

Civil protection of personal data in the digital environment: A comparative study

Waseim Mohamed Faraj*

Department of Private Law, Faculty of Law, Al-Zaytuna University, Tarhuna, Libya

*Email (for reference researcher): w.dew@azu.edu.ly

الحماية المدنية للبيانات الشخصية في البيئة الرقمية دراسة مقارنة

وسيم محمد فرج

قسم القانون الخاص، كلية القانون، جامعة الزيتونة، ترهونة، ليبيا.

تاريخ الاستلام: 2026-06-12، تاريخ القبول: 2026-08-20، تاريخ النشر: 2026-08-23

Abstract

The rapid digital transformation has reshaped numerous legal and social relationships, making personal data one of the most significant digital assets with economic and legal value. Personal data has moved beyond its traditional role as a means of identifying individuals to become a fundamental element in electronic transactions, digital commerce platforms, artificial intelligence applications, and smart governmental, financial, and healthcare services. This development has resulted in expanding risks threatening individuals' privacy and personal rights, which has necessitated the establishment of effective civil legal mechanisms to protect data subjects from unlawful use.

This study examines the civil protection of personal data in the digital environment from a private law perspective. It analyzes the legal principles established by the General Data Protection Regulation (GDPR) and their impact on French legislation, while conducting a comparative analysis with relevant Arab laws. The study aims to evaluate the adequacy of existing civil protection mechanisms and propose legal solutions that enhance the protection of personal rights in the digital age.

The research problem focuses on the extent to which traditional civil liability rules can address modern violations of personal data protection, and whether comparative legal systems provide effective protection for data subjects, particularly regarding the obligations imposed on data controllers and processors and the basis of compensation for damages resulting from unlawful data processing.

The study adopts an analytical comparative methodology by examining legal texts, jurisprudential principles, and relevant judicial decisions. It compares the European and French models with contemporary Arab legislation. The findings indicate that the European framework provides a comprehensive system for personal data protection through clear recognition of data subjects' rights, including the rights of access, rectification, erasure, objection, and data portability, in addition to regulating civil liability and compensation for digital damages.

The study concludes that Arab legislations should be further developed to keep pace with modern technological advancements and establish a more effective civil protection framework that balances the requirements of the digital economy with the protection of privacy and human dignity.

Keywords: Personal Data Protection , Digital Environment , Civil Liability , Digital Privacy , Comparative Law , Digital Rights.

الملخص

أدى التحول الرقمي المتسارع إلى إعادة تشكيل العديد من العلاقات القانونية والاجتماعية، وأصبحت البيانات الشخصية من أهم الأصول الرقمية ذات القيمة الاقتصادية والقانونية، بعد أن تجاوزت دورها التقليدي كوسيلة للتعريف بالأفراد لتصبح

عنصرًا أساسيًا في المعاملات الإلكترونية، ومنصات التجارة الرقمية، وتطبيقات الذكاء الاصطناعي، والخدمات الحكومية والمالية والصحية. وقد نتج عن هذا التطور اتساع نطاق المخاطر التي تهدد خصوصية الأفراد وحقوقهم الشخصية، الأمر الذي فرض ضرورة تطوير آليات قانونية مدنية فعالة تكفل حماية أصحاب البيانات من الاستخدام غير المشروع. تتناول هذه الدراسة الحماية المدنية للبيانات الشخصية في البيئة الرقمية من منظور القانون الخاص، من خلال تحليل المبادئ القانونية التي أرستها اللائحة العامة لحماية البيانات في الاتحاد الأوروبي (GDPR)، وبيان أثرها في القانون الفرنسي، مع إجراء مقارنة بالتشريعات العربية الحديثة، بهدف تقييم مدى كفاية وسائل الحماية المدنية القائمة واقتراح حلول تساهم في تعزيز حماية الحقوق الشخصية في العصر الرقمي.

وتتمثل مشكلة الدراسة في مدى قدرة قواعد المسؤولية المدنية التقليدية على مواجهة الاعتداءات الحديثة على البيانات الشخصية، ومدى نجاح التشريعات المقارنة في توفير حماية فعالة لصاحب البيانات، خاصة فيما يتعلق بالالتزامات الواقعة على متحكم البيانات ومعالجها، وأسس التعويض عن الأضرار الناتجة عن المعالجة غير المشروعة. اعتمدت الدراسة على المنهج التحليلي المقارن، من خلال دراسة النصوص القانونية والمبادئ الفقهية والأحكام القضائية ذات الصلة، ومقارنة النموذج الأوروبي والفرنسي بالتشريعات العربية. وتوصلت إلى أن النموذج الأوروبي يتميز بتكامل قواعد حماية البيانات، ووضوح حقوق صاحب البيانات، مثل الحق في الاطلاع والتصحيح والمحو والاعتراض ونقل البيانات، إضافة إلى تنظيم المسؤولية المدنية والتعويض عن الأضرار الرقمية. وتخلص الدراسة إلى ضرورة تطوير التشريعات العربية بما يواكب التطورات التقنية الحديثة، وإنشاء منظومة مدنية أكثر فاعلية تحقق التوازن بين متطلبات الاقتصاد الرقمي وحماية الخصوصية والكرامة الإنسانية.

الكلمات المفتاحية: حماية البيانات الشخصية، البيئة الرقمية، المسؤولية المدنية، الخصوصية الرقمية، القانون المقارن، الحقوق الرقمية.

المقدمة

يشهد العالم تحولاً رقمياً متسارعاً أعاد تشكيل العلاقات القانونية التي تنشأ بين الأفراد والجهات العامة والخاصة، وأصبحت البيانات الشخصية أحد أهم الأصول الاقتصادية والقانونية في البيئة الرقمية، بعد أن تجاوزت وظيفتها التقليدية بوصفها مجرد وسيلة للتعريف بالشخص إلى كونها مورداً رئيساً تعتمد عليه المعاملات الإلكترونية، ومنصات التجارة الرقمية، وتقنيات الذكاء الاصطناعي، والخدمات الحكومية الذكية، والقطاع المالي، والرعاية الصحية، وغيرها من المجالات التي تقوم في جوهرها على جمع البيانات وتحليلها وتبادلها (عبدالله علي، 2021، ص. 76).

وقد ترتب على هذا التحول اتساع نطاق المخاطر التي تهدد الحياة الخاصة للأفراد نتيجة التوسع في عمليات المعالجة الإلكترونية، الأمر الذي فرض على النظم القانونية البحث عن آليات مدنية فعالة تكفل حماية صاحب البيانات من صور الاستغلال غير المشروع، وتحقيق التوازن بين حرية تداول البيانات ومتطلبات حماية الحقوق اللصيقة بالشخصية، وقد ساهمت الأدبيات القانونية الحديثة في إبراز هذه الإشكالية من زوايا متعددة، سواء فيما يتعلق بمفهوم البيانات الشخصية، أو بضوابط معالجتها، أو بالآثار القانونية المترتبة على الإخلال بحمايتها (غالب، 2019، ص. 52).

ولم يعد تنظيم حماية البيانات الشخصية مسألة داخلية تقتصر على حدود التشريع الوطني، بل أصبح من الموضوعات التي شهدت تطوراً ملحوظاً على المستوى الدولي والإقليمي، ولا سيما بعد صدور اللائحة العامة لحماية البيانات بالاتحاد الأوروبي (GDPR) التي أرست منظومة متكاملة من المبادئ المدنية المنظمة لمعالجة البيانات الشخصية، وربطت بين حماية الخصوصية الرقمية وصيانة الحقوق الأساسية للإنسان، وأقامت نظاماً متقدماً للمسؤولية المدنية والالتزامات الواقعة على عاتق متحكم البيانات ومعالجها، مع منح صاحب البيانات مجموعة واسعة من الحقوق، من أبرزها الحق في الاطلاع، والتصحيح، والمحو، وتقييد المعالجة، والاعتراض، ونقل البيانات، فضلاً عن إقرار حقه في الحصول على التعويض عن الأضرار المترتبة على مخالفة أحكام اللائحة (Kuner, 2007, p. 214).

وقد انعكس هذا الاتجاه بصورة واضحة في التشريع الفرنسي الذي أعاد صياغة قواعد حماية البيانات الشخصية بما يتوافق مع اللائحة الأوروبية، وأصبح من أكثر النظم القانونية تطوراً في هذا المجال، سواء على مستوى التشريع أو القضاء (Bygrave, 2014, p. 147).

وفي المقابل، شهدت التشريعات العربية خلال السنوات الأخيرة اهتماماً متزايداً بحماية البيانات الشخصية، تجسد في إصدار قوانين متخصصة في عدد من الدول العربية، كان من بينها القانون المصري رقم (151) لسنة 2020، والقانون العماني لحماية البيانات الشخصية، والقوانين الإماراتية والسعودية وغيرها، غير أن المقارنة بين هذه التشريعات وبين النموذج الأوروبي تكشف استمرار وجود تفاوت في مدى اكتمال البناء القانوني للحماية المدنية، خاصة فيما يتعلق بتحديد طبيعة الالتزامات المدنية الواقعة على القائمين بمعالجة البيانات، وحدود المسؤولية المدنية، وأسس التعويض عن الأضرار الرقمية، ووسائل الحماية القضائية المستعجلة، ومدى الاعتماد بالإرادة الرقمية في إضفاء المشروعية على معالجة البيانات الشخصية.

ومن ثم تظل الحاجة قائمة إلى دراسة تحليلية مقارنة تستخلص أفضل الحلول التشريعية والقضائية، وتسهم في تطوير القواعد المدنية المنظمة لهذا المجال (التهامي، 2015، ص. 399).

وانطلاقاً من ذلك، تتناول هذه الدراسة الحماية المدنية للبيانات الشخصية في البيئة الرقمية من منظور القانون الخاص، من خلال تحليل المبادئ التي أرستها اللائحة الأوروبية لحماية البيانات، وبيان انعكاساتها على القانون الفرنسي، مع إجراء مقارنة بالتشريعات العربية ذات الصلة، وصولاً إلى تقييم مدى كفاية وسائل الحماية المدنية القائمة، والكشف عن مواطن القوة والقصور فيها، واقتراح حلول تشريعية وقضائية من شأنها تعزيز حماية الحقوق الشخصية في البيئة الرقمية، وبما يحقق التوازن بين متطلبات الاقتصاد الرقمي واعتبارات صون الخصوصية والكرامة الإنسانية، ويواكب التطور المتسارع الذي تشهده تطبيقات التكنولوجيا الحديثة.

أولاً- مشكلة الدراسة

تتبع مشكلة هذه الدراسة من أن البيانات الشخصية أصبحت تمثل محوراً رئيساً للعلاقات القانونية في البيئة الرقمية، ولم تعد مجرد بيانات تعريفية تتصل بشخص الإنسان، وإنما أضحت عنصراً اقتصادياً وقانونياً ذا قيمة متنامية، تقوم عليه العديد من المعاملات الرقمية والخدمات الإلكترونية وتطبيقات الذكاء الاصطناعي. وقد أدى هذا التحول إلى اتساع نطاق عمليات جمع البيانات ومعالجتها وتداولها، بما أفرز صوراً متعددة من الاعتداء على الحقوق اللصيقة بالشخصية، وأثار تساؤلات قانونية بشأن مدى كفاية قواعد المسؤولية المدنية التقليدية في استيعاب هذه المنازعات، وحدود التزامات القائمين على معالجة البيانات، وأسس التعويض عن الأضرار الناجمة عن معالجتها بصورة غير مشروعة، ولا سيما في ظل اختلاف النماذج التشريعية بين التشريعات العربية من ناحية، واللائحة العامة لحماية البيانات بالاتحاد الأوروبي والقانون الفرنسي من ناحية أخرى.

ومن ثم تتمثل الإشكالية الرئيسة لهذه الدراسة في التساؤل الآتي:

إلى أي مدى نجحت قواعد الحماية المدنية للبيانات الشخصية في البيئة الرقمية، في ضوء اللائحة العامة لحماية البيانات بالاتحاد الأوروبي والقانون الفرنسي، في توفير حماية قانونية فعالة لصاحب البيانات، وما مدى إمكانية الاستفادة من هذا النموذج في تطوير التشريعات العربية؟

ويتفرع عن هذا التساؤل الرئيس عدد من التساؤلات الفرعية، أهمها:

ما المقصود بالحماية المدنية للبيانات الشخصية، وما الأساس القانوني الذي تقوم عليه في البيئة الرقمية؟
ما المبادئ التي تحكم معالجة البيانات الشخصية في اللائحة الأوروبية والقانون الفرنسي، وما أثرها في تنظيم الحقوق المدنية لصاحب البيانات؟

ما نطاق الالتزامات المدنية الواقعة على متحكم البيانات ومعالجها، وما طبيعتها القانونية؟
ما الأساس القانوني للمسؤولية المدنية الناشئة عن الإخلال بقواعد حماية البيانات الشخصية، وما شروط قيامها وآثارها؟
ما مدى كفاية قواعد التعويض المدني في جبر الأضرار المترتبة على المعالجة غير المشروعة للبيانات الشخصية؟
إلى أي مدى تحقق التشريعات العربية مستوى من الحماية المدنية يتوافق مع المعايير الأوروبية، وما أبرز أوجه القصور التي تستدعي التدخل التشريعي؟

ثانياً: أهداف البحث

تسعى هذه الدراسة إلى تحقيق جملة من الأهداف، من أهمها:

بيان الأساس القانوني للحماية المدنية للبيانات الشخصية في البيئة الرقمية، وبيان طبيعتها القانونية في إطار قواعد القانون الخاص.

تحليل المبادئ المنظمة لمعالجة البيانات الشخصية في اللائحة العامة لحماية البيانات بالاتحاد الأوروبي والقانون الفرنسي، وبيان أثرها في تنظيم العلاقات المدنية.

تحديد الحقوق المدنية المقررة لصاحب البيانات الشخصية، وبيان نطاق الحماية القانونية المقررة لكل منها.

بيان الالتزامات المدنية الملقاة على عاتق متحكم البيانات ومعالجها، وتحليل طبيعتها القانونية وآثار الإخلال بها.

دراسة أحكام المسؤولية المدنية الناشئة عن معالجة البيانات الشخصية بصورة غير مشروعة، وبيان شروط قيامها وأسس التعويض عنها.

تقديم وسائل الحماية القضائية المدنية المقررة لصاحب البيانات الشخصية في التشريعات المقارنة.

الوقوف على أوجه الاتفاق والاختلاف بين النموذج الأوروبي والتشريعات العربية في مجال الحماية المدنية للبيانات الشخصية.

اقتراح عدد من الحلول التشريعية التي تسهم في تطوير القواعد المدنية المنظمة لحماية البيانات الشخصية بما يتوافق مع التطورات التقنية الحديثة.

ثالثاً: أهمية البحث

تكتسب هذه الدراسة أهميتها من أن البيانات الشخصية أصبحت تمثل أحد أهم عناصر الثروة الرقمية في العصر الحديث، وأضحى تداولها ومعالجتها من المقومات الأساسية للاقتصاد الرقمي، الأمر الذي جعلها محلاً لتعارض مصالح متعددة تتعلق بحق الفرد في الخصوصية من ناحية، وحرية تداول المعلومات ومتطلبات التنمية الاقتصادية والتطور التكنولوجي من ناحية أخرى. وقد أفرز هذا الواقع تحديات قانونية غير مسبقة أمام قواعد المسؤولية المدنية التقليدية، الأمر الذي يستوجب إعادة النظر في الأسس التي تقوم عليها الحماية المدنية للبيانات الشخصية، بما يحقق التوازن بين حماية الحقوق للصيقة بالشخصية وتشجيع الابتكار الرقمي.

وتردد أهمية الدراسة في ظل التطور الذي شهدته المنظومة الأوروبية لحماية البيانات الشخصية، ولا سيما بعد دخول اللائحة العامة لحماية البيانات حيز النفاذ، وما ترتب عليها من تطور ملحوظ في القضاء الأوروبي والفرنسي بشأن المسؤولية المدنية عن انتهاك البيانات الشخصية، في مقابل حداثة العديد من التشريعات العربية التي ما زالت في طور بناء منظومة قانونية متكاملة في هذا المجال. ومن ثم فإن الدراسة لا تقتصر على عرض الأحكام القانونية المنظمة للحماية المدنية، وإنما تمتد إلى تقييمها ومقارنتها واستخلاص أفضل الحلول التشريعية والقضائية التي يمكن الاستفادة منها في تطوير التشريعات العربية بما يواكب متطلبات البيئة الرقمية.

رابعاً: منهجية البحث

تقوم هذه الدراسة على المنهج التحليلي المقارن بوصفه المنهج الأكثر ملاءمة لطبيعة الموضوع، إذ يستهدف تحليل القواعد المدنية المنظمة لحماية البيانات الشخصية في البيئة الرقمية، وبيان الأسس القانونية التي تقوم عليها، واستجلاء مدى كفايتها في مواجهة التطورات التقنية المتلاحقة وما أفرزته من أنماط جديدة لمعالجة البيانات الشخصية واستغلالها، ولا يقتصر التحليل على النصوص التشريعية، وإنما يمتد إلى المبادئ العامة للقانون المدني، والاتجاهات الفقهية، والأحكام القضائية ذات الصلة، بما يسمح بالوقوف على حقيقة البناء القانوني للحماية المدنية ومدى اتساقه مع التطور الذي يشهده الاقتصاد الرقمي. وتطبيقاً لذلك، تعتمد الدراسة على إجراء مقارنة بين أحكام اللائحة العامة لحماية البيانات بالاتحاد الأوروبي (GDPR) باعتبارها النموذج التشريعي الأكثر تطوراً في هذا المجال، وبين أحكام القانون الفرنسي، بوصفه من أوائل التشريعات التي أعادت تنظيم حماية البيانات الشخصية في ضوء اللائحة الأوروبية، مع إجراء مقارنة بالتشريعات العربية ذات الصلة، وفي مقدمتها التشريع المصري والعُماني وبعض التشريعات العربية الحديثة، بقصد الوقوف على أوجه الاتفاق والاختلاف، والكشف عن مواطن القصور التشريعي، واستخلاص الحلول القانونية التي يمكن الاستفادة منها في تطوير الحماية المدنية للبيانات الشخصية في البيئة الرقمية.

خامساً: أسباب اختيار الموضوع

يرجع اختيار هذا الموضوع إلى مجموعة من الاعتبارات العلمية والعملية، من أبرزها: حداثة موضوع الحماية المدنية للبيانات الشخصية، وما يشهده من تطور تشريعي وقضائي متسارع على المستويين الأوروبي والوطني.

قلة الدراسات العربية التي تناولت الحماية المدنية للبيانات الشخصية بصورة مستقلة، إذ انصرف معظمها إلى الجوانب الجنائية أو التنظيمية.

تزايد المنازعات المدنية الناشئة عن إساءة معالجة البيانات الشخصية نتيجة التوسع في استخدام المنصات الرقمية وتقنيات الذكاء الاصطناعي.

أهمية التجربة الأوروبية، ولا سيما اللائحة العامة لحماية البيانات والقانون الفرنسي، بوصفها من أكثر النظم القانونية تطوراً في هذا المجال.

الحاجة إلى تقويم مدى كفاية التشريعات العربية في مواجهة صور الاعتداء المدني على البيانات الشخصية، واقتراح حلول تشريعية تساهم في تطويرها.

ارتباط موضوع الدراسة بمجالات حديثة في القانون الخاص، تجمع بين المسؤولية المدنية، والحقوق للصيقة بالشخصية، والتحول الرقمي، وهو ما يمنحه أهمية متزايدة على الصعيدين الأكاديمي والعملية.

سادساً: الدراسات السابقة

أولاً: باسل فايز حمد القطاطشة، الحماية الجنائية لخصوصية البيانات الشخصية الرقمية: دراسة مقارنة، رسالة دكتوراه، جامعة العلوم الإسلامية العالمية، 2022م.

تناولت هذه الدراسة الإطار القانوني لحماية خصوصية البيانات الشخصية الرقمية من منظور جنائي، مع إجراء مقارنة بين عدد من التشريعات المقارنة، وركزت على بيان صور الاعتداء الجنائي على البيانات الشخصية، وأركان الجرائم الماسة بها،

والعقوبات المقررة لمواجهتها، وانتهت إلى ضرورة تطوير التشريعات الوطنية بما يواكب التطور التقني، مع التوسع في تجريم صور الاعتداء المستحدثة على البيانات الشخصية وتعزيز التعاون الدولي في مكافحتها.

وتختلف الدراسة الحالية عن هذه الدراسة من حيث موضوعها ونطاقها؛ إذ تنصرف إلى الحماية المدنية للبيانات الشخصية، وتركز على تحليل المسؤولية المدنية والالتزامات الناشئة عن معالجة البيانات الشخصية، والحقوق المدنية المقررة لصاحب البيانات، ووسائل الحماية القضائية، في ضوء اللائحة الأوروبية والقانون الفرنسي والتشريعات العربية، وهو جانب لم يكن محل الدراسة السابقة إلا بصورة عرضية.

ثانياً: ضرغام عبدالله فاضل أبو خمرة، حماية بيانات الأفراد الشخصية عبر شبكة الإنترنت: دراسة مقارنة، رسالة ماجستير، جامعة الشرق الأوسط، 2021م.

استهدفت هذه الدراسة بيان التنظيم القانوني لحماية بيانات الأفراد عبر شبكة الإنترنت، من خلال عرض مفهوم البيانات الشخصية، ووسائل الاعتداء عليها، والضمانات القانونية المقررة لحمايتها في عدد من التشريعات المقارنة، وانتهت إلى ضرورة استحداث تشريعات متخصصة لمواكبة التطور المتسارع في البيئة الرقمية، مع تدعيم وسائل الرقابة على الجهات القائمة بمعالجة البيانات الشخصية.

وتتميز الدراسة الحالية عنها بأنها لا تقتصر على بيان التنظيم القانوني العام لحماية البيانات الشخصية، وإنما تتناول بالتحليل الأساس المدني للحماية، وأحكام المسؤولية المدنية والتعويض، والحقوق المستحدثة التي قررتها اللائحة الأوروبية، مع التركيز على التطبيقات القضائية الفرنسية والأوروبية وأثرها في تطوير قواعد القانون المدني.

ثالثاً: آلاء بنت سعيد بن ناصر الملكية، حماية البيانات الشخصية لمستخدمي شبكات التواصل الاجتماعي، رسالة ماجستير، جامعة السلطان قابوس، 2015م.

ركزت هذه الدراسة على حماية البيانات الشخصية في إطار استخدام شبكات التواصل الاجتماعي، من خلال بيان طبيعة البيانات التي يتم جمعها عبر تلك المنصات، وتحليل المخاطر القانونية المترتبة على معالجتها، واستعراض عدد من وسائل الحماية التشريعية والتنظيمية الكفيلة بصون خصوصية المستخدمين، وأوصت بضرورة تطوير التشريعات الوطنية بما يتلاءم مع التطور التقني المتسارع في وسائل التواصل الاجتماعي.

وتختلف الدراسة الراهنة عن هذه الدراسة من حيث نطاقها وغايتها؛ فهي لا تقتصر على البيانات المتداولة عبر شبكات التواصل الاجتماعي، وإنما تمتد إلى جميع صور معالجة البيانات الشخصية في البيئة الرقمية، مع التركيز على الحماية المدنية، وتحليل المبادئ التي أرستها اللائحة الأوروبية والقانون الفرنسي، وصولاً إلى وضع تصور تشريعي متكامل يمكن أن يسهم في تطوير التشريعات العربية في هذا المجال.

سادساً: خطة البحث

قوامها مقدمة ومبحثين ثم خاتمة البحث والنتائج والتوصيات ثم المراجع القانونية والأجنبية على النحو التالي:

المبحث الأول: الأساس القانوني للحماية المدنية للبيانات الشخصية في البيئة الرقمية.

المبحث الثاني: المسؤولية المدنية وآليات الحماية القضائية للبيانات الشخصية.

المبحث الأول: الأساس القانوني للحماية المدنية للبيانات الشخصية في البيئة الرقمية

تمهيد وتقسيم:

أصبحت حماية البيانات الشخصية من الموضوعات التي تحتل موقعاً متقدماً في نطاق القانون الخاص، بعد أن ارتبطت المعاملات المدنية ارتباطاً وثيقاً بالبيئة الرقمية التي تقوم في جوهرها على جمع البيانات الشخصية ومعالجتها وتخزينها وتبادلها عبر وسائل إلكترونية متطورة. وقد أدى هذا الواقع إلى تجاوز المفهوم التقليدي للخصوصية، فلم تعد الحماية القانونية تقتصر على صون الحياة الخاصة في صورتها المعروفة، وإنما امتدت لتشمل سلطة الشخص في السيطرة على بياناته الشخصية وتحديد أوجه استخدامها والجهات التي يجوز لها معالجتها والمدة التي تظل خلالها محل تداول (عبدالله علي، 2021، ص. 85).

ولهذا اتجه الفقه والتشريعات الحديثة إلى إرساء قواعد قانونية خاصة تضبط عمليات معالجة البيانات الشخصية، باعتبارها إحدى الحقوق للصيقة بالشخصية التي تفرض التزامات مدنية على عاتق القائمين بمعالجة البيانات، وتمنح صاحبها وسائل قانونية تكفل حمايتها من كل استعمال يجاوز الحدود التي رسمها القانون (الحسنات، 2025، ص. 989).

واتجهت التشريعات الأوروبية، وفي مقدمتها اللائحة العامة لحماية البيانات (GDPR)، إلى بناء إطار قانوني متكامل يقوم على اعتبار حماية البيانات الشخصية حقاً أساسياً يرتبط بكرامة الإنسان وحرية في التصرف في بياناته، وهو ما انعكس على التشريع الفرنسي بعد تعديل قانون المعلوماتية والحرية ليتوافق مع أحكام اللائحة الأوروبية (Bygrave, 2014, p. 44).

وقد نتج عن ذلك تطوير منظومة متكاملة من المبادئ القانونية التي تحكم جمع البيانات الشخصية ومعالجتها والإفصاح عنها، وربط هذه المبادئ بقواعد المسؤولية المدنية والالتزامات القانونية الواقعة على متحكم البيانات ومعالجها، مع توسيع نطاق الحقوق المقررة لصاحب البيانات بما يكفل له رقابة فعلية على مختلف صور المعالجة الإلكترونية (Kuner, 2007, p. 21).

ويقتضي الإحاطة بالأساس القانوني للحماية المدنية للبيانات الشخصية بيان المقصود بالبيانات الشخصية، وتحديد الأسس التنظيمية التي تحكم معالجتها في البيئة الرقمية، باعتبارها الإطار الذي تتحدد في ضوئه الالتزامات المدنية والضمانات القانونية المقررة لصاحب البيانات. كما يقتضي الأمر الوقوف على الحقوق المدنية التي كفلها المشرع لصاحب البيانات، باعتبارها الوسيلة القانونية التي تمكنه من ممارسة سلطته على بياناته وحمايتها من صور الاستخدام غير المشروع. ومن ثم يُقسم هذا المبحث إلى مطلبين؛ يُخصص أولهما لبيان الإطار المفاهيمي والتنظيمي لحماية البيانات الشخصية، بينما يُعنى ثانيهما بدراسة الحقوق المدنية المقررة لصاحب البيانات الشخصية في ضوء التشريعات المقارنة.

المطلب الأول: الإطار القانوني لحماية البيانات الشخصية

يقتضي تحديد الأساس القانوني للحماية المدنية للبيانات الشخصية الوقوف أولاً على الإطار المفاهيمي والتنظيمي الذي تقوم عليه هذه الحماية، إذ تتوقف سلامة تطبيق القواعد القانونية على تحديد المقصود بالبيانات الشخصية والبيئة الرقمية ونطاق الحماية التي تمتد إليها. كما يقتضي الأمر بيان المبادئ القانونية التي تحكم عمليات جمع البيانات الشخصية ومعالجتها واستخدامها، باعتبارها الضوابط التي تنشأ في ضوئها الحقوق والالتزامات المدنية للأطراف المرتبطة بمعالجة البيانات. ولهذا يُخصص هذا المطلب لفرعين؛ يُعنى أولهما ببيان مفهوم البيانات الشخصية والبيئة الرقمية ونطاق الحماية القانونية المقررة لها، بينما يتناول ثانيهما المبادئ المدنية الحاكمة لمعالجة البيانات الشخصية في ضوء أحكام اللائحة العامة لحماية البيانات بالاتحاد الأوروبي والقانون الفرنسي.

الفرع الأول: مفهوم البيانات الشخصية والبيئة الرقمية ونطاق الحماية

يتطلب تحديد نطاق الحماية المدنية للبيانات الشخصية الوقوف أولاً على المقصود بالبيانات الشخصية وتمييزها عن غيرها من البيانات، ثم بيان البيئة الرقمية التي تتم فيها عمليات المعالجة، باعتبار أن تحديد محل الحماية ونطاقها يمثل الأساس الذي تُبنى عليه الأحكام القانونية المنظمة لهذا المجال.

يستلزم تحديد المقصود بالبيانات الشخصية الوقوف على مدلولها في الفقه والتشريعات المقارنة، ثم بيان الاتجاه الذي استقر عليه التنظيم القانوني الحديث في تحديد العناصر التي تُكسب البيانات وصفها الشخصي، ولذلك يُعرض هذا الموضوع من خلال المحاور الآتية.

1- مفهوم البيانات الشخصية في الفقه القانوني

قد ترتب على التطور الرقمي إلى اتساع دائرة البيانات التي أصبحت تتمتع بالحماية القانونية، فلم تعد تقتصر على الاسم أو الرقم القومي أو محل الإقامة، وإنما امتدت لتشمل البيانات البيومترية، والبيانات الجينية، وبيانات الموقع الجغرافي، وعناوين بروتوكول الإنترنت، والمعرفات الإلكترونية، وسجلات الاستخدام الرقمي، وغيرها من البيانات التي تسمح بتحديد هوية الشخص أو تيسير التعرف عليه متى أمكن ربطها بغيرها من البيانات (عبدالله علي، 2021، ص. 85).

ويكشف هذا الاتجاه عن انتقال الحماية القانونية من حماية الوثيقة أو السجل إلى حماية المعلومة ذاتها بوصفها إحدى المظاهر الحديثة للحقوق للصيقة بالشخصية، الأمر الذي يفرض إخضاعها لقواعد القانون المدني متى ترتب على الاعتداء عليها المساس بالمركز القانوني لصاحبها أو الإضرار بمصالحه المشروعة (الحسنات، مرجع سابق، ص. 982).

وبلاحظ أن الفقه الحديث لم يعد ينظر إلى البيانات الشخصية باعتبارها مجرد محل لحق الخصوصية، وإنما اتجه إلى اعتبارها عنصراً قانونياً مستقلاً يتمتع بقيمة ذاتية تستوجب حماية خاصة، بالنظر إلى ما تمثله من امتداد للشخصية القانونية للفرد في الفضاء الرقمي. فالشخص في البيئة الرقمية لا يتعامل بذاته المادية بقدر ما يتعامل من خلال بياناته ومعرفاته الإلكترونية، وهو ما جعل السيطرة على تلك البيانات تمثل أحد مظاهر حرية الإنسان في إدارة شؤونه الخاصة وصون كيانه المعنوي (عبدالله علي، مرجع سابق، ص. 82).

ومن هذا المنطلق، اتجهت التشريعات المقارنة إلى تبني مفهوم واسع للبيانات الشخصية، يقوم على معيار إمكانية التعرف على الشخص، دون اشتراط أن تكون البيانات كافية بذاتها للكشف عن هويته، إذ يكفي أن يكون التعرف عليه ممكناً باستخدام وسائل معقولة أو من خلال الربط بين البيانات المتاحة. ويترتب على هذا المفهوم نتائج قانونية مهمة، من أبرزها اتساع نطاق الالتزامات المدنية الواقعة على عاتق القائمين بمعالجة البيانات، وامتداد الحماية إلى صور جديدة من المعلومات التي لم تكن تُعد في السابق داخلة في نطاق الحق في الخصوصية، وهو ما يعكس تطوراً ملحوظاً في فلسفة الحماية القانونية التي انتقلت

من الاهتمام بوسيلة حفظ البيانات إلى الاهتمام بالبيانات ذاتها وبالأثر القانونية الناشئة عن معالجتها (Bygrave, 2014, p. 25).

2- مفهوم البيانات الشخصية في التشريعات المقارنة

اتجهت التشريعات الحديثة إلى وضع تعريف قانوني للبيانات الشخصية يحدد نطاق الحماية المقررة لها، وذلك من خلال اعتماد معيار ارتباط المعلومة بشخص طبيعي محدد أو قابل للتحديد، وهو معيار اتسم بالمرونة لمواكبة التطورات التقنية المتلاحقة. ويقتضي بيان هذا المفهوم الوقوف على التنظيم التشريعي في النماذج المقارنة، وبصفة خاصة اللائحة الأوروبية لحماية البيانات والقانون الفرنسي، مع بيان موقف بعض التشريعات العربية الحديثة.

تُعد اللائحة العامة لحماية البيانات بالاتحاد الأوروبي ((Bygrave, 2014, p. 25)) من أكثر التنظيمات التشريعية تطوراً في مجال تحديد مفهوم البيانات الشخصية، إذ أقامت هذا المفهوم على فكرة إمكانية التعرف على الشخص الطبيعي، سواء بصورة مباشرة أو غير مباشرة، من خلال عنصر أو أكثر من العناصر المرتبطة بهويته، كالاسم أو رقم التعريف أو بيانات الموقع أو المعرف الإلكتروني أو الخصائص الجسدية أو الاقتصادية أو الاجتماعية (Haas, 2020, p. 51).

ويتميز هذا التعريف باتساع نطاقه، إذ لم يربط وصف البيانات الشخصية بطبيعة المعلومة ذاتها، وإنما بقدرتها على الوصول إلى تحديد صاحبها، وهو ما يسمح بإدخال صور مستحدثة من البيانات الرقمية ضمن نطاق الحماية القانونية كلما أصبح من الممكن ربطها بشخص معين باستخدام الوسائل المتاحة بصورة معقولة، وقد تبني المشرع الأوروبي هذا الاتجاه إدراكاً منه بأن البيئة الرقمية أوجدت أنماطاً جديدة من المعلومات لا تكشف عن هوية الفرد بصورة مباشرة، لكنها تتيح التعرف عليه من خلال عمليات التحليل والربط بين مجموعات البيانات المختلفة، الأمر الذي جعل معيار القابلية للتحديد هو الأساس الحاكم في تحديد نطاق الحماية.

ويلاحظ أن المشرع الفرنسي سار في الاتجاه ذاته عند تنظيمه لحماية البيانات الشخصية، إذ حافظ قانون المعلوماتية والملفات والحريات الفرنسي على المفهوم الواسع للبيانات الشخصية، باعتبارها كل معلومة تتعلق بشخص طبيعي محدد أو يمكن تحديده بصورة مباشرة أو غير مباشرة، سواء عن طريق رقم تعريف أو من خلال مجموعة من العناصر الخاصة بهويته (Leclerc, 2019, p. 46).

وقد أدى هذا المفهوم إلى توسيع مجال الحماية المدنية، فلم تعد البيانات الشخصية مرتبطة فقط بالمعلومات التي تكشف الاسم أو الهوية الظاهرة، وإنما امتدت إلى البيانات الناتجة عن الاستخدام الرقمي، مثل بيانات التصفح، والمعرفات الإلكترونية، وبيانات الموقع الجغرافي، وغيرها من المعلومات التي أصبحت تشكل جزءاً من الهوية الرقمية للفرد.

ويظهر من ذلك أن التشريع الفرنسي لم يتعامل مع البيانات الشخصية باعتبارها مجرد معلومات تقنية، وإنما اعتبرها مظهراً من مظاهر الشخصية الإنسانية، بما يبرر إحاطتها بضمانات قانونية تتجاوز مجرد تنظيم تداول المعلومات إلى حماية المصالح المعنوية والمالية المرتبطة بها (Lynskey, 2015, p. 55).

أما التشريعات العربية الحديثة فقد اتجهت بدورها إلى تبني مفهوم قريب من التصور الأوروبي، وإن اختلفت درجة التفصيل والتنظيم بينها. فقد عرفت بعض القوانين العربية البيانات الشخصية باعتبارها البيانات التي تؤدي إلى التعرف على الشخص الطبيعي بصورة مباشرة أو غير مباشرة، وهو اتجاه يظهر في التشريع المصري بشأن حماية البيانات الشخصية، وكذلك في التشريع العماني الذي وضع تنظيمات خاصة لحماية البيانات الشخصية في البيئة الإلكترونية (التهماني، 2015، ص. 42).

ويكشف هذا الاتجاه عن إدراك المشرع العربي لأهمية الانتقال من المفهوم التقليدي للخصوصية إلى مفهوم أكثر اتساعاً يرتبط بالسيطرة على المعلومات الشخصية والتحكم في طرق استخدامها. ومع ذلك، فإن المقارنة بين هذه التشريعات والنموذج الأوروبي تكشف أن اللائحة الأوروبية تتميز بدرجة أعلى من التفصيل، سواء من حيث تحديد أنواع البيانات المشمولة بالحماية أو من حيث بيان الالتزامات الواقعة على الجهات القائمة بالمعالجة والحقوق الممنوحة لصاحب البيانات (الأشقر، 2021، ص. 231).

الفرع الثاني: المبادئ المدنية الحاكمة لمعالجة البيانات الشخصية في ضوء اللائحة الأوروبية والقانون الفرنسي

تقوم الحماية المدنية للبيانات الشخصية في البيئة الرقمية على مجموعة من المبادئ القانونية التي تضبط مشروعية عمليات جمع البيانات ومعالجتها واستخدامها، وتحدد حدود العلاقة بين صاحب البيانات والجهة القائمة على معالجتها، وقد تبنت اللائحة العامة لحماية البيانات بالاتحاد الأوروبي والقانون الفرنسي هذه المبادئ باعتبارها أساساً للحماية القانونية، ولذلك يُقسم هذا الفرع إلى عنصرين؛ يتناول أولهما المبادئ المرتبطة بمشروعية معالجة البيانات الشخصية وضوابطها، بينما يخصص ثانيهما للمبادئ المتعلقة بالمسؤولية والشفافية وحماية حقوق صاحب البيانات.

أولاً- المبادئ المنظمة لمشروعية معالجة البيانات الشخصية وضمان سلامتها

تحدد مشروعية معالجة البيانات الشخصية من خلال مجموعة من القواعد التي تفرض على القائم بالمعالجة احترام حدود قانونية معينة، ويُعرض ذلك من خلال فقرتين؛ الأولى تتناول مبدأ المشروعية والشفافية وتحديد الغرض من المعالجة، والثانية تتعلق بمبدأ تقليل البيانات وضمان دقتها وأمنها.

1- مبدأ المشروعية والشفافية وتحديد الغرض من معالجة البيانات الشخصية

تقوم معالجة البيانات الشخصية في النظام الأوروبي على ضرورة وجود أساس قانوني يبرر تدخل الغير في بيانات الشخص، فلا يكفي مجرد القدرة التقنية على جمع البيانات، وإنما يجب أن تستند المعالجة إلى رضا صحيح من صاحب البيانات أو إلى سند قانوني يجيزها (Haas, 2020, p. 13).

وقد أخذ المشرع الفرنسي بهذا الاتجاه، حيث ربط مشروعية المعالجة باحترام حقوق الشخص وحرياته الأساسية، وبخاصة حقه في التحكم في بياناته الشخصية، وهو ما يجعل مبدأ المشروعية قيداً قانونياً على سلطة القائم بالمعالجة (Voigt & von dem Bussche, 2017, p. 92).

كما ترتبط المشروعية بمبدأ الشفافية، إذ يلتزم المسؤول عن معالجة البيانات بإحاطة صاحبها بطبيعة البيانات التي يتم جمعها، والغرض من استخدامها، والجهات التي يمكن أن تصل إليها، بما يسمح له باتخاذ موقف واع تجاه معالجة بياناته (زايد، 2024، ص. 1232).

ويكشف هذا الالتزام عن انتقال العلاقة بين صاحب البيانات ومتحكمها من مجرد علاقة تقنية إلى علاقة قانونية تقوم على الثقة والإفصاح، وهو ما يمثل ضماناً مدنية تحول دون الاستخدام غير المتوقع أو غير المشروع للبيانات (الدمياطي، 2022، ص. 69).

2- مبدأ تقليل البيانات وضمان دقتها وأمنها

لم تكتفِ القواعد الأوروبية والفرنسية بإخضاع معالجة البيانات الشخصية لوجود أساس مشروع، وإنما وضعت قيوداً تتعلق بمدى البيانات التي يجوز جمعها وطريقة الاحتفاظ بها، إذ يقتضي مبدأ تقليل البيانات ألا تمتد المعالجة إلى معلومات تتجاوز الغرض المحدد منها، حتى لا تتحول عملية الجمع إلى وسيلة للسيطرة غير المشروع على الحياة الخاصة للأفراد (Lynskey, 2015, p. 123).

ويترتب على ذلك التزام القائم بالمعالجة باختيار الوسائل الأقل تدخلاً في نطاق خصوصية الشخص، ويرتبط بذلك الالتزام بالمحافظة على دقة البيانات وسلامتها وتأمينها من مخاطر الفقد أو التغير أو الوصول غير المصرح به، حيث تتحمل الجهة القائمة بالمعالجة مسؤولية اتخاذ التدابير المناسبة لحماية البيانات طوال فترة الاحتفاظ بها.

وقد تبنى القانون الفرنسي هذا الاتجاه من خلال إلزام المسؤول عن المعالجة باتخاذ الاحتياطات اللازمة التي تمنع الإضرار بصاحب البيانات، بما يعزز الطابع المدني للحماية من خلال ترتيب آثار قانونية عند الإخلال بواجب المحافظة على البيانات (Franceschini, 2019, p. 91).

ثانياً- المبادئ المرتبطة بالمسؤولية والشفافية وحماية حقوق صاحب البيانات الشخصية

تتجاوز الحماية المدنية للبيانات الشخصية مجرد تنظيم عملية المعالجة إلى فرض مجموعة من الالتزامات القانونية التي تضمن خضوع القائمين عليها للمساءلة، مع تمكين صاحب البيانات من ممارسة حقوقه في مواجهة أي استخدام غير مشروع لمعلوماته، ولذلك يتناول هذا العنصر مبدأ المساءلة والرقابة على المعالجة، ثم يوضح أثر هذه المبادئ في تعزيز حقوق صاحب البيانات الشخصية.

1- مبدأ المساءلة والرقابة على القائم بمعالجة البيانات الشخصية

يمثل مبدأ المساءلة أحد المبادئ الأساسية التي أقرتها اللائحة العامة لحماية البيانات الأوروبية، إذ لم تعد الجهة القائمة على معالجة البيانات تلتزم بمجرد مراعاة القواعد الشكلية المتعلقة بجمع البيانات، وإنما أصبحت مطالبة بإثبات احترامها للضوابط القانونية التي تحكم المعالجة واتخاذ التدابير التي تكفل سلامتها. ويترتب على ذلك انتقال عبء المسؤولية من مجرد مراقبة التصرف بعد وقوع المخالفة إلى إلزام المسؤول عن المعالجة باتخاذ إجراءات وقائية تضمن توافق نشاطه مع المتطلبات القانونية (العتيبي، 2025، ص. 396).

وقد تبنى القانون الفرنسي هذا الاتجاه من خلال تحميل مسؤول المعالجة التزاماً مستمراً بتقييم المخاطر المرتبطة بالبيانات الشخصية، ووضع التدابير التنظيمية والتقنية المناسبة للحد من احتمالات الاعتداء عليها (Frison-Roche, 2021, p. 123). ويكتسب هذا المبدأ أهمية خاصة في المجال المدني؛ لأنه يشكل أساساً لتحديد مسؤولية متحكم البيانات عند الإخلال بواجباته، سواء ترتب على ذلك ضرر مادي أو معنوي لصاحب البيانات، بما يعزز من فعالية الحماية القانونية في البيئة الرقمية (Kuner, 2013, p. 112).

2- حماية حقوق صاحب البيانات الشخصية كأحد مرتكزات التنظيم المدني للمعالجة

أقامت اللائحة الأوروبية لحماية البيانات منظومتها القانونية على منح صاحب البيانات مجموعة من الحقوق التي تمكنه من ممارسة رقابة فعليه على بياناته الشخصية، ومن أهمها الحق في الاطلاع، وتصحيح البيانات، ومحوها، وتقييد معالجتها، والاعتراض عليها، ونقلها إلى جهة أخرى. وتكشف هذه الحقوق عن تحول مركز الفرد في العلاقة القانونية، فلم يعد مجرد محل للمعالجة الرقمية، وإنما أصبح طرفاً يتمتع بسلطة قانونية على بياناته، تمكنه من التحكم في مصيرها والاعتراض على استخدامها متى تجاوزت الحدود المشروعة (Leclerc, 2019, p. 135).

ويظهر أثر هذه الحقوق في المجال المدني من خلال ارتباطها المباشر بفكرة حماية الشخصية القانونية للفرد، إذ يؤدي الاعتداء على البيانات الشخصية إلى المساس بمصالح معنوية أو مالية تستوجب الحماية والتعويض (السحماوي، 2024، ص. 358). وقد سائر القانون الفرنسي هذا الاتجاه من خلال تعزيز دور صاحب البيانات في مواجهة الجهات القائمة بالمعالجة، وإقرار وسائل قانونية تمكنه من وقف المعالجة غير المشروعة والمطالبة بجبر الأضرار الناتجة عنها، وهو ما يؤكد أن حماية البيانات الشخصية أصبحت أحد التطبيقات الحديثة للحماية المدنية للحقوق اللصيقة بالشخصية (Lynskey, 2015, p. 206). يرى الباحث أن التشريعات العربية وإن بدأت في بناء إطار قانوني لحماية البيانات الشخصية، إلا أن أغلبها ما زال يحتاج إلى مزيد من التفصيل في بيان المبادئ المدنية الحاكمة لعمليات المعالجة مقارنة بالنموذج الأوروبي والقانون الفرنسي. فقد تميزت اللائحة الأوروبية بوضوح المبادئ المنظمة للمعالجة وربطها بمسؤولية القائم عليها، بما يحقق توازناً بين متطلبات الاقتصاد الرقمي وحماية حقوق الأفراد. ومن ثم يوصي الباحث بالاستفادة من هذا النموذج مع مراعاة الخصوصية التشريعية العربية، بما يؤدي إلى إقامة حماية مدنية أكثر فاعلية للبيانات الشخصية.

المطلب الثاني: الحقوق المدنية المقررة لصاحب البيانات الشخصية

تمثل الحقوق المدنية المقررة لصاحب البيانات الشخصية الجانب التطبيقي للحماية القانونية، إذ تمنحه مجموعة من السلطات التي تمكنه من التحكم في بياناته ومواجهة أوجه الاستخدام غير المشروع لها. ولا تقتصر هذه الحقوق على مجرد الاطلاع على البيانات أو تصحيحها، وإنما تمتد إلى تنظيم العلاقة القانونية بين صاحب البيانات والجهات القائمة على معالجتها، بما يحقق حماية فعالة لشخصيته الرقمية. ومن ثم يُقسم هذا المطلب إلى فرعين؛ يتناول أولهما الحقوق المرتبطة بالسيطرة على البيانات الشخصية، بينما يخصص ثانيهما لدراسة الضمانات المدنية لحماية الحقوق الرقمية وآليات ممارستها.

الفرع الأول: الحقوق المرتبطة بالسيطرة على البيانات الشخصية

تُعد سلطة الشخص على بياناته الشخصية من أهم مظاهر الحماية المدنية في البيئة الرقمية، إذ لم يعد صاحب البيانات مجرد طرف سلبي في عملية المعالجة، وإنما أصبح يتمتع بمجموعة من الحقوق التي تمكنه من متابعة استخدام بياناته والتحكم في نطاق تداولها. ولذلك يُقسم هذا الفرع إلى عنصرين؛ يتناول أولهما الحقوق المتعلقة بالعلم والاطلاع والتحكم في معالجة البيانات الشخصية، بينما يخصص ثانيهما لدراسة الحقوق المرتبطة بتعديل البيانات ومحوها والاعتراض على معالجتها.

أولاً- الحق في العلم والاطلاع والتحكم في معالجة البيانات الشخصية

تقوم السيطرة القانونية على البيانات الشخصية ابتداءً على تمكين صاحبها من معرفة طبيعة البيانات التي تتم معالجتها والغرض من استخدامها، وهو ما يقتضي دراسة حق العلم والاطلاع، ثم بيان أثر ذلك في منح الشخص قدرة فعليه على التحكم في عمليات المعالجة.

1- الحق في العلم بطبيعة معالجة البيانات الشخصية وأغراضها

يمثل الحق في العلم أحد الضمانات الأساسية التي أقرتها التشريعات الحديثة لصاحب البيانات الشخصية، إذ يلتزم القائم بالمعالجة بإعلام الشخص بطبيعة البيانات التي يجمعها، والأساس القانوني للمعالجة، والغاية المحددة من استخدامها (مشعل، 2017، ص. 231).

ويؤدي هذا الالتزام وظيفة مهمة في تحقيق التوازن بين مصلحة الجهات القائمة على معالجة البيانات وحق الفرد في معرفة الكيفية التي تُدار بها معلوماته الشخصية د سالم عبدالله ثاني النعيمي، قوانين خصوصية البيانات، مجلة الباحث للدراسات والأبحاث القانونية والاقتصادية والعلوم الإنسانية والشرعية، العدد (69)، 2024م، ص. 359.

وقد تبنت اللائحة الأوروبية لحماية البيانات هذا الاتجاه من خلال فرض التزامات واضحة بالإفصاح والشفافية، وسائرهما القانون الفرنسي باعتبار أن العلم السابق بالمعالجة يمثل شرطاً لازماً لسلامة رضا صاحب البيانات. أما التشريعات العربية الحديثة فقد بدأت في الأخذ بهذا الحق، إلا أن تنظيمه ما زال يحتاج إلى مزيد من التفصيل فيما يتعلق بوسائل الإخطار وحدوده وآثار الإخلال به (Haas, 2020, p. 143).

2- الحق في الاطلاع على البيانات الشخصية ومتابعة استخدامها

يمنح الحق في الاطلاع صاحب البيانات إمكانية التحقق من البيانات التي تحتفظ بها الجهات القائمة على المعالجة، ومعرفة مصادرهما وأوجه استخدامها والجهات التي تم الإفصاح لها عنها (خاطر، 2015، ص. 286).

ويكتسب هذا الحق أهمية خاصة في البيئة الرقمية؛ لأن الشخص قد يفقد السيطرة الواقعية على بياناته بمجرد انتقالها بين منصات إلكترونية متعددة، الأمر الذي يجعل الاطلاع وسيلة قانونية لإعادة بناء العلاقة بين الفرد والبيانات المرتبطة به . وقد نظم المشرع الفرنسي هذا الحق باعتباره امتداداً للحماية المدنية للحياة الخاصة، كما اعتبرته اللائحة الأوروبية وسيلة تمكن الشخص من ممارسة باقي حقوقه، كالتصحيح أو المحو أو الاعتراض. وفي المقابل، فإن التشريعات العربية التي قررت هذا الحق تحتاج إلى تعزيز آليات ممارسته بصورة أكثر وضوحاً، خاصة فيما يتعلق بمدد الاستجابة والجزاءات المترتبة على رفض الطلبات دون سند مشروع (Voigt & von dem Bussche, 2017, p. 178).

ثانياً- الحقوق المتعلقة بتعديل البيانات ومحوها والاعتراض على معالجتها

لا تكتمل سلطة الشخص على بياناته بمجرد العلم بها أو الاطلاع عليها، وإنما تمتد إلى تمكينه من تصحيح البيانات غير الدقيقة وإنهاء الاحتفاظ بها عند زوال مبررها، فضلاً عن الاعتراض على بعض صور المعالجة، وهو ما يتناولها هذا العنصر من خلال فقرتين.

1- الحق في تصحيح البيانات الشخصية ومحوها

يقوم الحق في تصحيح البيانات ومحوها على فكرة أساسية مؤداها أن استمرار الاحتفاظ بمعلومات غير صحيحة أو غير لازمة يمثل اعتداءً على المركز القانوني لصاحب البيانات، ولذلك منحت التشريعات الحديثة للشخص سلطة طلب تعديل البيانات غير الدقيقة أو حذفها متى فقدت مشروعيتها أو انتهت الغرض من معالجتها. وبعد هذا الحق من التطبيقات المدنية المباشرة لفكرة السيطرة على البيانات الشخصية (الأشقر جبور، 2018، ص. 96؛ الجندي، 2023، ص. 2789). وقد منح النظام الأوروبي لهذا الحق أهمية خاصة من خلال تنظيم "الحق في النسيان الرقمي"، الذي يسمح لصاحب البيانات بطلب محو معلوماته في حالات محددة، وهو ما تبناه القانون الفرنسي ضمن إطار حماية الحياة الخاصة. وتكشف هذه القواعد عن تطور مفهوم الحماية المدنية، بحيث أصبحت تمتد إلى حماية الشخص من الآثار المستقبلية لبقاء بياناته متداولة في البيئة الرقمية (Franceschini, 2019, p. 19).

2- الحق في الاعتراض على معالجة البيانات ونقلها

يمثل الحق في الاعتراض إحدى الوسائل القانونية التي تسمح لصاحب البيانات بمواجهة المعالجة التي تتم دون توافق مع مصالحه أو توقعاته المشروعة، إذ يستطيع الشخص طلب وقف بعض صور الاستخدام متى توافرت أسباب قانونية تبرر ذلك (العيش، 2023، ص. 314).

كما أضافت اللائحة الأوروبية حق نقل البيانات، بما يسمح للشخص باسترجاع بياناته في صورة منظمة وإعادة استخدامها لدى جهة أخرى، وهو ما يعزز قدرته على التحكم في علاقته بمقدمي الخدمات الرقمية (Lynskey, 2015, p. 227). ويكشف تنظيم هذه الحقوق عن توجه حديث في مجال الحماية المدنية، يقوم على منح الفرد سلطة إيجابية على بياناته بدلاً من الاكتفاء بحمايته من الاعتداء عليها بعد وقوعه. وقد بدأت التشريعات العربية في تبني بعض هذه الحقوق، إلا أن الحاجة ما زالت قائمة إلى تطوير تنظيمها الإجرائي بما يضمن سهولة ممارستها وفعالية الجزاءات المترتبة على مخالفتها (سيد أحمد، 2024، ص. 1393).

يرى الباحث أن التشريعات العربية قطعت خطوات مهمة في إقرار حقوق صاحب البيانات الشخصية، إلا أن الحماية المقررة ما زالت بحاجة إلى مزيد من التنظيم التفصيلي الذي يضمن ممارسة هذه الحقوق بصورة فعالة في البيئة الرقمية. ويتميز النموذج الأوروبي والفرنسي بوضوح البناء القانوني للحقوق المرتبطة بالسيطرة على البيانات، من خلال ربط حق الاطلاع والتصحيح والمحو والاعتراض بمبدأ استقلال إرادة صاحب البيانات. ومن ثم فإن تطوير التشريعات العربية يقتضي الاستفادة من هذه التجربة مع مراعاة الخصوصية القانونية والاجتماعية لكل نظام تشريعي.

الفرع الثاني: الضمانات المدنية لحماية الحقوق الرقمية وآليات ممارستها

لا تكتمل الحماية المدنية للبيانات الشخصية بمجرد تقرير الحقوق الموضوعية لصاحب البيانات، وإنما تتطلب توفير وسائل قانونية تمكنه من مواجهة الإخلال بهذه الحقوق والمطالبة بإزالة آثاره وجبر الأضرار الناتجة عنه. ومن ثم يُقسم هذا الفرع إلى عنصرين؛ يتناول أولهما المسؤولية المدنية الناشئة عن الاعتداء على البيانات الشخصية، بينما يخصص ثانيهما لآليات ممارسة الحقوق الرقمية ووسائل الحماية القضائية المقررة لصاحب البيانات.

أولاً- المسؤولية المدنية عن الاعتداء على البيانات الشخصية

تقوم الحماية المدنية للبيانات الشخصية على مساهمة كل من يخل بالالتزامات القانونية المرتبطة بمعالجتها، إذ يشكل الضرر الناتج عن الاستخدام غير المشروع للبيانات أساساً لقيام المسؤولية المدنية. ولذلك يتناول هذا العنصر أساس المسؤولية المدنية، ثم يوضح صور التعويض عن الأضرار الناشئة عن الاعتداء على البيانات الشخصية.

1- الأساس القانوني للمسؤولية المدنية عن معالجة البيانات الشخصية بصورة غير مشروعة

تستند المسؤولية المدنية في مجال حماية البيانات الشخصية إلى إخلال القائم بالمعالجة بالالتزامات التي فرضها القانون لضمان مشروعية جمع البيانات واستخدامها والاحتفاظ بها. ويكفي لقيام هذه المسؤولية ثبوت مخالفة القواعد المنظمة للمعالجة متى ترتب عليها ضرر لصاحب البيانات، سواء تمثل هذا الضرر في المساس بحياته الخاصة أو فقدان السيطرة على معلوماته الشخصية أو استغلالها في غير الغرض المحدد لها (السحماوي، 2024، ص. 432؛ زايد، 2024، ص. 1253)

وقد تبنت اللائحة الأوروبية لحماية البيانات هذا الاتجاه من خلال تحميل المسؤول عن المعالجة التزاماً قانونياً باتخاذ التدابير اللازمة لضمان سلامة البيانات، بينما سار القانون الفرنسي في الاتجاه ذاته بإقامة مسؤولية تقوم على أساس الإخلال بالالتزامات المهنية والتنظيمية المرتبطة بمعالجة البيانات. ويكشف ذلك عن انتقال الحماية من مجرد حماية الحق بعد الاعتداء عليه إلى إلزام الجهات القائمة على المعالجة باتخاذ وسائل وقائية تحول دون وقوع الضرر (Haas, 2021, p. 134)

2- التعويض المدني عن الأضرار المترتبة على الاعتداء على البيانات الشخصية

يمثل التعويض المدني الوسيلة الأساسية لجبر الأضرار التي تلحق بصاحب البيانات نتيجة المعالجة غير المشروعة أو إفشاء المعلومات الشخصية أو استخدامها خارج النطاق المسموح به. وتتميز الأضرار الناتجة عن الاعتداء على البيانات بطبيعتها الخاصة، إذ قد تكون أضراراً مادية تتمثل في خسارة مالية مباشرة، أو أضراراً معنوية تمس اعتبار الشخص وخصوصيته وثقته في التعاملات الرقمية (أبو خمرة، 2021، ص. 76)

وقد اتجه القضاء والفقه في الأنظمة المقارنة إلى الاعتراف بإمكانية التعويض عن الأضرار المعنوية المرتبطة بفقدان السيطرة على البيانات الشخصية، باعتبار أن البيانات تمثل امتداداً للشخصية القانونية للفرد. ويُعد هذا الاتجاه أكثر ملاءمة لطبيعة البيئة الرقمية، حيث قد يتحقق الضرر بمجرد تداول البيانات أو استخدامها دون انتظار تحقق خسارة مالية محددة (Frison-

Roche, 2020, p. 114)

ثانياً- آليات ممارسة الحقوق الرقمية ووسائل الحماية القضائية

تحتاج الحقوق الرقمية إلى وسائل إجرائية تكفل انتقالها من نطاق الاعتراف القانوني إلى نطاق الممارسة الفعلية، وهو ما يستلزم بيان الآليات التي يستطيع من خلالها صاحب البيانات تقديم طلباته ومتابعتها، فضلاً عن تحديد دور القضاء في توفير الحماية عند الإخلال بهذه الحقوق.

1- الآليات الإجرائية لممارسة الحقوق الرقمية أمام الجهات القائمة على المعالجة

أقرت التشريعات الحديثة مجموعة من الوسائل التي تمكن صاحب البيانات من ممارسة حقوقه بصورة مباشرة أمام الجهات المسؤولة عن المعالجة، من خلال تقديم طلبات الاطلاع أو التصحيح أو المحو أو الاعتراض، مع إلزام تلك الجهات بالرد خلال مدد محددة وبصورة تتفق مع متطلبات الشفافية. وتكتسب هذه الآليات أهمية خاصة في البيئة الرقمية؛ لأنها تمنح الشخص وسيلة سريعة للتدخل قبل تفاقم آثار الاستخدام غير المشروع لبياناته (الوادي، 2025، ص. 65؛ البلوشي، 2021، ص. 705).

ويتميز التنظيم الأوروبي بوضوح الإجراءات المتعلقة بممارسة الحقوق الرقمية، إذ حدد نطاق الطلبات وطرق تقديمها والتزامات المسؤول عن المعالجة تجاهها، وهو ما انعكس على التشريع الفرنسي الذي تبنى آليات مشابهة. أما التشريعات العربية، فرغم إقرارها بعدد من هذه الحقوق، فإنها تحتاج إلى مزيد من التنظيم الإجرائي لضمان سهولة ممارستها وفعاليتها الاستجابة لها (Franceschini، 2019، p. 206).

2- الحماية القضائية للحقوق الرقمية ودورها في ضمان فعالية الحماية المدنية

يمثل اللجوء إلى القضاء الضمانة النهائية لحماية الحقوق الرقمية متى تعذر الوصول إلى حل مباشر مع الجهة القائمة على معالجة البيانات، إذ يستطيع صاحب البيانات طلب وقف المعالجة غير المشروعة أو إزالة آثارها أو الحصول على التعويض المناسب عن الأضرار التي لحقت به. ويكتسب القضاء المدني أهمية خاصة في هذا المجال؛ لأن طبيعة الأضرار المرتبطة بالبيانات الشخصية غالباً ما تتصل بحقوق معنوية تستوجب تقديراً قانونياً دقيقاً (قنطار، 2025، ص. 265؛ رفرافي، 2025، ص. 386).

وقد أظهر التشريع الأوروبي والفرنسي اهتماماً واضحاً بتوفير وسائل قضائية فعالة لحماية صاحب البيانات، سواء من خلال الدعاوى الفردية أو آليات التمثيل الجماعي، بما يعزز الثقة في المعاملات الرقمية. ومن ثم فإن تطوير الحماية المدنية في

التشريعات العربية يتطلب تعزيز الدور القضائي وتوفير إجراءات تتلاءم مع خصوصية المنازعات الرقمية وسرعة تطورها (Lynskey, 2020, p. 186).

يرى الباحث أن التشريعات العربية، رغم إقرارها لوسائل متعددة لحماية الحقوق الرقمية، ما زالت بحاجة إلى تطوير قواعد المسؤولية المدنية وآليات إنفاذها بما يتناسب مع خصوصية الاعتداءات الواقعة على البيانات الشخصية. ويتميز التنظيم الأوروبي والفرنسي بوضوح الأساس القانوني للمساءلة وربط التعويض بخصوصية الضرر الرقمي، بما يوفر حماية أكثر فاعلية لصاحب البيانات. ومن ثم يقترح الباحث الاستفادة من هذا النموذج مع تطوير آليات قضائية عربية متخصصة تضمن سرعة حماية الحقوق الرقمية وجبر الأضرار الناشئة عن انتهاكها.

المبحث الثاني: المسؤولية المدنية وآليات الحماية القضائية للبيانات الشخصية

أدى اتساع نطاق الاعتماد على الوسائل الرقمية وتزايد عمليات جمع البيانات الشخصية ومعالجتها إلى ظهور صور متعددة من الاعتداء على هذه البيانات، الأمر الذي استلزم تجاوز مرحلة الاعتراف بالحقوق المرتبطة بها إلى تقرير وسائل قانونية تكفل مساءلة القائمين على المعالجة عند الإخلال بالتزاماتهم (السحماوي، 2024، ص. 336-452). وتكتسب المسؤولية المدنية في هذا المجال أهمية خاصة، باعتبارها الأداة القانونية التي تحقق التوازن بين متطلبات الاستفادة من البيانات في البيئة الرقمية وبين ضرورة صون مصالح أصحابها، سواء من خلال منع الاستخدام غير المشروع أو جبر الأضرار المترتبة عليه (التهامي، 2015، ص. 435).

وقد اتجهت اللائحة العامة لحماية البيانات بالاتحاد الأوروبي والقانون الفرنسي إلى بناء نظام متكامل للمساءلة يقوم على التزامات محددة تقع على عاتق المسؤول عن المعالجة، مع إقرار وسائل فعالة للتعويض عن الأضرار المادية والمعنوية التي تصيب صاحب البيانات. كما سارت بعض التشريعات العربية الحديثة في الاتجاه ذاته، من خلال وضع قواعد خاصة لمسؤولية حائز البيانات، وإن تفاوتت فيما بينها من حيث درجة التفصيل ومدى توفير ضمانات قضائية متخصصة (Haas, 2020, p. 189).

ويُعد تحديد آليات الحماية القضائية المدنية للبيانات الشخصية مرحلة مكتملة لبناء النظام القانوني للحماية، إذ إن تقرير المسؤولية لا يحقق غايته ما لم تقتزن به وسائل إجرائية تمكن صاحب البيانات من اللجوء إلى القضاء وطلب وقف الاعتداء أو إزالة آثاره أو الحصول على التعويض المناسب. ومن ثم يُقسم هذا المبحث إلى مطلبين؛ يتناول أولهما المسؤولية المدنية الناشئة عن الإخلال بحماية البيانات الشخصية، من خلال بيان أساسها القانوني وصورها وآثارها، بينما يخصص ثانيهما لدراسة وسائل الحماية القضائية المدنية في منازعات البيانات الشخصية، وبيان مدى ملائمة الآليات القضائية القائمة لطبيعة المنازعات الرقمية وخصوصيتها.

المطلب الأول: المسؤولية المدنية الناشئة عن الإخلال بحماية البيانات الشخصية

تُعد المسؤولية المدنية عن الإخلال بحماية البيانات الشخصية الوسيلة القانونية التي تضمن مساءلة الجهات القائمة على المعالجة عند تجاوز الحدود المقررة لاستخدام البيانات أو الإخلال بالتزامات المفروضة عليها. وتتعدد صور هذه المسؤولية بحسب مصدر الالتزام القانوني الذي تم مخالفته، فقد تنشأ عن إخلال بالتزامات تعاقدية تربط صاحب البيانات بمتحكم البيانات أو معالجها، وقد تقوم على أساس الإخلال بالواجب العام بعدم الإضرار بالغير. ومن ثم يُقسم هذا المطلب إلى فرعين؛ يتناول أولهما المسؤولية العقدية لمتحكم البيانات ومعالجها، بينما يخصص ثانيهما لدراسة المسؤولية التقصيرية والتعويض عن أضرار انتهاك البيانات الشخصية.

الفرع الأول: المسؤولية العقدية لمتحكم البيانات ومعالجها

تقوم المسؤولية العقدية في مجال حماية البيانات الشخصية متى ارتبط متحكم البيانات أو معالجها بصاحب البيانات بعلاقة تعاقدية تفرض على كل منهما التزامات محددة، ويترتب على الإخلال بهذه الالتزامات قيام المسؤولية متى توافرت شروطها القانونية. ولبيان ذلك، يُقسم هذا الفرع إلى عنصرين؛ يتناول أولهما الأساس القانوني لقيام المسؤولية العقدية والتزامات أطرافها، بينما يخصص ثانيهما لآثار الإخلال بهذه الالتزامات ووسائل جبر الضرر الناشئ عنها.

أولاً- الأساس القانوني للمسؤولية العقدية لمتحكم البيانات ومعالجها

يتحدد نطاق المسؤولية العقدية من خلال الالتزامات التي يربتها العقد على متحكم البيانات ومعالجها، ويقضي ذلك ببيان الطبيعة القانونية للعلاقة التعاقدية، ثم تحديد أهم الالتزامات التي يترتب على الإخلال بها قيام المسؤولية العقدية.

1- الطبيعة التعاقدية للعلاقة بين صاحب البيانات ومتحكم البيانات

تنشأ العلاقة بين صاحب البيانات ومتحكم البيانات في كثير من التطبيقات الرقمية بمناسبة إبرام عقد لتقديم خدمة إلكترونية أو تنفيذ معاملة رقمية، الأمر الذي يجعل الالتزامات المتعلقة بحماية البيانات جزءاً من الالتزامات العقدية التي يتعين تنفيذها بحسن نية. ويترتب على ذلك التزام متحكم البيانات باحترام الغرض المتفق عليه في جمع البيانات، والامتناع عن استخدامها

أو الإفصاح عنها خارج الحدود التي يجيزها العقد أو القانون، باعتبار أن الإخلال بهذه الالتزامات يمثل إخلالاً بالتوازن العقدي الذي قامت عليه إرادة الطرفين (السحماوي، 2024، ص. 374؛ التهامي، 2015، ص. 415). وقد عززت اللائحة العامة لحماية البيانات هذا الاتجاه عندما أوجبت أن تكون معالجة البيانات قائمة على أساس قانوني واضح، مع تحديد حقوق والتزامات كل من متحكم البيانات ومعالجها، وهو ما انعكس على القانون الفرنسي الذي أولى عناية خاصة بالالتزامات العقدية المرتبطة بحماية البيانات الرقمية، بما يوفر حماية مدنية تتناسب مع طبيعة العلاقات التعاقدية الحديثة (Haas, 2020, p. 183)

2- الالتزامات العقدية لمتحكم البيانات ومعالجها وأثر الإخلال بها

تتعدد الالتزامات العقدية التي يتحملها متحكم البيانات ومعالجها، وتشمل المحافظة على سرية البيانات، واتخاذ التدابير الكفيلة بحمايتها، والاقتصار على معالجتها في حدود الأغراض التي أنشئت العلاقة التعاقدية من أجلها، فضلاً عن تمكين صاحب البيانات من ممارسة حقوقه المقررة قانوناً. ويُعد تنفيذ هذه الالتزامات وفق معيار العناية المهنية أحد المقومات الأساسية لاستقرار التعاملات الرقمية (الدمياطي، 2022، ص. 13-138؛ عبدالله علي، 2021، ص. 73-118). ويؤدي الإخلال بأي من هذه الالتزامات إلى ترتيب المسؤولية العقدية متى ثبتت علاقة سببية بين الإخلال والضرر الذي أصاب صاحب البيانات، سواء تمثل ذلك في كشف البيانات لغير المصرح لهم أو استخدامها في غير الغرض المشروع. وقد اتجه القضاء والفقه المقارن إلى تشديد الالتزام الواقع على متحكم البيانات بالنظر إلى ما يملكه من سلطة فعلية على البيانات محل المعالجة، وهو اتجاه يحقق قدراً أكبر من الحماية المدنية في البيئة الرقمية (Voigt & von dem Bussche, 2017, p. 259).

ثانياً- شروط قيام المسؤولية العقدية وآثار الإخلال بالالتزامات حماية البيانات الشخصية

تتطلب مساءلة متحكم البيانات أو معالجها عقدياً توافر مجموعة من الشروط القانونية التي تربط بين الالتزام العقدي والإخلال به والضرر الناتج عنه، كما يترتب على تحقق هذه المسؤولية آثار مدنية تهدف إلى إعادة التوازن بين أطراف العلاقة القانونية. ولذلك يتناول هذا العنصر شروط قيام المسؤولية العقدية، ثم يوضح الآثار المترتبة على الإخلال بالالتزامات العقدية المتعلقة بحماية البيانات الشخصية.

1- شروط قيام المسؤولية العقدية في مجال معالجة البيانات الشخصية

تقوم المسؤولية العقدية لمتحكم البيانات أو معالجها متى وجدت علاقة تعاقدية صحيحة تجمعها بصاحب البيانات، وكان أحد الالتزامات الناشئة عنها قد تعرض للإخلال، سواء تعلق ذلك بالالتزام بالمحافظة على سرية البيانات أو الالتزام بقصر استخدامها على الغرض المحدد لها. ويشترط إلى جانب ذلك تحقق ضرر يصيب صاحب البيانات، مع قيام رابطة سببية بين المخالفة العقدية والضرر الناتج عنها، باعتبار أن مجرد مخالفة الالتزام دون ترتب أثر ضار لا يكفي وحده للحكم بالتعويض (زايد، 2024، ص. 1225؛ النعيمي، 2024، ص. 361).

وتتميز المسؤولية العقدية في مجال البيانات الشخصية بخصوصية ترتبط بطبيعة محل الالتزام، فالضرر قد لا يظهر في صورة خسارة مالية مباشرة، وإنما قد يتمثل في فقدان السيطرة على المعلومات الشخصية أو المساس بالاعتبار الشخصي والثقة في التعاملات الرقمية. ولهذا اتجهت التشريعات المقارنة إلى توسيع مفهوم الضرر القابل للتعويض، بما يتلاءم مع الطبيعة غير المادية لكثير من الاعتداءات الواقعة على البيانات الشخصية (Frison-Roche, 2020, p. 134).

2- آثار الإخلال بالالتزامات العقدية المتعلقة بحماية البيانات الشخصية

يترتب على ثبوت المسؤولية العقدية لمتحكم البيانات أو معالجها مجموعة من الآثار القانونية التي تستهدف حماية المركز القانوني لصاحب البيانات، وفي مقدمتها الالتزام بإزالة آثار المخالفة والتعويض عن الأضرار التي ترتبت عليها. ويشمل ذلك التعويض عن الأضرار المادية الناتجة عن إساءة استخدام البيانات، فضلاً عن الأضرار المعنوية المرتبطة بالمساس بالخصوصية أو فقدان الثقة في البيئة الرقمية (مشعل، 2017، ص. 86؛ العيش، 2023، ص. 235).

ويمتد أثر المسؤولية العقدية كذلك إلى إمكانية إلزام المسؤول عن المعالجة باتخاذ التدابير اللازمة لمنع استمرار الاعتداء أو تكراره، وهو ما يتفق مع طبيعة الحماية المدنية الحديثة التي لا تقتصر على جبر الضرر بعد وقوعه، وإنما تهدف أيضاً إلى الحد من آثاره المستقبلية. ويظهر في هذا المجال تميز التنظيم الأوروبي والفرنسي بربط الالتزامات العقدية بواجبات قانونية محددة، بما يحقق حماية أكثر فاعلية مقارنة ببعض التشريعات العربية التي ما زالت بحاجة إلى مزيد من التفصيل في تنظيم هذه الآثار (Leclerc, 2021, p. 198).

يرى الباحث أن التنظيم العقدي لحماية البيانات الشخصية يمثل أحد أهم الوسائل المدنية لضمان احترام إرادة صاحب البيانات، إلا أن التشريعات العربية ما زالت تحتاج إلى بناء تصور أكثر وضوحاً لمسؤولية متحكم البيانات ومعالجها في العلاقات الرقمية. ويتميز النموذجان الأوروبي والفرنسي بربط الالتزامات العقدية بمبدأ المساءلة وتحديد آثار الإخلال بها بصورة

دقيقة، بما يوفر حماية متقدمة لصاحب البيانات. ومن ثم فإن تطوير القواعد العربية يقتضي الاستفادة من هذا البناء مع مواظمته مع خصوصية النظام القانوني العربي.

الفرع الثاني: المسؤولية التقصيرية والتعويض عن أضرار انتهاك البيانات الشخصية

تقوم المسؤولية التقصيرية في مجال حماية البيانات الشخصية كلما وقع الاعتداء على البيانات خارج نطاق علاقة تعاقدية، أو تجاوز المسؤول عن المعالجة الحدود التي يفرضها القانون بما يترتب عليه الإضرار بصاحب البيانات أو بالغير. وتكتسب هذه المسؤولية أهمية متزايدة في البيئة الرقمية؛ لانتساع صور الاعتداء على البيانات الشخصية وتعدد الجهات القائمة بها. ولذلك يُقسم هذا الفرع إلى عنصرين؛ يتناول أولهما أساس المسؤولية التقصيرية عن انتهاك البيانات الشخصية وشروط قيامها، بينما يخصص ثانيهما للتعويض المدني عن الأضرار الناشئة عن هذا الانتهاك وتقدير نطاقه.

أولاً- أساس المسؤولية التقصيرية عن انتهاك البيانات الشخصية وشروط قيامها

تستند المسؤولية التقصيرية إلى الإخلال بالواجب القانوني العام المتمثل في عدم الإضرار بالغير، ويقتضي تطبيقها في مجال البيانات الشخصية بيان الأساس الذي تقوم عليه، ثم تحديد الشروط اللازمة لانعقادها في ضوء خصوصية البيئة الرقمية.

1- الأساس القانوني للمسؤولية التقصيرية عن انتهاك البيانات الشخصية

تتعدّد المسؤولية التقصيرية متى أخل متحكم البيانات أو معالجها بالواجب القانوني المفروض عليه في حماية البيانات الشخصية، دون أن تربطه بالمضروور علاقة تعاقدية، أو متى تجاوز حدود الحقوق التي خولها له القانون فألحق ضرراً بالغير. ويستند هذا الأساس إلى القواعد العامة في المسؤولية المدنية التي تقضي بالتزام كل من يرتكب فعلاً غير مشروع بتعويض الضرر المترتب عليه، وهو ما يتلاءم مع الاعتداءات الرقمية التي قد تصيب أشخاصاً لا تجمعهم بالمعتدي رابطة عقدية (القطاطشة، 2022، ص. 147؛ رفرافي، 2025، ص. 373).

وتظهر خصوصية هذا النوع من المسؤولية في أن الفعل غير المشروع قد يتمثل في جمع البيانات دون مسوغ قانوني، أو إفشائها، أو تداولها، أو الاحتفاظ بها بعد انتهاء الغرض من معالجتها، وهي صور أصبح لها أثر مباشر في المساس بالحقوق الصليقة بالشخصية. وقد اتجهت اللائحة الأوروبية والقانون الفرنسي إلى إقرار مسؤولية واسعة عن هذه الأفعال، بما يكفل حماية فعالة للبيانات الشخصية بصرف النظر عن وجود علاقة تعاقدية بين أطراف النزاع (Féral-Schuhl, 2022, p. 434).

2- شروط قيام المسؤولية التقصيرية في منازعات البيانات الشخصية

يشترط لقيام المسؤولية التقصيرية توافر الخطأ والضرر وعلاقة السببية، غير أن تطبيق هذه الأركان في منازعات البيانات الشخصية يثير اعتبارات خاصة ترتبط بطبيعة الاعتداء الرقمي وصعوبة إثبات آثاره في بعض الحالات. ولهذا اتجه الفقه الحديث إلى التوسع في مفهوم الخطأ ليشمل الإخلال بالالتزامات القانونية والتنظيمية المفروضة على القائمين بمعالجة البيانات، متى أدى ذلك إلى المساس بحقوق الأفراد (حسن، 2025، ص. 14؛ أبو خمر، 2021، ص. 27). ويمتد مفهوم الضرر في هذا المجال ليشمل الأضرار المادية والأدبية على السواء، إذ قد يتمثل الضرر في خسارة مالية، كما قد ينشأ عن المساس بالسمعة أو الخصوصية أو حرية الشخص في التحكم ببياناته. ويقتضي الحكم بالتعويض إثبات الصلة بين الفعل غير المشروع والضرر، مع مراعاة الطبيعة الفنية للبيانات الرقمية وما تفرضه من وسائل حديثة لإثبات عناصر المسؤولية (Byk, 2021, p. 116).

ثانياً- التعويض المدني عن أضرار انتهاك البيانات الشخصية

يترتب على ثبوت المسؤولية التقصيرية التزام المسؤول بجبر الضرر الذي أصاب صاحب البيانات، ويقتضي ذلك بيان صور الضرر القابل للتعويض، ثم تحديد الأسس التي يسترشد بها القضاء في تقدير التعويض في المنازعات المتعلقة بالبيانات الشخصية.

1- صور الضرر القابل للتعويض في منازعات البيانات الشخصية

يتخذ الضرر الناجم عن انتهاك البيانات الشخصية صوراً متعددة، فقد يكون ضرراً مادياً يتمثل في خسارة مالية أو استغلال غير مشروع للبيانات، كما قد يكون ضرراً أدبياً يصيب الحياة الخاصة أو السمعة أو الشعور بالأمان الرقمي. ويؤكد هذا التنوع أن البيانات الشخصية أصبحت تمثل قيمة قانونية مستقلة، وأن الاعتداء عليها قد يخل بمصالح تتجاوز الجانب المالي إلى الحقوق الملازمة للشخصية (قنطار، 2025، ص. 261-281؛ الجندي، 2023، ص. 2779).

وأخذت التشريعات الأوروبية بهذا الاتجاه عندما أقرت حق المتضرر في المطالبة بالتعويض عن الأضرار المادية وغير المادية، وهو ما انعكس على التطبيق القضائي الفرنسي الذي اعترف بالتعويض عن المساس بالخصوصية الرقمية حتى في غياب خسارة مالية مباشرة، متى ثبت وقوع ضرر حقيقي أصاب صاحب البيانات (Bazin-Beust, 2021, p. 165).

2- تقدير التعويض وضمان فعاليته في البيئة الرقمية

يراعي القضاء عند تقدير التعويض طبيعة البيانات محل الاعتداء، ومدى جسامته المخالفة، والآثار التي ترتبت عليها بالنسبة إلى صاحب البيانات، مع الأخذ في الاعتبار استمرار الضرر وإمكانية انتشار البيانات عبر الوسائط الرقمية. وبمنح ذلك القاضي سلطة تقديرية واسعة تمكنه من تحقيق جبر كامل للضرر وفقاً لظروف كل حالة (سيد أحمد، 2024، ص. 1389-1442؛ غالب، 2019، ص. 52).

ويظهر تميز اللائحة الأوروبية والقانون الفرنسي في عدم قصر الحماية على التعويض المالي، وإنما إجازة اتخاذ تدابير تكفل إزالة آثار الاعتداء ووقف استمراره، بما يحقق حماية مدنية أكثر ملاءمة لخصوصية المنازعات الرقمية. ويستدعي هذا الاتجاه تطوير التشريعات العربية بما يسمح للقضاء بالجمع بين التعويض المالي والتدابير القضائية الكفيلة بإعادة التوازن إلى المركز القانوني للمتضرر (Kuner, 2022, p. 315).

يرى الباحث أن التشريعات العربية ما زالت تعتمد بصورة أساسية على القواعد العامة للمسؤولية التقصيرية في مواجهة الاعتداءات على البيانات الشخصية، مع وجود محاولات حديثة لوضع تنظيمات خاصة لهذه المسؤولية. ويتميز النموذج الأوروبي والفرنسي بوجود قواعد أكثر تحديداً بشأن مسؤولية القائمين على معالجة البيانات، واتساع نطاق التعويض ليشمل الأضرار المادية والمعنوية المرتبطة بالخصوصية الرقمية. ومن ثم فإن تطوير التشريعات العربية يقتضي بناء نظام مدني متخصص يراعي طبيعة الضرر الرقمي وخصوصية البيانات باعتبارها امتداداً لشخصية الفرد القانونية.

المطلب الثاني: وسائل الحماية القضائية المدنية في منازعات البيانات الشخصية

تنوقف فعالية الحماية المدنية للبيانات الشخصية على مدى توافر وسائل قضائية قادرة على منع الاعتداء قبل وقوعه، واحتواء آثاره عند تحققه، وتمكين صاحب البيانات من استرداد مركزه القانوني وجبر ما لحقه من ضرر. وقد أولت اللائحة العامة لحماية البيانات بالاتحاد الأوروبي والقانون الفرنسي عناية خاصة بهذه الوسائل، من خلال تقرير تدابير وقائية وعلاجية تتلاءم مع خصوصية البيئة الرقمية، مع توفير ضمانات إجرائية تكفل سرعة التدخل القضائي وفعاليته. كما اتجهت بعض التشريعات العربية إلى إقرار صور متعددة للحماية القضائية، وإن تفاوتت في مدى اكتمال تنظيمها واستيعابها لخصوصية منازعات البيانات الشخصية. ومن ثم يُقسم هذا المطلب إلى فرعين؛ يتناول أولهما التدابير القضائية الوقائية والعلاجية في القانون الفرنسي واللائحة الأوروبية، بينما يخصص ثانيهما لتقييم التشريعات العربية وبيان مقترحات تطوير الحماية المدنية في ضوء التجربة الأوروبية.

الفرع الأول: التدابير القضائية الوقائية والعلاجية في القانون الفرنسي واللائحة الأوروبية

لا تقتصر الحماية القضائية للبيانات الشخصية على الفصل في النزاع بعد وقوع الاعتداء، وإنما تمتد إلى تمكين القضاء من اتخاذ تدابير تحول دون استمرار المخالفة أو تفاقم آثارها، فضلاً عن تقرير الوسائل الكفيلة بإعادة الحقوق إلى أصحابها بعد تحقق الضرر. وقد أولت اللائحة الأوروبية والقانون الفرنسي هذا الجانب اهتماماً خاصاً، من خلال الجمع بين التدابير الوقائية والتدابير العلاجية في إطار حماية مدنية متكاملة. ولذلك يُقسم هذا الفرع إلى عنصرين؛ يتناول أولهما التدابير القضائية الوقائية لحماية البيانات الشخصية، بينما يخصص ثانيهما للتدابير القضائية العلاجية وآثارها القانونية.

أولاً- التدابير القضائية الوقائية لحماية البيانات الشخصية

يقصد بالتدابير القضائية الوقائية الوسائل التي يتدخل بها القضاء لمنع وقوع الاعتداء على البيانات الشخصية أو الحد من آثاره قبل استفحالها، ويتناول هذا العنصر أوامر وقف المعالجة غير المشروعة، ثم التدابير المستعجلة الرامية إلى المحافظة على الحقوق الرقمية.

1- أوامر وقف معالجة البيانات الشخصية المخالفة للقانون

تملك الجهات القضائية، في ظل اللائحة العامة لحماية البيانات والقانون الفرنسي، سلطة إصدار أوامر بوقف معالجة البيانات الشخصية متى تبين أن المعالجة تفتقر إلى السند القانوني أو تجاوزت الغرض الذي جُمعت من أجله البيانات. ويستند هذا الاختصاص إلى فكرة الوقاية من الضرر، إذ يؤدي استمرار المعالجة غير المشروعة إلى اتساع نطاق الاعتداء وتعذر تدارك آثاره في كثير من الحالات (مشعل، 2017، ص. 248؛ التهامي، 2015، ص. 419).

وتتميز هذه الأوامر بطابعها الوقائي مع احتفاظها بأثر عملي بالغ، لأنها تحول دون استمرار تداول البيانات أو استغلالها إلى حين الفصل في أصل النزاع. ويؤكد ذلك أن الحماية القضائية الحديثة لم تعد تقتصر على التعويض اللاحق، وإنما أصبحت تمتد إلى منع الاعتداء قبل أن يستقر أثره القانوني أو الواقعي (Haas, 2020, p. 265).

2- التدابير القضائية المستعجلة للمحافظة على الحقوق الرقمية

يؤدي القضاء المستعجل دوراً مهماً في توفير حماية وقتية لصاحب البيانات كلما توافرت حالة استعجال يخشى معها من استمرار الاعتداء أو تعذر إزالة آثاره مستقبلاً. ويشمل ذلك الأمر بوقف نشر البيانات، أو حجب الوصول إليها، أو تعليق

بعض عمليات المعالجة إلى حين الفصل في موضوع النزاع، وهي تدابير تتلاءم مع الطبيعة المتسارعة للبيئة الرقمية (خاطر، 2015، ص. 349؛ العيش، 2023، ص. 321).

وقد عزز القانون الفرنسي هذا الاتجاه بمنح القضاء سلطة اتخاذ إجراءات تحفظية كلما ظهر خطر يهدد الحقوق المرتبطة بالبيانات الشخصية، وهو ما يتفق مع فلسفة اللائحة الأوروبية القائمة على توفير حماية فعالة وسريعة قبل استفحال الضرر، بما يحقق التوازن بين حرية تداول البيانات وصون الحقوق الشخصية (Frison-Roche, 2021, p. 225).

ثانياً- التدابير القضائية العلاجية وآثارها القانونية

إذا وقع الاعتداء على البيانات الشخصية وتعذر منعه، انتقلت الحماية القضائية إلى مرحلة إزالة آثار المخالفة وجبر الضرر، ويقتضي ذلك بيان سلطات القضاء في إعادة الأوضاع إلى ما كانت عليه، ثم بيان دوره في تنفيذ الأحكام وضمان فعاليتها.

1- السلطات القضائية في إزالة آثار الاعتداء على البيانات الشخصية

يمتلك القضاء المدني سلطة إصدار الأحكام الكفيلة بإزالة الآثار القانونية والواقعية المترتبة على الاعتداء على البيانات الشخصية، ومن ذلك الأمر بمحو البيانات محل النزاع، أو تصحيحها، أو تقييد معالجتها، أو إلزام المسؤول باتخاذ الإجراءات التي تكفل وقف استمرار المخالفة. ويستند هذا الاتجاه إلى أن الحماية المدنية لا تتحقق بمجرد الاعتراف بوقوع الخطأ، وإنما تقتضي إعادة المركز القانوني لصاحب البيانات إلى أقرب صورة ممكنة (الأشقر جبور، 2018، ص. 109؛ السحموي، 2024، ص. 435).

وتكشف أحكام اللائحة الأوروبية والقانون الفرنسي عن اتساع نطاق هذه السلطة القضائية، بحيث أصبح للقاضي دور إيجابي في إنهاء آثار المعالجة غير المشروعة، وهو ما يمنح الحماية المدنية فعالية تتجاوز مجرد التعويض المالي إلى إزالة مصدر الاعتداء ذاته (Leclerc, 2021, p. 237).

2- تنفيذ الأحكام القضائية وضمان فعالية الحماية المدنية

تنوقف القيمة العملية للأحكام القضائية على سرعة تنفيذها وقدرتها على إنهاء آثار الاعتداء على البيانات الشخصية، ولذلك اتجهت الأنظمة المقارنة إلى تدعيم وسائل التنفيذ بما يضمن الامتثال الفوري للأحكام المتعلقة بوقف المعالجة أو محو البيانات أو إزالة آثار نشرها. ويسهم ذلك في الحد من استمرار الضرر، ولا سيما في البيئة الرقمية التي تتسم بسرعة تداول المعلومات (زايد، 2024، ص. 1256؛ سيد أحمد، 2024، ص. 1397).

ويتميز النموذج الفرنسي بمرونة الوسائل التي تضمن تنفيذ الأحكام المدنية المتعلقة بحماية البيانات الشخصية، مع إمكان الجمع بين التدابير التنفيذية والجزاءات المالية عند الامتناع عن التنفيذ، وهو اتجاه يعزز فعالية الحماية القضائية ويحقق الغاية المقصودة من إقرار الحقوق الرقمية (Kuner, 2013, p. 329).

الفرع الثاني: تقييم التشريعات العربية ومقترحات تطوير الحماية المدنية في ضوء التجربة الأوروبية

تكشف المقارنة بين التشريعات العربية والتنظيم الأوروبي لحماية البيانات الشخصية عن وجود تطور تشريعي ملحوظ في عدد من الأنظمة العربية، إلا أن هذا التطور ما زال يتفاوت من حيث شمول الحماية المدنية وآليات إنفاذها. ويقتضي ذلك الوقوف على أبرز أوجه القصور التي تعترض التنظيم العربي، ثم بيان السبل الكفيلة بتطويره في ضوء الحلول التي استقرت عليها اللائحة الأوروبية والقانون الفرنسي. ولذلك يُقسم هذا الفرع إلى عنصرين؛ يتناول أولهما التقييم المقارن للتشريعات العربية في مجال الحماية المدنية للبيانات الشخصية، بينما يخصص ثانيهما مقترحات تطوير هذه الحماية في ضوء التجربة الأوروبية.

أولاً- التقييم المقارن للتشريعات العربية في مجال الحماية المدنية للبيانات الشخصية

يتطلب الوقوف على كفاءة التشريعات العربية بيان مدى استجابتها لمتطلبات الحماية المدنية للبيانات الشخصية، ثم مقارنتها بالحلول التي تبنتها اللائحة الأوروبية والقانون الفرنسي، بما يسمح بتحديد مواطن القوة والجوانب التي ما زالت بحاجة إلى تطوير.

1- مظاهر التطور في التشريعات العربية المنظمة لحماية البيانات الشخصية

شهدت التشريعات العربية خلال السنوات الأخيرة اتجاهاً واضحاً نحو إصدار قوانين مستقلة لحماية البيانات الشخصية، تضمنت تنظيمياً لحقوق أصحاب البيانات والتزامات القائمين على معالجتها، مع استحداث قواعد خاصة تتعلق بالموافقة والسرية وأمن البيانات. ويعكس هذا التطور إدراكاً متزايداً لأهمية حماية البيانات باعتبارها أحد عناصر حماية الشخصية القانونية في البيئة الرقمية، بعد أن كانت تخضع في الغالب للقواعد العامة في القانون المدني (البلوشي، 2021، ص. 704؛ الجندي، 2023، ص. 2758).

وتظهر أهمية هذه التشريعات في أنها أرست إطاراً قانونياً أولاً للحماية المدنية، إلا أن درجة التفصيل لا تزال تختلف من نظام إلى آخر، سواء في تحديد نطاق المسؤولية المدنية أو في تنظيم وسائل الحماية القضائية. ويؤكد ذلك أن البناء التشريعي

العربي بدأ يقترب من الاتجاهات المقارنة، مع استمرار الحاجة إلى مزيد من التحديث لمواكبة التطور التقني المتسارع (Kuner, 2022, p. 59).

2- أوجه القصور التشريعي في ضوء اللائحة الأوروبية والقانون الفرنسي

تُظهر المقارنة مع اللائحة الأوروبية والقانون الفرنسي أن عدداً من التشريعات العربية ما زال يعتمد على قواعد عامة في بعض مسائل المسؤولية المدنية، دون وضع تنظيم تفصيلي يتلاءم مع الطبيعة الخاصة للبيانات الشخصية. ويبرز ذلك في محدودية النصوص المتعلقة بالتدابير القضائية الوقائية، وضوابط تقدير التعويض عن الأضرار الرقمية، وآليات تنفيذ الأحكام المرتبطة بإزالة آثار الاعتداء على البيانات (السحماوي، 2024، ص. 353؛ العيش، 2023، ص. 296).

كما أن بعض التشريعات لم تفرد تنظيمياً دقيقاً للعلاقة بين متحكم البيانات ومعالجها، أو لم تحدد بصورة كافية آثار الإخلال بالالتزامات المدنية الناشئة عن المعالجة الرقمية، وهو ما يقلل من فعالية الحماية العملية مقارنة بالتشريع الأوروبي الذي تبنى منظومة متكاملة تجمع بين الحقوق الموضوعية والوسائل الإجرائية والجزاءات المدنية (Haas, 2020, p. 310).

ثانياً- مقترحات تطوير الحماية المدنية في ضوء التجربة الأوروبية

يفرض التطور المتسارع للتعاملات الرقمية إعادة النظر في البناء التشريعي التقليدي للحماية المدنية، بما يقتضي الاستفادة من التجارب المقارنة التي أثبتت فاعليتها، مع مراعاة خصوصية النظم القانونية العربية واحتياجاتها العملية.

1- تطوير الإطار التشريعي للحماية المدنية للبيانات الشخصية

يقتضي تطوير التشريعات العربية استكمال البناء القانوني للحماية المدنية من خلال النص صراحة على القواعد الخاصة بمسؤولية متحكم البيانات ومعالجها، وتحديد نطاق التعويض عن الأضرار الرقمية، وإقرار وسائل قضائية عاجلة تتلاءم مع سرعة تداول البيانات في البيئة الرقمية. كما يستحسن توحيد المبادئ الأساسية المنظمة لمعالجة البيانات بما يحقق قدراً أكبر من الاستقرار التشريعي ويحد من اختلاف التطبيقات العملية (عبدالله علي، 2021، ص. 79؛ الأشقر، 2021، ص. 223). ويؤدي استلزام المبادئ التي أرسنها اللائحة الأوروبية إلى تعزيز اليقين القانوني في العلاقات الرقمية، دون الإخلال بالخصوصية التشريعية للدول العربية، إذ يظل نقل التجربة المقارنة مرهوناً بمواءمتها مع القواعد العامة في القانون المدني والبنية المؤسسية لكل دولة (Frison-Roche، 2021، p. 255).

2- تعزيز فعالية الحماية القضائية المدنية في منازعات البيانات الشخصية

يتطلب تحقيق حماية مدنية فعالة تدعيم اختصاص القضاء المدني بوسائل إجرائية تتلاءم مع طبيعة المنازعات الرقمية، مع تمكين القاضي من إصدار أوامر وقائية لوقف الاعتداء وإزالة آثاره، إلى جانب تقرير تعويض يتناسب مع جسامة الضرر المادي أو المعنوي. كما يقتضي الأمر تطوير قواعد الإثبات بما ييسر إثبات الاعتداءات الرقمية ويعزز ثقة الأفراد في منظومة العدالة (قطار، 2025، ص. 274؛ سيد أحمد، 2024، ص. 1421).

ويؤكد التطبيق الأوروبي أن فعالية الحماية لا تتحقق بكثرة النصوص التشريعية، وإنما بوجود منظومة متكاملة تجمع بين وضوح الالتزامات وسرعة الإجراءات وفعالية التنفيذ. ويُعد هذا الاتجاه جديراً بالاستفادة منه عند تطوير التشريعات العربية، بما يرسخ الحماية المدنية للبيانات الشخصية باعتبارها أحد متطلبات الأمن القانوني في المجتمع الرقمي (Lynskey، 2015، p. 273).

الخاتمة

أظهرت الدراسة أن الحماية المدنية للبيانات الشخصية في البيئة الرقمية أصبحت تمثل أحد الموضوعات القانونية الحديثة التي تفرض إعادة النظر في المفاهيم التقليدية للحق في الخصوصية والمسؤولية المدنية، إذ لم تعد البيانات الشخصية مجرد معلومات قابلة للتداول، وإنما غدت عنصراً من عناصر الشخصية القانونية ومظهراً من مظاهر سلطة الفرد على ذاته ومعلوماته. وقد كشفت الدراسة أن التحول الرقمي أوجد أنماطاً جديدة من العلاقات القانونية تتطلب قواعد مدنية قادرة على تحقيق التوازن بين متطلبات الاستفادة من البيانات وبين ضرورة حماية أصحابها من مخاطر المعالجة غير المشروعة أو الاستخدام غير المصرح به.

وبيّنت الدراسة من خلال التحليل المقارن أن اللائحة العامة لحماية البيانات في الاتحاد الأوروبي والقانون الفرنسي قدما نموذجاً متكاملاً في تنظيم الحماية المدنية للبيانات الشخصية، من خلال وضع مبادئ واضحة لمعالجة البيانات، وتحديد مراكز الأطراف القائمة عليها، وإقرار حقوق متعددة لصاحب البيانات، فضلاً عن تنظيم المسؤولية المدنية ووسائل التدخل القضائي. وفي المقابل، كشفت المقارنة مع بعض التشريعات العربية عن وجود خطوات تشريعية مهمة تمثلت في إصدار قوانين خاصة بحماية البيانات الشخصية، مع استمرار الحاجة إلى تطوير بعض الجوانب المتعلقة بفعالية التعويض، وسرعة الحماية القضائية، وتحديد المسؤوليات المدنية في البيئة الرقمية.

وأكدت الدراسة أن فعالية الحماية المدنية لا ترتبط فقط بوجود قواعد موضوعية تنظم جمع البيانات ومعالجتها، وإنما تتوقف كذلك على وجود منظومة قضائية قادرة على التعامل مع خصوصية المنازل الرقمية، بما يشمل التدابير الوقائية لمنع تفاقم الاعتداء، والوسائل العلاجية لإزالة آثاره وجبر الضرر الناتج عنه. وقد أظهرت التجربة الأوروبية أن بناء نظام متوازن لحماية البيانات يقوم على تكامل المبادئ القانونية مع الآليات الإجرائية، وهو ما يمكن أن تستفيد منه التشريعات العربية عند تطوير تنظيمها القانوني بما يتوافق مع خصوصية نظمها المدنية.

وخلصت الدراسة إلى أن حماية البيانات الشخصية تمثل امتداداً طبيعياً للحماية المدنية للحقوق اللصيقة بالشخصية، وأن بناء إطار قانوني عربي أكثر فاعلية يتطلب الانتقال من مرحلة التنظيم الجزئي إلى مرحلة إنشاء منظومة مدنية متكاملة تستوعب التطورات التقنية المتلاحقة. ويقترح الباحث ضرورة تعزيز القواعد الخاصة بالمسؤولية المدنية، وتوسيع نطاق الحماية القضائية، والاستفادة من التجارب المقارنة، مع مراعاة تحقيق الموازنة بين حماية الحقوق الفردية وتشجيع الابتكار الرقمي، بما يرسخ الثقة في المعاملات الإلكترونية ويعزز الأمن القانوني في المجتمع الرقمي.

النتائج

أسفرت الدراسة عن مجموعة من النتائج التي تعكس طبيعة الحماية المدنية للبيانات الشخصية في البيئة الرقمية، ومدى قدرة القواعد القانونية المقارنة على تحقيق التوازن بين حماية الحقوق الفردية ومتطلبات التعاملات الرقمية، وذلك على النحو الآتي:

أكدت الدراسة أن البيانات الشخصية لم تعد مجرد عناصر معلوماتية قابلة للتداول، وإنما أصبحت من المقومات المرتبطة بالشخصية القانونية للفرد، الأمر الذي يقتضي إخضاعها لنظام قانوني خاص يكفل حماية صاحبها من صور الاستخدام غير المشروع. ويستند هذا التنظيم إلى الاعتراف بحق الشخص في التحكم في بياناته وتحديد نطاق جمعها ومعالجتها والاستفادة منها.

أوضحت الدراسة أن اللائحة العامة لحماية البيانات بالاتحاد الأوروبي والقانون الفرنسي قدما إطاراً قانونياً متكاملاً لحماية البيانات الشخصية، من خلال وضع مبادئ محددة لمعالجة البيانات، وتحديد التزامات متحكم البيانات ومعالجتها، وإقرار حقوق واسعة لصاحب البيانات. وقد ساعد هذا التنظيم على إقامة توازن بين حرية تداول المعلومات ومتطلبات حماية الخصوصية الرقمية.

كشفت الدراسة أن التشريعات العربية المتعلقة بحماية البيانات الشخصية شهدت تطوراً ملحوظاً من خلال إصدار قوانين خاصة تنظم جمع البيانات ومعالجتها، إلا أن مستوى الحماية المدنية ما زال متفاوتاً فيما بينها. وتحتاج هذه التشريعات إلى مزيد من التفصيل في تنظيم المسؤولية المدنية والوسائل القضائية بما يتلاءم مع الطبيعة الخاصة للمنازعات الرقمية. الدراسة إلى أن المسؤولية العقدية تمثل أحد الأسس القانونية المهمة لحماية البيانات الشخصية متى نشأت علاقة تعاقدية بين صاحب البيانات ومتحكمها أو معالجها. ويترتب على الإخلال بالالتزامات المتعلقة بالسرية أو حدود المعالجة أو اتخاذ التدابير الأمنية قيام المسؤولية العقدية متى توافرت عناصرها القانونية.

بينت الدراسة أن المسؤولية التقصيرية تؤدي دوراً رئيسياً في مواجهة الاعتداءات التي تقع على البيانات الشخصية خارج نطاق العلاقات التعاقدية، إذ توفر حماية قانونية للأشخاص الذين يتعرضون لأضرار نتيجة الجمع أو الاستخدام أو الإفشاء غير المشروع للبيانات. وتقوم هذه المسؤولية على توافر الخطأ والضرر وعلاقة السببية بينهما وفقاً للقواعد المدنية العامة. أظهرت الدراسة أن الضرر الناتج عن انتهاك البيانات الشخصية يتميز بطبيعة خاصة تختلف عن صور الضرر التقليدية، إذ قد يتعلق بمساس مباشر بالخصوصية أو السمعة أو المركز المعنوي لصاحب البيانات. ويمتد نطاق التعويض ليشمل الأضرار المادية والأدبية متى ثبت ارتباطها بالفعل غير المشروع الواقع على البيانات.

أكدت الدراسة أن الحماية القضائية المدنية للبيانات الشخصية لا تقتصر على مرحلة التعويض بعد وقوع الضرر، وإنما تشمل تدابير وقائية تهدف إلى منع استمرار الاعتداء أو الحد من آثاره. وتتمثل أهمية هذه التدابير في سرعة تدخل القضاء لوقف المعالجة غير المشروعة أو منع تداول البيانات محل النزاع.

أثبتت الدراسة أن النموذج الفرنسي والأوروبي يتميز بوجود منظومة متكاملة تجمع بين تحديد الالتزامات القانونية وفرض المسؤولية عن مخالفتها، مع منح صاحب البيانات وسائل متعددة لحماية حقوقه. ويُعد مبدأ المساءلة من أهم الضمانات التي تفرض على القائمين بالمعالجة إثبات احترامهم للقواعد القانونية المنظمة للبيانات الشخصية.

خلصت الدراسة إلى أن تطوير الحماية المدنية في التشريعات العربية يتطلب إعادة تنظيم بعض الجوانب المرتبطة بالمسؤولية والتعويض والإجراءات القضائية الخاصة بالمنازعات الرقمية. ويستلزم ذلك وضع قواعد أكثر دقة بشأن دور متحكم البيانات ومعالجتها، وتوفير وسائل قضائية تتناسب مع سرعة انتشار البيانات الإلكترونية.

انتهت الدراسة إلى أن بناء نظام قانوني فعال لحماية البيانات الشخصية في البيئة الرقمية يستوجب تحقيق التكامل بين القواعد الموضوعية والضمانات القضائية، مع الاستفادة من التجارب الأوروبية والفرنسية في حدود ما يتفق مع خصوصية النظم القانونية العربية. ويظل تطوير هذه الحماية ضرورة تشريعية لضمان الأمن القانوني وتعزيز الثقة في المعاملات الرقمية الحديثة.

التوصيات

استناداً إلى ما انتهت إليه الدراسة من نتائج، يقترح الباحث مجموعة من التوصيات التي تستهدف تطوير البناء القانوني للحماية المدنية للبيانات الشخصية وتعزيز فعاليتها في البيئة الرقمية، وذلك على النحو الآتي:

يوصي الباحث بضرورة استكمال التنظيم التشريعي العربي الخاص بحماية البيانات الشخصية من خلال وضع قواعد مدنية متخصصة تعالج طبيعة الاعتداءات الرقمية، بحيث تتجاوز الاعتماد على القواعد العامة للمسؤولية المدنية وتضع أحكاماً تتناسب مع خصوصية البيانات باعتبارها أحد مكونات الشخصية القانونية للفرد.

يقترح الباحث إعادة تنظيم المسؤولية المدنية لمتحكم البيانات ومعالجتها بصورة أكثر دقة، من خلال تحديد الالتزامات القانونية الواقعة على كل طرف، وبيان نطاق مسؤوليته عند الإخلال بواجبات الحماية أو تجاوز حدود المعالجة المسموح بها، بما يحقق وضوح المراكز القانونية للأطراف المختلفة.

يوصي الباحث بتطوير القواعد المنظمة للتعويض عن أضرار انتهاك البيانات الشخصية، بما يسمح باستيعاب الأضرار المادية والمعنوية الناتجة عن فقدان السيطرة على البيانات أو المساس بالخصوصية الرقمية، مع منح القضاء سلطة تقديرية تتناسب مع طبيعة الضرر وظروف كل حالة.

يقترح الباحث تعزيز وسائل الحماية القضائية المدنية في منازعات البيانات الشخصية، من خلال تمكين القضاء من اتخاذ تدابير وقائية وسريعة لوقف المعالجة غير المشروعة أو منع انتشار البيانات محل الاعتداء، تأسيساً على أن سرعة التدخل القضائي تعد عنصراً أساسياً في حماية الحقوق الرقمية.

يوصي الباحث بالاستفادة من المبادئ التي أقرتها اللائحة العامة لحماية البيانات بالاتحاد الأوروبي، وبصفة خاصة مبدأ المساءلة والشفافية وتحديد الغرض من المعالجة، مع مراعاة تكييف هذه المبادئ وفق الخصائص التشريعية والقضائية للنظم القانونية العربية.

يقترح الباحث إنشاء آليات قضائية أو دوائر متخصصة للنظر في المنازعات المتعلقة بالبيانات الشخصية والمعاملات الرقمية، لما تنسم به هذه المنازعات من طبيعة فنية وقانونية تستلزم خبرة متخصصة قادرة على تحقيق الحماية القضائية الفعالة.

يوصي الباحث بتعزيز التعاون بين الجهات التشريعية والقضائية والهيئات المختصة بحماية البيانات من أجل وضع معايير موحدة للأمن القانوني للمعالجة الرقمية، بما يضمن التوفيق بين تشجيع الابتكار التكنولوجي والمحافظة على الحقوق الشخصية للأفراد.

يقترح الباحث مراجعة التشريعات العربية المتعلقة بالإثبات المدني بما يتلاءم مع طبيعة الاعتداءات الرقمية، من خلال وضع قواعد أكثر مرونة في إثبات المخالفات المتعلقة بالبيانات الشخصية، نظراً لصعوبة إثبات بعض صور الضرر في البيئة الإلكترونية.

يوصي الباحث بضرورة تعزيز الثقافة القانونية الرقمية لدى الأفراد والجهات القائمة على معالجة البيانات، من خلال برامج تدريبية وتوعوية مستمرة توضح الحقوق والالتزامات المرتبطة بحماية البيانات الشخصية، بما يدعم فعالية الحماية القانونية ويحد من صور الاستخدام غير المشروع.

المراجع

أولاً- الكتب:

1. سالم، عبدالله ثاني النعيمي. (2024). قوانين خصوصية البيانات.
2. خاطر، شريف يوسف حلمي. (2015). حق الاطلاع على البيانات الشخصية في فرنسا.

ثانياً: الدوريات والمقالات

1. زايد، إبراهيم السيد حسنين. (2024). ضوابط معالجة البيانات الشخصية في العدالة الجنائية. مجلة العلوم القانونية والاقتصادية، 66(عدد خاص).
2. زايد، إبراهيم السيد حسنين. (2024). ضوابط معالجة البيانات الشخصية في العدالة الجنائية. في أعمال مؤتمر التحديات والآفاق القانونية والاقتصادية للذكاء الاصطناعي. جامعة عين شمس، كلية الحقوق.
3. العتيبي، أماني بنت محمد بن سيف. (2025). الوظيفة الرقابية لحماية البيانات الشخصية: دراسة مقارنة. مجلة جرش للبحوث والدراسات، 25(2).

4. الدمياطي، تامر محمد. (2022). الرضا الرقمي بمعالجة البيانات الشخصية: دراسة مقارنة. مجلة القانون والتكنولوجيا، 2. (1).
 5. الحسنات، حنان خضر حسن. (2025). مفهوم البيانات الشخصية وحدودها. مجلة جرش للبحوث والدراسات، 25. (2).
 6. البلوشي، راشد بن حمد بن حميد. (2021). حماية البيانات الشخصية في المنظومة القانونية العمانية. مجلة البحوث القانونية والاقتصادية، عدد خاص.
 7. رفرافي، عبدالرحمان. (2025). حماية البيانات الشخصية والأمن السيبراني: تحليل من منظور القانون الدولي. مجلة المفكر، 20. (1).
 8. التهامي، سامح عبدالواحد. (2015). ضوابط معالجة البيانات الشخصية: دراسة مقارنة بين القانون الفرنسي والقانون الكويتي. مجلة كلية القانون الكويتية العالمية، 3. (9).
 9. الأشقر، سلمى. (2021). التشريعات الدولية والأوروبية والداخلية لحماية البيانات الشخصية. مجلة جامعة دمشق للعلوم القانونية، 1. (2).
 10. العيش، الصالحين محمد. (2023). حماية البيانات الشخصية في القانون الأوروبي. مجلة كلية القانون الكويتية العالمية، 11. (43).
 11. غالب، عبدالقادر ورسمه. (2019). قانون حماية البيانات الشخصية. مجلة الاقتصاد الإسلامي العالمية، 87. (87).
 12. قنطار، كوثر. (2025). أثر حماية البيانات الشخصية على حقوق الإنسان: الحماية القانونية الدولية للحق في الخصوصية الرقمية نموذجاً. مجلة جرش للبحوث والدراسات، 25. (2).
 13. مشعل، محمد أحمد سلامة. (2017). الحق في محو البيانات الشخصية: دراسة تحليلية في ضوء لائحة حماية البيانات بالاتحاد الأوروبي. GDPR. مجلة الدراسات القانونية والاقتصادية، 3. (2).
 14. حسن، محمد جبريل إبراهيم. (2025). الجرائم الماسة بالبيانات الشخصية: دراسة تحليلية وصفية. مجلة الفقه والقانون، 158. (158).
 15. علي، محمد حسن عبدالله. (2021). النظام القانوني لحماية البيانات الشخصية المعالجة إلكترونياً: دراسة تحليلية مقارنة في ضوء اللائحة الأوروبية والتشريعات ذات الصلة. مجلة العلوم القانونية، 7. (14).
 16. جبور، منى الأشقر. (2018). القواعد الأوروبية لحماية البيانات الشخصية: الحق في المحو. مجلة الحقوق والعلوم السياسية، 19. (19).
 17. السحماوي، هيام إسماعيل عبدالفتاح. (2024). مسؤولية حائز البيانات الشخصية في القانون المصري: دراسة في ضوء القانون رقم 151 لسنة 2020: دراسة تحليلية. مجلة البحوث القانونية والاقتصادية، 36. (2).
 18. أحمد، وفاء حلمي السعيد سيد. (2024). تقنية الذكاء الاصطناعي وحماية البيانات الشخصية: دراسة مقارنة. مجلة الشريعة والقانون، 43. (43).
 19. الجندي، يارا حافظ. (2023). البيانات الشخصية بين التهديد والحماية: دراسة في ضوء أحكام القانون رقم 151 لسنة 2020. مجلة الدراسات القانونية والاقتصادية، 9. (4).
- ثالثاً: الرسائل العلمية
20. الوادي، آيات محمود حسين. (2025). حماية البيانات الشخصية الرقمية في التشريع الأردني (رسالة ماجستير). جامعة الشرق الأوسط.
 21. القطاطشة، باسل فايز حمد. (2022). الحماية الجنائية لخصوصية البيانات الشخصية الرقمية: دراسة مقارنة (رسالة دكتوراه). جامعة العلوم الإسلامية العالمية.
 22. أبو خمرة، ضرغام عبدالله فاضل. (2021). حماية بيانات الأفراد الشخصية عبر شبكة الإنترنت: دراسة مقارنة (رسالة ماجستير). جامعة الشرق الأوسط.

رابعاً: المراجع الأجنبية

1. Kuner, C. (2007). *European Data Protection Law*. Oxford University Press.
2. Kuner, C. (2007). *European Data Protection Law: Corporate Compliance and Regulation*. Oxford University Press.
3. Kuner, C. (2022). *European Data Protection Law: Corporate Compliance and Regulation*. Oxford University Press.
4. Kuner, C. (2013). *Transborder Data Flows and Data Privacy Law*. Oxford University Press.
5. Bygrave, L. A. (2014). *Data Privacy Law: An International Perspective*. Oxford University Press.
6. Lynskey, O. (2020). *Data Protection and the Legal Framework of the Digital Society*. Oxford University Press.

7. Lynskey, O. (2015). *The Foundations of EU Data Protection Law*. Oxford University Press.
8. Voigt, P., & von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer.

خامساً: المراجع الفرنسية

1. Byk, C. (2021). *Responsabilité civile et protection des données personnelles*. LGDJ.
2. Féral-Schuhl, C. (2022). *Cyberdroit – Le droit à l'épreuve de l'Internet*. Dalloz.
3. Bazin-Beust, D. (2021). *Protection des données personnelles et réparation du préjudice*. LexisNexis.
4. Haas, G. (2020). *Le droit des données personnelles*. LexisNexis.
5. Haas, G. (2021). *Responsabilité et protection des données personnelles*. LexisNexis.
6. Franceschini, L. (2019). *Le RGPD commenté*. LexisNexis.
7. Franceschini, L. (2019). *Le RGPD commenté et appliqué*. LexisNexis.
8. Frison-Roche, M.-A. (2021). *Droit de la Compliance et protection des données personnelles*. Dalloz.
9. Frison-Roche, M.-A. (2020). *La responsabilité civile à l'ère numérique*. Dalloz.
10. Leclerc, X. (2021). *Protection des données personnelles et responsabilité juridique*. Dalloz.
11. Leclerc, X. (2019). *Protection des données personnelles et vie privée*. Dalloz.

Disclaimer/Publisher's Note: The statements, opinions, and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of **SAJH** and/or the editor(s). **SAJH** and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.