبح غير مشروعة ويصبح الدليل المستمد منها باطلاً.

ثالثاً: تحديد المحل الذي ترد عليه إجراءات ضبط المراسلات ومراقبة الاتصالات: يجب أن تكون المحادثات الخاصة والرسائل المراد مراقبتها أو الاطلاع عليها محددة بدقة في إذن المراقبة لتجنب الأخطاء التنفيذية التي قد تعرض خصوصية الأفراد للانتهاك. وقد نص المشرع الكويتي في المادة (٨٧) فقرة ٣ من قانون الإجراءات والمحاكمات الجزائية رقم ١٧ لسنة ١٩٦٠ على ضرورة تحديد واضح للمكالمة أو المكالمات المطلوب تسجيلها، وإن كان هذا القصر مقصوراً على المحادثات الخاصة دون الرسائل والبرقيات، بينما كان الأجدر توسيع الحماية لتشمل جميع عناصر الخصوصية.<sup>٤٧</sup>

رابعاً: شرط كون المتهم طرفاً في المحادثات أو المراسلات: أشار بعض الفقهاء إلى أن يكون المتهم طرفاً في المحادثات أو صاحب الهاتف أو حائزه أو حاضراً أثناء الحديث. ويضمن هذا الشرط حماية خصوصية الأفراد وتحديد نطاق الإجراءات، حتى لو لم ينص عليه القانون صراحاً ولمعالجة النقص التشريعي العراقي فيما يخص الرقابة على الاتصالات وضبط المراسلات، يُنصح بإضافة نص مشابه للمادة (٩٥) من القانون المصري، يحدد الحالات والضمانات المتعلقة بإصدار وتنفيذ هذه الإجراءات، مع التأكيد على:

١. الجرائم الخطيرة فقط (جناية أو جنحة كبيرة).

٢. ضرورة استصدار إذن قضائي من السلطة المختصة.

٣ الالتزام بالضوابط لتوفيق الحق في الخصوصية مع تحقيق الغرض من التحقيق الجنائي كما يستند هذا التنظيم إلى المادة (٤٠) من دستور العراق لسنة ٢٠٠٥، التي تكفل حرية المراسلات والاتصالات الإلكترونية وغير الإلكترونية، ويُسمح بمسحها فقط لضرورة قانونية وأمنية وبقرار قضائي، مع مراعاة المادة (٤٦) التي تمنع المساس بجوهر الحق والحرية.

#### المطلب الثاني: دور القضاء في مواجهة الجرائم الإلكترونية وسد الثغرات الإجرائية

هناك حالات خاصة للحرمة المهنية مثل المراسلات بين الطبيب ومرضاه أو المحامي وموكله تظل محمية بعد انتهاء العلاقة أو القضية، وحتى بعد إنهاء مهنة المحامي أو الزواج حيث أن أعضاء البرلمان يتمتعون بحصانة دستورية تحمي رسائلهم ومراسلاتهم، كما ورد في المادة (٦٣) فقرة ٢ من دستور العراق ٢٠٠٥ والمادة (٩٠) من الدستور المصري ٢٠١٢ وأن المبعوث الدبلوماسي يظل مراسلاته الرسمية والشخصية محمية لضمان حرية الاتصال بدولته وفق الاتفاقيات الدولية.

ويتبادر التساؤل حول مدى إمكانية معاقبة الجريمة المعلوماتية، إذ تنص المادة (٧٤) من قانون الإجراءات الجنائية الليبي على انتقال المحقق لأي مكان لضبط الحالة المادية للأشياء والأشخاص ووجود الجريمة، ما يطرح سؤالاً حول وجود الجريمة المعلوماتية المادي، حيث أن المشرع من هذا النص لضبط الجرائم ذات الوجود الملموس في العالم الخارجي<sup>٨</sup>، وتؤكد المادة (٤٤) من ذات القانون ضرورة وضع الأشياء والأوراق المضبوطة في حزر مغلق ومربوط، وهو إجراء يطبق على الممتلكات الملموسة، بينما تواجه الجريمة المعلوماتية صعوبة في التطبيق لأنها تقع في بيئة افتراضية مليئة بالنبضات الكهرومغناطيسية والبيانات المخزنة داخل أنظمة معلوماتية حساسة، وليست أوراقاً أو أدوات قابلة للتحرير.

وفي الإطار القانوني العراقي، جاء دستور ٢٠٠٥ في المادة (٤٠) ليكفل حرمة الاتصالات

والمراسلات الإلكترونية، ويمنع مراقبتها أو التنصت عليها إلا بموجب ضرورة قانونية أو أمنية وبقرار قضائي، ما يجعل أي استخدام غير مشروع للبيانات الإلكترونية يشكل انتهاكا للحق في الخصوصية ويستلزم تشريعا واضحا لمعاقبة المخالفين أما الإطار المصري، فقد تناول قانون حماية البيانات الشخصية قانون رقم ١٥١ لسنة ٢٠٢٠ تنظيم معالجة البيانات الشخصية وحفظها واستخدامها إلكترونيا، بما يضمن عدم إفشاء المعلومات دون موافقة صاحب البيانات، ويحدد العقوبات ضد كل من يقوم بالمعالجة غير المشروعة أو الإفشاء غير القانوني<sup>٤٩</sup>.

وقد أعد مشروع قانون عراقي لمكافحة جرائم المعلوماتية منذ عام ٢٠١٠، ومعالجته لجرائم الاحتيال الإلكتروني، إساءة استخدام النشر الإلكتروني، والتشهير الإلكتروني، وغيرها، بما يتوافق مع حماية البيانات الشخصية وفق المادة (٤٠) من دستور العراق ٢٠٠٥، لضمان حماية المجني عليه وضمان استخدام المعلومات الشخصية وفق القانون وتجدر الإشارة إلى أن الجرائم الإلكترونية تتمثل عادة في جرائم التهديد الاحتيال الابتزاز المالي، التشهير، المقاومة الاستغلال الجنسي، والانتهاكات المتعلقة بالصور الفاضحة أو الحياة الخاصة، وهو ما يعزز أهمية ربط التشريعات الوطنية بحماية البيانات الشخصية عند مكافحة الجرائم المعلوماتية، وقد أكد العراق على أن استخدام الإنترنت جزء من خصائص الحضارة الحديثة، ويعكس مقياس التنمية والتفاعل الحضاري، إلا أن انتشار الجرائم الإلكترونية يزيد من ضرورة وضع لوائح أخلاقية وتنظيمية تتوافق مع خصوصيات كل مجتمع وأشار العراق إلى انتشار التطبيقات الرقمية للألعاب والترفيه، والتي تتطلب من المستخدمين السماح بالوصول إلى معلومات شخصية، مما يستدعي وضع معايير شفافة الغرض الوصول للبيانات، وتعزيز الثقة من خلال فرق تقييم تطوعية، بما يتماشى مع قوانين حماية البيانات الشخصية في العراق ومصر، كما أشار إلى ضرورة ضبط الأخبار والمعلومات المتداولة على الإنترنت، وتشجيع الشركات على التحقق من مصداقية الأخبار ومكافحة الأخبار المزيفة التي تضر على الكراهية، بالتعاون مع الفرق التطوعية والمؤسسات القانونية، بما يتوافق مع الإطار التشريعي لحماية البيانات والمعلومات الشخصية وبالنسبة للأطفال والشباب يوفر مجتمع المعلومات عالما رقميا متاحا فوراً، مع إمكانية الوصول إلى خدمات ومعلومات غير مسبقة، وهو ما يفرض على التشريعات الوطنية<sup>٥٠</sup>، بما في ذلك التشريع العراقي والمصري، وضع ضوابط حماية الأطفال والحقوق الرقمية، بما يوازن بين حرية الوصول وحماية الخصوصية.

وتواجه مكافحة الجرائم الإلكترونية تحديات خاصة، إذ لا يمكن تطبيق القواعد التقليدية لمعانة الجريمة كما نصت المادة (٧٤) من قانون الإجراءات الجنائية الليبي على إمكانية انتقال المحقق

لأي مكان لضبط الحالة المادية للأشياء والأشخاص ووجود الجريمة إلا أن الجرائم المعلوماتية تقع داخل بيانات رقمية مليئة بالبيانات المخزنة والإشارات الإلكترونية، وليست ملموسة أو قابلة للتحريز بالطريقة التقليدية وقد أدرك التشريع العراقي أهمية حماية البيانات الشخصية، فجاء دستور ٢٠٠٥ في المادة (٤٠) ليكفل حرمة الاتصالات والمراسلات الإلكترونية ويمنع التنصت أو المراقبة إلا بموجب ضرورة قانونية أو أمنية وبقرار قضائي، ما يوفر إطار حماية للأفراد من الانتهاكات الإلكترونية وعلى الصعيد التشريعي أصدر برلمان إقليم كردستان العراق القانون رقم ٦ لسنة ٢٠٠٨ لمكافحة إساءة استخدام الهواتف المحمولة والإنترنت، حيث حدد الجرائم المتعلقة باستخدام الأجهزة الإلكترونية في السياقات التالية:

١. إساءة استخدام الهواتف المحمولة أو غيرها من أجهزة الاتصالات اللاسلكية أو الإنترنت لغرض التهديد

٢. الاختيال عبر الاتصالات أو الإنترنت.

٣. الاستخدام المهين أو الإضرار بالآخرين عبر الوسائل الإلكترونية.

٤. نشر الأخبار المضللة أو الصور والفيديوهات المؤذية.

٥. التصوير أو التسجيل بدون إذن.

٦. تشجيع الفجور أو الجريمة.

٧. نشر الأسرار الشخصية أو الأسرية للأفراد بأي شكل من الأشكال إذا كان ضاراً للفرد، حيث ان العقوبات تتراوح بين ستة أشهر وخمس سنوات حبساً، وغرامة مالية من مليون إلى خمسة ملايين دينار عراقي، مع تشديد العقوبة إذا ارتكب الشخص الجريمة عبر أجهزة متعددة أو تسببت في أذى جسدي أو اجتماعي. كما تفرض العقوبات على شركات الاتصالات المخالفة للقوانين بما بين ٥٠ إلى ١٠٠ مليون دينار. ويبرز العراق أهمية حماية الأطفال والشباب من المخاطر الرقمية<sup>١</sup>، ومن أبرز هذه المخاطر

أ. التعرض للمحتوى غير المشروع والضارة مثل المواد الإباحية المقامرة مواقع إيذاء النفس، مشاهد العنف والإرهاب، والاتصال بالمستخدمين الآخرين، مع عدم اتخاذ مشغلي المواقع التدابير الكافية لتقييد الوصول للأطفال.

ب. الاستهداف من خلال الرسائل التطفلية والإعلانات الموجهة للأطفال والشباب لترويج منتجات أو محتوى غير مناسب. والاستخدام المفرط وغير الإرادي للإنترنت والألعاب الإلكترونية، مما يؤدي إلى الإدمان والمشكلات النفسية والسلوكية.

ج. التخويف والمضايقة والتهديد والابتزاز عبر الإنترنت والتعرض للتطرف والعنصرية وخطاب

الكرهية، بما يشكل تهديدًا مباشرًا لسلامة الأفراد. وإساءة استخدام البيانات الشخصية والكشف عنها، مما يؤدي إلى خطر الأذى الجسدي أو النفسي، أو انتهاك حقوق الآخرين، بما يشمل الصور غير اللائقة أو القرصنة على المحتوى الرقمي.

وأشار العراق إلى أن منصات الإنترنت الكبرى تمثل فرصة عظيمة للتنمية الاجتماعية والاقتصادية، إلا أن الاستخدام المجهول أو المزيف يمكن أن يؤدي إلى أنشطة إجرامية مثل نشر خطاب الكراهية التهديد، الابتزاز، والإرهاب، مما يستدعي تعاونًا وثيقًا بين الجهات الحكومية وشركات الإنترنت الضمان تقديم خدمات آمنة ومتوافقة مع أهداف التنمية المستدامة. وتشمل التحديات التي تواجه مكافحة الجرائم السيبرانية في العراق ما يلي<sup>٥٢</sup>:

١. عدم وجود اتفاقية عالمية شاملة بشأن الجرائم السيبرانية، صعوبة فهم الأدلة الرقمية أو فقدانها أو تدميرها.

٣. الجرائم السيبرانية تتجاوز الحدود الجغرافية، مع وجود المسافة بين المجرم والضحية.

٤. نقص التدريب وبناء القدرات لدى السلطات المختصة للتحقيق في الجرائم الإلكترونية.

٥. عدم الاستفادة الكاملة من خبرات المنظمات الحكومية وغير الحكومية في التحقيقات السيبرانية.

٦. ضعف البنية التحتية الإلكترونية لمكافحة الجريمة، وصعوبة تحديد أو تضيق طرق ارتكابها. واستخلص العراق الحاجة الملحة إلى زيادة التعاون بين جميع أصحاب المصلحة لضمان مستقبل رقمي آمن للأطفال والشباب والمجتمع بشكل عام حيث تواجه مكافحة الجرائم الإلكترونية تحديات خاصة، إذ لا يمكن تطبيق القواعد التقليدية لمعاقبة الجريمة<sup>٥٣</sup>.

#### الخاتمة والاستنتاجات

خلص البحث إلى أن حماية البيانات الشخصية في العراق ومصر ما زالت تواجه ثغرات وتحديات تشريعية وتطبيقية متفاوتة، نتيجة التطور المتسارع للتقنيات الرقمية وتنوع صور الاعتداء على البيانات. وأظهرت الدراسة المقارنة حاجة التشريع العراقي إلى تنظيم أكثر تكاملاً، مع ضرورة تعزيز وتطوير الإطار المصري وآليات تطبيقه بما يضمن حماية فعالة للخصوصية والبيانات الشخصية. ومن هنا نستنتج النتائج التالية:

١. أظهر البحث المقارنة وجود تفاوت واضح بين العراق ومصر في مستوى التنظيم التشريعي لحماية البيانات الشخصية؛ إذ يعاني العراق من عدم اكتمال إطار تشريعي متخصص ومتكامل، وتوزع الحماية بين نصوص دستورية وقوانين متفرقة، في حين اتجه المشرع المصري إلى وضع تنظيم خاص بموجب قانون حماية البيانات الشخصية رقم (١٥١) لسنة ٢٠٢٠، الأمر الذي

يجعل الحماية التشريعية المصرية أكثر وضوحًا من حيث المبادئ والالتزامات مقارنة بالإطار العراقي.

٢. تبين أن الحماية الدستورية للخصوصية والاتصالات في العراق ومصر تشكل أساسًا مهمًا لحماية البيانات الشخصية، إلا أن الحماية الدستورية وحدها لا تكفي لمواجهة التطورات التقنية الحديثة؛ ففي العراق تبرز الحاجة إلى ترجمة المبادئ الدستورية إلى قواعد تشريعية تفصيلية، بينما يحتاج التنظيم المصري إلى تطوير مستمر لمواكبة المستجدات الرقمية وتحديد نطاق تطبيق النصوص بصورة أكثر دقة.

٣. كشفت الدراسة أن من أبرز الثغرات في التشريع العراقي غياب تنظيم شامل يحدد بصورة دقيقة مفهوم البيانات الشخصية والبيانات الحساسة وحقوق أصحاب البيانات والتزامات الجهات التي تقوم بجمعها ومعالجتها وتخزينها، في حين قدم التشريع المصري إطارًا أكثر تفصيلًا لهذه المسائل، إلا أن فعالية الحماية في مصر تظل مرتبطة بمدى التطبيق العملي للنصوص وقدرة الجهات المختصة على فرض الالتزامات القانونية ومتابعة المخالفات.

٤. رابعًا: توصل البحث إلى أن التطور المتسارع للجرائم الإلكترونية يمثل تحديًا مشتركًا للنظامين العراقي والمصري، ولا سيما في حالات الاختراق وتسريب البيانات والابتزاز الإلكتروني والوصول غير المشروع إلى المعلومات الشخصية. غير أن العراق يواجه تحديًا أكبر بسبب تشتت القواعد القانونية ذات الصلة وعدم اكتمال التنظيم المتخصص، بينما يتمتع النظام المصري بوجود قانون خاص بحماية البيانات إلى جانب التشريعات المتعلقة بالجرائم الإلكترونية، بما يوفر أساسًا قانونيًا أكثر تكاملًا لمواجهة هذه الاعتداءات.

٥. خامسًا: أظهرت المقارنة أهمية الدور القضائي في سد النقص التشريعي وتفسير النصوص القائمة بما يتلاءم مع البيئة الرقمية، إذ يستطيع القضاء العراقي توظيف النصوص الدستورية والقانونية المتاحة لحماية الخصوصية في ظل محدودية التنظيم المتخصص، بينما يعمل القضاء المصري في إطار تشريعي أكثر تحديدًا بفضل قانون حماية البيانات الشخصية. ومع ذلك، فإن التطورات التقنية المتلاحقة تفرض على القضاء في كلا النظامين ضرورة تطوير التفسير القضائي بما يضمن حماية الحقوق الرقمية دون تجاوز حدود الوظيفة القضائية.

٦. سادسًا: خلصت الدراسة إلى أن تحقيق حماية فعالة للبيانات الشخصية في العراق ومصر يتطلب الانتقال من الحماية القانونية التقليدية إلى منظومة متكاملة تجمع بين التشريع المتخصص والرقابة المؤسسية والضمانات القضائية والتدابير التقنية. ويظهر أن العراق بحاجة بصورة أكبر إلى استكمال بنيته التشريعية والمؤسسية في هذا المجال، في حين تحتاج مصر إلى



تعزيز التطبيق العملي وتطوير التنظيم القائم بما يستجيب للتحديات المستحدثة، خصوصاً البيانات الحساسة وبيانات الأطفال ونقل البيانات عبر الحدود.

#### التوصيات:

١. نوصي المشرع العراقي بالإسراع في إصدار تشريع متكامل ومستقل لحماية البيانات الشخصية، يتضمن تعريفاً دقيقاً للبيانات الشخصية والحساسة، ويحدد حقوق أصحاب البيانات والتزامات الجهات التي تقوم بجمعها ومعالجتها وتخزينها ونقلها، مع وضع جزاءات فعالة على الاستخدام أو الإفصاح غير المشروع، بما يضع حداً لتشتت الحماية بين النصوص القانونية المتفرقة.

٢. نوصي المشرعين العراقي والمصري بتطوير النصوص القانونية بصورة دورية لمواكبة التطورات التقنية والجرائم الرقمية المستحدثة، ولا سيما ما يتعلق بالذكاء الاصطناعي، والحوسبة السحابية، والتعرف البيومتري، والتسريب الإلكتروني، ونقل البيانات عبر الحدود، مع ضمان عدم تحول التطور التكنولوجي إلى وسيلة للانتقاص من الحق في الخصوصية.

٣. نوصي المشرع العراقي بتعزيز البناء المؤسسي لحماية البيانات الشخصية من خلال إنشاء جهة متخصصة ومستقلة تتولى الرقابة على عمليات جمع البيانات ومعالجتها، واستقبال شكاوى الأفراد، ومتابعة المخالفات، ووضع المعايير الفنية والقانونية اللازمة للحماية، مع الاستفادة من التجربة المصرية في هذا المجال، في حين نوصي المشرع المصري بتعزيز فاعلية الجهات المختصة وتطوير آليات الرقابة والإنفاذ العملي للقواعد القائمة.

٤. نوصي المشرعين العراقي والمصري بتعزيز الضمانات القضائية المتعلقة بالوصول إلى البيانات الشخصية ومراقبة الاتصالات وضبط المراسلات والأدلة الرقمية، من خلال وضع شروط وضوابط دقيقة للحصول على الإذن القضائي، وتحديد نطاقه ومدته والجهات المخولة بتنفيذه، بما يحقق التوازن بين حماية خصوصية الأفراد ومتطلبات التحقيق الجنائي والأمن العام.

٥. نوصي المشرعين العراقي والمصري بإيلاء حماية خاصة للبيانات الحساسة وبيانات الأطفال والفئات الأكثر عرضة للمخاطر الرقمية، وتشديد الجزاءات على تسريبها أو استغلالها بصورة غير مشروعة، إلى جانب تعزيز التعاون القضائي والتشريعي الدولي في مواجهة الجرائم الإلكترونية العابرة للحدود، بما يضمن فاعلية الحماية القانونية للبيانات الشخصية في البيئة الرقمية الحديثة.

الهوامش

١. حسين الكبيسي، قانون الجرائم الإلكترونية في العراق، دار المنصور للنشر، بغداد، ٢٠٢٠، ص ٩٠.
٢. القانون رقم ٢٠٠٨/٦، قانون منع إساءة استخدام الأجهزة المحمولة وأجهزة الإنترنت، برلمان كردستان العراق، ٢٠٠٨.
٣. محمد صالح، قانون حماية البيانات الشخصية المصري، القاهرة، ٢٠٢١، ص ١٣٤.
٤. حسين الكبيسي، قانون الجرائم الإلكترونية في العراق، مصدر سابق، ص ٦٣.
٥. محمد صالح، قانون حماية البيانات الشخصية المصري، مصدر سابق، ص ٥٢.
٦. محمود سالم، الأمن السيبراني والقانون الجنائي، دار التحرير، القاهرة ٢٠١٨، ص ٧٤.
٧. أحمد جعفر الشاوي، المسؤولية التقصيرية الناشئة عن استعمال الإنترنت، أطروحة دكتوراه، كلية القانون، جامعة بغداد، ٢٠١٦، ص ١٠٢.
٨. European Data Protection Board, 2018, p. 23
٩. دستور جمهورية العراق، ٢٠٠٥، ص ٢٨
١٠. قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠، الجريدة الرسمية، القاهرة، ص. (٣).
١١. (European Union, ePrivacy Directive, 2002, Art. 5).
١٢. قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠، الجريدة الرسمية، القاهرة، ص. (٤).
١٣. (Federal Trade Commission, 2012, p. 22).
١٤. قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠، الجريدة الرسمية، القاهرة، ص. (٥).
١٥. (دستور جمهورية العراق، ٢٠٠٥، ص ٢٨).
١٦. قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠، الجريدة الرسمية، القاهرة، ص. (١٢).
١٧. Solove, D., Understanding Privacy, Harvard University Press, 2020, pp. 112–115
١٨. Zuboff, S., The Age of Surveillance Capitalism, PublicAffairs, 2019, p. 210.
١٩. CNIL, Rapport 2015 sur la protection des données, Paris, 2015, p. 22
٢٠. State v. Noll, Indiana Court of Appeals, 2017, p. 5.
٢١. قانون العقوبات المصري ١٩٣٧ المعدل المادة ٣٢٧، ص ٨٥
٢٢. قانون العقوبات المصري، ١٩٣٧ المعدل المادة ٣٢٧، ص ٨٥
٢٣. Greenwald, G., No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State, Metropolitan Books, 2014, pp. 45–47.
٢٤. قرار الجمعية العامة للأمم المتحدة رقم ١٦٧/٦٨ لسنة ٢٠١٣
٢٥. United Nations General Assembly, Resolution 68/167 on the Right to Privacy in the Digital Age, 2013, p. 5
٢٦. Commission Nationale de l'Informatique et des Libertés [CNIL], Rapport 2015 sur la protection des données, Paris, 2015.



- <sup>٢٧</sup> . Solove, D. J., Understanding Privacy, Harvard University Press, 2020, pp. 85–87.
- <sup>٢٨</sup> . Zuboff, S., The Age of Surveillance Capitalism, PublicAffairs, 2019, pp. 210–215
- <sup>٢٩</sup> . State v. Noll, Indiana Court of Appeals, 2017, No. 49A02–1610–CR–2217
- <sup>٣٠</sup> . Commission Nationale de l'Informatique et des Libertés [CNIL], Rapport 2015 sur la protection des données, Paris, 2015, pp. 112–118
- <sup>٣١</sup> . Zuboff, S., The Age of Surveillance Capitalism, PublicAffairs, 2019, pp.220–225
- <sup>٣٢</sup> . Daniel J. Solove, Understanding Privacy, Harvard University Press, 2020, p66.
- <sup>٣٣</sup> . Commission Nationale de l'Informatique et des Libertés [CNIL], Guide to Data Protection Laws in Europe, CNIL, 2015, p33
- <sup>٣٤</sup> . حسين الكبيسي، قانون حماية البيانات في العراق، مصدر سابق، ص ١١٢
- <sup>٣٥</sup> . أحمد محمود، حماية البيانات الإلكترونية في مصر الإطار القانوني والتحديات، دار النهضة العربية، القاهرة، ٢٠٢١، ص ٩٥
- <sup>٣٦</sup> . Shoshana Zuboff, The Age of Surveillance Capitalism, PublicAffairs, 2019, p218.
- <sup>٣٧</sup> . Commission Nationale de l'Informatique et des Libertés [CNIL], Guide to Data Protection Laws in) 114 (35) Europe, CNIL, 2015
- <sup>٣٨</sup> . Shoshana Zuboff, The Age of Surveillance Capitalism, PublicAffairs, 2019, p225.
- <sup>٣٩</sup> . حسين الكبيسي، قانون حماية البيانات في العراق، مصدر سابق، ص ١١٥.
- <sup>٤٠</sup> . أحمد محمود، حماية البيانات الإلكترونية في العراق، دار النهضة العربية، بغداد، ٢٠٢١، ص ٥٨.
- <sup>٤١</sup> . حسين الكبيسي، قانون الجرائم الإلكترونية في العراق، مصدر سابق، ص ٧١
- <sup>٤٢</sup> . محمد صالح، قانون حماية البيانات الشخصية المصري، مصدر سابق، ص ٦١
- <sup>٤٣</sup> . محمود سالم، الأمن السيبراني والقانون الجنائي، مصدر سابق، ص ٨٢.
- <sup>٤٤</sup> . صفا عبد المهدي جاسم إسماعيل، مدى فاعلية الحماية الإدارية للبيانات الشخصية في ظل نظام الحوكمة الإلكترونية المستحدث في العراق، مجلة لارك كلية الاداب جامعة واسط، مجلد ١٨، عدد ٣، ٢٠٢٦، ص ٥٤٤.
- <sup>٤٥</sup> . أحمد محمود، حماية البيانات الإلكترونية في مصر: الإطار القانوني والتحديات، مصدر سابق، ص ١٠٢.
- <sup>٤٦</sup> . حسين الكبيسي، قانون حماية البيانات في العراق، مصدر سابق، ص ١٢٥.
- <sup>٤٧</sup> . محمد الكويتي الإجراءات الجنائية في دول الخليج، دار الفكر الكويت، ٢٠١٦، ص ٧٨
- <sup>٤٨</sup> . محمد الليبي، الإجراءات الجزائية الليبية، منشورات طرابلس، ٢٠١٥، ص ١١٢

<sup>٤٩</sup>. طارق جمعة راشد، ٢٠١٩، الحماية القانونية لخصوصية البيانات الشخصية في العصر الرقمي، مجلة القانون والاقتصاد، ع ٧٢، القاهرة، ص ٢٠٦.

<sup>٥٠</sup>. رزق علي، ٢٠٢٢، الحماية الجنائية للبيانات الشخصية المعالجة إلكترونياً في ضوء القانون رقم ١٥١ لسنة ٢٠٢٠م، جامعة السادات، ورقة بحثية المؤتمر العلمي الأول لكلية الحقوق في الجامعة، ص ١٤.

<sup>٥١</sup>. منى تركي الموسوي، فضل الله، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها مجلة كلية بغداد للعلوم الاقتصادية الجامعة كلية بغداد للعلوم الاقتصادية الجامعة، عدد خاص بمؤتمر الكلية، ٢٠١٣، ص ١٥٤

<sup>٥٢</sup>. عبد الله فاضل حامد، تنازع الاختصاص القضائي في دعوى انتهاك الحقوق للصيقة بالشخصية، بحث منشور في مجلة دراسات قانونية وسياسية صادرة عن جامعة السليمانية، السنة الخامسة، العدد التاسع، حزيران ٢٠١٧، ص ٣٦٧.

<sup>٥٣</sup>. محمد قاسم الناصر الحق في سرية المراسلات في بعض النظم الدستورية، رسالة ماجستير، كلية القانون، جامعة، ٢٠٠٢، ص ٤٤

#### قائمة المصادر العربية

#### أولاً: الكتب

١. أحمد محمود، حماية البيانات الإلكترونية في العراق، دار النهضة العربية، بغداد، ٢٠٢١.
٢. أحمد محمود، حماية البيانات الإلكترونية في مصر الإطار القانوني والتحديات، دار النهضة العربية، القاهرة، ٢٠٢١.
٣. حسين الكبيسي، قانون الجرائم الإلكترونية في العراق، دار المنصور للنشر، بغداد، ٢٠٢٠.
٤. محمد الكويتي الإجراءات الجنائية في دول الخليج، دار الفكر الكويت، ٢٠١٦.
٥. محمد الليبي، الإجراءات الجزائية الليبية، منشورات طرابلس، ٢٠١٥.
٦. محمد صالح، قانون حماية البيانات الشخصية المصري، القاهرة، ٢٠٢١.
٧. محمود سالم، الأمن السيبراني والقانون الجنائي، دار التحرير، القاهرة ٢٠١٨.

#### ثانياً: الرسائل العلمية

١. أحمد جعفر الشاوي، المسؤولية التقصيرية الناشئة عن استعمال الإنترنت، أطروحة دكتوراه، كلية القانون، جامعة بغداد، ٢٠١٦.

٢. محمد قاسم الناصر الحق في سرية المراسلات في بعض النظم الدستورية، رسالة ماجستير، كلية القانون، جامعة، ٢٠٠٢.

#### ثالثاً: الأبحاث العلمية

١. رزق علي، ٢٠٢٢، الحماية الجنائية للبيانات الشخصية المعالجة إلكترونياً في ضوء القانون رقم ١٥١ لسنة ٢٠٢٠م، جامعة السادات، ورقة بحثية المؤتمر العلمي الأول لكلية الحقوق في الجامعة.



٢. صفا عبد المهدي جاسم إسماعيل، مدى فاعلية الحماية الإدارية للبيانات الشخصية في ظل نظام الحوكمة الإلكترونية المستحدث في العراق، مجلة لارك كلية الاداب جامعة واسط، مجلد ١٨، عدد ٣، ٢٠٢٦.
٣. طارق جمعة راشد، ٢٠١٩، الحماية القانونية لخصوصية البيانات الشخصية في العصر الرقمي، مجلة القانون والاقتصاد، ع ٧٢، القاهرة.
٤. عبد الله فاضل حامد، تنازع الاختصاص القضائي في دعوى انتهاك الحقوق للصيقة بالشخصية، بحث منشور في مجلة دراسات قانونية وسياسية الصادرة عن جامعة السليمانية، السنة الخامسة، العدد التاسع، حزيران ٢٠١٧.
٥. منى تركي الموسوي، فضل الله، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها مجلة كلية بغداد للعلوم الاقتصادية الجامعة كلية بغداد للعلوم الاقتصادية الجامعة، عدد خاص بمؤتمر الكلية، ٢٠١٣.

#### رابعا: القوانين

١. دستور جمهورية العراق، ٢٠٠٥.
٢. قانون العقوبات المصري ١٩٣٧ المعدل
٣. قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠، الجريدة الرسمية، القاهرة.
٤. القانون رقم ٢٠٠٨/٦، قانون منع إساءة استخدام الأجهزة المحمولة وأجهزة الإنترنت، برلمان كردستان العراق، ٢٠٠٨.
٥. قرار الجمعية العامة للأمم المتحدة رقم ١٦٧/٦٨ لسنة ٢٠١٣

#### References (المصادر العربية المترجمة للانكليزية)

##### First: Books

1. Ahmed Mahmoud, Protection of Electronic Data in Iraq, Dar Al-Nahda Al-Arabiya, Baghdad, 2021.
2. Ahmed Mahmoud, Protection of Electronic Data in Egypt: Legal Framework and Challenges, Dar Al-Nahda Al-Arabiya, Cairo, 2021.
3. Hussein Al-Kubaisi, Cybercrime Law in Iraq, Dar Al-Mansour for Publishing, Baghdad, 2020.
4. Mohammed Al-Kuwaiti, Criminal Procedures in Gulf States, Dar Al-Fikr, Kuwait, 2016.
5. Mohammed Al-Libi, Libyan Penal Procedures, Tripoli Publications, 2015.
6. Mohammed Saleh, Egyptian Personal Data Protection Law, Cairo, 2021.
7. Mahmoud Salem, Cybersecurity and Criminal Law, Dar Al-Tahrir, Cairo, 2018.

##### Second: Scientific Theses

1. Ahmed Jaafar Al-Shawi, Tort Liability Arising from Internet Use, PhD Thesis, College of Law, University of Baghdad, 2016. Academic Theses
2. Mohammed Qasim Al-Nasser, The Right to Confidentiality of Correspondence in Certain Constitutional Systems, Master's Thesis, College of Law, University, 2002.

##### Third: Scientific Research

1. Rizk Ali, 2022, Criminal Protection of Electronically Processed Personal Data in



Light of Law No. 151 of 2020, Sadat University, Research Paper, First Scientific Conference of the Faculty of Law at the University.

2. Safa Abdul-Mahdi Jassim Ismail, The Effectiveness of Administrative Protection for Personal Data under the Newly Introduced E-Governance System in Iraq, Lark Journal (College of Arts, Wasit University), Vol. 18, No. 3, 2026.

3. Tariq Jumaa Rashid, 2019, Legal Protection of Personal Data Privacy in the Digital Age, Journal of Law and Economics, Issue 72, Cairo.

4. Abdullah Fadhil Hamid, Conflict of Jurisdiction in Lawsuits Concerning the Violation of Rights Inherent to the Personality, research paper published in the Journal of Legal and Political Studies (University of Sulaymaniyah), Year 5, Issue 9, June 2017.

5. Mona Turki Al-Mousawi & Fadlallah, Informational Privacy: Its Importance and the Risks Posed by Modern Technologies, Journal of Baghdad College of Economic Sciences University; special issue dedicated to the college's conference, 2013.

#### Fourth: Laws

1. Constitution of the Republic of Iraq, 2005.

2. Egyptian Penal Code of 1937, as amended.

3. Egyptian Personal Data Protection Law No. 151 of 2020, Official Gazette, Cairo.

4. Law No. 6/2008: Law on the Prevention of Misuse of Mobile Devices and Internet Devices, Kurdistan Parliament – Iraq, 2008.

5. United Nations General Assembly Resolution 68/167 of 2013.

#### المصادر الاجنبية ان وجدت

1. CNIL, Rapport 2015 sur la protection des données, Paris, 2015.

2. Commission Nationale de l'Informatique et des Libertés [CNIL], Rapport 2015 sur la protection des données, Paris, 2015.

3. Daniel J. Solove, Understanding Privacy, Harvard University Press, 2020.

4. European Data Protection Board, 2018.

5. European Union, ePrivacy Directive, 2002.

6. Federal Trade Commission, 2012.

7. Greenwald, G., No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State, Metropolitan Books, 2014.

8. Shoshana Zuboff, The Age of Surveillance Capitalism, PublicAffairs, 2019.

9. Solove, D. J., Understanding Privacy, Harvard University Press, 2020.

10. State v. Noll, Indiana Court of Appeals, 2017, No. 49A02-1610-CR-2217

11. United Nations General Assembly, Resolution 68/167 on the Right to Privacy in the Digital Age, 2013.

12. Zuboff, S., The Age of Surveillance Capitalism, PublicAffairs, 2019.

