



مجلة أبحاث قانونية-المجلد الثاني عشر-العدد الأول - يونيو 2026م

Legal Research Journal – Volume 12, Issue 1 – June 2026

ISSN: 2959-0434Online

ISSN: 2959-0426Print

DOI: <https://doi.org/10.37375/lrj.v12i1.3143>



الصوابط القانونية لحماية البيانات الشخصية في التعامل الإلكتروني

"دراسة مقارنة"

فاطمة علي محمد النائب

ماجستير قانون خاص، كلية القانون، جامعة سرت

Fatima.altaib@su.edu.ly

تاريخ النشر	تاريخ القبول	تاريخ الاستلام
2026 / 06 / 30م	2026 / 07 / 23م	2026 / 06 / 09م

الملخص:

يُجسد موضوع الصوابط القانونية لحماية البيانات الشخصية في التعامل الإلكتروني، ركيزة أساسية لتحقيق التوازن بين حماية حقوق الأفراد، والاستفادة من التطور التقني، وتتمثل في مُراعاة المبادئ الأساسية لمُعالجة البيانات، كمبدأ المشروعية، وتحديد الغرض، ودقة البيانات، ومبدأ قابليتها للمُعالجة، وتحديد مدة للاحتفاظ بها عقب الانتهاء منها، بالإضافة إلى مُراعاة اتخاذ التدابير التي تكفل حمايتها من المخاطر التي تعترضها، وتكمن أهمية البحث في تزايد الاعتماد على التعامل الإلكتروني، مما يثير صعوبات تتعلق بحماية البيانات الشخصية، وتقوم إشكالية البحث حول: مدى كفاية الصوابط المقررة لحماية البيانات في التشريع الليبي، ومقارنتها بالتشريع السعودي والبحريني والأردني، كونها تشريعات عربية حديثة ناطمة لحماية البيانات بتشريعات خاصة، ويهدف البحث إلى دراسة الإطار القانوني لحماية البيانات الشخصية، وبيان مدى انسجام التشريع الليبي مع آليات الحماية التي وفرتها التشريعات محل المُقارنة، بالاعتماد على المنهج التحليلي والمُقارن، وخلص البحث إلى أن جُل التشريعات اتجهت إلى إرساء مبادئ للحماية، مع التباين فيما بينها من الناحية التنظيمية والتفصيلية، وأوصى البحث بتبني ضابط تشريعي ليبي يكفل حماية مُتكاملة ودقيقة للبيانات الشخصية.

الكلمات المفتاحية: (حماية البيانات، الصوابط القانونية، التعامل الإلكتروني، مُعالجة البيانات)

Legal framework for the protection of personal Data in Electronic Transactions (A comparative study)

Fatima Ali Mohamed altaib

Master of private Law, university of sirte

Fatima.altaib@su.edu.ly

Abstract:

The topic of legal controls for protecting personal data in electronic transactions embodies a fundamental pillar for achieving a balance between protecting individual rights and benefiting from technological development. This is represented in observing the basic principles of data processing, such as the principle of legality, specifying the purpose, data accuracy, the principle of data usability, and determining the retention period after its completion. In addition, it involves taking measures to ensure its protection from the risks it faces. The importance of this research lies in the increasing reliance on electronic transactions, which raises difficulties related to the protection of personal data. The research problem revolves around the adequacy of the controls established for data protection in Libyan legislation, and a comparison with Saudi, Bahraini, and Jordanian legislation, as these are modern Arab legislations that regulate data protection with specific laws. The research aims to study the legal framework for protecting personal data and demonstrate the extent to which Libyan legislation is consistent with the protection mechanisms provided by the legislations under comparison, relying on the analytical and comparative method. The research concluded that most legislations have moved towards establishing protection principles, with differences between them in terms of organization and detail. The research recommended adopting a Libyan legislative control that guarantees comprehensive and precise protection for personal data.

Keywords: Data Protection, Legal Controls, Electronic Transactions, Data processing.

المقدمة:

من أبرز خصائص التعامل الإلكتروني، اعتماده على شبكة الإنترنت التي تسمح بنقل البيانات بين عدة أطراف، وتركز إلى تسخير الذكاء الاصطناعي والتعلم الآلي لتحسين جودة هذا النقل، فعملية نقل البيانات على هذا النحو وبما يصاحبها من مخاطر وتحديات الاختراق أو حتى الاطلاع، تبرز معها الحاجة لتأمين حقوق المتعامل الإلكتروني، وإيجاد آليات وضوابط قانونية تحمي بياناته الشخصية.

وهو الأمر الذي حظي بوافر الاهتمام من التشريعات الناطقة للمعاملات الإلكترونية، فسنت نصوص قانونية تكفل حمايتها، وبالرغم من هذه الحماية التي تكفلها التشريعات، إلا أن الالاف فيها أنها محكومة برهان السباق مع الزمن بالنظر إلى التطور التكنولوجي المتسارع، والذي تتزايد معه مخاطر التعدي على البيانات الشخصية.

أهمية البحث:

تكمن أهمية الموضوع في تزايد استعمال التقنية الرقمية من قبل المؤسسات سواء العامة أو الخاصة، خاصة بتوسع استعمال الذكاء الاصطناعي والتعلم الآلي، كما تبرز أهمية ضوابط حماية البيانات في صونها لخصوصية الأفراد، وتفاذي إساءة استخدام بياناتهم في أغراض غير مشروعة، وتعزيز الثقة في المعاملات الإلكترونية.

إشكالية البحث:

أدى التطور التقني إلى اتساع تداول البيانات الشخصية، فأضحت محلاً لعمليات الجمع والمعالجة، وهو ما أثار العديد من المخاطر التي تمس بحياة الفرد وحقوقه، لذا برزت الحاجة إلى وضع ضوابط قانونية تكفل حمايتها، وفي ضوء ذلك تتمحور إشكالية البحث في التساؤل عن: مدى كفاية الضوابط المقررة لحماية البيانات الشخصية في التشريع الليبي؟ تفرعت عنه التساؤلات التالية:

. ما المقصود بالبيانات الشخصية؟ وماهي خصائصها، وأنواعها؟

. ما هو الإطار القانوني لحماية البيانات الشخصية؟

. ما الحقوق التي يتمتع بها صاحب البيانات الشخصية؟

. ما هي الالتزامات الواجبة على القائم بعملية معالجة البيانات؟

. ما هي أبرز المخاطر التقنية والقانونية التي تعترض عملية المعالجة؟

. ما هو الأساس القانوني للمسؤولية عن انتهاك البيانات الشخصية؟

أهداف البحث:

يهدف البحث إلى تحليل مفهوم البيانات الشخصية، وبيان خصائصها وأنواعها وكيفية معالجتها، فضلاً عن دراسة الإطار القانوني لحماية البيانات الشخصية، وتحديد المخاطر التي تعترض عملية المعالجة وسبل الحد منها، من خلال توضيح الحقوق التي يتمتع بها صاحب البيانات، وإبراز الالتزامات الملقة على عاتق القائم بالمعالجة، بالإضافة إلى تبيان المسؤولية القانونية الناشئة عن انتهاك البيانات الشخصية.

منهج البحث:

لتفصيل موضوع البحث تم الاعتماد على منهجين: المنهج التحليلي، بتحليل النصوص القانونية خاصة في قانون المعاملات الإلكترونية الليبي، رقم (6)، لسنة 2022م، وبيان ما تضمنته من أحكام، وتحليلها في ضوء المبادئ الأساسية لحماية البيانات الشخصية، والمنهج المقارن بين التشريع الليبي وبعض التشريعات العربية، كالسعودية، والبحرين، والأردن دون غيرها؛ لتقاربه معها في الإطار التشريعي، ولتبنيها تشريعاً مستقلاً خاص بحماية البيانات الشخصية، مما يمكن الاستفادة منها في تقدير كفاية التشريع الليبي،

فالغرض من المقارنة بما لا يتجسد في إبراز أوجه الاختلاف والتشابه فيما بينها فقط، بل في استنباط حل مُلائم لتطوير التشريع الليبي، كونها تمثل تجارب عربية حديثة.

خطة البحث:

للإجابة على الأسئلة المطروحة في الإشكالية، وتحقيقاً للأهداف التي نسعى إليها من خلال البحث، قُسم موضوعه في خطة ثنائية وفق مبحثين:

المبحث الأول: ماهية البيانات الشخصية.

المطلب الأول: مفهوم البيانات الشخصية.

المطلب الثاني: ضوابط معالجة البيانات الشخصية.

المبحث الثاني: الإطار القانوني لحماية البيانات الشخصية.

المطلب الأول: مخاطر معالجة البيانات الشخصية وآلية الحد منها.

المطلب الثاني: المسؤولية القانونية الناشئة عن انتهاك البيانات الشخصية.

الخاتمة: نتائج وتوصيات

المبحث الأول

ماهية البيانات الشخصية

للقوف على ماهية البيانات الشخصية للتعامل الإلكتروني، لا بد من بيان مفهومها في المطلب الأول، وضوابط معالجتها في المطلب الثاني:

المطلب الأول

مفهوم البيانات الشخصية

باعتبار أن مصطلح البيانات الشخصية قد أضحى مُتداولاً بكثرة، ويكتسب أهمية خاصة في المعاملات الإلكترونية، فإنه لا بد من أن نعرض موضوع هذا المطلب بتقسيمه إلى فرعين: الأول يتناول تعريف البيانات الشخصية، والثاني يُعنى ببيان نطاقها وتمييزها عن غيرها من البيانات، وفقاً لما يلي:

الفرع الأول

تعريف البيانات الشخصية

سنتناول من خلال هذا الفرع المقصود بالبيانات الشخصية، ثم نتطرق لبيان خصائصها، أنواعها، طبيعتها القانونية، ودورها في تطبيقات الذكاء الاصطناعي، وفقاً للفقرات الآتية:

أولاً: المقصود بالبيانات الشخصية:

يُعد إيضاح المقصود بالبيانات الشخصية خطوة جوهرية لمعرفة نطاق حمايتها، ولغرض البحث نتناول تعريفها وفق التشريع الليبي، والسعودي، والأردني، والبحريني، لإبراز أوجه المقارنة فيما بين هذه التشريعات:

1: في التشريع الليبي:

بالرغم من عدم وجود تشريع خاص بالبيانات الشخصية، نجد أن القانون رقم 2022/6م، بشأن المعاملات الإلكترونية الليبي، لم يتناول تعريف البيانات الشخصية، وإنما عرّف البيانات الإلكترونية وفق المادة (7/1) بأنها: "بيانات ومعلومات ذات خصائص

إلكترونية في شكل نصوص أو رموز أو أصوات أو رسوم أو صور أو برامج الحاسوب أو غيرها من أشكال تعتمد على التمثيل الإلكتروني".

بينما أورد المنشور رقم (18) لسنة 2025م، بشأن نظام حماية البيانات واللائحة التنظيمية للقطاع المصرفي، تعريفاً للبيانات الشخصية في المادة الأولى منه بأنها: "كل بيان من شأنه أن يؤدي إلى معرفة الفرد على وجه التحديد، أو يجعل التعرف عليه ممكناً بصفة مباشرة، أو غير مباشرة، مثل: الاسم، الرقم الوطني، رقم ورقة العائلة، رقم قيد العائلة، رقم الهاتف، العنوان، رقم الهوية الشخصية، الصور الشخصية، صور المستندات الشخصية، البريد الإلكتروني، الإقامة للأجانب وغير ذلك من البيانات ذات الطابع الشخصي". ويرتبط ذلك بالقواعد العامة، حيث نظم القانون المدني الليبي أهم عناصر الشخص الطبيعي كالاسم في المادة (38)، وأقر حمايته من الانتحال والتعدي وفق المادة (51)، ومنح الحجية القانونية للسجلات الرسمية على ما تم تدوينه فيها من بيانات وذلك وفق المادة (30)، وبذلك يُعد مفهوم البيانات الشخصية في المعاملات الإلكترونية تطوراً لهذه القواعد، ويتضمن كل بيان يُعرف ويُميز الشخص المُستخدم في البيئة الرقمية، مما يقتضي توفير آلية قانونية تُلاءم طبيعتها.

2: في التشريع السعودي:

عرّف البيانات الشخصية بأنها: "كل بيان - مهما كان مصدره أو شكله - من شأنه أن يؤدي إلى معرفة الفرد على وجه التحديد، أو يجعل التعرف عليه ممكناً بصفة مباشرة أو غير مباشرة، ومن ذلك: الاسم، ورقم الهوية الشخصية، والعناوين، وأرقام التواصل، وأرقام الرخص والسجلات والممتلكات الشخصية، وأرقام الحسابات البنكية والبطاقات الائتمانية، وصور الفرد الثابتة أو المتحركة، وغير ذلك من البيانات ذات الطابع الشخصي"، وذلك وفق المادة (4/1) من نظام حماية البيانات الشخصية الصادر بالمرسوم الملكي رقم (م/19) لسنة 1443هـ، والمعدل بالمرسوم الملكي رقم (م/148) لسنة 1444هـ.

3: في التشريع الأردني:

عرّف البيانات الشخصية بأنها: "أي بيانات أو معلومات تتعلق بشخص طبيعي ومن شأنها التعريف به بطريقة مباشرة أو غير مباشرة مهما كان مصدرها أو شكلها بما في ذلك البيانات المتعلقة بشخصه أو وضعه العائلي أو أماكن تواجده"، بموجب المادة (2) من قانون حماية البيانات الشخصية الأردني، رقم 24 لسنة 2023م.

4: في التشريع البحريني:

عرّف البيانات الشخصية بأنها: "أية معلومات في أية صورة تخص فرداً معرّفاً، أو قابلاً بطريق مباشر أو غير مباشر لأن يُعرف، وذلك بوجه خاص من خلال هويته الشخصية أو صفة أو أكثر من صفاته الشكلية أو الفسيولوجية أو الذهنية أو الثقافية أو الاقتصادية أو هويته الاجتماعية..."، وفق المادة (1) من قانون حماية البيانات البحريني، رقم 30 لسنة 2018م. مما سبق وبعرض التعريفات التي قُدمت للبيانات الشخصية، يتجلى لنا أن جُل التشريعات العربية السابقة تقتضي تحديد البيانات أو المعلومات مع تفاوت مصطلحاتها لشخصاً طبيعياً سواء بالتحديد المباشر أو غير المباشر، إلا أن التشريعات المُقارنة قد أجادت في تقديم تعريف شامل، ومُفصل للبيانات الشخصية، في حين نجد التشريع الليبي اقتصر في المنشور رقم 2025/18م، على البيانات المصرفية بهدف تنظيمها داخل المصارف الليبية، ولم يأت تعريفها في تشريع خاص بتنظيمها، وعُرض في البحث بغية المقارنة بتعريفات التشريعات الأخرى.

لذا يمكن تقديم تعريف للبيانات الشخصية بأنها: كل بيان يُمكن من معرفة هوية الشخص بطريقة مباشرة أو غير مباشرة، ويدخل في نطاق الحماية القانونية وفقاً لما نُص عليه في القانون رقم 2022/6م، بشأن المعاملات الإلكترونية الليبي.

ثانياً: خصائص البيانات الشخصية:

لأي مصطلح خصائص تميزه عن غيره، ومن خلال هذه الفقرة نعرض خصائص البيانات الشخصية بهدف إيضاح معناها، وإبراز دورها في حماية حق الفرد، ولضمان استخدامها بشكل آمن، ومن أبرز خصائصها أنها:

1: حقوق لصيقة بالشخص الطبيعي:

فهي حقوق ترتبط بالشخص الطبيعي ومن حق صاحبها وحده، كحقه في أن يحتفظ بأفكاره وسريته علاقته، فهذه الحقوق في الواقع لا تُتاح للأشخاص الاعتبارية. (سويلم، 2024م، صفحة 1889)

2: تسمح بالتعرف على الشخص الطبيعي:

تُمكن من التعرف على الشخص بصورة مباشرة، كبيانات حالته المدنية من اسم، وجنس، وعنوان، وتاريخ، ومواصفات جسمانية من صورة، وصوت، وبصمة يد، وجنسيته وغيرها، وقد تُمكن من التعرف على الشخص بطريقة غير مباشرة، وذلك من خلال الوظيفة والمواصفات. (الطيب، 2024م، صفحة 15)

3: عدم قابلية البيانات للتصرف فيها:

يرجع ذلك لتكوينها المادي، فهي تدل على شخص محدد دون سواه، كالبصمة التي تختلف من شخص لآخر، فأى إجراء مشابه لا يعتد به القانون ويكون باطلاً. (خالد، 2023م، صفحة 233)

4: عدم قابليتها للتقادم:

لأنها تمس الجانب المعنوي للشخص لا الذمة المالية له، لذا فهي لا تدخل في دائرة التعامل، ولا تخضع للتقادم، ويجب التمييز بين عدم خضوع البيانات في ذاتها للتقادم، وبين دعوى التعويض في حال حصل انتهاك أو اعتداء عليها، فهذه الدعوى بعد أن يحكم فيها لصالح من وقع عليه الاعتداء، تنشئ له حقاً مالياً قبل الشخص المعتدي، فهذا الحق يكون خاضعاً للتقادم. (عثمان أ.، 2023م، صفحة 300)

5: نسبية حمايتها:

في بعض الأحيان، قد يحدث تعرض لبيان منها دون أن يعد ذلك اعتداء على بيانات شخصية، متى ما استوجبت المصلحة العامة ذلك، كما قد لا يثير المساس بها أي مشكلة كحالته الاجتماعية، ومعتقداته الدينية، وحالته الصحية بشرط موافقته الصريحة، فالتعرف عليها حينها لا يُعد اعتداء على بيان شخصي. (عثمان أ.، 2023م، صفحة 302)

ثالثاً: أنواع البيانات الشخصية:

يستوجب تحديد ماهية البيانات الشخصية بيان أنواعها؛ كي لا يندرج ضمن مصطلحها ما لا يعد منها، وهي نوعان: بيانات بحسب طبيعتها، وبيانات بحسب أهميتها:

1: بيانات شخصية بحسب طبيعتها: بعضها متعلق بذات الشخص، والآخر بممتلكاته، وهي كالتالي:

أ: بيانات متعلقة بذات الشخص: تتمثل في اسم الشخص، وهويته، ولقبه، صورته، وصوته، وبياناته المهنية كاسم الوظيفة، ومهامها، وبريد الموظف، بالإضافة إلى بياناته العلمية كالدرجة العلمية، بيانات حسابه البنكي وبطاقته الائتمانية.

ب: بيانات متعلقة بممتلكاته: كرقم هاتفه الشخصي سواء المحمول، أو هاتف المنزل. (إمام، 2024م، صفحة 18)

2: بيانات شخصية بحسب أهميتها: تنقسم إلى بيانات عادية، وبيانات حساسة:

أ: البيانات الشخصية العادية: تتمثل في بيانات الفرد والتي لا مانع من اطلاع الغير عليها، ولا يشكل اطلاعه تعدياً على خصوصيتها، ومتداولة بشكل يومي كلوحة السيارة.

ب: **البيانات الشخصية الحساسة:** تتمثل في بيانات الشخص التي تفصح عن صحته العقلية، أو البدنية، أو بياناته المالية، أو حالته الأمنية، أو معتقداته الدينية، فيحظر التعامل عليها إلا بالموافقة الصريحة والكتابية من الشخص، وبموجب ترخيص من مركز حماية البيانات الشخصية. (رجب، الحماية القانونية للبيانات الشخصية في عصر التكنولوجيا الرقمية، 2024م، صفحة 424)

رابعاً: الطبيعة القانونية للبيانات الشخصية:

اختلف الفقه القانوني بشأن الطبيعة القانونية للبيانات الشخصية، فيرى البعض أنها من الحقوق اللصيقة بحقوق الشخص (سلطان، 2024م، صفحة 5)، وفقاً لما نصت عليه المادة (12) من الإعلان العالمي لحقوق الإنسان على أنه: " لا يجوز تعريض أحد لتدخل تعسفي في حياته الخاصة أو شؤون أسرته أو مسكنه أو مراسلاته ولا لحملات تمس شرفه وسمعته، ولكل شخص الحق في أن يحمي القانون من مثل ذلك التدخل، أو تلك الحملات".

وإلى جانبه، هناك من يرى بأنها حق ملكية باعتبار أن الشخص بإمكانه تعديلها، وحذفها، وإلغائها، وبناءً على ذلك تكون محللاً للتعامل، ولأهميتها التجارية والاقتصادية يمكن لكل من صاحبها، والمتحكم أو المعالج، الاستفادة منها بمقتضى الاتفاق فيما بينهم، وهو ما دفع التشريعات إلى وضع أحكام خاصة ناظمة لحمايتها، بما يضمن التوازن بين مصلحة صاحبها والمهني في الاستفادة منها. (مهدي، 2024م، صفحة 325)

ختاماً وبعرض الآراء الفقهية فيما يتعلق بالطبيعة القانونية للبيانات الشخصية، نرجح الرأي الأول باعتبارها حق شخصي، وأن الهدف من حمايتها هو المحافظة على كرامة وخصوصية الفرد، وهو ما أقرته أغلب التشريعات العربية الحديثة.

خامساً: دور البيانات الشخصية في تطبيقات الذكاء الاصطناعي:

للبيانات الشخصية دورٌ في مجال الذكاء الاصطناعي، بدونها لا يوجد ذكاء، ولا تعلم، ولا ابتكار، دقتها وجودتها تؤدي لوصول أنظمة الذكاء إلى أصح النتائج، وهي على أشكال متنوعة بحسب منشئها سواء كان آلياً أو بشرياً، ولكل منها خصائصه المميزة، فالبيانات البشرية لها قيمة في مجال الذكاء الاصطناعي؛ لتلبيتها لمتطلبات خاصة على خلاف البيانات المعدة آلياً، إلا أنها مكلفة وتحتاج إلى وقت لمعالجتها وجمعها، وعرضة للخطأ، وتتطلب حماية قانونية تكفل المحافظة على خصوصيتها. (Devoteam، د.ت)

الفرع الثاني

نطاق حماية البيانات الشخصية وتمييزها عن غيرها من البيانات

يُعد موضوع هذا الفرع من المسائل الجوهرية في الدراسات التقنية والقانونية؛ إذ أدى اتساع نطاق تداول البيانات وتنوع أوجه استخدامها إلى صعوبة التمييز بين ما يُعدّ بياناً ذا طابع شخصي يستوجب حماية قانونية خاصة، وبين ما لا يرتبط، بصورة مباشرة أو غير مباشرة، بشخص طبيعي. ويُعدّ تمييز البيانات الشخصية عن غيرها مدخلاً أساسياً لفهم نطاق الحماية المقررة لها، وتحديد حدود المسؤولية القانونية الناشئة عن الإفصاح عنها أو استخدامها أو جمعها. وعليه، نقسم موضوع هذا الفرع إلى فقرتين:

أولاً: نطاق حماية البيانات الشخصية:

1: من حيث الأشخاص:

تقتصر أغلب التشريعات المنظمة لحماية البيانات الحماية على الشخص الطبيعي، أما بيانات الشخص الاعتباري فتخرج عن نطاقها، إلا أنها قد تدخل إذا كانت مُرتبطة بأشخاص طبيعية مُحددة الهوية، أو بالإمكان تحديدها، إضافة إلى بيانات الطفل فهي محمية لكونه شخصاً طبيعياً، وبعض من التشريعات استوجبت موافقة ولي أمره عندما يكون غير بالغ لسن الرشد. (اللدان، 2025م، صفحة 17)

2: من حيث الموضوع:

تدخل في نطاق الحماية البيانات الشخصية سواء عُولجت داخل أو خارج البلد، وتُحمى من أغراض الترويج والدعاية والتسويق حفاظاً على سرّيتها، ويستبعد من نطاق الحماية بيانات الشخص الطبيعي الذي يقوم بمعالجتها بنفسه لغرض شخصي باعتباره مسؤولاً عنها، ولا تتطلب قانوناً ناظماً لها، وكذلك لا تدخل في نطاق الحماية البيانات المُعالجة من قبل الجهات القضائية والأمنية، باعتبار أن ذلك بغرض حفظ الأمن القومي في الدولة، كما يخرج عن نطاقها البيانات المُعالجة من جهة حكومية. (اللحدان، 2025م، صفحة 21)

ثانياً: تمييز البيانات الشخصية عن غيرها من البيانات:**1: التمييز بين البيانات الشخصية والبيانات الحساسة:**

تختلف البيانات الشخصية فيما بينها، لذا يبرز منها البيانات الحساسة والتي تقتضي تشديد الحماية، فيمكن اعتبار بعض البيانات الشخصية غير مُضرة، بينما يكون البعض الآخر مُضراً بسمعة الشخص، كالمعلقة بإصابته بمرض خطير، ولقاضي الموضوع سلطة تقدير مدى اعتبار البيانات قد تضر بصاحبها أكثر من غيرها. (سلطان، 2024م، صفحة 1103)

ويمكن الاختلاف بين البيانات الشخصية والبيانات الحساسة، في أن البيانات الشخصية يُمكن جمعها ومعالجتها آلياً، والأمر على خلافه بالنسبة للبيانات الحساسة التي لا يُمكن جمعها ومعالجتها آلياً. (راشد، 2019م، صفحة 221)

وتتسم البيانات الحساسة بتشديد حمايتها؛ لخصوصية دلالتها على شخصية الفرد، فلا يتم جمعها إلا في بعض الحالات المحددة قانوناً، بحسب فائدة المجتمع من جهة والفرد من جهة أخرى. (جبور، 2018م، صفحة 82)

فيُمكن أن يترتب على معالجة البيانات الحساسة ضرراً بالغاً إذا ما قورنت بالبيانات الشخصية العادية، فقد تُمكن البيانات الحساسة من كشف أصل الشخص، وتوجهاته ومعتقداته، وحالته الصحية، وهو ما يُمثل خطورة على خصوصيته. (لشهب، 2025م، صفحة 302)

2: التمييز بين البيانات الشخصية والبيانات المستعارة:

البيانات الشخصية تدخل في نطاق الحماية القانونية في حال إمكانية تحديد هوية الشخص بطريقة مباشرة، أو غير مباشرة، وبموجب القوانين الناظمة لها، أما البيانات المستعارة فهي بيانات لا تكشف هوية الشخص، ولا تدخل في نطاق الحماية إلا إذا أمكن ربطها بمعلومات أخرى تُوصل للتعرف على الشخص الطبيعي. (اللحدان، 2025م، صفحة 16)

3: التمييز بين البيانات الشخصية والبيانات المجهولة:

البيانات المجهولة: "هي البيانات التي لا تتعلق بشخص طبيعي محدد الهوية أو يمكن تحديد هويته"، وتخرج عن نطاق حماية البيانات الشخصية، على خلاف البيانات الشخصية التي تُمكن من تحديد هوية الشخص. (اللحدان، 2025م، صفحة 16)

المطلب الثاني**ضوابط معالجة البيانات الشخصية**

لأهمية البيانات الشخصية وارتباطها الوثيق بحق الفرد وخصوصيته، لذا فمن الضروري أن تخضع لأحكام وضوابط تُنظم عملية مُعالجتها، ضماناً لعدم التعدي عليها، لذا سنعرض من خلال هذا المطلب ضوابط المُعالجة ببيان مبادئها الأساسية في الفرع الأول، وشروط مشروعيتها في الفرع الثاني:

الفرع الأول**المبادئ الأساسية لمُعالجة البيانات الشخصية**

تحكم عملية معالجة البيانات جملة من المبادئ الأساسية لضمان حمايتها، وتتجسد هذه المبادئ فيما يلي:

أولاً: مشروعية المعالجة:

يكون ذلك بإعلام الشخص المعني بوجود عملية معالجة لبياناته، وإجراءاتها والهدف منها قبل البدء فيها، وتكون المعالجة غير مشروعة في حال تضليل الشخص، أو خداعة للحصول على بياناته. (الحروقي، 2023م، صفحة 1538)

ثانياً: تحديد الغرض منها:

لا بد أن يكون الغرض من تجميع البيانات مُحددًا، وواضحًا، ومشروعًا، فلا يجوز مُعالجتها على نحو يُنافي الغرض منها. (مشعل، 2017م، صفحة 37)

ثالثاً: تحديد مدة الاحتفاظ بالبيانات:

مُعالج البيانات مُكلف بمراجعة البيانات المخزنة، بحيث يُلغى كل البيانات التي تحقق الهدف من جمعها، ويفترض أن يُحدد المُعالج مدة لحفظها، ويكون ذلك على ضوء طبيعتها والغاية من مُعالجتها، فعليه اتلافها، أو محوها، أو تشفيرها عند تحقق ذلك. (جبور، 2018م، صفحة 125)

رابعاً: دقة البيانات:

تتطلب مُعالجة البيانات دقتها وعدم حفظها بشكل عشوائي، فيجب حديد صاحبها لتمكينه من مُزاولة حقوقه عليها، كحق الدخول أو التعديل. (عاشوري، 2025م، صفحة 145)

والالتزام بضمان دقتها يقع على المُتحكم، فيقوم بإشعار صاحبها عند البدء في مُعالجتها، وإبلاغه بأي تغيير فيها لا يحول دون مساءلته عن عدم تحديث البيانات. (مهدي، 2024م، صفحة 328)

خامساً: قابلية البيانات للمُعالجة:

يتعين على المُعالج تجنب مُعالجة البيانات المحظورة، كالبيانات الخاصة بالأطفال إلا بموافقة الأب، كذلك استخدام البيانات في أغراض إعلانية، بالإضافة إلى حظر مُعالجة البيانات الحساسة. (مدبولي، 2022م، صفحة 132)

واستثناءً إلى نص المادة (76) من القانون رقم 2022/6م، بشأن المعاملات الإلكترونية الليبي، نجد أن المُشرع نص فيه صراحة على مبدأ واحد من مبادئ المُعالجة وهو مبدأ تحديد الغرض، وضمنيًا على مبدأ دقة البيانات من خلال الإشارة إلى "طبيعة البيانات"، ولم يتضمن النص الصريح على مبدأ المشروعية، ولا مبدأ تحديد مدة الاحتفاظ بالبيانات، كما لم يتضمن النص على مبدأ قابليتها للمُعالجة.

أما التشريعات محل المُقارنة، فقد ورد فيها نصوص صريحة تحوي هذه المبادئ الأساسية:

ففي التشريع السعودي تم النص صراحة على مبدأ مشروعية المُعالجة، وتحديد الغرض وعدم مُعارضة المُعالجة له، وفق المادة (11/1)، وأوجب المُشرع السعودي على جهة التحكم ألا تُعالج البيانات دون التحقق من دقتها واكتمالها وحدائتها وارتباطها بالغرض، وذلك وفق المادة (14)، كما أجاز المُشرع السعودي مُعالجة البيانات الشخصية لأغراض تسويقية، واستثنى البيانات الحساسة، وفق المادة (26) من نظام حماية البيانات الشخصية.

وفي التشريع البحريني، ورد النص الصريح على مبدأ المشروعية، وتحديد الغرض وفق المادة (2/3)، ونص صراحة وفق المادة (4/3) على مبدأ الدقة، ووفق المادة (5/3) نص على مبدأ تحديد مدة الاحتفاظ بالبيانات، وعلى مبدأ قابليتها للمُعالجة في المادة (5) من قانون حماية البيانات الشخصية، كما نص المُشرع الأردني على تلك المبادئ بشكل صريح، فنص على المشروعية وفق المادة (7/أ)، وتحديد الغرض وفق المادة (7/ب)، والدقة وفق المادة (7/د)، وتحديد مدة الاحتفاظ وقابليتها للمُعالجة وفق المادة (6/ب) من قانون حماية البيانات الشخصية.

نتائج المقارنة: قصور النص الليبي الصريح على مبدأ واحد، وهو مبدأ تحديد الغرض من المعالجة، مما يُفيد بأن النص يُمثل تنظيمًا إجرائيًا جزئيًا، ولا يُمثل منظومة شاملة لحماية البيانات، مما يقتضي ضرورة تعزيز التنظيم التشريعي لجعل الحماية أكثر تنظيمًا وشمولًا.

الفرع الثاني

الشروط القانونية لمشروعية معالجة البيانات الشخصية

تُجسد الشروط القانونية لمشروعية معالجة البيانات الشخصية الضوابط التي تكفل مشروعية المعالجة في البيئة الرقمية، وتُعدّ متطلباتٍ أساسية لا بد من توافرها قبل مباشرة عملية المعالجة، ويتربط على مخالفتها عدم مشروعية المعالجة، وما قد ينشأ عن ذلك من مساءلة الجهة القائمة عليها. وتتمثل هذه الشروط فيما يلي:

أولاً: التصريح بالموافقة:

تناولته المادة (73) من القانون رقم 2022/6م، بشأن المعاملات الإلكترونية الليبي، بما تضمنته في نصها بأنه: لا يجوز لأي جهة عامة أو لأي مُقدم خدمات تصديق أن يجمع البيانات إلا بموافقة صريحة من صاحبها، وذلك لغرض إصدار شهادة أو الحفاظ عليها، كذلك لا يجوز جمعها، أو مُعالجتها، أو استخدامها لأي غرض آخر دون الموافقة الصريحة من صاحبها.

ثانيًا: الترخيص بالمعالجة:

إذا وجدت الجهة المسؤولة إن عملية المعالجة تُشكل تهديدًا لحقوق الفرد الأساسية، فإنها تُخضع عملية المعالجة لنظام الترخيص المسبق. (عيوني، 2025م، صفحة 738)

وبالرجوع إلى قانون المعاملات الإلكترونية الليبي، نجد المادة (29) التي تنص على أنه: "يجب على كل شخص طبيعي أو اعتباري يرغب في مزولة نشاط مقدم خدمات التصديق الحصول على التراخيص اللازمة من الهيئة قبل البدء في ممارسة النشاط". وفي التشريع السعودي، نجد نص المادة (5) من نظام الحماية، وبموجبه صرّح المُشرع بجعل المعالجة غير مشروعة إلا بموافقة صاحب البيانات، وتُحدد لوائح النظام شروط الموافقة، ومتى تكون صريحة، وشروط الحصول على الموافقة من الولي الشرعي في حال كان صاحبها ناقص أو عديم الأهلية، كذلك نص المادة (3/33) من نظام حماية البيانات، وبموجبه صرّح المُشرع السعودي بمنح الجهة المختصة صلاحية الترخيص للجهات القائمة على التدقيق، أو الفحص لأنشطة معالجة البيانات، بحسب طبيعة النشاط، ووفق أحكام تُحددها اللوائح، كما منح الجهة المختصة وضع مُتطلبات وشروط الترخيص، وأولاهها المُشرع السعودي تحديد الأدوات، والآليات المناسبة لمُتابعة التزام الجهات التي في خارج المملكة بالتزاماتها، وتحديد الإجراءات المتعلقة بإنفاذ أحكام النظام واللوائح خارج المملكة العربية السعودية.

وفيما يتعلق بالتشريع البحريني، نجد نص المادة (14) من قانون حماية البيانات، في فقرتها الأولى والتي بموجبها صرّح المُشرع بضرورة أن يُخطر مُدير البيانات الهيئة قبل البدء في المعالجة التي تتم آليًا كليًا أو جزئيًا، كما حدد في الفقرة الثانية ما يجب أن يتضمنه الإخطار بشكل مُفصل، وبينت الفقرة الثالثة متى يكون الإخطار مُبسط، وما يجب أن يتضمنه، كما أوجبت الفقرة السادسة على مُدير البيانات أن يُخطر الهيئة بأي تغيير في المعلومات التي سبق له إخطارها بها، خلال 30 يومًا من حدوث التغيير.

كما اعتمد المُشرع البحريني في المادة (15) من قانون الحماية على التصريح المُسبق كشرط لمشروعية المعالجة، وحدد المُعالجات المحظورة إلا بتصريح كتابي من الهيئة، نذكر منها المُعالجة الآلية للبيانات الحساسة، وأوضح في الفقرة الثانية من ذات المادة، ضرورة أن يتضمن التصريح نفس البيانات التي يجب أن يتضمنها الإخطار، والفقرة الثالثة أوجبت على الهيئة البت في طلب التصريح، وإخطار صاحبه بالنتيجة خلال 30 يومًا من تقديمه، وإلا عُدد رفضًا ضمنيًا.

وفي التشريع الأردني، نجد المادة (5) من قانون حماية البيانات، وبموجبها أكد المُشرع اعتماده على التصريح بالموافقة كشرط لمشروعية المعالجة، واشترط أن تكون صريحة ومُحددة، كما أوضح الحالات التي لا يعتد فيها بالموافقة المسبقة، وهي حالة ما إذا صدرت بناءً

على معلومات غير صحيحة، أو ممارسة الخداع والتضليل، وحالة إذا تم تغيير طبيعة المعالجة دون الحصول على الموافقة بذلك، وفيما يتعلق بالاعتماد على الترخيص كشرط للمعالجة، نجد النص الصريح في المادة (17/ج) من قانون حماية البيانات الأردني. نتائج المقارنة: أن المشرع الليبي يتفق مع التشريعات المقارنة في اعتماده على التصريح بالموافقة كشرط أساسي لمشروعية المعالجة، ونص على ذلك صراحة بموجب المادة (73) من قانون المعاملات الإلكترونية، بينما لم ينص على نظام الترخيص بالمعالجة، واقتصر النص على الترخيص بمزاولة نشاط مقدم خدمات التصديق، وهو ما يُفيد بالتنظيم الجزئي لشروط المعالجة، والأمر على خلافه بالنسبة للتشريعات المقارنة التي جاءت بتنظيم دقيق ومحدد، يكفل حماية فعالة للبيانات الشخصية.

المبحث الثاني

الإطار القانوني لحماية البيانات الشخصية

في ضوء التطور التقني، قامت الحاجة إلى وضع إطار قانوني يكفل حماية البيانات الشخصية من مخاطر مُعالجتها، ويركز على المسؤولية القانونية الناشئة عن إساءة استخدامها، لضمان الأمن القانوني في البيئة الرقمية، وهو ما نعرضه في المطلبين التاليين:

المطلب الأول

مخاطر مُعالجة البيانات الشخصية وآلية الحد منها

في ظل تزايد استعمال الذكاء الاصطناعي والتعلم الآلي في التعامل الإلكتروني، كالكشف عن الاحتيال، والتأكد من الهوية وخدمة العملاء الآلية، فإن عملية مُعالجة البيانات بما تتضمنه من جمع وتخزين ومشاركة، أصبحت عرضة لمخاطر قد تصل إلى انتهاك خصوصية الفرد، أو استغلال بياناته بطرق غير مشروع، مما يستدعي تعزيز الإطار القانوني لحماية البيانات، وتنوع هذه المخاطر إلى المخاطر التقنية والمخاطر القانونية، وفهماها يُمثل مُرتكزاً أساسياً من أجل التوعية الرقمية، واعتماد ضوابط تحد من إمكانية التعرض للبيانات، وهو ما نسعى لإيضاحه وفقاً لما يلي:

الفرع الأول

مخاطر مُعالجة البيانات الشخصية

نعرض من خلال هذا الفرع لبيان المخاطر التقنية لمُعالجة البيانات الشخصية، والتي تستوجب وجود تشريع يقر مسؤولية جهات المُعالجة في حال الإخلال بأمن وحماية البيانات، ويبي ذلك بيان للمخاطر القانونية:

أولاً: المخاطر التقنية لمُعالجة البيانات الشخصية: تتمثل في الاختراق، والتسريب، والقرصنة:

1: الاختراق:

يُعد من أشد المخاطر التي تواجه مُعالجة البيانات، إذ يُمكن للمُخترقين النفاذ غير المشروع إلى الأجهزة الشخصية، بواسطة استغلال ثغرات أمنية، مما يُتيح لهم الوصول للبيانات الشخصية للأفراد، وتكمن خطورته في استخدام الهواتف الذكية لتخزين كم هائل من المُعطيات، وهو ما يجعل اختراقها بمثابة انتهاك للخصوصية. (قاسمي، 2025م، صفحة 129)

إذ يتعين على القائم بمُعالجة البيانات أو جمعها، أن يتخذ كل الاحتياطات اللازمة لتأمينها، ويُمثل الاختراق وسيلة اعتداء حيث يتمكن بواسطته المُخترق من الوصول لمعلومات تخص الفرد وقيامه بالتهديد بنشرها. (بكر، 2019م، صفحة 21)

2: التسريب:

يُشكل ضرراً يُصيب الشخص صاحب البيانات سواء كان ضرراً مادياً، كابتزازه بعدم نشرها مُقابل مبلغ مالي، أو ضرراً معنوياً بانتهاك خصوصيته. (قاسيمي، 2025م، صفحة 130)

3: القرصنة:

نتيجة للتطور التكنولوجي وتزايد استعمال الذكاء الاصطناعي والتعلم الآلي، أضحت البيانات الشخصية الموجودة على شبكات الأنترنت عرضة للوصول غير المصرح به من قبل القراصنة، حيث يقوموا بالدخول غير المشروع على قواعد البيانات، لسرقتها وبيعها لجهة أخرى، أو للاستخدام غير المشروع، كما قد يكون فقد البيانات بسبب خطأ من أحد العاملين بالجهة المالكة لقواعد البيانات. (بكري، 2023م، صفحة 556)

هذه المخاطر المتمثلة في الاختراق والتسريب والقرصنة تلتقي في كونها تمس أمن البيانات، وهو ما جعل التشريعات محل المقارنة تسعى إلى توحيد الأساس القانوني للتصدي لها، باتباع تدابير تكفل حماية للبيانات في عملية المعالجة، فاستناداً إلى قانون المعاملات الإلكترونية الليبي، نجد أن المشرع أقر المحافظة على سرية المعلومات والبيانات التي تحويها الرسالة الإلكترونية وفق المادة (58)، كما نص على طرق لحماية نظم المعلومات نذكر منها: التشفير، الجدران النارية، والبرامج المضادة للفيروسات الإلكترونية، وذلك وفق المادة (59) من قانون المعاملات الإلكترونية الليبي.

كذلك بالرجوع لمنشور مصرف ليبيا المركزي بشأن نظام حماية البيانات، تحديداً في المادة (29) نجده أوجب إبلاغ الجهة المختصة خلال 24 ساعة عند حدوث أي تسريب أو وصول غير مشروع للبيانات.

كما أوجب المشرع السعودي على المُتحكم أن يتخذ التدابير سواء الإدارية، أو التقنية، أو التنظيمية، لحماية البيانات من الوصول غير المشروع أو التسريب، وفق المادة (19) من نظام حماية البيانات السعودي، كذلك ألزم جهة التحكم بأن تُشعر الجهة المختصة عند علمها بحدوث تسريب للبيانات، كما ألزمها بأن تُشعر صاحبها إذا كان من شأن هذا التسريب أن يُرتب ضرراً على بياناته، وفقاً لما تحدده اللوائح، وذلك وفق المادة (20) من نظام حماية البيانات.

وعلى ذات السياق، اتجه المشرع البحريني إلى ضرورة أن يُطبق مُدير البيانات كافة التدابير الفنية والتنظيمية التي تكفل حماية البيانات، وتناول هذه التدابير بشكل مُفصل وفق المادة (8)، كما نص المشرع الأردني على الاختراق في المادة (8/4) فجعل من حقوق صاحب البيانات علمه بأي خرق، أو انتهاك، أو إخلال بسلامة بياناته. نتائج المقارنة: حرص جُل التشريعات على توحيد الأسس القانونية لحماية البيانات الشخصية، وتناولتها بشكل أكثر شمولاً من التشريع الليبي.

ثانياً: المخاطر القانونية لمعالجة البيانات الشخصية:

1: سوء استخدام البيانات:

يُعد استخدام البيانات في غير الأغراض المُخصصة لها من مخاطر مُعالجتها، فيتم جمع بيانات عن الأفراد تتعلق بحياتهم الشخصية والصحية لغرض ما، فإن أُسيئ استخدامها، أو استخدمت لغير ما حُصصت له شكلت ضرراً بصاحبها. (سويلم، 2024م، صفحة 1892)

2: الإفصاح غير المصرح به:

يُشكل الإفصاح عن البيانات الحساسة خطراً متى تم بالمخالفة لنظام حمايتها، وبغرض الإضرار بصاحبها، أو نيل نفع من ورائه. (التركي، 2025م، صفحة 1129)

بالرجوع إلى التشريع الليبي، نجده أكد على ضرورة موافقة المعني على عملية الجمع، أو المعالجة، أو الاستخدام، أو الإفصاح، وفق المادة (73) من قانون المعاملات الإلكترونية، كما حدد المشرع السعودي الحالات التي يجوز فيها الإفصاح وفق المادة (15)، وحدد أيضاً الحالات التي لا يجوز فيها الإفصاح عنها وفق المادة (16) وبشكل مفصل ودقيق. وإلى جانب ذلك، نجد المشرع البحريني يُحظر الإفصاح إلا بموافقة صاحب البيانات، أو من الجهة المخولة، أو أمر قضائي وذلك وفق المادة (1/9)، كما نجد في التشريع الأردني المادة (2/14)، والتي بموجبها صرح المشرع بضرورة علم صاحب البيانات بالغرض الذي ستستخدم البيانات من أجله. نتائج المقارنة: توافق التشريعات محل المقارنة مع التشريع الليبي في عدم جواز الإفصاح عن البيانات دون مُبرر مقبول قانوناً، أو بموافقة صاحبها، إلا أن التشريعات كانت أكثر تنظيمًا لذلك.

الفرع الثاني

حقوق والتزامات أطراف العلاقة بالبيانات الشخصية كآلية للحد من المخاطر

تعد البيانات الشخصية عنصراً جوهرياً لضمان التوازن بين حماية الفرد، وبين الاستفادة من بياناته بطرق مشروعة، لذا يترتب على معالجة البيانات جملة من الحقوق والتزامات لصاحبها والمتحكم أو المُعالج، وفي نطاق هذا الفرع نعرض حقوق صاحب البيانات، ويليهما عرض للالتزامات المُلقاة على عاتق مُعالج البيانات، وفقاً لما يلي:

أولاً: حقوق صاحب البيانات:

لا شك في أن الفرد الذي تتم معالجة بياناته هو المعني بالحماية القانونية، والتي تُعد مُركباً أساسياً في استقرار الأمن وبث الاطمئنان في التعامل الإلكتروني، لذا نعرض لأهم حقوق صاحب البيانات:

1: الموافقة الصريحة على معالجة بياناته:

لا يُمكن معالجة البيانات إلا بموافقة صريحة من الشخص المعني، في حال كان رشيداً ومُتمتعاً بالأهلية، أما إذا كان ناقص الأهلية، فإنه لا تتم معالجة بياناته إلا بموافقة مُمثله، ويستثنى من ذلك حالة ما إذا كانت المعالجة ضرورية لاحترام التزام قانوني يخضع له الشخص المعني، أو المسؤول عن المعالجة، أو حفاظاً للصالح العام. (صامت، 2020م، صفحة 475) وتُعد الموافقة الصريحة من صاحب البيانات على مُعالجتها شرطاً ضرورياً في التعامل الإلكتروني، فاستوجب المشرع الليبي عدم جمع، أو معالجة، أو استخدام البيانات لأي غرض دون موافقة صريحة من صاحبها، وأوضح الحالات التي تكون فيها المعالجة مشروعة دون مُوافقتها وهي: أن تكون لغرض منع أو كشف جريمة، أو مُصرح بها بموجب قانون، أو قرار من المحكمة، أو لتحصيل رسوم أو ضريبة، أو لحماية مصلحة حيوية للشخص الذي جُمعت عنه، وذلك بموجب المواد (74/73) من قانون المعاملات الإلكترونية الليبي.

وأقر المشرع السعودي ضرورة موافقة صاحب البيانات على مُعالجتها، ومنحه الحق في سحبها في أي وقت، ووفق ضوابط تُحددها اللوائح وتُبين شروطها، والأحوال التي يجب أن تكون فيها الموافقة صريحة، وذلك بموجب المادة (1/5) من نظام حماية البيانات الشخصية.

كما أكد المشرع البحريني على ضرورة موافقة صاحب البيانات على مُعالجتها، وأُشترط أن تكون مُوافقتها صريحة ومكتوبة، وأن تكون صادرة عن شخص كامل الأهلية، وفي حال كان عديم أو ناقص الأهلية يُعتمد بموافقة الولي، أو الوصي، أو القيم، ومنح صاحبها مُكنة سحب موافقته على المعالجة في أي وقت، بموجب الإجراءات التي يُحددها مجلس الإدارة، وذلك وفق المادة (24) من قانون حماية البيانات البحريني.

وإلى جانبه، أشرت المشرع الأردني موافقة صاحب البيانات على معالجتها، وأن تكون موافقة صريحة، وموثقة خطياً، أو إلكترونياً، وأوضح المشرع أنه لا يُعتدّ بالموافقة إذا كان صاحب البيانات قد تعرّض للخداع أو التضليل، مما دفعه إلى إبدائها، وكذلك إذا جرى تغيير الغرض من معالجتها أو نوع البيانات محل المعالجة دون الحصول على موافقته. كما بيّن المشرع الأردني الحالات التي تكون فيها معالجة البيانات الشخصية مشروعة دون حاجة إلى الحصول على موافقة صاحب البيانات، وهي أن تكون ضرورية لأغراض طبية، أو لتقديم الرعاية الصحية، أو لحماية مصلحته الحيوية، أو لمنع جريمة أو كشفها، أو في حال كانت مُصرح بها بموجب أي من التشريعات، كذلك متى كانت ضرورية للبحث العلمي، أو لمتطلبات الأمن الوطني، وذلك وفق المواد (6/5/4) من قانون حماية البيانات الأردني.

نتائج المقارنة: أن المشرع الليبي أخذ كغيره من التشريعات محل المقارنة، بضرورة موافقة صاحب البيانات على المعالجة، إلا أن مسألة تنظيم الموافقة مختلفة فيما بينه وبين باقي التشريعات، إذ اقتصر الليبي على إقراره لها، ووجوب صدورها من صاحبها، ولم يبين مدى حقه في سحبها وكيفيةه بشكل صريح، وإنما أقر حق صاحبها في الاعتراض على معالجتها وفق المادة (79) من قانون المعاملات الإلكترونية، بينما توسعت باقي التشريعات في ضوابط الموافقة، ووضعت لها إطاراً يكفل دقتها، ويضمن سلامتها وسيطرة صاحبها عليها.

2: حقه في الإعلام:

المسؤول عن معالجة البيانات ملزم بإعلام صاحبها عن هويته والهدف من المعالجة، وفي حالة جمع البيانات عبر شبكات مفتوحة، يجب إعلامه بأن بياناته قد تكون عرضة للتداول دون ضمان كافٍ، مما قد يُتيح قراءتها، والاستخدام غير المُرخص به من قبل الآخرين، وقد يتعذر إعلامه، فإنه في هذه الحالة لا يكون المسؤول عن المعالجة ملزماً بالإعلام، لا سيما في معالجة البيانات لأغراض علمية، أو إحصائية، أو تاريخية، ويجب عليه إشعار السلطة الوطنية بتعذر الإعلام وتوضيح أسبابه، كما لا يكون ملزماً بالإعلام إذا تمت معالجة البيانات تطبيقاً لنص قانوني، أو لأغراض فنية، أو صحفية، أو أدبية. (عيوني، 2025، صفحة 739)

أقر المشرع الليبي ضرورة إعلام صاحب البيانات بكل ما يتعلق بعملية المعالجة، من غرضها، وهوية المسؤول عنها، ووسائلها وفق المادة (76) من قانون المعاملات الإلكترونية الليبي.

كذلك المشرع السعودي، أقر حق صاحب البيانات في العلم بمسوغات جمع بياناته، والغرض منه، وفق المادة (1/4) من نظام حماية البيانات الشخصية.

وعلى ذات السياق، منح المشرع البحريني صاحب البيانات الحق في علمه وإخطاره بعملية المعالجة وهدفها، كما أوضح أنه في حالة ما استلزم اتخاذ قرار ما، بناءً على هذه البيانات بصورة تمس مصلحة صاحبها، فإنه يجب بيان الطريقة التي تُستخدم في هذا الشأن، وذلك بموجب المادة (18)، من قانون حماية البيانات البحريني، كما أقر المشرع الأردني حق صاحب البيانات في الإعلام بعملية المعالجة، بموجب المادة (1/4)، من قانون حماية البيانات الأردني.

نتائج المقارنة: أن المشرع الليبي نظم حق صاحب البيانات في الإعلام بعملية المعالجة بشكل مُفصل، والأمر على خلافه في التشريع السعودي والبحريني والأردني، حيث اكتفت هذه التشريعات بإقرار حق الإعلام دون تفصيل كالمُشرع الليبي، فهذا الحق يُمكن صاحبه من ممارسة ما يترتب عليه من حقوق، فإذا لم يعلم بالمعالجة لا يُمكنه الوصول لبياناته، ولا يستطيع تصحيحها، ولا يكون له الاعتراض عليها، أو محوها.

3: حقه في الوصول لبياناته:

يُعد من الحقوق اللصيقة بحقوق الإنسان، وضمانة يكفلها القانون للفرد في جميع الأعراف والتشريعات الدولية، ويقصد به حقه في الوصول لبياناته الشخصية الموجودة لدى المُتحكم أو مُعالج البيانات، ويتمثل في اطلاعه عليها، وحصوله على نسخة منها وبصيغة واضحة. (الشمري، 2023م، صفحة 1661)

استنادًا إلى قانون المعاملات الإلكترونية الليبي، نجد المادة (77) التي ألزمت مُقدم خدمات التصديق بتمكين صاحب البيانات من النفاذ لبياناته، وتحديثها بطريقة إلكترونية.

وفي التشريع السعودي، نجد المادة (2/4) وبموجبها منح المُشرع لصاحب البيانات الحق في الوصول لبياناته المتوفرة لدى جهة التحكم، والحصول على نسخة منها، كما مكن جهة التحكم من تقييد هذا الحق إذا كان ذلك يُشكل ضررًا لصاحبها، وفي حال كانت جهة التحكم جهة عامة، وكان التقييد مطلوب لأغراض أمنية، أو لاستيفاء مُتطلبات قضائية، وذلك وفق المادة (9) من نظام حماية البيانات الشخصية.

وفي السياق ذاته، اتجه المُشرعان البحريني والأردني، فمنحا صاحب البيانات الحق في الوصول لبياناته وفق المادة (18) بحريني، والمادة (4) أردني.

نتائج المُقارنة: أن التشريعات تناولت حق صاحب البيانات في الوصول لبياناته بشكل مُفصل، واقتصر المُشرع الليبي على تناوله بشكل مختصر.

4: حقه في تصحيح بياناته:

يُعد حقًا ملازمًا لحقه في الوصول إلى البيانات الشخصية، ولا يجوز الفصل بينهما، وهذه البيانات تخضع بحكم طبيعتها للتغيير بسبب بعض الظروف التي تشوب عملية جمعها وتسجيلها أحيانًا، فقد يتبين للمتعامل الإلكتروني وجود خطأ في بياناته، أو نقصها، أو عدم دقتها؛ إما لسبب يرجع إليه، أو لإجراءات المُعالجة، ففي هذه الحالة له الحق في مُطالبة المتجر الإلكتروني بتصحيحه ومُراجعة بياناته. (ربضي، 2024م، صفحة 324)

تضمنت هذا الحق المادة (77) من قانون المعاملات الإلكترونية الليبي، كما سبق الإشارة إليها، والتي منحت صاحب البيانات مُكنة تحديثها بطريقة إلكترونية، كما نص المُشرع السعودي على حق صاحب البيانات في تصحيح بياناته، أو إتمامها، أو تحديثها، وفق المادة (4/4) من نظام حماية البيانات الشخصية.

وأقر المُشرع البحريني حق صاحب البيانات في المُطالبة بتصحيح بياناته، في حال كانت المُعالجة تحوي بيانات غير صحيحة، أو ناقصة، أو غير مُحدثة، أو غير مشروعة، وذلك بموجب طلب يُقدمه لمُدير البيانات، وأوجب على الأخير الاستجابة للطلب دون مُقابل، ما لم يكن لديه مُسوّغٌ مشروعٌ قانونًا، وذلك وفق المادة (23) من قانون حماية البيانات الشخصية.

وفيما يتعلق بالتشريع الأردني، نجده أيضًا قد منح صاحب البيانات الحق في تصحيح بياناته، أو تعديلها، أو الإضافة إليها، أو تحديثها، وذلك بموجب المادة (3/4) من قانون حماية البيانات الشخصية.

نتائج المُقارنة: أن التشريع الليبي أقر الحق في تصحيح البيانات كما أقرته التشريعات، إلا أن التشريعات فصلته تفصيلًا دقيقًا، خاصة التشريع البحريني الذي أوضح كيفية مُمارسة هذا الحق، وما يجب على مُدير البيانات القيام به.

5: حقه في الاعتراض على مُعالجة بياناته:

يكون لصاحب البيانات أن يعترض على مُعالجة بياناته لأسباب مشروعة، كما له رفض استخدامها في أبحاث تجارية دون أن يُبرر ذلك، ومُمارس هذا الحق سواء في مرحلة جمع البيانات، أو في مرحلة لاحقة. (جبور، 2018م، صفحة 148)

لم ينص المشرع الليبي بشكل صريح على حق صاحب البيانات في الاعتراض على عملية المعالجة، وإنما يفهم ضمناً حين حظر على الجهات المختصة أن ترسل له وثائق إلكترونية في حال رفض قبولها، وذلك بموجب المادة (79) من قانون المعاملات الإلكترونية الليبي.

كما نجد في التشريع السعودي ما يُفيد بإقرار المشرع لحق صاحب البيانات في الاعتراض على عملية معالجة بياناته، وذلك وفق الفصل الأول من لائحة نظام حماية البيانات. (اللائحة التنفيذية لنظام حماية البيانات الشخصية : دليل شامل في المملكة العربية السعودية، بلا تاريخ)

وإلى جانبه، أقر المشرع البحريني حق صاحب البيانات في الاعتراض على معالجة بياناته إذا كان من شأنها إلحاق الضرر به، وذلك بموجب نص صريح وفق المادة (21)، كما منحه المشرع الحق في الاعتراض على المعالجة الآلية لبياناته، بموجب المادة (22) من قانون حماية البيانات، كذلك التشريع الأردني، نص على حق صاحب البيانات في الاعتراض على عملية المعالجة وفق المادة (6/4) من قانون حماية البيانات الأردني.

نتائج المقارنة: تفوق التشريع البحريني على باقي التشريعات بنصه الصريح وتنظيمه المفصل لحق الاعتراض على المعالجة.

6: حقه في محو البيانات:

يُبنى هذا الحق على عدم الحاجة للاحتفاظ بها، فمتى انتهت الجهة المسؤولة عن جمعها واستخدامها من الغاية التي تم لأجلها الجمع والمعالجة، يكون لصاحبها الحق في مطالبتها بمحوها أو إتلافها لانتهاؤ الغاية من جمعها ومعالجتها؛ لأن بقائها بعد استيفاء الغاية قد يكون سبباً في معالجتها بطريقة خاطئة مرة أخرى أو تسريبها. (الشمري، 2023م، صفحة 1666)

وباستقراء نصوص قانون المعاملات الإلكترونية الليبي، يتضح عدم ورود نص صريح يقرر حق صاحب البيانات في محو بياناته الشخصية، إلا أن هذا الحق يمكن استنتاجه ضمناً من بعض الأحكام المتعلقة بعدم الاحتفاظ بالبيانات، وعدم استخدامها في غير الغرض المخصص لها.

ونص المشرع السعودي على حق صاحب البيانات في طلب إتلاف بياناته الشخصية، متى ما انتهت جهة التحكم من معالجتها، وذلك وفق المادة (5/4)، ومنح الجهة الحق في الاحتفاظ بالبيانات حتى بعد الانتهاء من عملية الجمع، إذا تمت إزالة كل ما يؤدي إلى معرفة صاحبها على وجه التحديد، وفق الضوابط التي تُحددها اللوائح، وذلك بموجب المادة (1/18)، كما حدد في ذات المادة (2/18) الحالات التي يجوز فيها الاحتفاظ بالبيانات وهي: توافر مسوغ قانوني يوجب الاحتفاظ بها مدة محددة، هنا تجري عملية الإتلاف عقب انتهاء المدة، كذلك في حال اتصال البيانات بقضية منظورة أمام جهة قضائية، فإنه يحتفظ بالبيانات لحين استكمال إجراءات القضية.

كما نص المشرع البحريني على حق صاحب البيانات في مسح بياناته الخاصة، في حال تمت معالجتها بالمخالفة لأحكام القانون، وذلك بموجب المادة (23) من قانون البيانات الشخصية، كذلك نجد النص في التشريع الأردني على حق صاحب البيانات في محوها، وذلك وفق المادة (10/أ) من قانون حماية البيانات.

نتائج المقارنة: أن التشريع الليبي يفتقر للنص الصريح على حق المحو، خلاف التشريعات المقارنة التي نظمته بنصوص صريحة وأوضحت آليته.

ختاماً، نخلص للقول بأنه متى مارس صاحب البيانات حقوقه تمكن من التحكم في بياناته، وهو بذلك يحد من مخاطر معالجتها، ويُعزز الثقة ويضمن حمايتها في إطار التعامل الإلكتروني، وأن التشريع الليبي مقارنة بالتشريعات الأخرى في حاجة لمواكبة التطور، بإصدار تقنين يكفل حماية البيانات بتحديد حقوق صاحبها بوضوح.

ثانيًا: التزامات مُعالج البيانات:

نظرًا للدور المحوري الذي يقوم به مُعالج البيانات، فإنه يخضع لعدة التزامات تندرج بين الالتزامات القانونية العامة وتتمثل في السرية والشفافية، والالتزامات التقنية المتمثلة في استعمال وسائل الأمان الإلكتروني، بالإضافة إلى توفير أدوات تحقق إلكترونية، نعرضها على التوالي:

1: الالتزامات العامة:

ضمانًا لسلامة التعامل، يلتزم المسؤول عن مُعالجة البيانات بالالتزامات عامة، تهدف لتنظيم الممارسة المهنية، نعرضها وفقًا لما يلي:

أ: الالتزام بالسرية:

يعد التزامًا قانونيًا توجهه القواعد العامة على المهني بعدم إفشاء السر المهني، فالمُتفاوض مُلزم بالاحتفاظ على ما أطلع عليه من أسرار أثناء التفاوض، فقد يستوجب التفاوض أن يفضي أحد الطرفين للآخر ببعض أسرار المهنة، ولو لم تحظ بحماية قانونية كالتكنولوجيا، والمعرفة الفنية. (منصور، 2007م، صفحة 50)

وقد أكد المُشرع الليبي على ضرورة الالتزام بالسرية، وعدم إفشاء البيانات، أو تحويلها، أو إعلانها، أو نشرها، إلا بموافقة مُسبقة من الشخص الذي جمعت عنه البيانات، وفقًا للمادة (75) من قانون المعاملات الإلكترونية، ويتوافق مع التشريعات المُقارنة في التشديد على سرية البيانات، بموجب المادة (15) من نظام حماية البيانات السعودي، المادة (37) من القانون البحريني، والمادة (7) من القانون الأردني.

ب: الالتزام بالشفافية:

يُعد عنصرًا هامًا للأمن القانوني واستقرار التعامل، وغيابه يُشكل عائقًا أمام الوصول للعدالة وتطبيق القانون بشكل صحيح، ويقتضي هذا الالتزام جمع ومُعالجة البيانات بطرق مشروعة، وعلم المعنيين بجمعها، والهدف من مُعالجتها. (الرمحي، 2025م، صفحة 430) أكد المُشرع الليبي على ضرورة الالتزام بالشفافية في المادة (48) من قانون المعاملات الإلكترونية، وهو في هذا يتوافق مع ما أكدت عليه جُل التشريعات بضرورة الالتزام بالشفافية، والامتثال لمبادئ القانون ذات العلاقة بحماية البيانات الشخصية، بموجب المادة (4) من نظام الحماية السعودي، المادة (17) من قانون الحماية البحريني، والمادة (4) من قانون الحماية الأردني.

2: الالتزامات التقنية:

إلى جانب الالتزامات العامة يلتزم المُعالجون بالالتزامات تقنية، وهي كالتالي:

أ: استعمال وسائل أمان:

نظرًا لتزايد المخاطر الناجمة عن الاختراق عبر شبكة الأنترنت، وما يترتب عليه من مساس بسرية وخصوصية البيانات التي يتم تبادلها، فإنه لا بد من استعمال وسائل أمان تقنية، لضمان حمايتها من مخاطر التزوير، وتتمثل هذه الوسائل فيما يلي:

- التشفير:

هو تحويل البيانات لرموز لا يمكن قراءتها إلا باستخدام هذه الرموز، وهذا الإجراء يُعد مهمًا لحماية البيانات أثناء تخزينها أو نقلها، وتكمن أهميته في توفير حماية فعالة ولتجاوز الكثير من المخاطر المُهددة للبيانات الشخصية، ويحقق الثقة بها ويضمن وصولها سليمة من الاعتداء، أو أي خلل من قبل المُستخدم غير المُصرح له، ويشترط فيه أن يتم بواسطة جهة مُختصة يحددها القانون؛ لارتباطه ببيانات ومعلومات سرية وهامة، لذا فإن التشفير يتعلق باعتبارات ترتبط بالنظام العام، ولا بد من أن تكون الجهة المُشرفة عليه جهة حكومية. (بودوشة، 2017م، صفحة 17)

كما يُعد التشفير وسيلة لمنع الوصول للبيانات من قبل غير المُرخص لهم، وله نوعان: التشفير المُماثل باستعمال مفتاح سري واحد للمرسل والمستقبل لتأمين البيانات، والتشفير غير المُماثل ويُعد أكثر أمانًا من النوع الأول، ويُستخدم فيه مفتاح خاص وآخر عام،

المفتاح العام لتشفير البيانات، وبعد إتمام إرسالها للطرف الآخر يقوم باستخدام المفتاح الخاص لفك التشفير. (عمودي، 2023م، صفحة 19)

وقد تبني المشرع الليبي نظام التشفير كوسيلة لحماية المعاملات الإلكترونية، بالنص عليه في المادة (58) من قانون المعاملات الإلكترونية الليبي، أما فيما يتعلق بالتشريعات محل المقارنة فلم نجد نص صريح على التشفير. نتائج المقارنة: تميز التشريع الليبي بالنص صراحة على نظام التشفير في قانون المعاملات الإلكترونية، أما التشريعات المقارنة فأكتفت بالنص على اتخاذ تدابير عامة تكفل حماية للبيانات.

- التوقيع الرقمي:

له دورٌ في حماية المعاملات الإلكترونية وتبادل البيانات، ويُعد أهم صور التوقيع الإلكتروني؛ لقدرته على تحديد هوية أطراف العقد بشكلٍ مُميزٍ ودقيقٍ، وتحقيقه لأعلى درجة من الثقة في العمل القانوني، ولتوخي أقصى درجات الحيلة والحذر من عمليات الاختراق والقرصنة، والمحافظة على السلامة من التحريف، إلا أنه بفعل التطور التكنولوجي يُمكن أن يحصل تزوير واحتيال، وذلك بكسر المفتاح الخاص برسالة البيانات، والتوصل لاكتشاف المفاتيح الخاصة مصدر الأمان وتغيير مضمون الرسالة، لذا يقترح أن يمتلك الشخص زوج من المفاتيح إذا أراد القيام بتوقيع رسالة بيانات وتشفيرها. (بودوشة، 2017م، صفحة 35)

استناداً إلى قانون المعاملات الإلكترونية الليبي، نجد أن المادة (1) تُفيد باعتماد المشرع الليبي على التوقيع الإلكتروني كوسيلة لإثبات صحة المُحرر الإلكتروني، ووضع ضوابط لقبوله، منها أن ينفرد به الشخص الذي استخدمه، وأن يدل على هوية صاحبه، وارتباطه بالمحرر، وسيطر صاحبه على معلومات إنشائه، وذلك وفق المادة (10) من قانون المعاملات الإلكترونية.

أما التشريع السعودي والبحريني والأردني فلم يتم تنظيم التوقيع الرقمي في قوانين حماية البيانات، وإنما في قوانين المعاملات الإلكترونية. نتائج المقارنة: دمج التشريع الليبي بين نظام التوقيع وحماية البيانات في قانون واحد وهو المعاملات الإلكترونية الليبي، أم التشريعات المقارنة فقد تناولت كل منهما في تشريع خاص.

بالإضافة إلى وسائل أمان أخرى، كالتحكم في الوصول، وأنظمة الحماية كالجدران النارية التي تكفل حماية لبيانات المُستخدم من الوصول غير المُصرح به، بواسطة فلترة وتحليل تدفق البيانات لهذا النظام، عن طريق الخادم الوكيل، بالإضافة إلى كشف التسلل ومنعه، والنسخ الاحتياطي والاسترجاع. (لشهب، 2025م، صفحة 313)

ب: توفير أدوات تحقق إلكترونية:

- بروتوكولات الأمان مثل SSL/TLS:

تسمح بتشفير الاتصال بين الخادم والعميل، مما يضمن عدم مقدرة أي طرف آخر من قراءة البيانات أو التلاعب بها، وتستخدم للتحقق من هوية الطرفين، ولذلك دورٌ مهمٌ في التعامل الإلكتروني، فبواسطتها يُمكن للعميل التأكد من تواصله مع الخادم الصحيح، حيث يُرسل الخادم شهادة SSL/TLS الخاصة به إلى العميل، والذي بدوره يتحقق من صحتها لدى جهة إصدار موثوقة، ويؤكد على هوية الخادم. (www.acunetix.com)

- التصديق الإلكتروني:

يعتمد على الشهادات الرقمية، فمقدم الخدمة ملزم بضرورة مسك سجل إلكتروني تُخزن به البيانات على نحو يمنع الغير من التلاعب فيه، ومن خلال هذا السجل يتم التأكد من أن الشخص الطبيعي الممثل للشخص المعنوي والذي وقع على المعاملة، هو ذات الشخص الذي قُيدت بياناته حين أُصدرت شهادة التصديق. (ليبض، 2023م، صفحة 545)

بالرجوع إلى قانون المعاملات الإلكترونية الليبي، نجده خصص فصل للتصديق الإلكتروني في المادة (27) التي تُعطي للهيئة الوطنية صلاحية مراقبة عملية التصديق الإلكتروني، كذلك المادة (28) أولتها عدة مهام نذكر منها منح رخصة مُزاولة مُقدم خدمات التصديق.

ولم نجد في التشريع السعودي ما يُفيد اعتمده على نظام التصديق الإلكتروني، كذلك الأمر بالنسبة للتشريعين البحريني والأردني، فلم ينظما التصديق الإلكتروني في قوانين حماية البيانات.

نتائج المقارنة: أن التشريع الليبي تناول حماية البيانات والتصديق الإلكتروني في تشريع واحد، وهو قانون المعاملات الإلكترونية، وخصص الفصل الثالث للتصديق، والسابع لحماية البيانات الخاصة، بينما تناولت التشريعات المقارنة حماية البيانات في قوانين خاصة، وما يتعلق بالتصديق تناولته في قوانين المعاملات الإلكترونية.

المطلب الثاني

المسؤولية القانونية الناشئة عن انتهاك البيانات الشخصية

في إطار تعدد المخاطر التي تعترض عملية المعالجة، وما ينتج عنها من مساس بالبيانات الشخصية للفرد، فقد ينجم عن انتهاك البيانات آثار مُتنوعة حسب طبيعته ونتائجه، إذ يُمكن أن ينتج عنه ضرر يمس خصوصية صاحبها أو مصلحة مالية له، مما يستوجب جبره وتعويض صاحب البيانات، كما قد ينتج عنه جريمة تقتضي فرض عقوبة على مرتكبها.

ورغم أهمية المسؤولية الجنائية في ردع التعدي على البيانات، إلا أن دراسة موضوع هذا المطلب تقتصر على المسؤولية المدنية، باعتبارها الأساس القانوني الأقرب لجبر الضرر الناشئ عن انتهاك البيانات وتعويض صاحبها، لذا نقسم موضوع المطلب إلى فرعين، الأول لدراسة المسؤولية المدنية، والثاني لبيان سُبل الحماية القانونية للبيانات الشخصية:

الفرع الأول

المسؤولية المدنية

بالرجوع إلى قانون المعاملات الإلكترونية الليبي، نجد أن المُشرع لم ينظم المسؤولية المدنية عن انتهاك البيانات، مما يقتضي الرجوع إلى القواعد العامة، استناداً إلى المادة (50) مدني ليبي، لذا نقسم موضوع الفرع إلى فقرتين، الأولى لبيان طبيعة المسؤولية المدنية، أما الفقرة الثانية فستكون مداراً للبحث في أنواعها:

أولاً: طبيعة المسؤولية المدنية عن انتهاك البيانات الشخصية:

باستقراء التشريعات محل المقارنة، يتجلى لنا أنها أرست تنظيمًا مختلطاً بين المسؤولية المدنية والجنائية والإدارية عن انتهاك البيانات، لضمان حماية شاملة لها، فالتشريع السعودي كَيّفها بأنها مسؤولية مدنية تمنح الحق في المطالبة بالتعويض وفق المادة (40)، ومسؤولية جنائية توجب فرض عقوبة بالسجن لمدة لا تزيد عن سنتين، وغرامة لا تزيد عن ثلاثة ملايين ريال، لكل من أفصح عن بيانات حساسة، أو نشرها بالمخالفة للنظام، وقابلة للزيادة في حال العود، وذلك بموجب المادة (35)، ومسؤولية إدارية فأقر العقوبة بالإلزام أو الغرامة، وفق المادة (36) من نظام حماية البيانات الشخصية.

كذلك التشريع البحريني كَيّفها بأنها مسؤولية مدنية توجب التعويض وفق المادة (57)، ومسؤولية جنائية تفرض عقوبات بالحبس، والغرامة التي لا تقل عن 1000 دينار، ولا تزيد عن 20000 دينار، وفق المادة (58)، كما ومنح مجلس الإدارة سلطة اتخاذ تدابير عند وقوع مُخالفة، نذكر منها سحب الترخيص، وفرض غرامة تهديدية، وذلك بموجب المادة (55) من قانون حماية البيانات.

وعلى ذات السياق، كيّف التشريع الأردني المسؤولية الناشئة عن انتهاك البيانات، بأنها مسؤولية تتضمن عدة صور منها: مسؤولية توجب التعويض وفق المادة (20/ب)، واتخاذ تدابير في حال ثبوت المخالفة كالإنذار بإيقاف الترخيص، أو إلغائه، وفق المادة (21) من قانون حماية البيانات.

نتائج المقارنة: أن التشريعات أقرت نظام يشمل المسؤولية المدنية والجنائية والإدارية عن انتهاك البيانات الشخصية، في حين أن التشريع الليبي يرد المسؤولية للقواعد العامة.

ثانياً: أنواع المسؤولية المدنية:

نظراً لطبيعة العلاقة بين أطراف التعامل الإلكتروني، فإنه ينطق بشأنها أحكام المسؤولية المدنية العقدية أو التقصيرية متى ما توافرت أركانها، لذا نعرض في هذه الفقرة لبيان أنواع المسؤولية المدنية لإمكانية تطبيقها على انتهاك البيانات:

1: المسؤولية العقدية:

يستوجب لقيام المسؤولية العقدية أن يكون الضرر ناشئاً عن إخلال بالتزام عقدي، حينها يمكن للمضرور رفع دعوى المسؤولية، للمطالبة بتعويضه عن الضرر الذي لحقه من جراء الإخلال بتنفيذ الالتزام العقدي. (وهذان، 2011م، صفحة 15) ولنهوض المسؤولية العقدية في إطار المعاملات الإلكترونية، لابد من وجود عقد بين المعالج والمستخدم، وأن يُقدم المستخدم بياناته الشخصية، وأن تُؤخذ موافقته على مُعالجتها، وتتمثل صور الإخلال بالالتزام العقدي في المعاملات الإلكترونية؛ في عدم التزام مُقدم الخدمة بضوابط مُعالجة البيانات الشخصية، أو بالمبادئ الأساسية لجمع ومُعالجة البيانات، فتكون مسؤولية المُعالج مسؤولية عقدية؛ لإخلاله بالتزام عقدي. (مساها، 2025م، صفحة 793)

وبعرض سابق لما اتجهت إليه التشريعات المقارنة فيما يتعلق بضوابط المُعالجة، اتضح لنا أنها تركز إلى إقرار ضوابط تكفل مشروعية المُعالجة، وفصلتها بصورة أكثر من التشريع الليبي.

وفي إطار المسؤولية الناشئة عن انتهاك البيانات، قد لا يكون الانتهاك دائماً صادراً عن طرف يرتبط بعقد مع صاحب البيانات، مما يُفيد بأن تأسيس مسؤولية الانتهاك على أنها عقدية لا يكفي لتغطية كافة صور التعدي على البيانات، كما في حال اختراق قواعد البيانات، وابتزاز الضحية وتهديده بنشر ما تم الحصول عليه من صور، ومعلومات خاصة مقابل دفع الأموال، وهذا ما يُمكن معه تأسيسها على أنها مسؤولية تقصيرية؛ لإمكان جبر الضرر الناشئ عن انتهاك البيانات، وهو ما نتناوله في الفقرة التالية:

2: المسؤولية التقصيرية:

تقوم على الإخلال بالتزام قانوني بعدم الإضرار بالغير، تقتضي أن يكون الفعل مُضراً، وأن يكون الضرر بسبب الفعل سواء مباشرة أو بالتسبب. (السنهوري، د.ت، صفحة 748)

ويتم التعويض في المسؤولية التقصيرية عن الأضرار المتوقعة وغير المتوقعة، لأنها لا تنشأ بموجب اتفاق يمكن أن يلاحظ فيه الضرر، وإنما تنشأ عن فعل طارئ. (قزمان، 2006م، صفحة 9)

فإذا لم يلتزم مُعالج البيانات بشروط مشروعية مُعالجتها، فإنه يُعد مُرتكباً لخطأ تقصيري يترتب عليه التزام بتعويض من تمت مُعالجة بياناته، إذا ما لحقه ضرر من جراء المُعالجة المُخالفة، ويتطلب لقيام المسؤولية التقصيرية توافر أركانها من خطأ، وضرر، وعلاقة سببية تربط بينهما، ويقوم الخطأ التقصيري على ركنين: ركن مادي، وهو ارتكاب فعل التعدي كالمُعالجة البيانات دون مُوافقة من صاحبها، أو رغم اعتراضه عليها، كذلك الخطأ الناتج عن عدم الاحتفاظ بسريتها وإفشاءها، إضافة لتجميع وحفظ البيانات بطرق غير مشروعة. (أبوبكر، 2020م، صفحة 18)

أما الركن المعنوي للخطأ التقصيري، فيتجسد في إدراك المُتعدّي لعواقب فعله الخاطئ الذي ارتكبه، فلا يُسأل المجنون ولا غير المُميز ولا المعتوه عن نتيجة فعله إذا ترتب عليه إضرار بالغير، وبالتطبيق على المسؤول عن مُعالجة البيانات، نجد شخصاً عاقلاً بالغاً مخاطباً

بأحكام القانون، وقيامه بإجراء المعالجة قد يكون فعل مُضر، يترتب عليه ضرر بصاحب البيانات. (رجب، المسؤولية التقصيرية الناشئة عن انتهاك خصوصية البيانات الشخصية الرقمية، 2023م، صفحة 931)

واستخلاص الخطأ التقصيري يعد من اختصاص قاضي الموضوع، من خلال ما عُرض عليه من وقائع، في حين أن تكييف الفعل بأنه خطأ يعد مسألة قانونية يقوم بها تحت رقابة المحكمة العليا. (أوبكر، 2020م، صفحة 19)

فالأساس القانوني الأكثر تماشيًا مع المسؤولية عن انتهاك البيانات، هو فكرة تحمل التبعة القائمة على أن من يعمل في مجال مُعين يتحمل ما يترتب على عمله من نتائج، فمسؤولية مُعالج البيانات تقوم على ما له من دور في جمعها وتخزينها وتداولها، ومُلزَم بامتلاكه الوسائل التقنية المطلوبة لممارسة الرقابة والسيطرة على بيانات المتعاملين معه؛ ضماناً لاحترامها وعدم الإضرار بها. (إبراهيم، 2025م، صفحة 8)

وللفعل الضار عدة صور، منها الإتجار بالبيانات الشخصية، وعدم تطبيق حق الحو الرقمي للبيانات، مما يؤثر على خصوصيتها بانتقالها من موقع إلى آخر، الأمر الذي أوجب الاحتفاظ بها لمدة مُحددة، فالضرر الذي يلحق بصاحبها هو أساس المسؤولية المدنية المترتبة على انتهاكها، والذي قد يكون مادياً، كبيع موقع التواصل الاجتماعي السيرة الذاتية الخاصة بالمستخدم للشركات، من أجل التسويق وتحسين إنتاجها، كما قد يكون الضرر معنوياً، كحفظ البيانات التي لم يعد مرغوب فيها لمدة طويلة، فتكون ظاهرة للجميع وتمس السمعة الرقمية، وهو أكثر شيوعاً من الضرر المادي. (مسهل، 2025م، صفحة 797)

كما تعد علاقة السببية بين الخطأ والضرر ركناً أساسياً لقيام هذه المسؤولية، فمن الطبيعي ألا يُسأل مُرتكب الخطأ في المجال الإلكتروني إلا على ما يسببه من أضرار إلكترونية مُختلفة، فإذا كان الضرر قد نتج عن حادث مُفاجئ أو لسبب أجنبي، أو بفعل الشخص المضروب، فإنه لا تكون هناك علاقة سببية، ولا يُسأل مُرتكبه عن جبر الضرر. (مدبولي، 2022م، صفحة 166)

ختاماً لما سبق، يتضح أن المشرع الليبي لم يُنظم المسؤولية الناشئة عن انتهاك البيانات في قانون خاص بالبيانات، وبالرجوع للقواعد العامة نجد نص المادة (50) من القانون المدني على حماية الحقوق المُلازمة للفرد، ونجد نصوص في القانون رقم (5)، لسنة 2022م، بشأن مكافحة الجرائم الإلكترونية على صور الاعتداء الإلكتروني، أما التشريعات المُقارنة اعتمدت على نظام مُختلط يجمع بين المسؤولية المدنية والجنائية والإدارية، مما يُفيد أن الاعتماد على القواعد العامة لم يعد كافياً لاستيعاب كافة التحديات في ظل التطور التقني، ويوجب مُعالجته بتنظيم تشريعي خاص بالبيانات الشخصية.

الفرع الثاني

سُبل الحماية القانونية للبيانات الشخصية

بفعل الانتهاكات المتكررة على البيانات الشخصية، بُرزت الحاجة لوضع سُبل قانونية تكفل حمايتها، وتنقسم إلى: السُبل الوقائية المُتمثلة في التدابير التصحيحية، الإجراءات القضائية، والجزاءات النظامية والإدارية، والسُبل اللاحقة المُتمثلة في التعويض المدني:

أولاً: السُبل الوقائية:

1: التدابير التصحيحية لإزالة المخالفة:

أ: تصحيح البيانات أو تحديثها:

البيانات الشخصية قد لا تمثل هوية الشخص الرقمية الحقيقية في الوقت الحاضر، لذا يجب استبدالها سواء بتصحيحها أو تحديثها، وعلى المُعالج أن يحرص على عدم تأثر هوية الشخص الرقمية بمرور الزمن، كأن تُنشر بشكل قانوني بيانات حول تورطه في جريمة، فإن ذلك يستلزم تصحيح أو تحديث بياناته في حال رُدَّ إليه اعتباره، أو تبرئته. (ربضي، 2024م، صفحة 324)

ب: حذف البيانات:

يُتاح لصاحب البيانات الحق في طلب حذفها ومحوها من جهة التحكم، في حال انتهاء الغرض من جمعها، كما وقد يكون بواسطة سحب موافقته، ويجب على الجهة إتلافها بمجرد الانتهاء من غرض جمعها، إلا في حال وجود مسوغ قانوني يتطلب حفظها، كالبيانات المدونة في السجلات المالية أو الإدارية، كما تحفظ في حال موافقة صاحبها على استمرارية حفظها. (التركي، 2025م، صفحة 1125)

سبق وأن تم عرض موقف التشريعات المقارنة فيما يتعلق بهذه التدابير التصحيحية، عند البحث في حقوق صاحب البيانات.

2: الإجراءات القضائية الوقائية:

الهدف من هذه الإجراءات ضمان حماية وقائية تحفظية قبل وقوع الضرر، وتمثل فيما يلي:

أ: وقف الاعتداء أو المعالجة:

قد يتبين للقاضي أن الأكثر إرضاءً هو تعويض المضرور تعويضاً عينياً، في حال التعدي على بياناته، حينها يحكم بإعادة الحال إلى ما كان عليه قبل التعدي، وذلك بإيقاف الانتهاك وإزالة أثره الضار، ويكون ذلك إما بحذف البيانات التي لم تعد مرغوبة من صاحبها، أو منع الغير من التوصل إليها، لما تمثله من إضرار بسمعته، أو كشفها عن هويته عبر مواقع التواصل. (مساها، 2025م، صفحة 800)

فيُمكن للمعتدى على بياناته أن يطلب من المحكمة منع ووقف الاعتداء سواء وقع على اسمه، أو صورته، أو كان بقصد التشهير به، أو ابتزازه، دون الالتزام بقواعد المسؤولية التقصيرية التي تستوجب الخطأ، والضرر، ورابطة سببية تجمعهما. (عثمان، 2019م، صفحة 29)

ولا يشترط بدء الاعتداء لبدء إيقافه، فالمقصود بوقف الاعتداء لا يعني إيقافه بعد وقوعه، وإنما يشمل كذلك منعه قبل وقوعه، فهو بمثابة منع المخطئ من الشروع في ارتكاب فعل جرمه القانون، ولا يعتبر تعويضاً. (صبيح، 2025م، صفحة 248)

بالرجوع إلى قانون المعاملات الإلكترونية الليبي، لم نجد نص على وقف المعالجة، وورد فيه النص على عدم جواز المعالجة إلا بموافقة من صاحب البيانات، وفق المادة (73) من قانون المعاملات الإلكترونية.

وفي التشريع السعودي نجد المادة (2/5) من نظام الحماية، تفيد بحق صاحب البيانات في الرجوع عن موافقته على معالجة بياناته. كما أجاز التشريع البحريني للرئيس التنفيذي في الحالات المستعجلة الوقف المؤقت عن معالجة البيانات كلياً أو جزئياً وفق المادة (56/أ) من قانون حماية البيانات، كذلك التشريع الأردني وفق المادة (10) من قانون حماية البيانات.

نتائج المقارنة: اكتفاء التشريع الليبي بالنص على عدم مشروعية المعالجة إلا بموافقة صاحب البيانات، ولم يرد فيه نص على صلاحية وقف المعالجة، بخلاف التشريعات المقارنة، مما يُفيد بعدم اعتماد التشريع الليبي على تدابير وقائية قبل وقوع الضرر.

ب: إصدار أوامر قضائية مُستعجلة:

الهدف منها منع وقوع الضرر الذي يحدث عند المعالجة غير المشروعة، وعلى الرغم من عدم وجود تشريع ليبي خاص بالبيانات الشخصية، إلا أنه يوجد في قانون المعاملات الإلكترونية الليبي نص يُفيد بمشروعية المعالجة إذا كانت: "2: مطلوبة أو مُصرحاً بها بموجب القانون أو قرار من المحكمة"، وباستقراء نص المادة (2/47) من قانون المعاملات الليبي، يتضح أنه يُمكن للقاضي أن يتدخل لحماية البيانات من خلال الأوامر القضائية.

3: الجزاءات النظامية والإدارية على انتهاك البيانات الشخصية:

تبعاً للتعويل المتزايد على البيانات الشخصية، أضحى انتهاكها سلوكاً مخالفاً لما تقضي به الأنظمة النافذة، لذا أقرت التشريعات جزاءات نظامية لحمايتها، وتعزيز الثقة في المعاملات الإلكترونية، وتمثل فيما يلي:

أ: الغرامات المالية:

بالرجوع إلى التشريع الليبي، نجد أن القانون رقم 2022/5م، بشأن مكافحة الجرائم الإلكترونية، يحتوي على جزاءات نظامية تتضمن غرامات تفرض على الدخول غير المصرح به، بما لا يقل عن 100 دينار، ولا يزيد عن 500 دينار، وذلك إذا كان الدخول بهدف إلغاء، أو حذف، أو إضافة، أو إفشاء، أو إتلاف بيانات، وشدّد العقوبة بفرض غرامة لا تقل عن 10000 دينار، إذا نجم عن الدخول غير المصرح به عرقلة عمل النظام المعلوماتي، وذلك وفق المادتين (12/11) من قانون مكافحة الجرائم الإلكترونية الليبي. وباستقراء التشريع السعودي، نجد أنه أقر الغرامة كجزء نظامي على انتهاك البيانات، وقدرها بقيمة 3 ملايين ريال في حال الإفصاح عن بيانات حساسة، قابلة للزيادة في حالة العود، وذلك بموجب المادة (35) من نظام حماية البيانات الشخصية. كذلك قدّر المشرع البحريني غرامة لا تقل عن 1000 دينار، ولا تزيد عن 2000 دينار في حال مخالفة أحكام القانون، وذلك وفق المادة (58) من قانون حماية البيانات، كما فرض المشرع الأردني غرامة مالية لا تزيد عن 500 دينار على المسؤول المخالف، بموجب المادة (4/21) من قانون حماية البيانات الشخصية. نتائج المقارنة: أن المشرع الليبي لم يفرد للبيانات الشخصية نظاماً خاصاً يتضمن فرض غرامات مالية في حال المخالفة، إنما جاء ذلك في قانون الجرائم الإلكترونية.

ب: الإنذار:

يكون للجهة المسؤولة عن أمن وسلامة المعلومات أن تنذر مُعالج البيانات بضرورة التوقف عن مُعالجتها، في حال عدم الحصول على الترخيص متى ما اقتضت الحاجة ذلك، وفي حال عدم الإخطار بإنشاء المُعالجة، إضافة إلى إخلاله بالالتزام بعدم إفشاء البيانات. (التهمامي، الحماية القانونية للبيانات الشخصية، 2011م، صفحة 244) باستقراء قانون المعاملات الإلكترونية الليبي، لم نجد نصاً يقضي بإنذار المُتحمك أو المُعالج، أما التشريع السعودي فقد أقر العقوبة بالإنذار متى ثبتت مخالفة أحكام النظام أو لوائح، وفق المادة (36) من نظام حماية البيانات الشخصية، كما منح التشريع البحريني مجلس الإدارة سلطة اتخاذ تدابير عند وقوع مُخالفة، وذلك بموجب المادة (55) من قانون حماية البيانات. ويمكن المشرع الأردني مجلس الإدارة من إنذار المُخالف بإيقاف الترخيص، أو التصريح كلياً أو جزئياً، وذلك وفق المادة (1/21) من قانون حماية البيانات الشخصية. نتائج المقارنة: عدم نص التشريع الليبي على الإنذار كتدبير يكفل حماية للبيانات، في حين أن التشريعات المقارنة نصت عليه بنصوص صريحة.

ج: سحب الترخيص:

يُعد من أشد الجزاءات الإدارية الموقعة على المُخالف، ويتجسد هذا الجزاء في حرمان المُخالف حرماناً مؤقتاً، أو دائماً من ممارسة أعمال مُرخّص بها، فتقوم الإدارة بسحب التراخيص من الجهة المُرخّص لها في حال مُخالفتها لشروط القيام بنشاطها. (الأوجلي، 2024م، صفحة 1195) وفي التشريع الليبي، لم نجد نص في قانون المعاملات الإلكترونية يُفقد بسحب الترخيص، وإنما اقتصر على اشتراط موافقة صاحب البيانات موافقة صريحة على مُعالجتها. أما التشريع السعودي فقد منح صاحب البيانات الحق في سحب موافقته والرجوع عنها، بالنص الصريح على ذلك، وفق المادة (5) من نظام حماية البيانات. وأجاز المشرع البحريني لمجلس الإدارة في حال ثبوت المُخالفة، أن يأمر بالتوقف عن المُعالجة، ومنحه الحق في إصدار قرار مُسبب بسحب الترخيص، وذلك وفق المادة (55) من قانون حماية البيانات الشخصية، كما أجاز المشرع الأردني للمجلس أن يُلغي الترخيص، أو التصريح كلياً، أو جزئياً، بموجب المادة (21) من قانون حماية البيانات الشخصية.

نتائج المقارنة: أن التشريعات نصت صراحة على سحب الترخيص أو موافقة صاحب البيانات، ووضعت له آلية خاصة، أما التشريع الليبي فلم يقر ذلك صراحة، واكتفى باشتراط موافقة مسبقة، مما يُشكل فراغاً تشريعياً يستوجب المعالجة.

ثانياً: السبل اللاحقة (التعويض المدني):

يُعد انتهاك البيانات الشخصية خطأً تقصيرياً، يمنح لصاحبها الحق في المطالبة بتعويضه عن الضرر الناجم عن المعالجة، متى ما قام المُعالج بأحد الأخطاء التالية: مُعالجتها بالرغم من مُعارضة صاحبها، وعدم تمكينه من الاطلاع عليها، بالإضافة إلى امتناع المُعالج عن القيام بتعديلها، أو إلغاؤها رغم توافر الشروط المُوجبة للتعديل أو الإلغاء. (التهامي، ضوابط معالجة البيانات الشخصية، 2015م، صفحة 435)

ولم يُنظم المُشرع الليبي حق المضرور في المطالبة بالتعويض عن انتهاك بياناته الشخصية، مما يوجب الرجوع للقواعد العامة في القانون المدني الليبي في المادة (166)، التي تنص على أنه: "كل خطأ سبب ضرر للغير يلتزم من ارتكبه بالتعويض"، واعتبارها أساساً لحقه في التعويض عن الضرر الناجم عن انتهاك بياناته الشخصية.

وبالرغم من سهولة إثارة مسؤولية معالجي البيانات لإلحاقهم الضرر بصاحبها، إلا أنه يصعب من الناحية العملية تحديد هويتهم، فالكثير منهم قاموا باستغلالها في الدعاية لغرض مادي منتهكين حرمة خصوصية الفرد، فإذا أثبت صاحب البيانات أركان المسؤولية من خطأ وضرر وعلاقة سببية تربطهما، فإن القاضي يحكم له بتعويض مادي أو معنوي، ويكون التعويض العيني بإعادة الحال إلى ما كانت عليه وإزالة الضرر الناجم عن المعالجة، كأن يحكم بمحو ما وقع من بيانات المضرور في يد المُعالج. (رجب، المسؤولية التقصيرية الناشئة عن انتهاك خصوصية البيانات الشخصية الرقمية، 2023م، صفحة 937)

فإذا استحال التعويض العيني يلجأ القاضي للتعويض النقدي، يدفعه المسؤول للمضرور صاحب البيانات، ويكون بقدر الضرر، يقدره القاضي مع مراعاة الاعتبارات الخاصة بصاحب البيانات، كمركزه الأدبي والاجتماعي والعلمي، ومدى تأثير ذلك على سمعته، إضافة لمراقبته ألا يستفيد مُعالج البيانات من انتهاكها. (رجب، المسؤولية التقصيرية الناشئة عن انتهاك خصوصية البيانات الشخصية الرقمية، 2023م، صفحة 938)

وباستقراء التشريعات محل المقارنة، نجد أنها عاجلت الموضوع بنصوص قانونية نازمة له، تكفل حق صاحب البيانات في المطالبة بتعويضه عن الضرر الناشئ عن مُعالجة بياناته، وذلك وفق الآتي:

أجاز المُشرع السعودي لصاحب البيانات الحق في المطالبة بتعويضه أمام المحكمة المختصة، عن الضرر الناشئ نتيجة ارتكاب أي من المخالفات المنصوص عليها في النظام، أو اللوائح، بموجب المادة (40) من نظام حماية البيانات.

كما نظم المُشرع البحريني أحكام المسؤولية المدنية عن مُعالجة البيانات، وفق المادة (57) من قانون حماية البيانات الشخصية، فأجاز لمن لحقه ضرر ناشئ عن مُعالجة بياناته الشخصية من قبل مُدير البيانات، أو عن إخلال مُراقب حمايتها بأحكام القانون، أن يُطالب أيهما حسب الأحوال بتعويضه.

والى جانب ذلك، منح المُشرع الأردني صاحب البيانات الحق في أن يُطالب المسؤول بالتعويض، متى ما لحقه ضرر ناشئ عن مُعالجة بياناته، وذلك وفق المادة (20/ب) من قانون حماية البيانات.

نتائج المقارنة: أن جميع التشريعات محل المقارنة نصت على الحق في المطالبة بالتعويض، على خلاف التشريع الليبي، فلم نجد فيه ما يُغيد بإقرار حق التعويض عن انتهاك البيانات، مما أوجب الرجوع للقواعد العامة، واعتماد نص المادة (166) مدني ليبي كأساس للمطالبة بالتعويض.

الخاتمة:

بالانتهاء من بحث مختلف جوانب الموضوع، نعرض ما تم التوصل إليه من نتائج، مع تقديم بعض التوصيات:

أولاً: النتائج:

- 1: على الرغم من توافق التشريع الليبي مع التشريعات المقارنة في وضع أسس قانونية لحماية البيانات الشخصية، إلا أنها تناولت تنظيم الحماية بصورة تفصيلية وواضحة، وأفردت لها تنظيمًا قانونيًا مُستقلًا، تضمن المبادئ الأساسية للمعالجة، وحقوق صاحب البيانات، والتزامات المُتحكم أو المُعالج، إضافة إلى إقرارها وتحميدها للمسؤولية القانونية الناشئة عن انتهاك البيانات، ومنحت صاحبها الحق في المطالبة بالتعويض، في حين أن التشريع الليبي يُنظمها بصورة مُوجزة وغير كاملة، وضمن قانون المعاملات الإلكترونية، وهو ما يحد من فعالية الحماية المكفولة للبيانات الشخصية.
- 2: لم ينظم المشرع الليبي أحكام المسؤولية عن انتهاك البيانات الشخصية، مما أوجب الرجوع للقواعد العامة في المسؤولية المدنية، والتي لم تعد كافية لاستيعاب كافة الأضرار في ظل التطور التكنولوجي.
- 3: لا توجد نصوص قانونية في التشريع الليبي تكفل حق صاحب البيانات في المطالبة بالتعويض عند انتهاك بياناته.

ثانيًا: التوصيات:

- من خلال النتائج التي تم التوصل إليها، يمكن أن نقدم بعض التوصيات لعلها تسهم في حماية البيانات بشكل أفضل، وهي كالتالي:
- 1: الحاجة إلى تبني تشريع ليبي خاص بحماية البيانات الشخصية، ويُقترح أن يتضمن تقنين نصوص تتفق مع المعايير الحديثة، وتعالج كافة أوجه القصور في التشريع الليبي، فلا بد من إبراز المراكز القانونية لكل من صاحب البيانات ومُعالجها، من حقوق والتزامات بشكل أكثر تفصيلًا وتنظيمًا، إضافة إلى ضرورة تضمينه نصوص تحدد المسؤولية، وتوضح حق صاحب البيانات في المطالبة بالتعويض، مما يضمن حماية كافية وشاملة للبيانات الشخصية من مخاطر التعدي عليها.
 - 2: التوعية بأهمية حماية البيانات الشخصية والمخاطر التي تعترضها، من خلال عقد ندوات حول الموضوع لمواكبة التطور، وتحقيق الهدف من إصدار قانون المعاملات الإلكترونية الليبي.
 - 3: يتيح هذا البحث مجالاً لدراسات مستقبلية تُجري مقارنة موسعة بين التشريعات العربية، والتجارب الدولية فيما يتعلق بحماية البيانات الشخصية.

قائمة المراجع:

أولاً: الكتب:

- 1: جبور، منى، 2018م، البيانات الشخصية والقوانين العربية، ط.1، جامعة الدول العربية، بيروت.
- 2: السنهوري، عبد الرزاق، د.ت، مصادر الالتزام، د. ط، دار إحياء التراث العربي، بيروت.
- 3: قزمان، منير، 2006م، التعويض المدني، ط.1، دار الفكر الجامعي، الإسكندرية.
- 4: منصور، محمد، 2007م، المسؤولية الإلكترونية، د. ط، دار الجامعة الجديدة، الإسكندرية.
- 5: وهدان، رضا، 2011م، الوجيز في المسؤولية المدنية، ط.1، دار الفكر والقانون، مصر.

ثانيًا: الرسائل العلمية:

- 1: أبوبكر، قارس، 2020م، المسؤولية المدنية في مجال المعاملات الإلكترونية، رسالة دكتوراه في العلوم، تخصص عقود ومسؤولية مدنية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، الجزائر.
- 2: بن الطيب، شهناز، 2024م، حماية البيانات الشخصية في مجال التجارة الإلكترونية، رسالة ماجستير في الحقوق، كلية الحقوق والعلوم السياسية، جامعة باتنة، الجزائر.

- 3: بودوشة، أميرة، 2017م، حماية البيانات الشخصية في مجال التجارة الإلكترونية، مذكرة لنيل شهادة الماستر في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة محمد بن يحيى، الجزائر.
 - 4: لعمودي، عبد الفتاح، 2023م، آليات حماية البيانات الشخصية في التجارة الإلكترونية، مذكرة ماجستير في الحقوق، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر، الجزائر.
- ثالثاً: الدوريات:**
- 1: إبراهيم، إخلاص، 2025م، المسؤولية التقصيرية عن التعامل بالبيانات الشخصية في الوسط الرقمي، كلية الحقوق، المؤتمر الدولي التاسع للقضايا القانونية (ILIC)، العراق.
 - 2: إمام، ماهر، 2024م، الحماية القانونية للبيانات الشخصية في النظامين السعودي والعُماني "دراسة مقارنة"، مجلة الدراسات الفقهية والقانونية، ملحق خاص، كلية الشريعة والقانون، جامعة نزوى، عُمان، العدد 19.
 - 3: الأوجلي، فرج، 2024م، الجزاءات الإدارية، المجلة القانونية، كلية القانون، جامعة بنغازي، ليبيا، المجلد 19، العدد 2.
 - 4: بكري، محمود، 2023م، الحق في حماية البيانات الشخصية لدى الهيئة القومية للتأمين الاجتماعي، مجلة الفكر القانوني والاقتصادي، كلية الحقوق، جامعة بنها، مصر، بدون مجلد، بدون عدد.
 - 5: بن لشهب، أسماء، 2025م، حماية البيانات الشخصية للمستخدم في إطار عقود الحوسبة السحابية، مجلة الفكر القانوني والسياسي، كلية الحقوق، جامعة الأخوة منتوري، الجزائر، المجلد 9، العدد 1.
 - 6: التركي، عبد الله، 2025م، حماية البيانات الشخصية في النظام السعودي، مجلة الدراسات القانونية والاقتصادية، جامعة الإمام محمد بن سعود الإسلامية، السعودية، المجلد 11، العدد 3.
 - 7: التهامي، سامح، 2015م، ضوابط معالجة البيانات الشخصية، مجلة كلية القانون الكويتية العالمية، الكويت، المجلد 3، العدد 8: التهامي، سامح، 2011م، الحماية القانونية للبيانات الشخصية، مجلة الحقوق، جامعة الكويت، الكويت، المجلد 35، العدد 9: خالد، محمد، 2023م، الحماية القانونية للبيانات الشخصية في إطار القانون المدني، مجلة القانون للعلوم القانونية والسياسية، كلية القانون، جامعة كركوك، العراق، المجلد 12، العدد 47.
 - 10: راشد، طارق، 2019م، الحماية القانونية لخصوصية البيانات الشخصية في العصر الرقمي، مجلة القانون والاقتصاد، كلية الحقوق، جامعة القاهرة، مصر، ملخص خاص، العدد 92.
 - 11: رضوي، عيسى، 2024م، ضوابط معالجة المتاجر الإلكترونية بيانات العملاء الشخصية، مجلة كلية القانون الكويتية العالمية، الكويت، بدون مجلد، العدد 2.
 - 12: رجب، هبة، 2024م، الحماية القانونية للبيانات الشخصية في عصر التكنولوجيا الرقمية، مجلة الفكر القانوني والاقتصادي، عين شمس، المجلد 66، العدد 3.
 - 13: رجب، هبة، 2017م، المسؤولية التقصيرية الناشئة عن انتهاك خصوصية البيانات الشخصية الرقمية، بحث مقدم إلى المؤتمر العلمي السنوي الخامس عشر، كلية القانون، جامعة بنها، مصر، بدون مجلد، بدون عدد.
 - 14: الرححي، لينا، 2025م، الحماية القانونية للبيانات الشخصية في المعاملات الإلكترونية، المجلة العلمية للنشر العلمي، الأردن، الإصدار الثامن، العدد 77.
 - 15: سلطان، سمير، 2024م، تعزيز الحماية القانونية للبيانات الشخصية الحساسة في مجال الاستدلالات، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنصورة، مصر، بدون مجلد، العدد 88.
 - 16: سويلم، خالد، 2024م، الحماية القانونية للبيانات الشخصية الإلكترونية، المجلة القانونية، مصر، المجلد 14، العدد 6.

- 17: الشمري، فهد، 2023م، الإطار القانوني لحماية البيانات الشخصية في تشريعات المملكة العربية السعودية، مجلة البحوث الفقهية والقانونية، كلية الشريعة والقانون بدمنهو، جامعة الأزهر، مصر، بدون مجلد، العدد 43.
- 18: صامت، جوهري، 2020م، الضوابط القانونية لمعالجة البيانات الشخصية إلكترونياً، مجلة الدراسات القانونية المقارنة، الجزائر، المجلد 6، العدد 2.
- 19: عثمان، أحمد، 2023م، الخطأ المدني المترتب على مخالفة الضوابط الحمائية للبيانات الشخصية، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنصورة، مصر، بدون مجلد، العدد 85.
- 20: عثمان، عثمان، 2019م، المسؤولية عن الاعتداء على البيانات الشخصية لمستخدمي شبكات التواصل الاجتماعي، مؤتمر كلية الحقوق، جامعة طنطا، مصر.
- 21: عاشوري، وهيب، 2025م، ضوابط مشروع معالجة البيانات الشخصية، مجلة الدراسات القانونية والاقتصادية، المركز الجامعي سي الحواس، الجزائر، المجلد 8، العدد 2.
- 22: عيوني، فؤاد، 2025م، الحماية القانونية للأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، مجلة الفكر القانوني والسياسي، الجزائر، المجلد 9، العدد 2.
- 23: قاسمي، آمال، 2025م، حماية الحق في الخصوصية الرقمية، مجلة القانون والأعمال الدولية، كلية العلوم القانونية والاقتصادية والاجتماعية، جامعة الحسن الأول، المغرب، الإصدار 59.
- 24: اللحدان، فهد، 2025م، نطاق الحماية القانونية للبيانات الشخصية، مجلة البحوث القانونية والاقتصادية، كلية القانون، جامعة الشارقة، المجلد 15، العدد 92.
- 25: لبيض، فائزة، 2023م، الضمانات القانونية الخاصة بمؤدي خدمات التصديق الإلكتروني، مجلة العلوم الإنسانية، كلية الحقوق، جامعة الأخوة منشوري، الجزائر، المجلد 34، العدد 2.
- 26: المحروقي، ميادة، 2023م، الحماية الجنائية لبيانات الأفراد الشخصية المعالجة إلكترونياً، المجلة القانونية، كلية القانون، جامعة القاهرة، مصر، المجلد 16، العدد 7.
- 27: مدبولي، باسم، 2022م، المسؤولية التقصيرية عن معالجة البيانات الشخصية في البيئة الرقمية، مجلة الدراسات الفقهية والقانونية، المعهد العالي للقضاء، عُمان، بدون مجلد، العدد 10.
- 28: محمد، أم كلثوم؛ علوان، أسماء، 2025م، الحماية المدنية لحقوق الشخصية، مجلة كلية الإسرائ الجامعة للعلوم الاجتماعية والإنسانية، كلية القانون، الجامعة المستنصرية، العراق، المجلد 7، العدد 13.
- 29: مهدي، الصغير، 2024م، الطبيعة القانونية للخصوصية الرقمية، مؤتمر التحديات القانونية في العصر الرقمي، المؤتمر العلمي الثامن لكلية الحقوق، جامعة السلطان قابوس، الإمارات العربية المتحدة.
- 30: مساهل، أميرة، 2025م، المسؤولية المدنية لموقع التواصل الاجتماعي الناجمة عن انتهاك الحق في الخصوصية، المجلة الأكاديمية للبحوث القانونية والسياسية، الجزائر، المجلد 9، العدد 1.
- 31: مشعل، محمد، 2017م، الحق في محو البيانات الشخصية، مجلة الدراسات القانونية والاقتصادية، كلية القانون، جامعة مدينة السادات، مصر، المجلد 3، العدد 2.

رابعاً: القوانين:

- 1: القانون رقم (6) لسنة 2022م، بشأن المعاملات الإلكترونية الليبي، الجريدة الرسمية، العدد الأول، لسنة 2023م.
- 2: القانون رقم (5) لسنة 2022م، بشأن مكافحة الجرائم الإلكترونية الليبي، الجريدة الرسمية، العدد الأول، لسنة 2023م.

- 3: القانون المدني الليبي، لسنة 1953م، إصدار 1953/11/28م.
 - 4: المنشور رقم (18) لسنة 2025م، بشأن نظام حماية البيانات واللائحة التنظيمية للقطاع المصرفي، مصرف ليبيا المركزي، 2025/7/2م
 - 5: القانون رقم (30) لسنة 2018م، بشأن حماية البيانات الشخصية البحريني، الجريدة الرسمية، العدد(3375).
 - 6: القانون رقم (24) لسنة 2023م، بشأن حماية البيانات الشخصية الأردني، الجريدة الرسمية، العدد (5881).
 - 7: نظام حماية البيانات الشخصية السعودي، الصادر بالمرسوم الملكي رقم (م/19) لسنة 1443هـ، والمعدل بموجب المرسوم الملكي رقم(م/148) لسنة 1444هـ، ولائحته التنفيذية، جريدة أم القرى، العدد 14901.
- خامساً: المواقع الإلكترونية:

www.acunetix.com

<https://www.devoteam.com>

<https://adelqaff.com>