التحديات التكنولوجية الرئيسية في حماية البيانات الشخصية في القانون العراقي والإيراني والاوربي

علي حسين علوان موحان الركابي

bmwali066@gmail.com

الطالب، دكتوراة، قانون الخاص، كلية القانون، جامعة قم، قم، الجمهورية الاسلامية الايرانية.

المشرف د.سيدحسن شبيرى زنجانى

الاستاذ المشارک، قانون الخاص و الملكية الفكرية، كلية القانون، جامعة قم، قم، الجمهورية الاسلامية الايرانية.

shshobeiri@gmail.com

الكلمات المفتاحية: التحديات، التكنلوجيا، البينات الشخصية، الذكاء الاصطناعي، المخاطر الرقمية.

كيفية اقتباس البحث

الركابي ، علي حسين علوان موحان ، سيدحسن شبيرى زنجانى ، التحديات التكنولوجية الرئيسية في حماية البيانات الشخصية في القانون العراقي والإيراني والاوربي،مجلة مركز بابل للدراسات الانسانية، آيار ٢٠٢٦، المجلد:١٦ ،العدد:٥ .

مفهرسة في Indexed
IASJ

مسجلة في Registered
ROAD

Key technological challenges in protecting personal data under Iraqi, Iranian, and European law

Ali Hussein Alwan Mohan Al-Rikabi
bmwali066@gmail.com
Ph.D. Student, Private Law, Faculty of Law, University of Qom, Qom, Islamic Republic of Iran.

Seyed Hassan Shobeiri (Zanjani)
shshobeiri@gmail.com
Associate Professor, Intellectual Property Rights and Private Law, Faculty of Law, University of Qom, Qom, Islamic Republic of Iran.

Keywords : Challenges, Technology, Personal Data, Artificial Intelligence, Digital Risks.

How To Cite This Article
Al-Rikabi ، Ali Hussein Alwan Mohan ،Seyed Hassan Shobeiri (Zanjani ،)Key technological challenges in protecting personal data under Iraqi, Iranian, and European law ,Journal Of Babylon Center For Humanities Studies, May 2026,Volume:16,Issue 5.

Abstract

This study addresses the contemporary technological challenges facing the protection of personal data in the digital age, focusing on a comparative analysis of the legal systems of Iraq, Iran, and the European Union. The research is significant because personal data has become a "vital asset" requiring special legal protection that goes beyond traditional texts to bridge the legislative gap resulting from the rapid advancement of big data processing technologies. The study reviews privacy-enhancing tools such as end-to-end encryption, privacy-enhanced computing (PEC) techniques, and data loss prevention (DLP) strategies, considering them the first line of defense in the digital environment. It

also analyzes the risks arising from Internet of Things (IoT) technologies, such as the lack of encryption and malware, as well as the challenges of artificial intelligence related to the accuracy of big data analysis and ensuring transparency. The comparison reveals the pioneering role of the European model (GDPR) in imposing strict standards of accountability and explicit consent, while Iraq and Iran rely on scattered texts or general civil liability rules to address violations. The study concludes that the Iraqi judiciary, despite the absence of a specialized law, has attempted to fill the gap by relying on Article 204 of the Civil Code to compensate for damages resulting from digital violations. The study recommends the need to expedite the enactment of comprehensive national laws that adopt the principle of "privacy from design" and keep pace with global cyber developments to enhance trust in electronic transactions..

المستخلص

تتناول هذه الدراسة التحديات التكنولوجية المعاصرة التي تواجه حماية البيانات الشخصية في ظل الثورة الرقمية، مع التركيز على تحليل مقارن بين الأنظمة القانونية في العراق وإيران والاتحاد الأوروبي. تبرز أهمية البحث من كون البيانات الشخصية أصبحت "أصولاً حيوية" تتطلب حماية قانونية خاصة تتجاوز النصوص التقليدية، لسد الفجوة التشريعية الناتجة عن تسارع تقنيات معالجة البيانات الضخمة. وتستعرض الدراسة الأدوات التقنية لتعزيز الخصوصية مثل التشفير من طرف إلى طرف، وتقنيات الحساب المعزز للخصوصية (PEC)، واستراتيجيات منع فقدان البيانات (DLP)، معتبرة إياها خط الدفاع الأول في البيئة الرقمية. كما تحلل الدراسة المخاطر الناشئة عن تقنيات إنترنت الأشياء (IoT) مثل نقص التشفير والبرمجيات الخبيثة، وتحديات الذكاء الاصطناعي المتعلقة بدقة تحليل البيانات الضخمة وضمان الشفافية. وتكشف المقارنة عن ريادة النموذج الأوروبي (GDPR) في فرض معايير صارمة للمساءلة والموافقة الصريحة، في حين يعتمد العراق وإيران على نصوص متفرقة أو قواعد المسؤولية المدنية العامة لمواجهة الانتهاكات. وتخلص الدراسة إلى أن القضاء العراقي، رغم غياب قانون متخصص، حاول سد الفراغ بالاستناد إلى المادة ٢٠٤ من القانون المدني لتعويض أضرار الانتهاكات الرقمية. وتوصي الدراسة بضرورة الإسراع في تشريع قوانين وطنية متكاملة تتبنى مبدأ "الخصوصية منذ التصميم" وتواكب التطورات السيبرانية العالمية لتعزيز الثقة في التعاملات الإلكترونية. اعتمدت الدراسة على المنهج المقارن بصفة أساسية، من خلال استعراض وتحليل القوانين العراقية والإيرانية في مقابل اللائحة الأوروبية (GDPR). كما تم استخدام المنهج

التحليلي الاستنباطي لتفكيك النصوص القانونية التقليدية (مثل القانون المدني) وبيان مدى قابليتها للتطبيق على الجرائم والانتهاكات الإلكترونية المعاصرة.

المقدمة

أصبحت البيانات الشخصية في العصر الرقمي من أهم القيم القانونية التي تتطلب حماية خاصة، نظرًا لما تتسم به من سهولة الجمع والمعالجة والتداول عبر التقنيات الحديثة، وما يترتب على ذلك من مخاطر تمسّ الخصوصية والحريات الفردية. وقد أفرز هذا الواقع حاجة ملحّة إلى تنظيم قانوني متوازن يضمن حماية البيانات الشخصية من جهة، ولا يقيّد حرية تداول المعلومات والحق في الوصول إليها من جهة أخرى، وهو ما دفع العديد من الدول إلى تبني تشريعات خاصة لمعالجة هذه الإشكالية.

في العراق، يواجه تنظيم حماية البيانات الشخصية تحديات جوهرية، في مقدمتها غياب قانون موحد ومتكامل ينظم هذا المجال بشكل صريح وشامل. فعلى الرغم من التطور الملحوظ في استخدام الوسائل الرقمية وانتشار المنصات الإلكترونية في التعاملات الحكومية والخاصة، لا يزال الإطار القانوني العراقي يقتصر على نصوص متفرقة لا ترقى إلى مستوى الحماية التشريعية المتخصصة. إذ أقرّ الدستور العراقي لسنة ٢٠٠٥ في المادة (١٧) حق الفرد في الخصوصية الشخصية بما لا يتعارض مع حقوق الآخرين والآداب العامة، كما تضمّن قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩ بعض الأحكام التي تجرّم الاعتداء على الخصوصية، كأفعال التنصت أو إفشاء الأسرار دون مسوّغ قانوني. وإلى جانب ذلك، طُرحت في السنوات الأخيرة، ولا سيما بعد عام ٢٠١٩، مشاريع ومسودات لقوانين تهدف إلى حماية البيانات الشخصية، غير أنها لم تُعتمد بصورة نهائية، الأمر الذي أوجد فراغًا تشريعيًا واضحًا في مواجهة التحديات المتنامية للواقع الرقمي.

أما في إيران، فتتجسد تحديات حماية البيانات الشخصية بصورة أوضح في إطار الحكومة الإلكترونية وتوسّع الخدمات الرقمية. وقد حُددت في هذا السياق أربعة تحديات رئيسية تتمثل في حماية خصوصية معلومات المواطنين مع تطور الحكومة الإلكترونية، وتحقيق التوازن بين حماية الخصوصية ومتطلبات المصلحة العامة، وضبط العلاقة بين حماية البيانات وحرية تداول المعلومات، فضلًا عن ضمان حق المواطن في الوصول إلى المعلومات دون الإخلال بسرية بياناته الشخصية. وتعكس هذه التحديات سعي المشرّع الإيراني إلى التوفيق بين متطلبات الإدارة الإلكترونية الحديثة وحماية الحقوق الأساسية للأفراد، في ظل تعدد الجهات القائمة على جمع ومعالجة البيانات.

وعلى الصعيد الأوروبي، يُعدّ الاتحاد الأوروبي من أكثر النظم القانونية تقدمًا في مجال حماية البيانات الشخصية، إذ اعتمد اللائحة العامة لحماية البيانات (GDPR) التي دخلت حيز التنفيذ عام ٢٠١٨. وتمثل هذه اللائحة إطارًا قانونيًا متكاملًا ونموذجًا عالميًا رائدًا، لما تتضمنه من مبادئ صارمة تفرض الشفافية والمشروعية في جمع ومعالجة البيانات، وتكفل حقوقًا واسعة لأصحاب البيانات. كما تمتاز باتساع نطاق تطبيقها، حيث تُلزم أي جهة تتعامل مع بيانات شخصية لمواطني الاتحاد الأوروبي، ولو كانت خارج إقليمه، بالامتثال لأحكامها، الأمر الذي عزّز من مستوى الحماية القانونية للبيانات الشخصية ورسّخ مكانة التشريع الأوروبي كمرجع مقارن في هذا المجال.

أولا: الأهمية

تنبثق أهمية البحث من كون البيانات الشخصية أصبحت "أصولاً حيوية" وقيمًا قانونية تتطلب حماية خاصة في العصر الرقمي. وتتجلى هذه الأهمية في:

١. ضرورة سد الفراغ التشريعي في العراق الذي يعتمد حالياً على نصوص متفرقة وقواعد تقليدية لا تواكب مخاطر الفضاء الإلكتروني.

٢. توضيح العلاقة الارتباطية بين حماية البيانات والحق الدستوري في الخصوصية وحرمة الحياة الخاصة.

٣. مواكبة التطورات التقنية العالمية والدروس المستفادة من التجربة الأوروبية لتعزيز الثقة الرقمية والتنمية المستدامة.

ثانيا: الأهداف

يسعى البحث إلى تحقيق جملة من الأهداف، أبرزها:

١.تحديد المفهوم القانوني والتقني للبيانات الشخصية وخصائصها في البيئة الرقمية.

٢.تحليل التقنيات الأمنية المستخدمة لحماية البيانات مثل التشفير وتدابير منع فقدان البيانات (DLP).

٣.رصد التحديات القانونية والتقنية التي تواجه النظم القانونية (العراقي، الإيراني، الأوروبي) في حماية البيانات.

٤.تقديم رؤية تشريعية تساهم في صياغة قانون موحد ومتكامل لحماية البيانات في البيئة الوطنية.

Journal Of Babylon Center For Humanities Studies 2026 Volume :16 Issue : 5
(ISSN): 2227-2895 (Print) (E-ISSN):2313-0059 (Online)

ثالثا: الإشكالية

تتمثل الإشكالية الرئيسية في وجود "فجوة تشريعية" واضحة في العراق وإيران بين واقع تقني متسارع يعتمد على جمع ومعالجة البيانات الضخمة، وبين إطار قانوني قاصر يفتقر لتعريفات جامعة مانعة وقواعد مسؤولية متخصصة. ويؤدي هذا الغياب إلى صعوبة الموازنة بين متطلبات المصلحة العامة والحكومة الإلكترونية من جهة، وبين الحق الفردي في الخصوصية المعلوماتية من جهة أخرى، مما يجعل البيانات عرضة للانتهاكات دون رادع قانوني كافٍ.

رابعا: التساؤلات

١.ما هو المفهوم القانوني للبيانات الشخصية وما هي الخصائص التي تميزها في النظم المقارنة؟.

٢.ما مدى تساهم التقنيات الحديثة (كالتشفير وSASE) في تعزيز خصوصية البيانات؟.

٣.ما هي أبرز التحديات التي يفرضها إنترنت الأشياء والذكاء الاصطناعي على أمن المعلومات الشخصية؟.

٤.كيف تعامل القضاء العراقي والإيراني مع انتهاكات البيانات في ظل غياب تشريع متخصص؟.

رابعاً: منهج البحث

اعتمدت الدراسة على المنهج المقارن بصفة أساسية، من خلال استعراض وتحليل القوانين العراقية والإيرانية في مقابل اللائحة الأوروبية (GDPR). كما تم استخدام المنهج التحليلي الاستنباطي لتفكيك النصوص القانونية التقليدية (مثل القانون المدني) وبيان مدى قابليتها للتطبيق على الجرائم والانتهاكات الإلكترونية المعاصرة.

خامسا: هيكلية البحث

تم تقسيم البحث إلى مبحثين أساسيين وفق التقسيم الآتي:

* المبحث الأول: الإطار المفاهيمي والتقني لحماية البيانات الشخصية.
* المبحث الثاني: التحديات التكنولوجية الرئيسية لحماية البيانات الشخصية.

المبحث الأول/ الإطار المفاهيمي والتقني لحماية البيانات الشخصية

يعتبر اندماج نظم المعلومات والاتصال وظهور تكنولوجيا تقنية المعلومات الحديثة دافعًا أساسيًا لاستحداث أطر قانونية متطورة لحماية البيانات الشخصية على الإنترنت، إذ بات هذا الحق من المتطلبات الأساسية لضمان خصوصية الفرد في حياته الخاصة والمهنية. ففي **جمهورية العراق**، يتجلى هذا التوجه في محاولات تنظيم الجرائم المتعلقة بالبيانات الشخصية مثل التخزين

غير المشروع، وإفشاء البيانات سواء عمدًا أو نتيجة إهمال، والمعالجة غير المصرح بها التي تتجاوز الغرض القانوني المخصص لها. وعلى الرغم من إمكانية تطبيق القوانين التقليدية على بعض هذه الجرائم، إلا أن الواقع الرقمي المتغير يستدعي صياغة نصوص قانونية متخصصة تواكب التطورات التقنية وتحقق حماية فعّالة للمعلومات الشخصية[١].

وعلى الجانب الآخر، تواجه **دولة إيران** تحديات مماثلة في ظل تبادل البيانات الإلكترونية بين المؤسسات العامة والخاصة، مما جعل مسألة حماية المعلومات قضية استراتيجية ذات أهمية بالغة. ففي هذا السياق تُصنف المعلومات إلى نوعين رئيسيين: المعلومات العامة والمعلومات الشخصية، حيث تُعد الأخيرة من أصول الدولة الحيوية. ويترتب على ذلك ضرورة منع الوصول غير المصرح به إلى هذه البيانات من قبل جهات أجنبية، إذ أن مثل هذا الوصول قد يُستخدم لاستغلال المعلومات البيومترية في تطوير أسلحة بيولوجية مدمرة أو لاختراق نظم الرواتب مما يهدد الاستقرار الاقتصادي. وتعكس هذه التجربة الحاجة إلى تبني آليات تشريعية وتنفيذية قوية تحمي المعلومات في ظل التحولات الرقمية والعولمة.

وعليه سنقسم المبحث الى مطلبين وعلى النحو الاتي:

المطلب الأول/ مفهوم البيانات الشخصية وأنواعها في البيئة الرقمية.

المطلب الثاني/ مفهوم التقنيات المستخدمة لحماية البيانات في القانون العراقي والإيراني والاوربي.

المطلب الأول /مفهوم البيانات الشخصية في القانون العراقي والإيراني والاوربي

كلمة البيانات مشتقة من الجذر اللغوي بين، أي إظهار الشيء وإخراجه من حيز الإبهام إلى حيز الوضوح. وتشير البيانات إلى المعلومات التفصيلية المتعلقة بشخص معين أو بشيء ما، والتي يمكن من خلالها الاستدلال عليه. أما مصطلح "الشخصية" في اللغة، فيرتبط بما يميز فردًا بعينه عن غيره، مما يعني أن البيانات تصبح "شخصية" عندما تتعلق بأشخاص طبيعيين يمكن تحديد هويتهم بشكل مباشر أو غير مباشر[٢].

أما اصطلاحًا، فتُعرَّف البيانات الشخصية بأنها مجموعة من الحقائق التي تأتي عادةً على هيئة أرقام أو حروف، مثل بيانات الهوية الشخصية، أو المعلومات المدخلة في النماذج، أو قراءات أجهزة الاستقبال. كما يُعرفها البعض بأنها "مجموعة من المعلومات التي ترتبط بالفرد وتمسه بشكل مباشر".

وقد جاءت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لتعريف البيانات الشخصية بأنها "كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة تقنية المعلومات، مثل الأرقام، الحروف، الرموز

وما إلى ذلك". كما عرّفتها الاتفاقية الأوروبية لحماية الأشخاص من المعالجة الآلية للبيانات بأنها "أي معلومة تتعلق بشخص طبيعي محدد أو قابل للتحديد".

يتضح مما سبق أن حماية البيانات الشخصية تهدف إلى الحفاظ على خصوصية الأفراد ومنع انتهاك معلوماتهم الشخصية، سواء دستوريًا أو تشريعيًا. وتتكون البيانات الشخصية من معلومات من شأنها التعريف بشخص معين، مثل الاسم، الصورة، الصوت، رقم الهوية، البريد الإلكتروني، الرموز، البصمة، بالإضافة إلى الحالة الشخصية، والوضع العائلي، والمالي، وغيرها من البيانات التي يمكن من خلالها تحديد هوية الشخص الطبيعي.

وبناءً على ما تقدم، يمكن **مفهوم البيانات الشخصية** بأنه "حق الإنسان في الحفاظ على بياناته الشخصية وحمايتها من الانتهاك أو الاعتداء[٣].

ولا بد من التأكيد على أن في ظل غياب قانون محدد لحماية البيانات الشخصية[٤] في العراق، تبرز أهمية تشريع قانون يُعنى بحماية خصوصية الأفراد وسرية بياناتهم. **فالدستور العراقي** لعام ٢٠٠٥، في المادة ١٧، يركز على حماية الحياة الخاصة، دون التطرق بشكل صريح إلى حماية سرية البيانات الشخصية. مع التطور التكنولوجي السريع، أصبحت البيانات الشخصية من أهم الموارد في العالم الرقمي، حيث تعتمد العديد من الشركات التقنية الكبرى على جمع وتحليل بيانات المستخدمين وتفضيلاتهم. هذا الواقع يستدعي من السلطة التشريعية التعامل مع هذا الموضوع بحساسية عالية، والعمل على سن قانون خاص لحماية البيانات الشخصية، لمواجهة أي انتهاكات أو تلاعب ببيانات الأفراد، خاصة مع تزايد حوادث تسريب وبيع البيانات في الفضاء الإلكتروني. تشريع مثل هذا القانون سيساهم في تعزيز حقوق المواطنين الرقمية، ويضع إطارًا قانونيًا يضمن حماية بياناتهم الشخصية من أي انتهاكات محتملة[٥].

يلاحظ لم يقم **المشرع العراقي**[٦] **بتعريف البيانات الشخصية** بدقة في قانون البطاقة الوطنية. حيث عُرف القيد المدني بأنه "الوحدة الأساسية لقاعدة البيانات القابلة للتطوير، والتي تحتوي على المعلومات السكانية والحياتية المتعلقة بمراحل حياة المواطن منذ ولادته وحتى وفاته، ويكون له رقم تعريفي مستقل وغير قابل للتكرار، يمكن للوسيط الإلكتروني الوصول إلى معلومات القيد غير المحدد من خلاله". يشير هذا النص إلى أن بيانات أي شخص تتحول من الصيغة الورقية إلى الصيغة الرقمية بموجب القانون المذكور. كما أن تعريف القيد المدني السابق يختلف بشكل كبير عن التعريف الوارد في قانون الأحوال المدنية العراقي الملغي[٧].

عرف القيد المدني "التوضيحات الخاصة بالمكلف العراقي في السجل المدني"، ويشير السجل المدني بموجب القانون إلى "السجل الأساسي الذي يتضمن قيود الأحوال المدنية للعراقيين".

من خلال ما سبق، نستنتج أن **البيانات الشخصية** تنقسم إلى نوعين: النوع الأول هو التقليدي، والذي يعتمد على الوثائق الورقية، وكان معمولاً به سابقاً في معظم الدول، بما في ذلك العراق. حيث تشير القوانين العراقية القديمة إلى أن جميع قيود المواطنين كانت تُسجل في سجلات يمكن الرجوع إليها عند الحاجة.

وقد تطور هذا النظام القديم إلى الصيغة الرقمية، حيث أصبح لكل شخص رقم تعريفي خاص به، يمكن من خلاله معرفة الصفات الطبيعية والشخصية والعائلية التي تميز هذا الشخص عن غيره. يُمنح هذا الرقم للفرد مرة واحدة طوال حياته، ويستمر حتى بعد وفاته. كما يمكن منح الأسرة رقم تعريفي يميزها عن الأسر الأخرى، مما يدل على أن المشرع العراقي قد اتجه، من خلال قانون البطاقة الوطنية، نحو التحول الرقمي، معتمداً على البطاقة الوطنية كمفتاح لكافة البيانات الشخصية لأي عراقي.

وبناءً على ما تقدم، يمكن تعريف البيانات الشخصية بأنها المعلومات التي يمكن الاستدلال منها على هوية شخص طبيعي معين، والتي تشمل الحروف والأرقام[٨].

وفي **الاتحاد الأوروبي تُعرَّف البيانات الشخصية** كأحد المفاهيم الأساسية في تشريعات حماية البيانات الشخصية، وفقًا للائحة العامة لحماية البيانات[٩]، على أنها أي معلومات تتعلق بشخص يمكن التعرف عليه أو له هوية محددة. يمكن ربط البيانات بشخص حقيقي وإمكانية التعرف عليه من خلال محتوى البيانات أو الغرض من معالجتها أو تأثير هذه المعالجة على الشخص. في إطار قانون الاتحاد الأوروبي، لتحديد ما إذا كان يمكن التعرف على هوية الشخص من خلال معالجة البيانات، يجب أخذ جميع الوسائل التي قد يستخدمها المتحكم أو المعالج بعين الاعتبار. يتعين مراعاة جميع العوامل الموضوعية، مثل التكلفة والوقت اللازمين لتحديد الهوية والتكنولوجيا المتاحة في وقت المعالجة، لتحديد ما إذا كان هناك احتمال معقول لتحديد هوية الشخص. وبناءً على معيار تحديد الهوية، فإن البيانات التي قد تؤدي إلى التعرف على شخص ما في المستقبل تشملها القوانين أيضًا؛ حيث يمكن أن يساهم هذا المعيار في خلق الديناميكيات اللازمة في التشريعات،

كذلك تعرف المادة ٤/١ من اللائحة العامة لحماية البيانات (GDPR) التابعة **للاتحاد الأوروبي**، رقم ٦٧٩ لسنة ٢٠١٦، "**البيانات الشخصية**" بأنها: "أي معلومات تتعلق بشخص طبيعي محدد أو يمكن تحديده"[١٠].

أما المادة الثانية من قانون حماية البيانات الشخصية الفرنسي التابع للاتحاد الأوربي رقم ٨٠١ لسنة ٢٠٠٤، فتعرّف "البيانات الشخصية" بأنها: "أي معلومة تتعلق بشخص طبيعي يمكن تحديد

هويته، سواء بشكل مباشر أو غير مباشر، سواء كان ذلك من خلال رقمه الشخصي أو أي شيء آخر يتعلق به".

وبناءً على التعريفين الأوروبي والإيراني [١١]، يمكن القول إن أي معلومة تتعلق بشخص طبيعي – وليس بالشخص المعنوي – تُعتبر بيانات شخصية تخضع للحماية القانونية، طالما أن هذا الشخص يمكن تحديد هويته بشكل مباشر أو غير مباشر.

وأشار الباحث إلى أن "الخصوصية وبيع البيانات الشخصية أصبحتا من الظواهر الشائعة في سوق العالم الافتراضي، خاصة مع تسرب البيانات بين الحين والآخر نتيجة التعديات على أنظمة شبكات التواصل الاجتماعي". وأكد على أهمية "وضع قانون يعالج هذه القضية ويضمن حقوق المواطنين في الفضاء الرقمي".

لذا تتميز البيانات الشخصية[١٢] بعدة خصائص تميزها عن غيرها، ومن أبرز هذه الخصائص أنها ترتبط بالشخص نفسه، مما يعني أن حقوق استخدامها تعود فقط لصاحبها، فهو الوحيد المخول باستعمالها. وبالتالي، يمتلك الإنسان مجموعة من الحقوق الشخصية التي لا يمكن المساس بها أو التنازل عنها، مثل الحق في الاسم والحق في الصورة، بالإضافة إلى البيانات الشخصية التي هي محور حديثنا.

ومن الخصائص الأخرى للبيانات الشخصية أنها تعتبر حقوقًا غير مالية، أي أنها لا تتعلق بالأموال، بل تشكل جزءًا من الهوية القانونية للفرد. فلا يمكن تحديد قيمة مالية للاسم الشخصي إلا إذا تم استخدامه كاسم تجاري، وفي غير ذلك، يُعتبر حقًا معنويًا وعنصرًا من عناصر إثبات الذات[١٣].

كما أن البيانات الشخصية تتميز بإمكانية تحويلها من الصيغة الورقية التقليدية إلى الصيغة الرقمية باستخدام برامج معينة. وقد أشار المشرع العراقي إلى ذلك في نصه الذي ينص على أن "القيد المدني هو الوحدة الأساسية لقاعدة البيانات القابلة للتطوير، والتي تحتوي على المعلومات السكانية والحياتية المتعلقة بمراحل حياة المواطن منذ ولادته وحتى بعد وفاته... إلخ".

وتجدر الإشارة انه شهد العالم تطورًا تكنولوجيًا هائلًا، حمل معه العديد من المزايا لكنه في الوقت ذاته تسبب في خسائر وجرائم عديدة، خاصة في مجال انتهاك البيانات الشخصية. فقد أصبحت هذه الانتهاكات محط اهتمام كبير من قبل المشرعين والخبراء، نظرًا لما تسببه من أضرار واسعة النطاق لا يمكن إصلاحها، مما دفع الحكومات إلى إقرار قوانين جديدة لحماية البيانات الشخصية.

وعلى الرغم من أن الخصوصية كانت محمية بالقوانين التقليدية منذ فترة طويلة، فإن البيانات الشخصية، التي تعد جزءًا أساسيًا من الخصوصية في عصر الإنترنت، باتت بحاجة إلى تشريعات حديثة تتماشى مع التغيرات التقنية. ولذلك، أصبح تطوير القوانين لتلبية احتياجات العصر الرقمي أمرًا ضروريًا وموضع اهتمام مستمر[١٤].

في هذا السياق، **تناول الباحث دراسة** مفهوم البيانات الشخصية[١٥] في لوائح الاتحاد الأوروبي والنظام القانوني العراقي والإيراني، حيث تم تحليل الحاجة إلى تحديث القوانين بما يتماشى مع التقدم الرقمي. كما تؤكد على ضرورة تقديم تعريف واضح وشامل للبيانات الشخصية، ودعمه داخل الأطر القانونية. إذ يُلاحظ أن القوانين والعراقية الإيرانية الحالية تفتقر إلى تعريف متماسك للبيانات الشخصية، وهو ما يستوجب سد هذه الفجوة التشريعية.

لطالما كانت حماية الخصوصية الفردية مبدأً عالميًا يحظى باهتمام المؤسسات الدولية، وقد نصت العديد من الوثائق القانونية على ضرورة احترامها. ومع تطور التكنولوجيا، ازدادت أهمية البيانات الشخصية، حيث أصبح من السهل معالجتها ونقلها بسرعة عبر الفضاء الإلكتروني، مما استدعى تدخلًا تشريعيًا أكبر لحمايتها[١٦].

حيث تسلط دراستنا هذه الضوء على الحاجة إلى تشريع قانون حماية البيانات الشخصية في العراق وإيران، لتعزيز حماية الخصوصية في الفضاء الإلكتروني وتحديث البنية القانونية لمواكبة التطورات الرقمية.

يقترح الباحث تحديث الإطار القانوني المتعلق بالعيوب الصناعية وتطوير آليات الرقابة الفنية بما يتماشى مع التطورات التكنولوجية العالمية، مع ضرورة إعادة النظر في معايير الفحص والتقييم لضمان تقديم منتجات آمنة وخالية من العيوب. ويؤكد على أهمية الاستفادة من التجارب الأوروبية الناجحة في هذا المجال، مع تكييفها لتناسب السياقات المحلية في العراق وإيران، بحيث يتم إنشاء آليات رقابية متكاملة تشمل جميع مراحل العملية الإنتاجية من البداية وحتى التوزيع النهائي.

كما يرى الباحث ضرورة تعزيز التعاون الفني والقانوني مع الجهات الدولية المختصة، وذلك لتبادل الخبرات وتحسين معايير الفحص الفني والتصنيعي، مع توفير برامج تدريبية مستمرة للمختصين في الرقابة الصناعية. وفي هذا السياق، يقترح الباحث مراجعة العقوبات والإجراءات القانونية بحيث تكون رادعة وتضمن حماية حقوق المستهلك دون التأثير سلبًا على بيئة الابتكار الصناعي.

وعلاوة على ذلك، **يوصي الباحث** بضرورة تشريع قانون خاص بحماية البيانات الشخصية يشمل كلا من البيانات التي تُنقل عبر الإنترنت والتقليدية. ويعتبر هذا التشريع خطوة أساسية لتعزيز الثقة بين المستهلكين والمؤسسات، وضمان توازن دقيق بين حماية الخصوصية وحرية تداول المعلومات في عصر تكنولوجيا المعلومات والتواصل الرقمي. إذ ينبغي أن يتضمن القانون معايير صارمة لمعالجة البيانات وحمايتها، إلى جانب آليات رصد فعالة لمعالجة أي انتهاكات محتملة في هذا المجال.

وكذلك، يؤكد الباحث أن تبني نهج متكامل يجمع بين الابتكار القانوني والتطوير التقني ليس مجرد ضرورة لتحسين جودة المنتجات والخدمات الصناعية، بل هو استراتيجية أساسية لتعزيز التنمية الاقتصادية المستدامة وبناء بيئة تجارية تحترم حقوق المستهلكين وتواكب التطورات العالمية في عصر المعلومات.

المطلب الثاني/ مفهوم التقنيات المستخدمة لحماية البيانات في القانون العراقي والإيراني والاوربي

يلاحظ انه أدى الانتشار الواسع والتطور المستمر للتقنيات التكنولوجية الحديثة إلى رقمية حياة الأفراد، حيث انتقلت معالجة البيانات من الشكل الورقي التقليدي إلى المعالجة الإلكترونية. ولم تعد البيانات الشخصية حبيسة الملفات والدفاتر، بل أصبحت متاحة في بيئة رقمية يسهل الوصول إليها، مما يجعلها عرضة للعديد من الانتهاكات.

مع ظهور الحواسيب، تم إنشاء قواعد بيانات رقمية تحتوي على المعلومات الشخصية للأفراد، وربطها بشبكات تسهل تبادل البيانات بين مختلف الجهات. كما انتشر مفهوم التسويق الإلكتروني، الذي يعتمد على استغلال البيانات الشخصية للأفراد في عمليات الدعاية والإعلان، وهو ما قد يمثل انتهاكًا لخصوصيتهم ويمس حقوقهم وحرياتهم الأساسية. ويكتسب هذا الأمر أهمية خاصة، نظرًا لأن حماية البيانات الشخصية ترتبط ارتباطًا وثيقًا بالحق الدستوري في حرمة الحياة الخاصة[١٧].

وقد تطور مفهوم الحق في الخصوصية مع تقدم التقنيات الرقمية، ليشمل الحق في حماية الخصوصية المعلوماتية، وضمان سرية الاتصالات، وحماية البيانات الشخصية من أي انتهاك أو استخدام غير مشروع. وهناك علاقة وثيقة بين الحق في الخصوصية والحق في حماية البيانات الشخصية، حيث تُعد البيانات الشخصية جزءًا لا يتجزأ من الحق في الحياة الخاصة، وأي انتهاك لها يُعد تعديًا صارخًا على خصوصية الأفراد.

لذلك، أصبح التدخل التشريعي ضرورة حتمية في عصر التكنولوجيا الرقمية، حيث أصبح من السهل جمع البيانات الشخصية للأفراد وتخزينها وتعديلها ونقلها وحتى حذفها في ثوانٍ معدودة. هذا الواقع يستوجب وضع ضوابط قانونية صارمة لحماية البيانات الشخصية وضمان عدم إساءة استخدامها[١٨].

وقد دفع هذا التحدي العديد من الدول، سواء في أوروبا أو العالم العربي، إلى اتخاذ إجراءات تشريعية لمواجهة مخاطر انتهاك الخصوصية. ومن أبرز هذه الإجراءات إصدار اللائحة الأوروبية لحماية البيانات الشخصية من قبل البرلمان والمجلس الأوروبي، بهدف وضع إطار قانوني يحمي حقوق الأفراد في بيئتهم الرقمية.

مفهوم التقنيات المستخدمة لحماية البيانات الشخصية[١٩]: تُعتبر تقنيات تعزيز الخصوصية وسائل فعّالة لحماية البيانات. تتيح هذه التقنيات لمستخدمي الإنترنت الحفاظ على خصوصية معلومات التعريف الشخصية (PII) التي تقدمها التطبيقات والخدمات أو التي يتم معالجتها. تُستخدم هذه الأساليب لتقليل احتكار البيانات الشخصية دون التأثير على كفاءة أداء نظام المعلومات.

يهدف استخدام هذه **التقنيات إلى حماية البيانات الشخصية** وضمان سرية المعلومات لمستخدميها. تُعتبر إدارة حماية البيانات أولوية للمنظمات التي تتحمل مسؤولية المعلومات التي تحدد هوية الأفراد، مما يمكّن المستخدمين من اتخاذ مجموعة من الإجراءات المتعلقة ببياناتهم الشخصية التي يتم إرسالها إلى مزودي خدمات الإنترنت أو الشركات أو مستخدمين آخرين، أو التي يتم استخدامها من قبلهم.

تشمل الأهداف المرتبطة بالتقنيات المعززة للخصوصية[٢٠] زيادة السيطرة على المعلومات الشخصية المرسلة إلى مزودي خدمات الإنترنت أو الشركات (أو مستخدمين آخرين على الشبكة) (تقرير المصير). تهدف هذه التقنيات إلى تقليل كمية البيانات الشخصية التي يتم جمعها واستخدامها من قبل مزودي الخدمات والشركات، بالإضافة إلى استخدام أسماء مستعارة وبيانات مجهولة الهوية لحماية الهوية. كما تسعى هذه التقنيات لتحقيق الموافقة المستنيرة عند تقديم المعلومات الشخصية لمزودي الخدمات على الإنترنت أو الشركات. في سياق المفاوضات المتعلقة بالخصوصية، يقوم المستهلك ومزودو الخدمات بوضع سياسات الخصوصية والحفاظ عليها وتطويرها من خلال اتفاقات فردية، مما يتيح لهم الاختيار المستمر بين بدائل الخدمة.

ولابد من الإشارة الى تقنيات التي تستخدم حماية خصوصية البيانات الشخصية وهي على النحو الاتي[٢١]:

١. **تشفير البيانات:** تعمل تقنية تشفير البيانات على تحويل المعلومات إلى رموز، مما يمنع الوصول غير المصرح به ويضمن سرية البيانات وأمانها أثناء النقل والتخزين. يتضمن ذلك استخدام خوارزميات لتشفير البيانات في نقطة المصدر قبل إرسالها عبر الشبكات أو تخزينها في قواعد البيانات. يُعتبر التشفير أمرًا حيويًا لحماية المعلومات الحساسة من الاعتراض والوصول غير المصرح به، حتى في حال تعرض تدابير الأمان المادية للخطر[٢٢].

تُعد إدارة المفاتيح جزءًا أساسيًا من عملية التشفير، حيث أن سوء التعامل مع المفاتيح يمكن أن يعرض البيانات المشفرة للخطر. ينبغي على المؤسسات اعتماد ممارسات آمنة لإدارة المفاتيح وتحديث أساليب التشفير بانتظام لمواجهة التهديدات المتطورة. يضمن استخدام التشفير من طرف إلى طرف في أدوات الاتصال، بالإضافة إلى تشفير البيانات الثابتة وأثناء النقل، حماية البيانات والامتثال للوائح الخصوصية.

٢. **تسجيل الدخول الأحادي (SSO):** تسجيل الدخول الأحادي (SSO) هو نظام مصادقة يتيح للمستخدمين الوصول إلى عدة تطبيقات باستخدام مجموعة واحدة من بيانات الاعتماد. يُحسن تسجيل الدخول الأحادي تجربة المستخدم من خلال تقليل الحاجة إلى تذكر كلمات مرور متعددة، مما يسهل عملية الدخول ويعزز الأمان.

واستناد اً الى ما سبق ذكره تُعد التقنيات التكنولوجية المستخدمة في حماية البيانات الشخصية مجموعة من الوسائل الفنية والإجراءات الأمنية التي تهدف إلى تأمين المعلومات والحفاظ على سريتها وسلامتها في ظل التطورات الرقمية المتسارعة. تشمل هذه التقنيات أدوات مثل التشفير الذي يحول البيانات إلى صيغة غير قابلة للقراءة بدون مفتاح فك تشفير صحيح، والتعمية وإخفاء الهوية والتجزئة التي تقلل من إمكانية ربط البيانات بمستخدمها الأصلي، بالإضافة إلى التوقيع الإلكتروني الذي يضمن سلامة ومصداقية المعاملات الرقمية. كما تتضمن الإجراءات الأمنية أنظمة المراقبة والكشف عن الاختراق، والتدابير الوقائية لحماية شبكات المعلومات من التهديدات السيبرانية، مما يجعل حماية البيانات الشخصية عملية شاملة تتطلب تضافر الجهود التقنية والتشريعية.

٣. **استراتيجيات منع فقدان البيانات (DLP)**[٢٣]:تتضمن استراتيجيات منع فقدان البيانات (DLP) مجموعة من الممارسات والأدوات التي تهدف إلى حماية البيانات من الخروقات، مما يضمن عدم فقدان المعلومات الحساسة أو إساءة استخدامها أو الوصول إليها من قبل مستخدمين غير مصرح لهم. تقوم حلول DLP بمراقبة أنشطة نقاط النهاية وحركة مرور الشبكة

وتخزين البيانات، مما يمكّن المؤسسات من تحديد المخاطر المرتبطة بتسرب البيانات والتقليل من آثارها. كما تسهم هذه الحلول في الامتثال للمتطلبات التنظيمية المتعلقة بحماية البيانات.

يتطلب تنفيذ DLP تصنيف البيانات، ووضع السياسات، وتطبيق الأدوات القادرة على اكتشاف الأنشطة المشبوهة والاستجابة لها. من الضروري تحديث هذه السياسات بانتظام ودمج DLP مع بروتوكولات الأمان الأخرى لضمان حماية ديناميكية للبيانات. كما أن المراقبة المستمرة والاستعداد للاستجابة للحوادث يعدان أمرين حيويين لضمان فعالية نظام منع فقدان البيانات[٢٤].

٤. **الحساب المعزز للخصوصية (PEC)**:يشمل الحساب المعزز للخصوصية (PEC) تقنيات تتيح معالجة البيانات دون التأثير على الخصوصية. تتضمن هذه التقنيات الحساب الآمن متعدد الأطراف، والتشفير المتماثل، والتعلم الموحد. يسمح PEC باستخدام البيانات لأغراض التحليل وتدريب النماذج دون المساس بالخصوصية.

٥. **حافة خدمة الوصول الآمن (SASE)**: حافة خدمة الوصول الآمن (SASE) هي إطار عمل يجمع بين خدمات أمان الشبكة وإمكانات الشبكة واسعة النطاق (WAN) لتلبية احتياجات الوصول الآمن للمؤسسات الموزعة. تدمج SASE تقنيات مثل SD-WAN، وبوابات الويب الآمنة، والوصول إلى الشبكة بدون ثقة (ZTNA) لضمان اتصالات شبكة آمنة وفعالة وموثوقة للمستخدمين بغض النظر عن موقعهم.

يتطلب تنفيذ SASE بنية تحتية للشبكة قادرة على دعم تدابير أمنية شاملة. يجب على المؤسسات أن تعطي الأولوية للتوافق بين مكونات الأمان والشبكة المختلفة. يمكن أن يؤدي اعتماد نموذج SASE إلى تعزيز أمان البيانات بشكل كبير من خلال توفير إطار عمل متكامل يعالج تحديات الأمن السيبراني الحديثة بشكل ديناميكي[٢٥].

على المستوى النظري يمكن تصنيف تقنيات تعزيز الخصوصية وفقًا لافتراضاتها[٢٦]:

أ. **تقنيات الخصوصية البسيطة** : تفترض هذه التقنيات إمكانية الوثوق بالطرف الثالث لمعالجة البيانات. يعتمد هذا النموذج على الالتزام والموافقة والتنظيم والمراجعة.

من الأمثلة على هذه التقنيات التحكم في الوصول وتشفير القناة (مثل بروتوكول طبقة المقابس الآمنة SSL/TLS).

ب. **تقنيات الخصوصية المعقدة** : تعتبر هذه التقنيات أن أي كيان لا يمكنه انتهاك خصوصية المستخدم، حيث تفترض أنه لا يمكن الوثوق بالطرف الثالث في معالجة البيانات. الهدف هنا هو تقليل كمية البيانات وتقليل الاعتماد على الثقة بالطرف الثالث.

Journal Of Babylon Center For Humanities Studies 2026 Volume :16 Issue : 5
(ISSN): 2227-2895 (Print) (E-ISSN):2313-0059 (Online)

واستخلاصا لما سبق ذكره انه في العراق، تعتمد التشريعات ذات الصلة على مجموعة من القوانين المتفرقة مثل قانون مكافحة جرائم المعلوماتية وقانون المعاملات الإلكترونية والتوقيع الإلكتروني. وعلى الرغم من أن هذه التشريعات تسعى إلى تطبيق تقنيات مثل التشفير والتوقيع الإلكتروني وإجراءات الأمن السيبراني لحماية البيانات أثناء نقلها وتخزينها، إلا أن غياب إطار قانوني شامل يؤدي إلى بعض الثغرات في التطبيق العملي لهذه التقنيات، مما يستدعي ضرورة تطوير تشريعات متكاملة تراعي التطورات التقنية وتوفر حماية فعالة للبيانات الشخصية[٢٧].

أما في إيران، فيتسم الإطار القانوني بتركيزه على حماية البيانات في إطار الأمن القومي، حيث تُستخدم تقنيات التشفير القوية وأنظمة حماية الاتصالات لضمان تأمين المعلومات أثناء نقلها عبر الشبكات الرقمية. تبرز هنا أهمية الإجراءات الأمنية الدقيقة التي تُراقب تدفق البيانات وتمنع محاولات التجسس أو الاعتراض غير المشروع. ومع ذلك، فإن هذا النهج الذي يعطي الأولوية للأمن قد يؤدي إلى تقييد بعض حقوق الخصوصية الفردية، حيث يُنظر إلى حماية البيانات من منظور يركز بشكل أكبر على السيطرة والأمن القومي[٢٨].

على النقيض من ذلك، **يُعد النظام الأوروبي**[٢٩] نموذجًا متقدمًا وشاملاً في مجال حماية البيانات، خاصةً بموجب اللائحة العامة لحماية البيانات (GDPR). يعمل الإطار الأوروبي على تبني أحدث التقنيات مثل التشفير، والتعمية، وإخفاء الهوية والتجزئة، بالإضافة إلى التوقيع الإلكتروني الذي يضمن صحة وسلامة المعاملات الإلكترونية. كما تفرض اللائحة متطلبات تنظيمية صارمة تشمل تقييم المخاطر المستمر واتباع مبادئ حماية البيانات منذ التصميم وحتى التنفيذ، مما يحقق توازنًا دقيقًا بين تأمين البيانات الشخصية والحفاظ على حقوق الأفراد وخصوصيتهم.

بالمقارنة، نجد أن جميع النظم القانونية الثلاثة تسعى إلى حماية البيانات الشخصية باستخدام تقنيات تكنولوجية متطورة، إلا أن الفروق الرئيسية تكمن في الإطار التنظيمي والتشريعي المُطبق. ففي العراق، يُستخدم مزيج من التقنيات في ظل تشريعات متفرقة، بينما تتبنى إيران نهجًا أمنيًا يركز على حماية المعلومات في إطار الأمن القومي، في حين يوفر النظام الأوروبي منظومة متكاملة تجمع بين التقنيات الحديثة والضوابط القانونية الصارمة لضمان حقوق الأفراد وشفافية التعاملات الرقمية. تُبرز هذه المقارنة الحاجة الملحّة لتحديث التشريعات الوطنية بحيث تتماشى مع التطورات التقنية وتوفر حماية شاملة للبيانات الشخصية في عصر الرقمية.

المبحث الثاني/ التحديات التكنولوجية الرئيسية في حماية البيانات الشخصية

رغم المزايا الواسعة التي أتاحها التطور التكنولوجي في مجال معالجة البيانات الشخصية، إلا أن هذا التطور أفرز في القانون العراقي جملة من التحديات القانونية والعملية، لاسيما أن معظم

التشريعات النافذة لم تُصغَ في الأصل لمواكبة التحولات الرقمية المتسارعة. ويبرز في مقدمة هذه التحديات ضعف الإطار التشريعي المنظم لحماية البيانات الشخصية، ولا سيما في ما يتعلق بالسجلات الإلكترونية، وأمن المعلومات، والمسؤولية القانونية الناشئة عن الأعطال التقنية أو الاختراقات السيبرانية.

كما يعاني النظام القانوني العراقي من قصور في البنية التحتية الرقمية، الأمر الذي يحدّ من فعالية تطبيق القوانين ذات الصلة، فضلًا عن ضعف التأهيل التقني للكوادر القضائية والقانونية مما يقلل من الاستفادة المثلى من التكنولوجيا في حماية الحقوق المرتبطة بالبيانات الشخصية[٣٠].

وعليه سنقسم المبحث الى مطلبين وعلى النحو الاتي:

المطلب الأول/ تحديات الخصوصية في إنترنت الأشياء (IoT).

المطلب الثاني/ تحديات الذكاء الاصطناعي وتحليل البيانات.

المطلب الأول/ تحديات الخصوصية في إنترنت الأشياء (IoT)

تعتبر التحديات الأمنية في عالم إنترنت الأشياء (IoT) أمر هام جداً فهي تعبر الترابط بين الأجهزة المادية والبرامج وأجهزة الاستشعار والاتصال التي تمكن هذه الكائنات من الاتصال وتبادل البيانات الشخصية بهدف تقديم اتصال متقدم للأجهزة والأنظمة والخدمات التي تتجاوز الاتصالات من أنه الأخرى كما تغطي مجموعة متنوعة من البروتوكولات والمحالات والتطبيقات[٣١].

أولاً: نقص التشفير

يُعدّ التشفير من أهم الوسائل التقنية الرامية إلى حماية البيانات الشخصية ومنع الوصول غير المصرح به إليها، إلا أن ضعف آليات التشفير أو اعتماد خوارزميات غير متطورة يُشكّل تحدياً أمنياً حقيقياً في البيئة الرقمية. فبخلاف أنظمة الحوسبة التقليدية التي تتمتع بقدرات تخزين ومعالجة عالية، تعاني العديد من الأنظمة الحديثة، ولا سيما أجهزة إنترنت الأشياء، من محدودية الإمكانات التقنية، الأمر الذي يجعلها أكثر عرضة للاختراق، خاصة في ظل تطور أدوات القراصنة وقدرتهم على التعامل مع الخوارزميات المصممة للحماية.

ثانياً: عدم كفاية الاختبار والتحديث

أدى التوسع المتسارع في استخدام أجهزة إنترنت الأشياء إلى تركيز الشركات المصنّعة على سرعة الإنتاج وطرح الأجهزة في الأسواق، على حساب متطلبات الأمن السيبراني. وغالباً ما تُطرح هذه الأجهزة دون إخضاعها لاختبارات أمنية كافية، أو دون توفير تحديثات دورية لمعالجة

الثغرات الأمنية، مما يجعلها عرضة للاختراق ويُضعف من مستوى حماية البيانات التي تعالجها[٣٢].

ثالثاً: مخاطر كلمات المرور الافتراضية

تمثل كلمات المرور الافتراضية وبيانات الاعتماد الضعيفة أحد أبرز مصادر التهديد لأمن أجهزة إنترنت الأشياء، إذ يسهل على القراصنة استغلالها للوصول غير المشروع إلى الأنظمة. وإن استمرار الشركات أو المستخدمين في الاعتماد على بيانات اعتماد المصنع الافتراضية يُعرّض الأعمال والأصول ومعلومات العملاء الحساسة لمخاطر جسيمة، ويقوّض مبدأ حماية البيانات الشخصية[٣٣].

رابعاً: البرمجيات الخبيثة وبرامج الفدية في بيئة إنترنت الأشياء

تُعد البرمجيات الخبيثة، ولا سيما برامج الفدية، من أخطر التهديدات التقنية، إذ تعمل على تعطيل الأجهزة والأنظمة ومنع المستخدمين من الوصول إلى بياناتهم، مع الاستمرار في استغلال هذه البيانات أو احتجازها مقابل فدية مالية. وقد يمتد هذا الخطر إلى اختراق كاميرات وأجهزة ذكية أخرى والتجسس على المستخدمين، فضلاً عن استخدام نقاط الضعف كوسيلة لابتزاز الضحايا وإجبارهم على دفع مقابل لإعادة تشغيل الأجهزة أو استرجاع البيانات.

خامساً: الروبوتات المرتبطة بإنترنت الأشياء والعملات المشفرة

تشكل الروبوتات الخبيثة المرتبطة بإنترنت الأشياء تهديداً متزايداً لسوق العملات المشفرة، إذ قد تُستغل الأجهزة المخترقة في عمليات تعدين غير مشروعة أو في شن هجمات تؤثر على استقرار وقيمة العملات الرقمية. ويُعد هذا النوع من الاستغلال دليلاً على تداخل المخاطر التقنية بين حماية البيانات وأمن الأنظمة المالية الرقمية.

سادساً: عدم كفاية أمن الأجهزة

يشير ضعف أمن الأجهزة إلى غياب التدابير الوقائية اللازمة لحماية الأجهزة الإلكترونية، بما في ذلك الحواسيب والهواتف الذكية وأجهزة إنترنت الأشياء، من الهجمات الإلكترونية وسرقة البيانات. ويعود ذلك إلى أسباب متعددة، من بينها استخدام برمجيات قديمة، أو كلمات مرور ضعيفة، أو عدم معالجة الثغرات الأمنية، أو غياب أنظمة التشفير الفعالة، مما يؤدي إلى تسهيل الوصول غير المصرح به إلى البيانات الشخصية[٣٤].

سابعاً: الافتقار إلى التوحيد القياسي

يتمثل الافتقار إلى التوحيد القياسي في غياب معايير وبروتوكولات موحدة تحكم عمل الأنظمة والأجهزة المختلفة، الأمر الذي يؤدي إلى عدم التوافق بينها ويُضعف قابلية التشغيل البيني. وينعكس هذا الخلل سلباً على أمن البيانات، إذ يعرقل تبادل المعلومات بشكل آمن ويزيد من صعوبة تطبيق تدابير حماية موحدة وفعّالة[٣٥].

ثامناً: قابلية التعرض لهجمات الشبكة

تعتمد أجهزة إنترنت الأشياء اعتماداً أساسياً على الشبكات، مما يجعلها عرضة لمختلف أنواع الهجمات الشبكية، كاختراق الأنظمة أو هجمات حجب الخدمة (DoS). وتنشأ هذه القابلية نتيجة وجود ثغرات في البنية التحتية للشبكة، أو ضعف إدارة كلمات المرور، أو غياب التدابير الأمنية المناسبة، الأمر الذي قد يؤدي إلى سرقة البيانات، وانتهاك الخصوصية، وتعطيل الخدمات، والتسبب بخسائر مالية جسيمة.

تاسعاً: النقل غير الآمن للبيانات

يُقصد بالنقل غير الآمن للبيانات إرسالها عبر الشبكات أو الإنترنت دون توفير حماية تقنية كافية، مما يجعلها عرضة للاعتراض أو العبث أو السرقة، لا سيما عند استخدام بروتوكولات اتصال غير آمنة أو غير مشفرة. ولتفادي هذه المخاطر، يتعين اعتماد بروتوكولات آمنة مثل SSL أو TLS أو VPN، إلى جانب تشفير البيانات قبل إرسالها، بما يضمن الحفاظ على سريتها وسلامتها حتى في حال اعتراضها أثناء عملية النقل[٣٦].

يلاحظ انه يعاني النظام القانوني العراقي من نقص في التشريعات الحديثة التي تواكب التطورات التقنية والاجتماعية، ومنها حماية البيانات الشخصية عبر الإنترنت، مما يستدعي البحث في مدى إمكانية اعتماد قواعد المسؤولية المدنية المنصوص عليها في القانون المدني كإطار قانوني لحماية هذه البيانات. فقد نصت المادة (٢٠٤) من القانون المدني العراقي على أن "كل تعدٍ يصيب الغير بأي ضرر يستوجب التعويض"، ومن هذا المنطلق يمكن اعتبار أي فعل يؤدي إلى إلحاق ضرر بشخص نتيجة استعمال أو الاطلاع على بياناته الشخصية، فعلًا قابلاً للمساءلة المدنية. وتشمل البيانات الشخصية معلومات أساسية عن الفرد مثل الاسم، وتاريخ الميلاد، والحالة الاجتماعية، والحالة الصحية، ومستوى التعليم، وفصيلة الدم، وغيرها من البيانات التي تحدد هوية الشخص[٣٧].

ويُعرف فعل الاعتداء، أو ما يُسمى بالخطأ التقصيري، بأنه إخلال بالتزام قانوني سابق صادر عن سبق إدراك وتمييز. والالتزام القانوني السابق يقصد به واجب احترام حقوق الآخرين وعدم

الإضرار بهم، ويشمل الالتزام ببذل العناية اللازمة لمنع أو الحد من الأضرار التي قد تلحق بالآخرين. ويتحقق التعدي عندما يتجاوز المتعدي الحدود المقررة في السلوك القانوني سواء أكان الفعل متعمدًا أو غير متعمد، مع اعتماد معيار موضوعي لتحديد الانحراف عن الالتزام، إضافة إلى توفر عنصر الإدراك والتمييز لدى المتعدي، بحيث يكون مدركًا أن فعله يشكل تعديًا على الغير، وأنه مؤهل قانونيًا لتحمل المسؤولية المدنية[٣٨].

ومن الناحية الجنائية، عالج المشرع العراقي الاعتداء على البيانات الشخصية عبر الإنترنت بجرم التجاوز على سرية المعلومات وسلامة البيانات، إذ نص القانون على أنه: "يعاقب بالحبس مدة لا تقل عن سنتين ولا تزيد على خمس سنوات، وبغرامة لا تقل عن ثلاثة ملايين دينار ولا تزيد على خمسة ملايين دينار، كل من دخل عمدًا دون إذن موقعًا إلكترونيًا أو نظامًا معلوماتيًا أو أحد أجهزة الحاسوب أو ما في حكمها، وقام بالاطلاع على محتواها أو نسخه، أو حذف أو تدمير البيانات، أو الإفشاء عنها أو تغييرها، وتشدد العقوبة إذا كان مرتكب الجريمة موظفًا أو مكلفًا بخدمة عامة"[٣٩].

أما موقف القضاء العراقي، فقد أظهر قدرة على التعامل مع المنازعات الناشئة عن انتهاك البيانات الشخصية عبر الإنترنت رغم غياب قانون خاص ينظم هذه المنازعات، حيث لم يقف نقص التشريع عائقًا أمام معالجة القضايا الإلكترونية. ويعمل مشروع القانون العراقي المقترح على تقديم تعريفات واضحة للبيانات والممارسات الإلكترونية، وتوفير الحماية القانونية لشبكة المعلومات، ومعاقبة مرتكبي الأفعال التي تمثل اعتداء على حقوق مستخدمي الإنترنت، بما يسهم في الحد من إساءة استخدام الحاسب الآلي ووقوع المنازعات الرقمية[٤٠].

يرى الباحث أن النظام القانوني العراقي لا يزال يفتقر إلى تشريع حديث لحماية البيانات الشخصية عبر الإنترنت، مما يستدعي الاعتماد على المسؤولية المدنية المنصوص عليها في المادة (٢٠٤) من القانون المدني لتعويض الضرر الناشئ عن التعدي على البيانات.

ويكفل القانون الإيراني حماية الأفراد من الضرر الناجم عن أي اعتداء على حقوقهم الشخصية، بما في ذلك البيانات الشخصية، من خلال نص المادة الأولى من القانون المدني الإيراني، التي تنص على أن "أي شخص يتسبب في ضرر للحياة أو الصحة أو الممتلكات أو الحرية أو الكرامة أو السمعة التجارية أو أي حق آخر قانونيًا يكون مسؤولًا عن تعويض الضرر المادي والمعنوي الناتج عن فعله". ويمتد هذا الحق ليشمل البيانات الشخصية للأفراد وأفراد أسرهم، بحيث يمكن للمتضرر المطالبة بالتعويض عند حدوث أي انتهاك يؤدي إلى ضرر مادي أو معنوي[٤١].

يعتمد النظام الإيراني في تحديد المسؤولية المدنية على ركائز أساسية، أبرزها نظرية الخطأ ونظرية المخاطر. فوفقًا لنظرية الخطأ، يتحقق التعويض إذا ثبت وجود علاقة سببية بين خطأ الفاعل والخسارة التي لحقت بالمتضرر، ويقع عبء الإثبات على الشخص المتضرر. أما وفقًا لنظرية المخاطر، يتحمل الشخص المسؤولية عن الأضرار الناتجة عن أفعاله، حتى وإن لم يرتكب خطأً، ويهدف هذا النظام إلى ضمان تعويض المتضرر بفعالية والحفاظ على حقوقه[٤٢].

وتتجلى صور الاعتداء على البيانات الشخصية عبر الإنترنت في إيران بعدة أشكال، أبرزها جمع البيانات الشخصية دون إذن، أو الاطلاع على معلومات حساسة مثل الاسم، وتاريخ الميلاد، والحالة الصحية أو الاقتصادية، أو تعديلها أو حذفها أو الإفصاح عنها بطريقة غير مشروعة. كما يشمل الاعتداء نشر بيانات كاذبة تؤثر على سمعة الشخص أو مصداقيته، أو استخدام البيانات بطريقة تتجاوز الغرض المخصص لمعالجتها، بما يؤدي إلى الإضرار بالحقوق الفردية وحجب المنافع أو الفرص التي تستحق للفرد[٤٣].

وفق القانون الأوربي يمثل انتشار الإنترنت وتطوره تحديًا جوهريًا لحماية البيانات الشخصية، حيث وسّع نطاق جمع البيانات ومعالجتها وصولاً إلى مستوى عالمي، مما زاد من مخاطر الاعتداءات عليها[٤٤]. وقد استجاب القانون الأوروبي لهذا التحدي عبر تشريع صارم يرتكز على اللائحة العامة لحماية البيانات (GDPR)، التي تُعد حجر الزاوية في النظام القانوني الأوروبي لحماية الخصوصية في العصر الرقمي[٤٥].

ويرى الباحث إن طبيعة الإنترنت التي تتيح جمع وتدفق البيانات عبر الحدود بسهولة قد حولت البيانات الشخصية إلى سلعة ومعرضة لانتهاكات متنوعة. وتعرّف اللائحة "الاعتداء على البيانات" أو خرق البيانات الشخصية بأنه أي خرق أمني يؤدي إلى التدمير أو الفقدان أو التغيير أو الإفصاح غير المصرح به أو الوصول إلى البيانات الشخصية بشكل عرضي أو غير قانوني. وتتراوح هذه الاعتداءات من الهجمات الإلكترونية والاختراقات إلى الإفصاح غير المشروع أو جمع البيانات المفرط دون موافقة واضحة.

للمواجهة هذه التهديدات، أنشأت اللائحة العامة لحماية البيانات (GDPR) إطارًا قانونيًا شاملاً يعيد التوازن في العلاقة بين الأفراد والكيانات التي تعالج بياناتهم. ويعتمد هذا الإطار على مبادئ أساسية تهدف إلى تقليل فرص الاعتداء على البيانات منذ البداية، مثل مبدأ تقليل البيانات الذي يلزم جمع ومعالجة أقل قدر ممكن من البيانات اللازمة فقط للغرض المحدد، ومبدأ النزاهة والسرية الذي يتطلب تنفيذ ضمانات أمنية مناسبة[٤٦].

Journal Of Babylon Center For Humanities Studies 2026 Volume :16 Issue : 5
(ISSN): 2227-2895 (Print) (E-ISSN):2313-0059 (Online)

ويلزم القانون الشركات والمنظمات بتنفيذ تدابير فنية وتنظيمية ملائمة لضمان مستوى أمن يتناسب مع درجة الخطورة. وتشمل هذه التدابير أمورًا مثل التشفير، وإجراءات التحقق من الهوية، وتدريب الموظفين، وتقييد الوصول إلى البيانات. كما يفرض مبدأ المساءلة الذي يلزم من يتحكم في البيانات بإثبات امتثاله لكل هذه المبادئ.

المطلب الثاني/تحديات الذكاء الاصطناعي وتحليل البيانات الشخصية

مع استمرار الثورة الرقمية، يبرز الذكاء الاصطناعي في تحليل البيانات الشخصية كواحدة من الأدوات الأكثر تأثيرًا في عالم الأعمال. يتزايد الاعتماد على تقنيات الذكاء الاصطناعي والتعلم الآلي لتحسين جودة التحليل البياني وتسريع العمليات. إلا أن هذا التقدم لا يخلو من تحديات التي تتطلب من الشركات والمؤسسات التفكير بذكاء لمواجهتها[٤٧].

١. حجم البيانات الضخمة

أدّى التنامي المتسارع في حجم البيانات إلى بروز تحديات جوهرية تتعلق بعمليات التخزين والمعالجة والتحليل. إذ تتطلب البيانات الضخمة بنى تحتية تقنية متطورة قادرة على استيعاب هذا الكم الهائل من المعلومات ومعالجته بكفاءة عالية، بما يضمن دقة النتائج وسرعة الوصول إليها[٤٨].

٢. نقص المهارات التقنية

يستوجب توظيف تقنيات الذكاء الاصطناعي في تحليل البيانات توافر كفاءات متخصصة تمتلك خبرات متقدمة في مجالات تعلم الآلة، وهندسة البيانات، وتحليل النظم الذكية. غير أن محدودية هذه المهارات في سوق العمل تشكل عائقًا رئيسًا أمام الاستخدام الأمثل لهذه التقنيات.

٣. قضايا الخصوصية والأمان

مع الاعتماد المتزايد على البيانات، ولا سيما البيانات ذات الطابع الشخصي، تبرز إشكاليات قانونية وتقنية متعلقة بحماية الخصوصية وضمان أمن المعلومات. كما تتعاظم التحديات التنظيمية المرتبطة بالامتثال للتشريعات الوطنية والدولية، الأمر الذي يفرض أعباء إضافية على الجهات المستخدمة لتقنيات الذكاء الاصطناعي[٤٩].

٤. التكلفة المرتفعة

تُعد التكلفة العالية لتقنيات الذكاء الاصطناعي، سواء من حيث البنية التحتية أو البرمجيات أو الكوادر البشرية المتخصصة، من أبرز التحديات التي تواجه المؤسسات، ولا سيما الشركات الصغيرة والمتوسطة. الأمر الذي يستدعي البحث عن حلول تقنية واقتصادية تسهم في خفض التكاليف وتعزيز شمولية الوصول إلى هذه التكنولوجيا[٥٠].

ويُلاحظ أن القوانين العراقية، كقانون الاتصالات رقم ١٥٩ لسنة ١٩٨٠ وقانون مكافحة الجرائم الإلكترونية رقم ١٢ لسنة ٢٠٠٨، وإن شكّلت محاولات أولية لتنظيم استخدام التكنولوجيا، إلا أنها لم تواكب التطورات الحديثة في مجال حماية البيانات الشخصية، ولا سيما ما يتعلق بالأمن السيبراني، ومعالجة البيانات، والمسؤولية عن إساءة استخدامها. وقد أدى هذا القصور التشريعي إلى وجود فجوة قانونية تستدعي تحديثًا تشريعيًا مستمرًا يوازن بين التطور التقني وضمان حماية الخصوصية الرقمية. وفي هذا السياق، تبرز الحاجة إلى تعزيز التدريب المتخصص، وتوفير الموارد التقنية، وتطوير آليات تشريعية أكثر مرونة قادرة على الاستجابة للتغيرات التكنولوجية المتلاحقة.

أما في القانون الإيراني، فتُعد البيانات الشخصية ركيزة أساسية في منظومة تكنولوجيا المعلومات، حيث تعتمد المؤسسات العامة والخاصة على جمعها ومعالجتها لتحسين الخدمات. غير أن هذا الواقع يثير إشكالات قانونية وأخلاقية متعددة، أبرزها ضعف وعي المستخدمين بكيفية جمع بياناتهم واستخدامها، والموافقة الشكلية على شروط المعالجة دون إدراك آثارها. كما تمثل البيانات الحساسة، كالمعلومات الصحية والمالية، تحديًا خاصًا يتطلب التزامًا صارمًا بمبادئ الخصوصية والمسؤولية القانونية[٥١].

وتزداد هذه التحديات مع توسع استخدام تقنيات المراقبة والذكاء الاصطناعي، التي قد تؤدي إلى انتهاكات للحياة الخاصة، وإلى قرارات آلية تفتقر إلى الشفافية، وتثير إشكالات تتعلق بتحديد المسؤولية القانونية عن الأضرار الناجمة عنها. ويكشف ذلك عن حاجة ملحّة إلى أطر قانونية أوضح في النظام الإيراني، تعزز حماية البيانات الشخصية، وتضمن المساءلة، وترسخ الثقة المجتمعية في استخدام التكنولوجيا[٥٢].

يُعدّ الاتحاد الأوروبي من أبرز الجهات الرائدة في مجال تطوير وتحديث التشريعات المرتبطة بالتكنولوجيا الرقمية، ولا سيما في ميدان حماية البيانات الشخصية. فقد كان من أوائل الكيانات التي اعتمدت تنظيمًا قانونيًا متقدمًا في هذا المجال من خلال إصدار اللائحة العامة لحماية البيانات (GDPR)، التي دخلت حيّز النفاذ في أيار/مايو ٢٠١٨، وشكّلت منذ ذلك الحين مرجعًا عالميًا في حماية الخصوصية. وقد أرست هذه اللائحة قواعد دقيقة وصارمة تنظم آليات جمع البيانات الشخصية ومعالجتها، ومن أبرز ما ميّزها إقرار مبدأ الموافقة الصريحة، الذي يوجب الحصول على رضا واضح ومسبق من الأفراد قبل استخدام بياناتهم. كما عززت اللائحة حقوق أصحاب البيانات، فأقرت لهم الحق في الاطلاع على كيفية استخدام بياناتهم، وحق الاعتراض وتقديم الشكاوى عند وقوع أي انتهاك[٥٣].

الخاتمة

اختمت الدراسة إلى أن حماية البيانات الشخصية لم تعد ترفاً قانونياً، بل هي ركيزة للأمن القومي والاستقرار الاقتصادي في ظل "رقمية الحياة". وبينما يمتلك الاتحاد الأوروبي إطاراً صلباً، لا يزال العراق وإيران بحاجة ماسة إلى نقلة تشريعية تتجاوز القواعد التقليدية لتوفير حماية ديناميكية تواكب عصر الذكاء الاصطناعي وإنترنت الأشياء.

النتـــائج

* يعاني النظام القانوني العراقي من افتقاره لقانون ينظم حماية البيانات الشخصية .

* تعتبر البيانات الشخصية حقوقاً غير مالية مرتبطة بالهوية القانونية للفرد، ومع ذلك أصبحت عرضة للسلعية والانتهاك في سوق العالم الافتراضي.

* يتميز النموذج الأوروبي (GDPR) بمبدأ "اتساع نطاق التطبيق"، حيث يفرض حمايته على بيانات مواطنيه حتى خارج الحدود الإقليمية للاتحاد.

* تشكل أجهزة إنترنت الأشياء (IoT) ثغرة أمنية كبرى بسبب نقص التشفير، والاعتماد على كلمات مرور افتراضية، وغياب التوحيد القياسي.

* أثبت القضاء العراقي مرونة في التعامل مع المنازعات الرقمية من خلال الاستناد إلى قواعد المسؤولية المدنية (المادة ٢٠٤ من القانون المدني) لتعويض أضرار انتهاك البيانات.

التوصيات

١. يجب الإسراع في تشريع "قانون حماية البيانات الشخصية" في العراق، بحيث يتضمن تعريفات دقيقة ومعايير صارمة للمعالجة والحماية.

٢.تبني تقنيات تعزيز الخصوصية (PETs) مثل التشفير من طرف إلى طرف وإخفاء الهوية كمتطلبات قانونية للمؤسسات التي تعالج البيانات.

٣.إلزام الشركات المصنعة لأجهزة إنترنت الأشياء والذكاء الاصطناعي بتطبيق مبدأ "الخصوصية منذ التصميم" لضمان أمن الأجهزة قبل طرحها في الأسواق.

٤.تعزيز الكفاءة التقنية للكوادر القضائية والقانونية من خلال برامج تدريبية متخصصة في المنازعات الالكترونية وتحليل البيانات الضخمة.

٥.الاستفادة من التجارب الدولية، ولا سيما النموذج الأوروبي، وتكييفها بما يتلاءم مع السياق الوطني لتعزيز الثقة بين المستهلك والمؤسسات الرقمية.

الهوامش

[١] حسام الدين الاهواني، الحق في احترام الحياة الخاصة الحق في الخصوصية دراسة مقارنة دار النهضة العربية ١٩٧٨ص٢٣.

[٢] آلاء كليب، قانون حماية البيانات الشخصية في ضوء المعايير الدولة، ورقة بحثية منشورة بموقع مؤسسة حرية الفكر ،والتعبير https://afteegypt.org/legislations/legislative-analysis/23692/14/07/2021 ، الأربعاء، ١٤ يوليو، ٢٠٢١، تاريخ الولوج ، ١/١/٢٠٢٢، الساعة، ١١.٥. html.a

[٣] هوزان عبد المحسن عبد الله، المسئولية التقصيرية الناجمة عن التعدي على الحياة الخاصة في القانون الفرنسي، دراسة مقارنة، بحث منشور بمجلة دفاتر السياسة والقانون، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، الجزائر، المجلد ١٢، العدد ١ ، ٢٠٢٠ ص١٧

[٤] (ينظر الموقع الإلكتروني على شبكة الأنترنيت) ماهية البيانات الشخصية، البيانات الحساسة https://webcache.googleusercontent.com/search?q=cache:TsPF7HCqL4YJ:https://sdai a.gov.sa/ndmo/Files/QA.pdf&cd=13&hl=ar&ct=clnk&gl=iq

[٥] سوزان عدنان ، (٢٠١٤) ، انتهاك حرمة الحياة الخاصة عبر الأنترنيت، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد (٢٩)، العدد ٣، ص٤٢٥.

[٦] انظر: قانون البطاقة الوطنية العراقي رقم ٣ لسنة٢٠٠٦.

[٧] انظر: قانون الأحوال المدنية العراقي الملغي رقم ٦٥. لسنة ١٩٧٢.

[٨] سامان فوزي عمر، (٢٠٠٩) ، إساءة استعمال حق النقد، " دراسة تحليلية مقارنة في القانون المدني" ، ط١، دار الكتب القانونية ، ص٢٣.

[٩] شريف يوسف خاطر، (٢٠١٥) ،حق الاطلاع على البيانات الشخصية في فرنسا ، مجلة كلية القانون الكويتية العالمية ، السنة الثالثة العدد ٩، ص ٢٨١-٢٨٣-٢٨٢.

[١٠] انظر: المادة ٤/١ من اللائحة العامة لحماية البيانات (GDPR) التابعة **للاتحاد الأوروبي**، رقم ٦٧٩ لسنة ٢٠١٦.

[١١] فتحي، يونس وخير الله شاه مرادي (٢٠١٧)، "نطاق وإقليم الخصوصية في الفضاء الإلكتروني"، المجلة القانونية عدد رقم ٩٩، ص٦٧.

[١٢] طارق جمعه السيد راشد، **الحماية القانونية لخصوصية البيانات الشخصية في العصر الرقمي دراسة مقارنة(مقالة)،٢٠١٩،ص١١.**

[١٣] خالد محمد علي، الحماية القانونية للبيانات الشخصية في أطار القانون المدني، دراسة مقارنة جامعة ديالى-كلية القانون والعلوم السياسي، مجلة كلية القانون للعلوم القانونية والسياسية/المجلد/ ١٢ / العدد ٧٤ العام ٢٠٢٣،ص٢٢٨.

[١٤] خالد محمد علي، الحماية القانونية للبيانات الشخصية في أطار القانون المدني، المرجع السابق، ص٢٢٩.

[١٥] محمد تالات ياداك ،الإطار القانوني للمعالجة الإلكترونية للبيانات الشخصية دراسة تحليلية مقارنة (٢٠٢٢)، ص٧.

[16] Benoit TABAKA et Yann TESAR, Loi “informatique et liberes”: un nouveau cadre juridique pour le traitement des donnees a caractere personnel , Dossier disponiblesur www.foruminternet. org, la date de mise en ligneest :Octobre 2004, p 8.

[١٧] طارق جمعه السيد ارشد، الحماية القانونية لخصوصية البيانات الشخصية فى العصر الرقمي، د ارسة مقارنة، مجلة القانون والاقتصاد، كلية الحقوق، جامعة القاهرة، ملحق خاص، ع ،٩٢ ص ،١٠٩.

[١٨] سليم محمد سليم حسين، الحماية الجنائية للبيانات الشخصية المعالجة آليا، دراسة مقارنة، مجلة العلوم القانونية والاقتصادي ة، كلية الحقوق جامعة عين شمس، مج ،٦٢ ع ،١ ،٢٠٢٠ ص٢.

[١٩] انظر: لائحة الاتحاد الأوروبي ٦٧٩/٢٠١٦ الصادرة عن البرلمان الأوروبي والمجلس الأوروبي بتاريخ ٢٧ أبريل ٢٠١٦ بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية وحرية نقل هذه البيانات؛ والذى ألغى التوجيه ٩٥/٤٦، انظر الرابط الآتيhttps://www.cnil.fr/en/official-texts :

[٢٠] شلواح ميرة، بشيري كهينة، المسؤولية المدنية عن انتهاك حق الخصوصية في المجال الرقمي، رسالة ماجستير، كلية الحقوق ٧ والعلوم السياسية، جامعة عبدالرحمان ميرة-بجاية، ،٢٠٢٠-٢٠١٩ ص ١٠.

[٢١] علاء عيد طه، فيما يتعلق بمعالجة البيانات الشخصية وتداولها، دراسة فى ضوء اللائحة التنظيمية الحماية القانونية للأشخاص رقم /٦٧٩ ٢٠١٦الصادرة عن البرلمان والمجلس الأوروبي، مجلة كلية الحقوق للبحوث القانونية والاقتصادية، ع ،٢ ،٢٠١٩ ص٢٤.

[٢٢] علاء الدين عبد الله فواز الخصاونة، الحماية القانونية للخصوصية والبيانات الشخصية فى نطاق المعلوماتية، مجلة جامعة الشارقة للعلوم الشرعية والقانونية، جامعة الشارقة، مج ،٨ ع ،٢ ،٢٠١١ ص ٥ وما يليها.

[٢٣] المعالج هو "ذلك الشخص الطبيعي أو الاعتباري المختص بطبيعة عمله بمعالجة البيانات الشخصية، لصالحه أو لصالح المتحكم، بالاتفاق معه ووفقا لتعليماته"، التعريف الوارد ب المادة (١) من قانون حماية البيانات الشخصية ؛ ذات التعريف الوارد في (٤/٨) من اللائحة الأوروبية.

[٢٤] علاء الدين عبد الله فواز الخصاونة، الحماية القانونية للخصوصية والبيانات الشخصية فى نطاق المعلوماتية، المرجع السابق، ص ٧.

[٢٥] المادة الثالثة من قانون حماية البيانات الشخصية Cynthia chassigneux, L'encadrement juridique du traitement des données personnelles sur les sites de commerce en ligne, Thèse, Université Panthéon-Assas , Paris II 2003, nº 278, p. 154

[٢٦] محمود عبدالرحمن، تطورا ت الحديثة لمفهوم الحق فى الخصوصية -الحق فى الخصوصية المعلوماتية، مجلة كلية القانون الكويتية العالمية، ع ،٩ س ،٣ مارس ،٢٠١٥ ص ١٠٩.

[٢٧] تركى الموسوي، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها، مجلة كلية بغداد للعلوم الاقتصادية ، عدد ٢٩ خاص بمؤتمر الكلية، جامعة بغداد، ،٢٠١٣ ص٣١٢.

[٢٨] علي جعفري محمد رضا رحبور، المسؤولية المدنية عن انتهاك خصوصية البيانات في الفقه والقانون الإمامي ،١٣٩٥ص٤٥.

[29] Yves Poullet, La loi des données à caractère personnel: un enjeu fondamental pour nos sociétés et démocraties? , LEGICOM, n°42 –2009/1, pp. 47-69

[٣٠] عبدالله فاضل حامد، تنازع القوانين في انتهاك حقوق الشخصية عبر وسائل الأعلام، بحث منشور في مجلة رسالة الحقوق الصادرة عن لكلية القانون في جامعة كربلاء، السنة التاسعة، العدد الثالث، ٢٠١٧،ص١١٠

[٣١] محمد حسن علي النظام القانوني الحماية البيانات الشخصية المعالجة الكترونيا دراسة تحليلية مقارنة في ضوء اللائحة الأوروبية وبعض التشريعات ذات العلاقة مجلة العلوم القانونية كلية القانون جامعة عجمان الإمارات مع ٧، ١٤ يوليو ٢٠٠١ص ٢٣.

[٣٢] مزينب اصلانی،علی جعفری ، جعفر سلمان زاده سئولیت مدنی رسانه ها در قبال نقض حریم خصوصی در حقوق ایران و انگلستان،دوره و شماره :دوره ١٢، شماره ٤٦، بهار ١٤٠٢ ،صفحه- ١١ ٣٣.

[٣٣] الموسوي، منى تركي وفضل الله، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها .**مجلة كلية بغداد للعلوم الاقتصادية الجامعة**، كلية بغداد للعلوم الاقتصادية الجامعة، عدد خاص بمؤتمر الكلية (٢٠١٣)، ص١٥٤

[٣٤] عمر أحمد حسبو حماية الحريات في مواجهة نظم المعلومات دراسة مقارنة دار النهضة العربية، القاهرة، ٢٠٠٠، ص١٢٩

[35] Guy Braibant, Données personnelles et société de l'information, Rapport au Premier ministre sur la transposition en droit français de la directive 95/46. La documentation française, 1998.

[٣٦] **حيدر طالب الأحمر ،ادمان الأنترنت ،استاذ بجامعة بابل العراق ، ٢٠١٤** www.alnoor.se/author.asp?id=1616

[٣٧] انظر: المادة (٢٠٤) من القانون المدني العراقي رقم ٤٠ لسنة١٩٥١.

[٣٨] احمد جعفر الشاوى ، المسؤولية التقصيرية الناشئة عن استعمال الانترنت، اطروحة دكتوراه، كلية القانون جامعة بغداد، ٢٠١٦/١٠/٢٠،ص١٠٢

[٣٩] المادة (٨) فقرة (د) من مشروع قانون الجرائم الالكترونية العراقي لسنة ٢٠١٩

[٤٠] عبدالله فاضل حامد، تنازع الاختصاص القضائي في دعوى انهتاك الحقوق اللصيقة بالشخصية، بحث منشور في مجلة دراسات قانونية وسياسية الصادرة عن جامعة السليمانية، السنة الخامسة، العدد التاسع، حزيران ٢٠١٧،ص٣٦٧.

[٤١] انظر : المادة الأولى من قانون مدني ايراني لسنة١٣٣٥

[٤٢] امين ابراهيم آبادى محمد حسين؛ متين راد على محمد (١٤٠٣)، مطالعه تطبيقى مسئوليت مدنى ناشى از استفاده از هوش مصنوعى در حقوق ايران و كشورهاى اتحاديه اروپا چاپ اول انتشارات پژوهشگران پارسه ،ص٥٨

[٤٣] حامد بهرامي أحمدي، عموميات العقود والاتفاقيات – القانون المدني ٣ – نُشر في مايو ٢٠٠٢، الصفحات ١٧ و ١٨.

[44] Information Privacy Fundamentals for Librarians and Information Professionals, Rowman & Littlefield Publishers, 2015

[45] Tapungduend des 20. Intemaan Rechtformats Sympomona-RS 2017 Proceedings of the 200 tematon Leger mats Sympa Austrian Computer Society 1-8

[46] Le droit à l'oubli sur Internet, Mémoire de Master 2 recherche, Mention DNP, université paris-sud, 2012

[47] Fumara. P. & F. Spoto 2018. Sutic analysis for GDPR compliance CEUR Workshop Proceedings Germany 20581-10

[48] Jacqueline Dutheil De La Rochere, Droit matériel de l'Union européenne, 2ème éd. 2004.

[٤٩] احمد جعفر ألشاوى ، ألمسؤولية ألتقصيرية ألناشئة عن استعمال ألانترنت، اطروحة دكتوراه، كلية ألقانون جامعة بغداد، ٢٠١٦/١٠/٢٠،ص١٠٢

[٥٠] عبدالله فاضل حامد، تنازع ألاختصاص ألقضائي في دعوى انهتاك ألحقوق ألللصيقة بألشخصية، بحث منشور في مجلة دراسات قانونية وسياسية ألصادرة عن جامعة ألسليمانية، ألسنة ألخامسة، ألعدد ألتاسع، حزيران ٢٠١٧،ص٣٦٧.

[٥١] ليلى رئيسي ، فلورا قاسم زاده لياسي تحديات النظام القانوني الإيراني في انتهاك البيانات الشخصية والخصوصية في الفضاء الإلكتروني ،المجلد ٨٤، العدد ١١٠ – العدد الدوري ١١٠ ،صيف ٢٠٢٠،الصفحات ١١٩-١٤.

[٥٢] حسن بيجي، إبراهيم ،**تطوير شبكة البيانات الوطنية، التحديات والتهديدات للأمن القومي**، مجلة فكر الثورة الإسلامية، العدد ٩، ص٥٧

[53] Peter Wirtz, Les meilleures pratiques de gouvernements d'entreprises, La Δέσουverte, Repères, Paris, 2008.

المصادر والمراجع

أولًا: الكتب القانونية الخاصة

١. حسام الدين الأهواني، الحق في احترام الحياة الخاصة (الحق في الخصوصية) – دراسة مقارنة، دار النهضة العربية، ١٩٧٨.

٢. سامان فوزي عمر، إساءة استعمال حق النقد – دراسة تحليلية مقارنة في القانون المدني، دار الكتب القانونية، ٢٠٠٩.

٣. عمر أحمد حسبو، حماية الحريات في مواجهة نظم المعلومات – دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠٠٠.

ثانيًا: الكتب القانونية العامة

١. حامد بهرامي أحمدي، عموميات العقود والاتفاقيات – القانون المدني (٣)، منشور في مايو ٢٠٠٢.

ثالثًا: الكتب القانونية الإيرانية

١. امبن إبراهيم آبادي، محمد حسين؛ متين راد، علي محمد، دراسة مقارنة للمسؤولية المدنية الناشئة عن استخدام الذكاء الاصطناعي في حقوق إيران ودول الاتحاد الأوروبي، انتشارات پژوهشگران پارسه، ١٤٠٣هـ.

٢. علي جعفري، محمد رضا رحبور، المسؤولية المدنية عن انتهاك خصوصية البيانات في الفقه والقانون الإمامي، ١٣٩٥هـ.

رابعًا: الرسائل والأطاريح

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

٢. شلواح ميرة، بشيري كهينة، المسؤولية المدنية عن انتهاك حق الخصوصية في المجال الرقمي، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة – بجاية، ٢٠١٩–٢٠٢٠.

خامسًا: المجلات والمقالات القانونية

١. تركي الموسوي، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها، مجلة كلية بغداد للعلوم الاقتصادية، جامعة بغداد، ٢٠١٣.

٢. حسن بيجي، إبراهيم، تطوير شبكة البيانات الوطنية والتحديات والتهديدات للأمن القومي، مجلة فكر الثورة الإسلامية.

٣. خالد محمد علي، الحماية القانونية للبيانات الشخصية في إطار القانون المدني – دراسة مقارنة، مجلة كلية القانون والعلوم السياسية، ٢٠٢٣.

٤. سليم محمد سليم حسين، الحماية الجنائية للبيانات الشخصية المعالجة آليًا – دراسة مقارنة، مجلة العلوم القانونية والاقتصادية، ٢٠٢٠.

٥. سوزان عدنان، انتهاك حرمة الحياة الخاصة عبر الإنترنت، مجلة جامعة دمشق، ٢٠١٤.

٦. شريف يوسف خاطر، حق الاطلاع على البيانات الشخصية في فرنسا، مجلة كلية القانون الكويتية العالمية، ٢٠١٥.

٧. طارق جمعة السيد أرشد، الحماية القانونية لخصوصية البيانات الشخصية في العصر الرقمي – دراسة مقارنة، مجلة القانون والاقتصاد.

٨. طارق جمعة السيد راشد، الحماية القانونية لخصوصية البيانات الشخصية في العصر الرقمي – دراسة مقارنة، ٢٠١٩.

٩. عبد الله فاضل حامد، تنازع الاختصاص القضائي في دعوى انتهاك الحقوق اللصيقة بالشخصية، مجلة دراسات قانونية وسياسية، جامعة السليمانية، ٢٠١٧.

١٠. عبد الله فاضل حامد، تنازع القوانين في انتهاك الحقوق الشخصية عبر وسائل الإعلام، مجلة رسالة الحقوق، جامعة كربلاء، ٢٠١٧.

١١. علاء الدين عبد الله فواز الخصاونة، الحماية القانونية للخصوصية والبيانات الشخصية في نطاق المعلوماتية، مجلة جامعة الشارقة، ٢٠١١.

١٢. علاء عيد طه، معالجة البيانات الشخصية وتداولها في ضوء اللائحة الأوروبية، مجلة كلية الحقوق للبحوث القانونية والاقتصادية، ٢٠١٩.

١٣. فتحي يونس، خير الله شاه مرادي، نطاق وإقليم الخصوصية في الفضاء الإلكتروني، المجلة القانونية، ٢٠١٧.

١٤. ليلى رئيسي، فلورا قاسم زاده لياسي، تحديات النظام القانوني الإيراني في انتهاك البيانات الشخصية والخصوصية في الفضاء الإلكتروني، ٢٠٢٠.

١٥. محمد تالات ياداك، الإطار القانوني للمعالجة الإلكترونية للبيانات الشخصية – دراسة تحليلية مقارنة، ٢٠٢٢.

١٦. محمد حسن علي، النظام القانوني لحماية البيانات الشخصية المعالجة إلكترونيًا – دراسة تحليلية مقارنة، مجلة العلوم القانونية، جامعة عجمان، ٢٠٠١.

١٧. محمود عبد الرحمن، التطورات الحديثة لمفهوم الحق في الخصوصية (الخصوصية المعلوماتية)، مجلة كلية القانون الكويتية العالمية، ٢٠١٥.

١٨. مزينب أصلاني، علي جعفري، جعفر سلمان زاده، المسؤولية المدنية لوسائل الإعلام عن انتهاك الخصوصية في القانون الإيراني والإنكليزي، ١٤٠٢هـ.

١٩. منى تركي الموسوي، فضل الله، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها، مجلة كلية بغداد للعلوم الاقتصادية، ٢٠١٣.

٢٠. هوزان عبد المحسن عبد الله، المسؤولية التقصيرية الناجمة عن التعدي على الحياة الخاصة في القانون الفرنسي – دراسة مقارنة، مجلة دفاتر السياسة والقانون، ٢٠٢٠.

سادسًا: المواقع الإلكترونية (باللغة الإنكليزية)

1.https://afteegypt.org/legislations/legislative-analysis/23692/

2.https://www.alnoor.se/author.asp?id=1616

3.https://webcache.googleusercontent.com/search?q=cache:TsPF7HC7HCqL4YJ:https://sdai.gov.sa/ndmo/Files/QA.pdf

4.https://www.cnil.fr/en/official-texts

سابعًا: القـــــوانين

١.القانون المدني الإيراني لسنة ١٣٣٥.

٢.القانون المدني العراقي رقم ٤٠ لسنة ١٩٥١.

٣.قانون الأحوال المدنية العراقي الملغي رقم ٦٥ لسنة ١٩٧٢.

٤.قانون البطاقة الوطنية العراقي رقم ٣ لسنة ٢٠٠٦.
٥.لائحة الاتحاد الأوروبي رقم ٦٧٩ لسنة ٢٠١٦ بشأن حماية البيانات الشخصية.
٦.مشروع قانون الجرائم الإلكترونية العراقي لسنة ٢٠١٩.

ثامنًا: المراجع الأجنبية

1.Benoit Tabaka & Yann Tesar, Loi "informatique et libertés", 2004.

2.Cynthia Chassigneux, L'encadrement juridique du traitement des données personnelles sur les sites de commerce en ligne, Thèse, Université Panthéon-Assas (Paris II), 2003.

3.Fumara, P. & Spoto, F., Static Analysis for GDPR Compliance, CEUR Workshop Proceedings, 2018.

4.Guy Braibant, Données personnelles et société de l'information, La documentation française, 1998.

5.Information Privacy Fundamentals for Librarians and Information Professionals, Rowman & Littlefield Publishers, 2015.

6.Jacqueline Dutheil De La Rochere, Droit matériel de l'Union européenne, 2ème éd., 2004.

7.Le droit à l'oubli sur Internet, Mémoire de Master, Université Paris-Sud, 2012.

8.Peter Wirtz, Les meilleures pratiques de gouvernements d'entreprises, Paris, 2008.

9.Tapungduend des 20. International Legal Informatics Symposium Proceedings, Austrian Computer Society, 2017.

10.Yves Poullet, La loi des données à caractère personnel: un enjeu fondamental pour nos sociétés et démocraties?, LEGICOM, 2009.

Sources and References

First: Specialized Legal Books

1.Hossam El-Din El-Ahwani, The Right to Respect for Private Life (The Right to Privacy) – A Comparative Study, Dar Al-Nahda Al-Arabiya, 1978.

2.Saman Fawzi Omar, Abuse of the Right to Criticism – A Comparative Analytical Study in Civil Law, Dar Al-Kutub Al-Qanuniyya, 2009.

3.Omar Ahmed Hasabo, Protecting Freedoms in the Face of Information Systems – A Comparative Study, Dar Al-Nahda Al-Arabiya, Cairo, 2000.

Second: General Legal Books

1.Hamed Bahrami Ahmadi, Generalities of Contracts and Agreements – Civil Law (3), published in May 2002.

Third: Iranian Legal Books

1.Amin Ibrahim Abadi, Mohammad Hossein; Matin Rad, Ali Mohammad, A Comparative Study of Civil Liability Arising from the Use of Artificial Intelligence in the Laws of Iran and the European Union, Pajouheshgaran Parseh Publications, 1403 AH.

2.Ali Jafari, Mohammad Reza Rahpour, Civil Liability for Data Privacy Violation in Imami Jurisprudence and Law, 1395 AH.

Fourth: Theses and Dissertations

1.Ahmed Jaafar Al-Shawi, Tort Liability Arising from Internet Use, PhD Dissertation, College of Law, University of Baghdad, 2016.

2.Shalwah Mira, Bashiri Kahina, Civil Liability for Violation of the Right to Privacy in the Digital Sphere, Master's Thesis, Faculty of Law and Political Science, Abdel Rahman Mira University – Bejaia, 2019–2020.

Fifth: Legal Journals and Articles

1. Turki Al-Mousawi, Information Privacy: Its Importance and the Risks of Modern Technologies, Baghdad College of Economic Sciences Journal, University of Baghdad, 2013.

2. Hassan Beiji, Ibrahim, Developing the National Data Network and the Challenges and Threats to National Security, Islamic Revolution Thought Journal.

3. Khaled Mohammed Ali, Legal Protection of Personal Data within the Framework of Civil Law – A Comparative Study, Journal of the College of Law and Political Science, 2023.

4. Salim Mohammed Salim Hussein, Criminal Protection of Personal Data Processed by Mechanism – A Comparative Study, Journal of Legal and Economic Sciences, 2020.

5. Suzan Adnan, Violation of Privacy Online, Damascus University Journal, 2014.

6. Sharif Yousef Khater, The Right to Access Personal Data in France, Kuwait International Law School Journal, 2015.

7. Tariq Jumaa Al-Sayed Arshad, Legal Protection of Personal Data Privacy in the Digital Age – A Comparative Study, Journal of Law and Economics. 8. Tariq Jumaa Al-Sayed Rashid, The Legal Protection of Personal Data Privacy in the Digital Age – A Comparative Study, 2019.

9. Abdullah Fadel Hamed, Jurisdiction Conflicts in Lawsuits Concerning Violations of Personal Rights, Journal of Legal and Political Studies, University of Sulaimani, 2017.

10. Abdullah Fadel Hamed, Conflicts of Laws in Violations of Personal Rights Through the Media, Journal of the Message of Rights, University of Karbala, 2017.

11. Alaa Al-Din Abdullah Fawaz Al-Khasawneh, The Legal Protection of Privacy and Personal Data in the Field of Information Technology, University of Sharjah Journal, 2011.

12. Alaa Eid Taha, Processing and Handling of Personal Data in Light of the European Regulation, Journal of the College of Law for Legal and Economic Research, 2019.

13. Fathi Younis and Khairallah Shah Moradi, The Scope and Territory of Privacy in Cyberspace, The Legal Journal, 2017.

14. Leila Raisi and Flora Ghasemzadeh Liasi, Challenges Facing the Iranian Legal System in Violations of Personal Data Privacy in Cyberspace, 2020.

15. Mohammad Talat Yadak, The Legal Framework for Electronic Processing of Personal Data – A Comparative Analytical Study, 2022.

16. Mohammad Hassan Ali, The Legal System for the Protection of Electronically Processed Personal Data – A Comparative Analytical Study, Journal of Legal Sciences, Ajman University, 2001.

17. Mahmoud Abdel Rahman, Recent Developments in the Concept of the Right to Privacy (Information Privacy), Kuwait International Law School Journal, 2015.

18. Mozainab Aslani, Ali Jafari, Jafar Salmanzadeh, Civil Liability of Media Outlets for Privacy Violations in Iranian and English Law, 1402 AH.

مجلة مركز بابل للدراسات الإنسانية ٢٠٢٦ المجلد ١٦/ العدد ٥

Privacy in Cyberspace, 2020. 19. Mona Turki Al-Mousawi, Fadlallah, Information Privacy: Its Importance and the Risks of Modern Technologies, Baghdad College of Economic Sciences Journal, 2013.

20. Houzan Abdul-Muhsin Abdullah, Tort Liability Arising from Intrusion into Privacy in French Law – A Comparative Study, Journal of Political and Legal Studies, 2020.

Sixth: Websites (in English)

5.https://afteegypt.org/legislations/legislative-analysis/23692/

6.https://www.alnoor.se/author.asp?id=1616

7.https://webcache.googleusercontent.com/search?q=cache:TsPF7HC7HCqL4YJ:https://sdai.gov.sa/ndmo/Files/QA.pdf

8.https://www.cnil.fr/en/official-texts

Seventh: Laws

1. Iranian Civil Code of 1335 AH (1916 CE).

2. Iraqi Civil Code No. 40 of 1951.

3. Repealed Iraqi Civil Status Law No. 65 of 1972.

4. Iraqi National Identity Card Law No. 3 of 2006.

5. European Union Regulation No. 679 of 2016 on the Protection of Personal Data.

6. Draft Iraqi Cybercrime Law of 2019.

Eighth: Foreign References

11.Benoit Tabaka & Yann Tesar, Loi “informatique et libertés”, 2004.

12.Cynthia Chassigneux, L’encadrement juridique du traitement des données personnelles sur les sites de commerce en ligne, Thèse, Université Panthéon-Assas (Paris II), 2003.

13.Fumara, P. & Spoto, F., Static Analysis for GDPR Compliance, CEUR Workshop Proceedings, 2018.

14.Guy Braibant, Données personnelles et société de l’information, La documentation française, 1998.

15.Information Privacy Fundamentals for Librarians and Information Professionals, Rowman & Littlefield Publishers, 2015.

16.Jacqueline Dutheil De La Rochere, Droit matériel de l’Union européenne, 2ème éd., 2004.

17.Le droit à l’oubli sur Internet, Mémoire de Master, Université Paris-Sud, 2012.

18.Peter Wirtz, Les meilleures pratiques de gouvernements d’entreprises, Paris, 2008.

19.Tapungduend des 20. International Legal Informatics Symposium Proceedings, Austrian Computer Society, 2017.

20.Yves Poullet, La loi des données à caractère personnel: un enjeu fondamental pour nos sociétés et démocraties?, LEGICOM, 2009.