العراقية
المجلات الاكاديمية العلمية
IRAQI Academic Scientific Journals
Al-Itqan Journal of Humanities
available online at
https://iasj.rdd.edu.iq/journals/journal/view/575
ISSN: 3105-1073 (OnIne)
المجلة معتمدة بالترقيات العلمية حسب كتاب وزارة التعليم العراقية (46404-1410) في 2026/4/27

الإطار القانوني والمدني في حماية البيانات الشخصية لمواقع التواصل الاجتماعي

م.م سهى جواد احمد الشماع
كلية الامام الكاظم (عليه السلام) للعلوم الإسلامية الجامعة
Suha Jawad Ahmed AL – Shammaa
Suha.juad@iku.edu-iq

المستخلص

يتناول هذا البحث موضوع الإطار القانوني والمدني لحماية البيانات الشخصية لمستخدمي مواقع التواصل الاجتماعي، في ظل التطور التكنولوجي المتسارع والانتشار الواسع لهذه المنصات. ويهدف إلى بيان مفهوم البيانات الشخصية وأنواعها، وتحليل المخاطر التي تتعرض لها خصوصية المستخدمين، مثل تسريب البيانات والابتزاز الإلكتروني والاستخدام غير المشروع للمعلومات.كما يستعرض البحث التشريعات الدولية، وفي مقدمتها اللائحة العامة لحماية البيانات(GDPR) ، إلى جانب التشريعات الوطنية، مع التركيز على الواقع القانوني في العراق ومدى كفاية النصوص الحالية في حماية البيانات الشخصية. ويتناول أيضًا دور المسؤولية المدنية في تعويض الأضرار الناتجة عن انتهاك البيانات.وقد توصل البحث إلى أن الحماية القانونية الحالية لا تزال غير كافية، خاصة في الدول التي تفتقر إلى تشريع خاص، مما يستدعي تطوير القوانين وتشديد العقوبات، إضافة إلى تعزيز الحلول التقنية ونشر الوعي لدى المستخدمين لضمان حماية فعالة للبيانات الشخصية. الكلمات المفتاحية: البيانات الشخصية، مواقع التواصل الاجتماعي، حماية الخصوصية، الإطار القانوني .

Abstract

This research addresses the topic of the legal and civil framework for the protection of personal data of social media users, in light of rapid technological advancements and the widespread use of these platforms. It aims to clarify the concept and types of personal data, and to analyze the risks facing users' privacy, such as data breaches, cyber extortion, and the unlawful use of personal information.The study also reviews international legislations, particularly the General Data Protection Regulation (GDPR), as well as national laws, with a focus on the legal situation in Iraq and the adequacy of existing regulations in protecting personal data. In addition, it examines the role of civil liability in compensating damages resulting from data violations.The research concludes that current legal protection remains insufficient, especially in countries lacking comprehensive data protection laws. Therefore, it recommends developing legislation, strengthening legal sanctions, adopting technical protection measures, and raising user awareness to ensure effective protection of personal data.

Keywords Personal Data, Social Media, Privacy Protection, Legal Framework

المقدمة

شهد العالم في السنوات الأخيرة تطورًا كبيرًا في تكنولوجيا المعلومات والاتصالات، رافقه انتشار واسع لمواقع التواصل الاجتماعي التي أصبحت جزءًا أساسيًا من الحياة اليومية للأفراد. وقد أدى هذا التطور إلى زيادة حجم البيانات الشخصية التي يتم جمعها ومعالجتها عبر هذه المنصات، مما أثار العديد من الإشكاليات القانونية المتعلقة بحماية خصوصية الأفراد وبياناتهم. وفي ظل هذه التطورات، برزت الحاجة إلى وضع إطار قانوني ينظم حماية البيانات الشخصية، ويوازن بين استخدام التكنولوجيا وحقوق الأفراد في الخصوصية، خاصة في ظل المخاطر المتزايدة مثل تسريب البيانات والابتزاز الإلكتروني.

أهمية البحث

تتمثل أهمية هذا البحث في كونه يتناول موضوعًا حديثًا وحيويًا يمس حياة الأفراد بشكل مباشر، نظرًا لاعتمادهم الكبير على مواقع التواصل الاجتماعي. كما تكمن أهميته في إبراز دور القانون في حماية البيانات الشخصية، ومواجهة الانتهاكات التي قد يتعرض لها المستخدمون، إضافة إلى تسليط الضوء على واقع التشريعات الوطنية ومدى كفايتها في هذا المجال.

مشكلة البحث

تتمحور مشكلة البحث حول التساؤل الرئيس التالي :إلى أي مدى يوفر الإطار القانوني والمدني حماية فعالة للبيانات الشخصية لمستخدمي مواقع التواصل الاجتماعي؟ويتفرع عن هذا التساؤل عدة تساؤلات فرعية:ما المقصود بالبيانات الشخصية وما أنواعها؟ ما هي التشريعات الدولية والوطنية المنظمة لحمايتها؟ ما مدى كفاية هذه التشريعات في مواجهة التحديات الرقمية؟ ما دور المسؤولية المدنية في حماية البيانات؟

أهداف البحث

يهدف هذا البحث إلى تحقيق مجموعة من الأهداف، من أبرزها:بيان مفهوم البيانات الشخصية وأنواعها .توضيح الإطار القانوني الدولي والوطني لحماية البيانات الشخصية .تحليل مدى كفاية التشريعات الوطنية في حماية البيانات .بيان دور المسؤولية المدنية في التعويض عن الأضرار الناتجة عن انتهاك البيانات .اقتراح حلول قانونية وتقنية لتعزيز حماية البيانات الشخصية .

منهجية البحث

يعتمد هذا البحث على المنهج الوصفي التحليلي، من خلال عرض المفاهيم القانونية المتعلقة بالبيانات الشخصية، وتحليل النصوص التشريعية الدولية والوطنية، إضافة إلى دراسة الآراء الفقهية ذات الصلة، وذلك بهدف الوصول إلى نتائج دقيقة حول مدى فعالية الحماية القانونية للبيانات الشخصية.

حدود البحث

الحدود الموضوعية :يقتصر البحث على دراسة الإطار القانوني والمدني لحماية البيانات الشخصية في مواقع التواصل الاجتماعي .

الحدود المكانية :يركّز البحث على التشريعات الدولية وبعض التشريعات العربية، مع التركيز على الوضع القانوني في العراق .

الحدود الزمانية :يتناول البحث التطورات الحديثة في مجال حماية البيانات، خاصة بعد انتشار مواقع التواصل الاجتماعي.

المبحث الأول: ماهية البيانات الشخصية ومواقع التواصل الاجتماعي

المطلب الأول : مفهوم البيانات الشخصية

تُعد البيانات الشخصية من أهم المفاهيم القانونية الحديثة التي ظهرت مع تطور التكنولوجيا وانتشار مواقع التواصل الاجتماعي، لأنها لم تعد تقتصر على الاسم أو العنوان فقط، بل أصبحت تشمل كل معلومة يمكن من خلالها التعرف على الشخص بصورة مباشرة أو غير مباشرة، مثل الاسم، رقم الهاتف، البريد الإلكتروني، الصورة الشخصية، الموقع الجغرافي، أو المعرّف الإلكتروني.(أحمد، ٢٠٢٠: ٥٥)وقد أشار المعداوي إلى أن البيانات الشخصية تشمل كل المعلومات التي تتعلق بشخص طبيعي، سواء أمكن التعرف عليه مباشرة أو بصورة غير مباشرة، وذلك عن طريق الاسم أو رقم التعريف الشخصي أو بيانات الموقع أو المعرّف الإلكتروني أو غيرها من العناصر المرتبطة بالهوية الشخصية أو الاجتماعية أو الاقتصادية أو الثقافية للفرد، مما يعني أن نطاق الحماية يمتد إلى مختلف أشكال البيانات المرتبطة بالشخص. (المعداوي، ٢٠١٨: ١٢)وتزداد أهمية هذا المفهوم في مواقع التواصل الاجتماعي، لأن المستخدم يضع كمية كبيرة من البيانات أثناء استعماله للمنصة، مثل الصور، المنشورات، التعليقات، الإعجابات، الرسائل، قائمة الأصدقاء، الموقع، والاهتمامات، وهذه البيانات قد تُستخدم لأغراض مشروعة، لكنها قد تُستغل أيضًا في التتبع أو الإعلانات الموجهة أو الابتزاز أو انتهاك الخصوصية. (بوخميس، ٢٠٢٤: ٩)كما أن البيانات الشخصية لا تشمل كل البيانات بصورة مطلقة، بل يشترط أن تكون مرتبطة بشخص طبيعي يمكن تحديده، لذلك فإن البيانات المجهولة التي لا يمكن ربطها بشخص معين لا تُعد بيانات شخصية، أما إذا أمكن ربطها بالمستخدم عن طريق رقم الحساب أو البريد الإلكتروني أو رقم الهاتف أو عنوان IP فإنها تدخل ضمن نطاق الحماية القانونية . (سويلم، ٢٠٢٢: ١٨)ومن جانب آخر، يفرّق الفقه القانوني بين البيانات الشخصية العادية والبيانات الشخصية الحساسة، حيث تشمل البيانات العادية مثل الاسم والعنوان ورقم الهاتف، بينما تتعلق البيانات الحساسة بالجوانب الدقيقة من حياة الإنسان مثل الحالة الصحية، المعتقد الديني، الرأي السياسي، أو البيانات البيومترية، والتي تتطلب حماية قانونية أشد نظرًا لخطورة إساءة استخدامها. (محمد، ٢٠٢٥: ٢٥)وقد بيّنت إحدى الرسائل القانونية أن جمع أو تخزين البيانات الشخصية دون رضا صاحبها يُعد اعتداءً على الخصوصية، سواء تم ذلك بوسائل تقليدية أو إلكترونية، مثل جمع البريد الإلكتروني أو استخراج البيانات من الحسابات الرقمية، وأن الخطر لا يقتصر على نشر

البيانات بل يبدأ من مرحلة جمعها ومعالجتها. (الحماية الجزائية، ٢٠٢٢: ٨٣-٨٤)وعليه يمكن القول إن البيانات الشخصية في مواقع التواصل الاجتماعي هي كل معلومة يقدّمها المستخدم أو تُجمع عنه أثناء استخدامه للمنصة، متى كانت هذه المعلومة تكشف هويته أو تساعد على التعرف عليه، الأمر الذي يجعلها محلًا للحماية القانونية والمدنية باعتبارها تمس خصوصية الفرد وكرامته. (داوود، ٢٠١٧: ٣٢٠)

اولاً : تعريف البيانات الشخصية

تُعرَّف **البيانات الشخصية** بأنها كل معلومة تتعلق بشخص طبيعي محدد أو قابل للتحديد، سواء تم التعرف عليه بصورة مباشرة كالاسم والصورة ورقم الهاتف، أو بصورة غير مباشرة كالمعرّف الإلكتروني أو بيانات الموقع أو رقم الهوية، متى كانت هذه البيانات تؤدي إلى تحديد هوية الشخص أو تمييزه عن غيره . **(المعداوي، ٢٠١٨: ١٢)**كما تُعرّف بأنها كل بيان أو معلومة، أياً كان شكلها أو مصدرها، من شأنها أن تكشف عن هوية الشخص أو تسمح بالوصول إليه، سواء كانت بيانات مكتوبة أو رقمية أو صوتية أو مرئية، وهو ما يجعل نطاقها واسعًا ليشمل مختلف صور المعلومات في البيئة الرقمية. **(سويلم، ٢٠٢٢: ١٥)**ويذهب جانب من الفقه إلى أن البيانات الشخصية لا تقتصر على البيانات الظاهرة، بل تمتد إلى البيانات غير المباشرة التي يمكن من خلال الربط بينها تحديد هوية الشخص، مثل عنوان البريد الإلكتروني أو عنوان IP أو النشاط الإلكتروني للمستخدم، وهو ما يبرز أهمية حمايتها في مواقع التواصل الاجتماعي **(بوخميس، ٢٠٢٤: ٨)**

ثانياً : أنواع البيانات

تنقسم البيانات الشخصية غالبًا إلى نوعين رئيسيين :بيانات شخصية عادية و بيانات شخصية حساس .ويكون الفرق بينهما حسب درجة خطورة المعلومة ومدى تأثيرها على خصوصية الإنسان إذا أُسيء استخدامها.

١- البيانات الشخصية العادية

يقصد بـ البيانات الشخصية العادية كل بيان أو معلومة تتعلق بشخص طبيعي، وتؤدي إلى التعرف عليه بصورة مباشرة أو غير مباشرة، مثل الاسم، رقم الهاتف، العنوان، البريد الإلكتروني، رقم الهوية، الصورة الشخصية، أو رقم الحساب البنكي. وتُسمى "عادية" لأنها لا تكشف بالضرورة جوانب شديدة الخصوصية من حياة الإنسان، لكنها تبقى محمية قانونًا لأنها مرتبطة بهويته ، ولا يعني وصفها بالعادية أنها غير خطيرة؛ لأن جمعها أو نشرها أو تداولها دون موافقة صاحبها قد يؤدي إلى انتهاك الخصوصية أو انتحال الشخصية أو الاحتيال الإلكتروني. لذلك تشمل الحماية البيانات المتداولة إلكترونيًا والبيانات المحفوظة يدويًا أو المؤرشفة، ولاتقتصر على البيانات الموجودة في العالم الافتراضي فقط(الشمري،٢٠٢٣: ٨٥)

ومن أمثلة البيانات العادية في مواقع التواصل الاجتماعي: الاسم المستخدم في الحساب، الصورة الشخصية، رقم الهاتف المرتبط بالحساب، البريد الإلكتروني، قائمة الأصدقاء، المنشورات العامة، وموقع المستخدم إذا لم يكن مرتبطًا ببيانات حساسة. وهذه البيانات قد تبدو بسيطة، لكنها عند جمعها وتحليلها تكشف صورة واضحة عن الشخص وسلوكه واهتماماته .(البدري، ٢٠٢٣: ٢٩٠-٣٣٢)

٢-البيانات الشخصية الحساسة

أما البيانات الشخصية الحساسة فهي البيانات التي تكشف جوانب دقيقة وخاصة من حياة الإنسان، ولذلك تحتاج إلى حماية أقوى من البيانات العادية. وتشمل عادةً البيانات التي تكشف الأصل العرقي أو الإثني، الآراء السياسية، المعتقدات الدينية أو الفلسفية، الانتماء النقابي، البيانات الجينية، البيانات البيومترية المستخدمة للتعرف على الشخص، البيانات الصحية، أو البيانات المتعلقة بالحياة الخاصة جدًا للفرد (الاتحاد الأوروبي، ٢٠١٦: المادة ٩)وسبب اعتبارها حساسة هو أن إساءة استخدامها قد تُحدث ضررًا أشد من البيانات العادية، مثل التمييز، التشهير، الابتزاز، الإقصاء الوظيفي أو الاجتماعي، أو الإضرار بسمعة الشخص. لذلك تمنع التشريعات الحديثة معالجة هذا النوع من البيانات إلا في حالات محددة، مثل وجود موافقة صريحة من صاحب البيانات أو وجود سبب قانوني واضح (مكتب مفوض المعلومات البريطاني، ٢٠٢٤: فقرة البيانات ذات الفئة الخاصة)وفي مواقع التواصل الاجتماعي، تظهر البيانات الحساسة من خلال منشور يوضح الحالة الصحية، أو تعليق يكشف الرأي السياسي، أو صورة تكشف المعتقد الديني، أو استخدام بصمة الوجه والصوت للتحقق من الحساب. ولهذا تكون خطورتها أكبر؛ لأنها لا تكشف هوية المستخدم فقط، بل تكشف تفاصيل عميقة قد تُستغل ضده (أبوخميس، ٢٠٢٤: ٨٧)

وجه المقارنة	البيانات العادية	البيانات الحساسة
المعنى	معلومات تعرف بالشخص مباشرة أو غير مباشرة	معلومات تكشف جوانب عميقة وخاصة من حياة الشخص

الأمثلة	الاسم، الهاتف، البريد، العنوان، الصورة	الصحة، الدين، السياسة، البصمة، البيانات الجينية
درجة الخطورة	متوسطة غالبًا	عالية
الحماية القانونية	محمية قانونًا	تحتاج حماية أشد وشروطًا أقوى
الضرر عند التسريب	إزعاج، احتيال، انتحال شخصية	تمييز، ابتزاز، تشهير، ضرر اجتماعي أو نفسي

الجدول (١) المقارنة بين البيانات العادية والحساسة

المطلب الثاني: مفهوم مواقع التواصل الاجتماعي

تُعرَّف مواقع التواصل الاجتماعي بأنها منصات إلكترونية تتيح للمستخدمين إنشاء حسابات شخصية، والتفاعل مع الآخرين من خلال تبادل الرسائل والصور والفيديوهات والمعلومات، وبناء شبكات اجتماعية رقمية تربط بينهم رغم البعد الجغرافي. وهي تُعد من أبرز تطبيقات الإنترنت الحديثة التي غيّرت طريقة التواصل بين الأفراد والمجتمعات. (بوخميس، ٢٠٢٤: ٥)كما تُعرَّف بأنها مجموعة من التطبيقات الرقمية التي تعتمد على شبكة الإنترنت، وتسمح بإنشاء محتوى من قبل المستخدمين أنفسهم، ومشاركته مع الآخرين، مثل الكتابة، التعليق، النشر، الإعجاب، وإعادة المشاركة، وهو ما يجعل المستخدم ليس متلقيًا فقط بل منتجًا للمحتوى أيضًا(Kaplan & Haenlein, 2010: 61) .وتتميّز مواقع التواصل الاجتماعي بعدة خصائص، أهمها التفاعلية، وسهولة الاستخدام، والسرعة في نشر المعلومات، وإمكانية الوصول إلى جمهور واسع، إضافة إلى القدرة على تكوين مجتمعات افتراضية قائمة على الاهتمامات المشتركة. وقد أدت هذه الخصائص إلى انتشارها الواسع واعتمادها في مختلف مجالات الحياة الاجتماعية والاقتصادية والسياسية. (البدري، ٢٠٢٣: ٢٩٥)ومن ناحية قانونية، تُعد مواقع التواصل الاجتماعي بيئة رقمية يتم فيها جمع وتخزين ومعالجة كميات كبيرة من البيانات الشخصية للمستخدمين، سواء من خلال المعلومات التي يقدمها المستخدم بنفسه أو التي يتم جمعها أثناء استخدامه للمنصة، مما يجعلها مجالًا مهمًا لتنظيم الحماية القانونية للبيانات الشخصية. (سويلم، ٢٠٢٢: ٢٠)كما أن هذه المواقع لا تقتصر على التواصل الاجتماعي فقط، بل أصبحت وسيلة للتأثير في الرأي العام، ونشر الأخبار، والتسويق الإلكتروني، والتعليم، والتعبير عن الآراء، وهو ما يزيد من أهميتها وخطورتها في نفس الوقت، خصوصًا فيما يتعلق بانتهاك الخصوصية أو إساءة استخدام البيانات. (داوود، ٢٠١٧: ٣٢٥)تُعرَّف مواقع التواصل الاجتماعي بأنها خدمات إلكترونية تُقدَّم عبر الإنترنت، تُمكّن المستخدمين من إنشاء ملفات تعريف شخصية، وبناء علاقات مع مستخدمين آخرين، والتفاعل معهم من خلال مشاركة المحتوى والمعلومات داخل بيئة رقمية مشتركة (Boyd & Ellison, 2007: 211) .

كما تُعرَّف بأنها تطبيقات رقمية قائمة على الإنترنت تسمح للأفراد بإنشاء شبكات اجتماعية افتراضية، وتبادل الرسائل والمحتوى الرقمي، والمشاركة في النقاشات العامة، مما يجعلها وسيلة اتصال حديثة تتجاوز الحدود الجغرافية والزمنية. (البدري، ٢٠٢٣: ٢٩٤)ويذهب بعض الباحثين إلى أن مواقع التواصل الاجتماعي تمثل فضاءً إلكترونيًا مفتوحًا يُستخدم للتفاعل الاجتماعي، وتبادل الآراء، وبناء العلاقات، ونشر المعلومات، بحيث أصبح لها دور كبير في تشكيل الرأي العام والتأثير في السلوك الاجتماعي للأفراد. (الشمري، ٢٠٢٣: ٧٨)ومن منظور قانوني، تُعد مواقع التواصل الاجتماعي بيئة رقمية تجمع وتعالج كميات كبيرة من البيانات الشخصية، سواء من خلال البيانات التي يقدمها المستخدم طوعًا أو التي يتم جمعها أثناء استخدامه للمنصة، وهو ما يثير إشكاليات قانونية تتعلق بحماية الخصوصية والبيانات الشخصية .(سويلم، ٢٠٢٢: ٢٠)

اولاً: خصائص مواقع التواصل الاجتماعي

تتميّز مواقع التواصل الاجتماعي بعدة خصائص تجعلها مختلفة عن وسائل الاتصال التقليدية، وهذه الخصائص هي السبب في انتشارها الواسع وتأثيرها الكبير، خاصة في مجال البيانات الشخصية:

١- التفاعلية

تتميّز مواقع التواصل الاجتماعي بكونها وسيلة اتصال تفاعلية، حيث لا يقتصر دور المستخدم على استقبال المعلومات فقط، بل يشارك في إنتاجها والتفاعل معها من خلال التعليق والمشاركة والإعجاب، مما يجعل الاتصال ثنائي الاتجاه. (الشمري، ٢٠٢٣: ٧٩)

٢-إنتاج المحتوى من قبل المستخدم

تعتمد هذه المواقع على المحتوى الذي ينشئه المستخدمون أنفسهم، مثل النصوص والصور والفيديوهات، وهو ما يجعل المستخدم عنصرًا أساسيًا في تكوين المحتوى الرقمي، وليس مجرد متلقٍ له. (البدري، ٢٠٢٣: ٢٩٥)

٣- سهولة الاستخدام والانتشار

تتميّز مواقع التواصل بسهولة الاستخدام، حيث يمكن لأي شخص إنشاء حساب والتفاعل مع الآخرين دون الحاجة إلى خبرة تقنية كبيرة، مما أدى إلى انتشارها الواسع بين مختلف فئات المجتمع. (عبد الرزاق، ٢٠٢١: ١١٢)

٤- السرعة في نقل المعلومات

تُعد السرعة من أبرز خصائص مواقع التواصل الاجتماعي، إذ يمكن نشر المعلومات وانتقالها إلى عدد كبير من المستخدمين خلال وقت قصير جدًا، وهو ما يزيد من تأثيرها في تشكيل الرأي العام. (حسين، ٢٠٢٠: ٨٨)

٥- تكوين العلاقات والشبكات الاجتماعية

تتيح مواقع التواصل للمستخدمين تكوين علاقات اجتماعية افتراضية، سواء مع الأصدقاء أو مع أشخاص جدد، مما يسهم في توسيع دائرة العلاقات الاجتماعية خارج الحدود الجغرافية .(الطائي، ٢٠٢٢: ٦٧)

٦-جمع البيانات الشخصية

تقوم مواقع التواصل الاجتماعي بجمع كميات كبيرة من البيانات الشخصية عن المستخدمين، سواء من خلال المعلومات التي يقدمها المستخدم أو من خلال تتبع نشاطه داخل المنصة، وهو ما يثير قضايا قانونية تتعلق بحماية الخصوصية. (سويلم، ٢٠٢٢: ٢١)

٧-العالمية

تتميّز هذه المواقع بطابعها العالمي، حيث تتيح التواصل بين المستخدمين في مختلف دول العالم، مما يجعلها وسيلة اتصال عابرة للحدود، لكنها في نفس الوقت تطرح تحديات قانونية بسبب اختلاف الأنظمة القانونية بين الدول. (داوود، ٢٠١٧: ٣٢٦)

ثانياً: مخاطر مواقع التواصل الاجتماعي على الخصوصية

١- جمع البيانات المفرط

تعتمد منصات التواصل الاجتماعي على جمع كميات ضخمة من البيانات الشخصية، بما في ذلك البيانات التي يقدمها المستخدم والبيانات التي يتم جمعها تلقائيًا مثل الموقع وسلوك التصفح، وغالبًا ما يتم ذلك دون فهم كامل من المستخدم لطبيعة هذا الجمع ومداه (European Data Protection Board, 2021: 6) .

٢-التتبع المستمر والسلوك الرقمي

تقوم المنصات بتتبع نشاط المستخدم داخل الموقع وخارجه باستخدام تقنيات مثل Cookies و Tracking Pixels، بهدف تحليل السلوك وتقديم إعلانات موجهة، مما يشكل تدخلاً مستمرًا في الحياة الخاصة(ICO, 2024: Online Tracking Guidance).

٣-تسريب البيانات والاختراقات

تتعرض مواقع التواصل لاختراقات تؤدي إلى تسريب بيانات ملايين المستخدمين، مثل كلمات المرور والمعلومات الشخصية، مما يعرضهم لسرقة الهوية والاحتيال(ENISA, 2023: Threat Landscape Report, p. 45) .

٤-فقدان السيطرة على البيانات

بمجرد نشر البيانات على مواقع التواصل، يصبح من الصعب على المستخدم التحكم في كيفية استخدامها أو إعادة نشرها، حيث يمكن نسخها أو مشاركتها أو تخزينها من قبل أطراف أخرى دون موافقته(OECD, 2022: Digital Environment Report, p. 98) .

٥-التنميط والتأثير على السلوك

تستخدم الشركات البيانات الشخصية لإنشاء ملفات تعريف دقيقة للمستخدمين(Profiling) ، مما يسمح بالتأثير على قراراتهم وسلوكهم، خاصة في الإعلانات أو حتى في المجالات السياسية(European Commission, 2022: Data Strategy Report, p. 34) .

٦-المخاطر على البيانات الحساسة

قد تكشف مواقع التواصل عن بيانات حساسة مثل المعتقدات أو الحالة الصحية أو الآراء السياسية، سواء من خلال المنشورات أو التحليل غير المباشر، مما يزيد من خطر التمييز أو الاستغلال(GDPR, 2016: Article 9).

٧- الابتزاز الإلكتروني والاستغلال

تُستخدم البيانات الشخصية، خاصة الصور والمعلومات الخاصة، في الابتزاز الإلكتروني أو التهديد، وهو ما يُعد من أخطر أشكال انتهاك الخصوصية في البيئة الرقمية(Europol, 2023: Cybercrime Report, p. 52) .

٨- تضليل المستخدم وضعف الشفافية

غالبًا لا يكون المستخدم على دراية كاملة بكيفية جمع بياناته أو استخدامها، بسبب سياسات الخصوصية المعقدة، مما يؤدي إلى ضعف الموافقة الحقيقية(World Economic Forum, 2022: Digital Trust Report, p. 21)

المبحث الثاني: الإطار القانوني لحماية البيانات الشخصية

المطلب الأول: التشريعات الدولية

اولاً: التشريعات الدولية لحماية البيانات الشخصية

تُعد التشريعات الدولية الأساس في تنظيم حماية البيانات الشخصية، خاصة مع الطابع العالمي للإنترنت ومواقع التواصل الاجتماعي، حيث تتجاوز البيانات حدود الدول، مما يستلزم وجود قواعد قانونية دولية تنظم جمع البيانات ومعالجتها وحمايتها.

١-اللائحة العامة لحماية البيانات(GDPR)

تُعد اللائحة العامة لحماية البيانات (GDPR) الصادرة عن الاتحاد الأوروبي سنة ٢٠١٦ من أهم وأقوى التشريعات الدولية في مجال حماية البيانات الشخصية، حيث وضعت إطارًا قانونيًا شاملاً لتنظيم كيفية جمع البيانات ومعالجتها وتخزينها. وقد عرّفت البيانات الشخصية بأنها كل معلومة تتعلق بشخص طبيعي محدد أو قابل للتحديد .(الاتحاد الأوروبي، ٢٠١٦: المادة ٤)

كما أقرت اللائحة مجموعة من المبادئ الأساسية، مثل:

أ- مبدأ المشروعية والشفافية

ب- مبدأ تحديد الغرض

ت- مبدأ تقليل البيانات

ث- مبدأ الدقة

ج- مبدأ حماية البيانات

وتهدف هذه المبادئ إلى ضمان عدم استخدام البيانات إلا في حدود الغرض الذي جُمعت من أجله. (الاتحاد الأوروبي، ٢٠١٦: المادة ٥)

كما منحت اللائحة للأفراد حقوقًا مهمة، مثل:

أ- الحق في الوصول إلى البيانات

ب- الحق في تصحيحها

ت- الحق في محوها (الحق في النسيان)

ث- الحق في الاعتراض على المعالجة (الاتحاد الأوروبي، ٢٠١٦: المواد ١٢-٢٣)

٢-اتفاقية مجلس أوروبا رقم ١٠٨

تُعد هذه الاتفاقية من أقدم الاتفاقيات الدولية في مجال حماية البيانات، حيث صدرت سنة ١٩٨١ عن مجلس أوروبا، وهدفت إلى حماية الأفراد من مخاطر المعالجة الآلية للبيانات الشخصية، وضمان احترام حياتهم الخاصة. (مجلس أوروبا، ١٩٨١: المادة ١)

كما أكدت على ضرورة:

أ- جمع البيانات بطريقة مشروعة

ب- استخدامها لأغراض محددة

ت- ضمان أمن البيانات (مجلس أوروبا، ١٩٨١: المادة ٥)

٣-منظمة التعاون الاقتصادي والتنمية – (OECD) مبادئ حماية الخصوصية

وضعت منظمة التعاون الاقتصادي والتنمية سنة ١٩٨٠ (وتم تحديثها لاحقًا) مجموعة من المبادئ الإرشادية لحماية البيانات الشخصية، والتي تُعد أساسًا للعديد من التشريعات الحديثة.

ومن أهم هذه المبادئ: (OECD , 2013: 13) :

أ- مبدأ تحديد الغرض

ب- مبدأ جودة البيانات

ت- مبدأ الأمن والحماية

ث- مبدأ المساءلة

٤-الأمم المتحدة -الحق في الخصوصية

أكدت الأمم المتحدة في الإعلان العالمي لحقوق الإنسان على حماية الخصوصية، حيث نصت المادة (١٢) على أنه لا يجوز التدخل التعسفي في حياة الفرد الخاصة أو أسرته أو مراسلاته(.الأمم المتحدة، ١٩٤٨: المادة ١٢)

كما نص العهد الدولي الخاص بالحقوق المدنية والسياسية على نفس المبدأ، مما يعطي حماية البيانات أساسًا حقوقيًا دوليًا .(الأمم المتحدة، ١٩٦٦: المادة ١٧)

ثانياً: مبادئ حماية البيانات الشخصية تُعد مبادئ حماية البيانات الشخصية الأساس الذي تقوم عليه التشريعات الحديثة، خاصة في البيئة الرقمية ومواقع التواصل الاجتماعي، حيث تهدف إلى تنظيم كيفية جمع البيانات ومعالجتها واستخدامها بطريقة تضمن احترام خصوصية الأفراد.

١- مبدأ المشروعية والشفافية

يقضي هذا المبدأ بأن يتم جمع ومعالجة البيانات الشخصية بطريقة قانونية وواضحة، بحيث يكون المستخدم على علم بكيفية استخدام بياناته، ومن هي الجهة التي تقوم بجمعها، ولأي غرض تُستخدم .(الاتحاد الأوروبي، ٢٠١٦: المادة ٥/١-أ)

٢-مبدأ تحديد الغرض

يجب أن تُجمع البيانات الشخصية لغرض محدد وواضح ومشروع، ولا يجوز استخدامها لاحقًا في أغراض أخرى تختلف عن الغرض الذي جُمعت من أجله .(الاتحاد الأوروبي، ٢٠١٦: المادة ٥/١-ب)

٣-مبدأ تقليل البيانات

يقضي هذا المبدأ بأن تقتصر البيانات التي يتم جمعها على الحد الأدنى الضروري لتحقيق الغرض المطلوب، دون جمع بيانات زائدة لا حاجة لها. (الاتحاد الأوروبي، ٢٠١٦: المادة ٥/١-ج)

٤-مبدأ الدقة

يجب أن تكون البيانات الشخصية دقيقة ومحدثة، وعلى الجهة التي تعالج البيانات تصحيح أي معلومات غير صحيحة أو حذفها عند الحاجة .(الاتحاد الأوروبي، ٢٠١٦: المادة ٥/١-د)

٥- مبدأ تحديد مدة الاحتفاظ

يجب ألا يتم الاحتفاظ بالبيانات الشخصية لفترة أطول من اللازم لتحقيق الغرض الذي جُمعت من أجله، وبعد ذلك يجب حذفها أو إتلافها بطريقة امنة. (الاتحاد الأوروبي، ٢٠١٦: المادة ٥/١-هـ)

٦-مبدأ الأمن والحماية

يجب حماية البيانات الشخصية من الوصول غير المصرح به أو الاستخدام غير المشروع، وذلك من خلال اتخاذ تدابير تقنية وتنظيمية مناسبة مثل التشفير وأنظمة الحماية. (الاتحاد الأوروبي، ٢٠١٦: المادة ٥/١-و)

٧- مبدأ المساءلة

يلزم هذا المبدأ الجهات التي تتعامل مع البيانات الشخصية بأن تكون مسؤولة عن الالتزام بهذه المبادئ، وأن تكون قادرة على إثبات ذلك عند الحاجة .(الاتحاد الأوروبي، ٢٠١٦: المادة ٥/٢)

٨- مبدأ الموافقة(Consent) يجب الحصول على موافقة صريحة من صاحب البيانات قبل جمع أو معالجة بياناته، خاصة في الحالات التي لا يوجد فيها أساس قانوني آخر للمعالجة(OECD, 2013: 14) .

المطلب الثاني: التشريعات الوطنية

اولاً: التشريعات الوطنية في العراق: القوانين المحلية المتعلقة بحماية البيانات

القوانين المحلية المتعلقة بحماية البيانات الشخصية على خلاف العديد من الدول العربية، لا يوجد في العراق حتى الآن قانون مستقل وشامل لحماية البيانات الشخصية، وإنما تتوزع الحماية القانونية على مجموعة من النصوص العامة في قوانين مختلفة، والتي توفر حماية جزئية وغير متكاملة لخصوصية الأفراد وبياناتهم.

١- :قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩

يُعد قانون العقوبات من أهم القوانين التي توفر حماية غير مباشرة للبيانات الشخصية، حيث يجرّم الأفعال التي تمس الخصوصية، مثل إفشاء الأسرار أو الاعتداء على الحياة الخاصة.

فقد نص القانون على تجريم نشر أو إفشاء الأسرار الخاصة بالأفراد دون إذنهم، خاصة إذا كان ذلك يسبب ضررًا لهم، سواء تم ذلك عن طريق النشر أو أي وسيلة أخرى(.قانون العقوبات العراقي، ١٩٦٩: المادة ٤٣٧)

كما يعاقب على انتهاك حرمة الحياة الخاصة، مثل نشر صور أو معلومات شخصية دون رضا صاحبها، وهو ما يشمل في الوقت الحالي النشر عبر مواقع التواصل الاجتماعي(.قانون العقوبات العراقي، ١٩٦٩: المادة ٤٣٨)

٢- قانون أصول المحاكمات الجزائية العراقي رقم ٢٣ لسنة ١٩٧١

يوفر هذا القانون حماية إجرائية لخصوصية الأفراد، من خلال تنظيم إجراءات التفتيش وضبط البيانات، حيث لا يجوز الاطلاع على المعلومات الشخصية أو الرسائل الخاصة إلا وفق إجراءات قانونية محددة وبإذن من الجهات المختصة(.قانون أصول المحاكمات الجزائية، ١٩٧١: المادة ٥١)

٣-قانون حقوق الصحفيين العراقي رقم ٢١ لسنة ٢٠١١

ينص هذا القانون على ضرورة احترام الحياة الخاصة للأفراد، وعدم نشر معلومات أو صور تمس خصوصيتهم دون موافقتهم، حتى في إطار العمل الإعلامي(.قانون حقوق الصحفيين، ٢٠١١: المادة ٧)

٤- دستور جمهورية العراق لسنة ٢٠٠٥

يُعد الدستور الأساس في حماية الخصوصية، حيث نص على أن:لكل فرد الحق في الخصوصية الشخصية لا يجوز انتهاك حرمة المراسلات والاتصالات (دستور العراق، ٢٠٠٥: المادة ١٧) وهذا يشمل البيانات الشخصية المتداولة عبر الوسائل الإلكترونية ومواقع التواصل الاجتماعي.

٥-مشروع قانون جرائم المعلوماتية العراقي (غير مُقر)يهدف هذا المشروع إلى تنظيم الجرائم المرتبطة بالإنترنت، بما في ذلك:

أ- اختراق الحسابات

ب- نشر البيانات دون إذن

ت- إساءة استخدام المعلومات

إلا أنه لم يتم إقراره حتى الآن، مما يترك فراغًا قانونيًا في مجال حماية البيانات الشخصية. (العاني، ٢٠١٩: ١٤٢)

ثانياً: مدى كفاية التشريعات العراقية لحماية البيانات الشخصية وتطبيقها

تُعد مسألة كفاية التشريعات العراقية لحماية البيانات الشخصية من أبرز الإشكاليات القانونية في العصر الرقمي، خاصة مع الانتشار الواسع لمواقع التواصل الاجتماعي وتزايد مخاطر انتهاك الخصوصية. ورغم وجود نصوص قانونية متفرقة، إلا أن مدى كفايتها وتطبيقها يظل محل نقاش.

مدى كفاية التشريعات

١-غياب قانون مستقل وشامل

تعاني المنظومة القانونية في العراق من غياب قانون خاص ينظم حماية البيانات الشخصية بشكل متكامل، حيث تعتمد الحماية على نصوص عامة في قوانين مختلفة، مثل قانون العقوبات والدستور، وهي نصوص لم تُصمَّم لمواكبة البيئة الرقمية الحديثة. (العاني، ٢٠١٩: ١٤٥)

٢- قصور النصوص التقليدية

إن القوانين الحالية، مثل قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩، تركز على حماية الخصوصية بصورتها التقليدية (مثل إفشاء الأسرار)، لكنها لا تعالج مسائل حديثة مثل:

أ- جمع البيانات الرقمية

ب- معالجتها

ت- نقلها عبر الإنترنت

ث- استخدام الذكاء الاصطناعي في تحليلها (العبيدي، ٢٠٢١: ٨٨)

٣-غياب حقوق واضحة للمستخدم

لا تمنح التشريعات العراقية الحالية حقوقًا صريحة للمستخدمين فيما يتعلق ببياناتهم، مثل:

- الحق في الوصول إلى البيانات
- الحق في تصحيحها
- الحق في حذفها
- وهي حقوق أساسية موجودة في القوانين الحديثة مثل .GDPR (سويلم، ٢٠٢٢: ٣٠)

٤- ضعف التنظيم الرقابي

لا توجد جهة مستقلة متخصصة في العراق تُشرف على حماية البيانات الشخصية، مثل "هيئة حماية البيانات"، مما يؤدي إلى ضعف الرقابة على الجهات التي تجمع أو تعالج البيانات. (الشمري، ٢٠٢٣: ٩٠)

مدى التطبيق العملي

١- ضعف التنفيذ القانوني

حتى النصوص الموجودة لا يتم تطبيقها بشكل فعّال، بسبب ضعف الوعي القانوني، وقلة الخبرة في الجرائم الرقمية، وصعوبة تتبع الانتهاكات التي تحدث عبر الإنترنت. (داوود، ٢٠١٧: ٣٤٠)

٢-صعوبة إثبات الجرائم الإلكترونية

تُعد جرائم انتهاك البيانات الشخصية من الجرائم المعقدة، حيث يصعب إثباتها تقنيًا، خاصة في حالات الاختراق أو التتبع أو سرقة البيانات، مما يحد من فعالية الحماية القانونية. (العاني، ٢٠١٩: ١٥٠)

٣-الطابع العابر للحدود

نظرًا لأن مواقع التواصل الاجتماعي تعمل على مستوى عالمي، فإن الانتهاكات قد تحدث خارج حدود الدولة، مما يصعّب تطبيق القوانين العراقية عليها.(العبيدي، ٢٠٢١: ٩٥)

.4ضعف الوعي المجتمعي

يُسهم ضعف وعي المستخدمين بخطورة نشر بياناتهم الشخصية في زيادة الانتهاكات، حيث يقوم الكثير من الأفراد بمشاركة معلوماتهم دون إدراك للمخاطر القانونية. (الشمري، ٢٠٢٣: ٩٢)

المبحث الثالث: الحماية المدنية للبيانات الشخصية

المسؤولية المدنية عن انتهاك البيانات

تُعدّ المسؤولية المدنية وسيلة قانونية لحماية الأفراد من الأضرار الناتجة عن انتهاك بياناتهم الشخصية، خاصة في بيئة مواقع التواصل الاجتماعي، حيث قد يؤدي نشر البيانات أو استخدامها دون إذن إلى أضرار مادية أو معنوية تستوجب التعويض.

أولاً: مفهوم المسؤولية المدنية

تُعرَّف المسؤولية المدنية بأنها التزام قانوني يقع على عاتق الشخص الذي يرتكب خطأً يسبب ضررًا للغير، يلزمه بتعويض هذا الضرر. وتقوم هذه المسؤولية على فكرة إصلاح الضرر وإعادة التوازن بين الأطراف .(السنهوري، ١٩٥٢: ٦٧٥)

وفي مجال البيانات الشخصية، تتحقق المسؤولية المدنية عندما يقوم شخص أو جهة بجمع أو نشر أو معالجة بيانات شخص آخر دون وجه حق، مما يؤدي إلى الإضرار به(.داوود، ٢٠١٧: ٣٤٥)

ثانيًا: أساس المسؤولية المدنية في انتهاك البيانات

تستند المسؤولية المدنية في هذا المجال إلى المسؤولية التقصيرية، أي أنها تنشأ عن فعل غير مشروع (خطأ) يؤدي إلى ضرر، حتى في غياب علاقة تعاقدية بين الطرفين. فمثلاً: نشر صور شخص دون إذنه على مواقع التواصل يُعد فعلًا غير مشروع يترتب عليه مسؤولية مدنية. (العبيدي، ٢٠٢١: ١٠٢)

ثالثًا: أركان المسؤولية المدنية

لكي تتحقق المسؤولية المدنية عن انتهاك البيانات الشخصية، يجب توافر ثلاثة أركان أساسية:

١- الخطأ: ويقصد به كل فعل غير مشروع يخالف القانون أو العرف أو يتعدى على حقوق الآخرين، مثل:

- نشر بيانات شخصية دون إذن
- تسريب معلومات خاصة
- استخدام البيانات لأغراض غير مشروعة (السنهوري، ١٩٥٢: ٦٧٨)

٢-الضرر: وهو الأذى الذي يصيب الشخص نتيجة هذا الخطأ، وقد يكون:

- ضرر مادي : مثل خسارة مالية بسبب سرقة البيانات
- ضرر معنوي : مثل التشهير أو الإحراج أو المساس بالسمعة (داوود، ٢٠١٧: ٣٥٠)

٣-العلاقة السببية: يجب أن يكون هناك رابط مباشر بين الخطأ والضرر، أي أن يكون الضرر نتيجة مباشرة لانتهاك البيانات، وليس بسبب عامل آخر .(العبيدي، ٢٠٢١: ١٠٥)

رابعًا: صور المسؤولية المدنية في مواقع التواصل:

تظهر المسؤولية المدنية في عدة صور، منها:

أ- نشر الصور أو الفيديوهات دون إذن

ب- اختراق الحسابات وتسريب البيانات

ت- استخدام المعلومات الشخصية في الاحتيال أو الابتزاز

ث- إنشاء حسابات وهمية (انتحال شخصية) (الشمري، ٢٠٢٣: ٩٥)

خامسًا: آثار المسؤولية المدنية (التعويض)

إذا ثبتت المسؤولية المدنية، يلتزم المسؤول بـ تعويض المتضرر، ويشمل التعويض:

- تعويض مادي (خسائر مالية)
- تعويض معنوي (الضرر النفسي أو الاجتماعي)
- ويقدّر القاضي التعويض حسب حجم الضرر وظروف الواقعة .(السنهوري، ١٩٥٢: ٦٨٢)

المبحث الرابع: التحديات القانونية في حماية بيانات مستخدمي مواقع التواصل

المطلب الأول: صعوبات التطبيق

تُعد حماية البيانات الشخصية في مواقع التواصل الاجتماعي من القضايا القانونية الحديثة التي تواجه تحديات كبيرة في التطبيق العملي، رغم وجود تشريعات تهدف إلى تنظيم هذا المجال. ويرجع ذلك إلى الطبيعة التقنية المتطورة لهذه المنصات، واعتمادها على بيئة رقمية مفتوحة وسريعة التغير، مما يجعل من الصعب فرض رقابة فعّالة أو تطبيق القوانين بشكل كامل، كما أن التوسع الكبير في استخدام مواقع التواصل، وتعدد الجهات التي تتعامل مع البيانات، يزيد من تعقيد عملية الحماية، خاصة في ظل غياب التنسيق الدولي الكافي واختلاف الأنظمة القانونية بين الدول. لذلك، تظهر عدة صعوبات تعيق التطبيق الفعلي لحماية البيانات الشخصية، من أبرزها صعوبة الرقابة والطابع العابر للحدود.**(الشمري، ٢٠٢٣: ١٠٠؛ سويلم، ٢٠٢٢: ٣٩)**

أولاً: صعوبة الرقابة

تُعد صعوبة الرقابة من أبرز التحديات التي تواجه حماية البيانات الشخصية، إذ يصعب على الجهات المختصة مراقبة الكم الهائل من البيانات التي يتم تداولها يوميًا عبر مواقع التواصل الاجتماعي. فهذه المنصات تعتمد على ملايين المستخدمين الذين ينشرون محتوى بشكل مستمر، مما يجعل من الصعب تتبع الانتهاكات أو السيطرة عليها في الوقت المناسب. (سويلم، ٢٠٢٢: ٤٠)كما أن التطور التكنولوجي السريع وتنوع وسائل الاتصال الرقمية يزيد من تعقيد الرقابة، حيث تستخدم منصات التواصل تقنيات متقدمة مثل التشفير والذكاء الاصطناعي، مما يجعل اكتشاف الانتهاكات أو تتبع مصدرها أكثر صعوبة .(الشمري، ٢٠٢٣: ١٠٢)إضافة إلى ذلك، تعاني الجهات الرقابية في بعض الدول من ضعف الإمكانيات

التقنية والبشرية، وقلة الخبرة في التعامل مع الجرائم الإلكترونية، مما يؤدي إلى محدودية قدرتها على فرض القوانين بشكل فعّال.(داوود، ٢٠١٧: ٣٦٠)

ثانيًا: الطابع العابر للحدود

تتميّز مواقع التواصل الاجتماعي بأنها بيئة عالمية لا تعترف بالحدود الجغرافية، حيث يمكن للمستخدم في دولة معينة نشر بيانات تصل إلى مستخدمين في مختلف أنحاء العالم، مما يخلق إشكالية قانونية تتعلق بتحديد القانون الواجب التطبيق. (العبيدي، ٢٠٢١: ١٢٠)كما أن الشركات المالكة لمواقع التواصل غالبًا ما تكون مقارها في دول أخرى، مما يصعّب على الدول فرض قوانينها الوطنية عليها، خاصة في حال وقوع انتهاكات تتعلق ببيانات المستخدمين. (سويلم، ٢٠٢٢: ٤٢)ويؤدي هذا الطابع العابر للحدود إلى تضارب القوانين بين الدول، حيث تختلف التشريعات في مستوى الحماية والضوابط، مما قد يستغله البعض للتهرب من المسؤولية أو استغلال الثغرات القانونية.(الشمري، ٢٠٢٣: ١٠٥)

المطلب الثاني: الجرائم والانتهاكات الشائعة في مواقع التواصل

تُعد مواقع التواصل الاجتماعي بيئة خصبة لارتكاب العديد من الجرائم والانتهاكات المرتبطة بالبيانات الشخصية، نتيجة سهولة تداول المعلومات وضعف الوعي أو الحماية التقنية، ومن أبرز هذه الجرائم:

أولاً: تسريب البيانات

يُقصد بتسريب البيانات إفشاء أو نشر البيانات الشخصية للمستخدمين دون إذنهم، سواء نتيجة اختراق الأنظمة أو بسبب إهمال في حمايتها من قبل الجهة المسؤولة. وقد يشمل ذلك تسريب الأسماء، أرقام الهواتف، كلمات المرور، أو الصور والمعلومات الخاصة ، ويؤدي تسريب البيانات إلى تعريض الأفراد لمخاطر متعددة، مثل الاحتيال، وانتحال الشخصية، وانتهاك الخصوصية، خاصة إذا كانت البيانات المسربة حساسة .(الهيئة الوطنية للأمن السيبراني، السعودية، ٢٠٢٣: دليل حماية البيانات)

ثانيًا: الابتزاز الإلكتروني

يُعد الابتزاز الإلكتروني من أخطر الجرائم المرتبطة بمواقع التواصل، حيث يتم استغلال البيانات أو الصور أو المعلومات الشخصية لتهديد الضحية بهدف الحصول على المال أو تحقيق منفعة معينة، وغالبًا ما يعتمد المبتز على معلومات حصل عليها من الحسابات الشخصية أو من خلال الاختراق أو الخداع، ويهدد بنشرها إذا لم يتم تنفيذ مطالبه .(مكتب الأمم المتحدة المعني بالمخدرات والجريمة، ٢٠٢٢: جرائم الإنترنت)

ثالثًا: الاستخدام غير المشروع للبيانات

يقصد به استخدام البيانات الشخصية دون موافقة صاحبها أو خارج الغرض الذي جُمعت من أجله، مثل بيع البيانات لشركات إعلانية، أو استخدامها في التسويق الموجه، أو تحليل سلوك المستخدم دون علمه.

ويُعد هذا النوع من الانتهاك شائعًا في مواقع التواصل، حيث تقوم بعض المنصات أو الجهات الخارجية بجمع البيانات واستغلالها لأغراض تجارية أو سياسية دون شفافية كافية. (اللجنة الأوروبية، ٢٠٢٢: سياسة البيانات الرقمية)

المطلب الثالث: آليات تعزيز حماية البيانات الشخصية

تتطلب حماية البيانات الشخصية، خاصة في مواقع التواصل الاجتماعي، تبني مجموعة متكاملة من الآليات القانونية والتقنية والتوعوية، لمواجهة المخاطر والانتهاكات المتزايدة في البيئة الرقمية.

اولاً: الحلول القانونية

١-تطوير التشريعات

يُعد تطوير التشريعات من أهم الوسائل لتعزيز حماية البيانات الشخصية، حيث يجب على الدول إصدار قوانين حديثة ومتخصصة تواكب التطور التكنولوجي، وتنظم عمليات جمع البيانات ومعالجتها وتخزينها، وتحدد حقوق الأفراد والتزامات الجهات التي تتعامل مع البيانات.كما ينبغي أن تستند هذه التشريعات إلى المعايير الدولية، مثل مبادئ الشفافية والمشروعية، ومنح الأفراد حقوقًا واضحة كحق الوصول إلى البيانات وتصحيحها وحذفها .(سويلم، ٢٠٢٢: ٥٠)

٢-تشديد العقوبات

يُسهم تشديد العقوبات القانونية في ردع الأفراد والجهات عن ارتكاب جرائم انتهاك البيانات، مثل تسريب المعلومات أو استخدامها دون إذن أو الابتزاز الإلكتروني ، وتشمل هذه العقوبات الغرامات المالية والعقوبات السالبة للحرية، ويجب أن تكون متناسبة مع خطورة الفعل المرتكب، خاصة في الجرائم التي تتعلق بالبيانات الحساسة.(الشمري، ٢٠٢٣: ١١٠)

ثانياً: الحلول التقنية والتوعوية

١-التشفير وحماية الحسابات

يُعد استخدام التقنيات الحديثة، مثل التشفير، من أهم وسائل حماية البيانات الشخصية، حيث يساعد على تأمين المعلومات ومنع الوصول غير المصرح به إليها، كما أن اعتماد إجراءات أمنية مثل كلمات المرور القوية، والمصادقة الثنائية(Two-Factor Authentication) ، يسهم في حماية حسابات المستخدمين من الاختراق. (ENISA, 2023: 60)

٢-نشر الوعي لدى المستخدمين

يُعد الوعي الرقمي من أهم وسائل الحماية، حيث إن الكثير من انتهاكات البيانات تحدث بسبب قلة معرفة المستخدمين بمخاطر نشر المعلومات الشخصية، لذلك يجب توعية المستخدمين بأهمية حماية بياناتهم، مثل عدم مشاركة المعلومات الحساسة، وضبط إعدادات الخصوصية، والحذر من الروابط المشبوهة.(المركز الوطني للأمن السيبراني، ٢٠٢٤: التوعية الرقمية)

الخاتمة

تناول هذا البحث موضوع الإطار القانوني والمدني لحماية البيانات الشخصية في مواقع التواصل الاجتماعي، وهو من الموضوعات الحديثة التي فرضها التطور التكنولوجي والانتشار الواسع للمنصات الرقمية. وقد تبيّن أن هذه المواقع، رغم فوائدها الكبيرة، تشكل بيئة محفوفة بالمخاطر فيما يتعلق بخصوصية الأفراد، نتيجة اعتمادها على جمع وتحليل كميات ضخمة من البيانات الشخصية.كما أظهر البحث أن الحماية القانونية للبيانات الشخصية تتطلب تكاملًا بين التشريعات الدولية والوطنية، إضافة إلى دور المسؤولية المدنية في تعويض الأضرار الناتجة عن انتهاك البيانات. ومع ذلك، فإن التطبيق العملي لهذه الحماية يواجه تحديات عديدة، خاصة في الدول التي تفتقر إلى تشريعات حديثة ومتخصصة.

النتائج

٦- عدم وجود قانون مستقل وشامل لحماية البيانات الشخصية في العراق، والاكتفاء بنصوص متفرقة .

٧- قصور التشريعات التقليدية في مواكبة التطور الرقمي ومخاطر مواقع التواصل الاجتماعي .

٨- أهمية التشريعات الدولية، خاصة اللائحة العامة لحماية البيانات(GDPR) ، في وضع مبادئ متقدمة لحماية البيانات .

٩- تعدد الجرائم المرتبطة بالبيانات الشخصية، مثل تسريب البيانات والابتزاز الإلكتروني والاستخدام غير المشروع .

١٠- صعوبة التطبيق العملي للقوانين بسبب ضعف الرقابة والطابع العابر للحدود .

١١- دور المسؤولية المدنية في حماية الأفراد من خلال التعويض عن الأضرار .

١٢- الحاجة إلى تكامل بين الحلول القانونية والتقنية والتوعوية لتحقيق حماية فعالة .

التوصيات

١- الإسراع في إصدار قانون عراقي خاص بحماية البيانات الشخصية يواكب التطورات الحديثة .

٢- تطوير التشريعات الحالية لتشمل تنظيم جمع البيانات ومعالجتها ونقلها .

٣- إنشاء جهة مستقلة مختصة بحماية البيانات الشخصية والإشراف على تطبيق القوانين .

٤- تشديد العقوبات على الجرائم المتعلقة بانتهاك البيانات، خاصة في مواقع التواصل الاجتماعي .

٥- تعزيز التعاون الدولي لمواجهة الجرائم الإلكترونية ذات الطابع العابر للحدود .

٦- اعتماد وسائل تقنية حديثة لحماية البيانات، مثل التشفير وأنظمة الأمن السيبراني .

٧- نشر الوعي لدى المستخدمين حول مخاطر مشاركة البيانات الشخصية وكيفية حمايتها.

المصادر

أولا: الكتب والبحوث العربية

١- أحمد، خالد حسن .(2020) .الحق في خصوصية البيانات الشخصية .دار الكتب العربية.

٢- أبوخميس، عبد القادر. (٢٠٢٤). حماية الخصوصية في مواقع التواصل الاجتماعي .مجلة قانونية.
٣- البدري، محمد .(2023) .القانون الرقمي وحماية البيانات .دار النشر العربية.
٤- الشمري، أحمد .(2023) .الخصوصية في العصر الرقمي .دار الفكر القانوني.
٥- العبيدي، أحمد .(2021) .القانون الرقمي والجرائم المعلوماتية .دار الثقافة للنشر.
٦- العاني، محمد .(2019) .الجرائم المعلوماتية في القانون العراقي .بغداد: دار النشر القانونية.
٧- السنهوري، عبد الرزاق .(1952) .الوسيط في شرح القانون المدني .القاهرة: دار النهضة العربية.
٨- الطائي، سعد .(2022) .الإعلام الرقمي والتواصل الاجتماعي .دار الأكاديمية.
٩- عبد الرزاق، علي .(2021) .الإعلام الجديد والتواصل الاجتماعي .دار المعرفة.
١٠- حسين، محمود .(2020) .وسائل التواصل الاجتماعي وتأثيرها .دار الفكر.
١١- داوود، إبراهيم. (٢٠١٧). الحماية القانونية للبيانات الشخصية .مجلة الحقوق.
١٢- سويلم، محمد .(2022) .الحماية القانونية للبيانات الشخصية الإلكترونية .دار النهضة.
١٣- المعداوي، أحمد محمد. (٢٠١٨). حماية الخصوصية المعلوماتية للمستخدم عبر شبكات التواصل الاجتماعي. رسالة ماجستير.
١٤- محمد، وليد خالد. (٢٠٢٥). حماية البيانات الشخصية في البيئة الرقمية .مجلة علمية.

ثانيًا: القوانين والتشريعات

١- دستور جمهورية العراق.(2005) .
٢- قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩.
٣- قانون أصول المحاكمات الجزائية العراقي رقم ٢٣ لسنة ١٩٧١.
٤- قانون حقوق الصحفيين العراقي رقم ٢١ لسنة ٢٠١١.
٥- الاتحاد الأوروبي. (٢٠١٦). اللائحة العامة لحماية البيانات.(GDPR)
٦- مجلس أوروبا. (١٩٨١). اتفاقية حماية الأفراد بشأن المعالجة الآلية للبيانات.
٧- الأمم المتحدة. (١٩٤٨). الإعلان العالمي لحقوق الإنسان.
٨- الأمم المتحدة. (١٩٦٦). العهد الدولي الخاص بالحقوق المدنية والسياسية.

ثالثًا: المصادر والتقارير الدولية

1- Boyd, D., & Ellison, N. (2007). Social network sites: Definition, history, and scholarship. Journal of Computer-Mediated Communication*, 13(1), 210–230.*
2- Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! Business Horizons*, 53(1), 59–68.*
3- European Data Protection Board. (2021). Guidelines on social media users.
4- ENISA. (2023). Threat Landscape Report.
5- OECD. (2013). Privacy Guidelines.
6- OECD. (2022). Digital Environment Report.
7- European Commission. (2022). Data Strategy Report.
8- Europol. (2023). Cybercrime Report.
9- World Economic Forum. (2022). Digital Trust Report.
10- ICO. (2024). Online Tracking Guidance.

رابعًا: تقارير عربية

١- الهيئة الوطنية للأمن السيبراني (السعودية). (٢٠٢٣). دليل حماية البيانات الشخصية.
٢- المركز الوطني للأمن السيبراني (البحرين). (٢٠٢٤). التوعية بالأمن السيبراني.
٣- مكتب الأمم المتحدة المعني بالمخدرات والجريمة. (٢٠٢٢). تقرير الجرائم الإلكترونية